Carlos Ivorra Castillo

GEOMETRÍA ALGEBRAICA

Mientras el álgebra y la geometría han estado separadas, su progreso ha sido lento y sus aplicaciones limitadas; pero cuando estas dos ciencias se han unido, han intercambiado sus fuerzas y han avanzado juntas hacia la perfección.

J.L.Lagrange

Índice General

Introducción

La geometría algebraica estudia los sistemas de ecuaciones polinómicas con coeficientes en un cuerpo. Conviene comparar esta “definición” con otra más conocida: El álgebra lineal estudia los sistemas de ecuaciones lineales con coeficientes en un cuerpo. Cualquiera que conozca el álgebra lineal reconocerá que ésta es una buena forma de describirla en pocas palabras, pero también sabrá que en realidad el álgebra lineal trasciende su propósito original, de modo que es fácil encontrar libros de álgebra lineal en los que los sistemas de ecuaciones sean una herramienta secundaria. En efecto, el estudio de los sistemas de ecuaciones lineales pasó hace mucho tiempo de ser una mera manipulación de fórmulas a convertirse en el estudio de una serie de estructuras algebraicas abstractas, como espacios vectoriales, variedades afines, anillos de matrices, etc., y las aplicaciones que las conectan. Estas estructuras permiten comprender en profundidad el comportamiento de los sistemas de ecuaciones lineales. Más aún, por una parte los conectan con la geometría, de modo que —por ejemplo— podemos pensar que la solución de un sistema de dos ecuaciones lineales con tres incógnitas es el conjunto de puntos de la recta en que se cortan los dos planos determinados por las ecuaciones (salvo que éstos sean paralelos o coincidentes, lo cual tiene también su interpretación en cuanto al comportamiento de las ecuaciones). Por otra parte, su nivel de generalidad permite aplicar sus técnicas y resultados y, en particular, el razonamiento geométrico, a muchos contextos en los que en principio no hay ninguna interpretación geométrica subyacente. Así, en el ejemplo de las dos ecuaciones lineales, todo lo dicho vale igualmente aunque sus coeficientes pertenezcan, por ejemplo, a un cuerpo finito, de modo que las nociones de “recta” y “plano” no tienen ninguna interpretación intuitiva directa, si no es a través de la analogía que proporciona la propia álgebra lineal.

Sin entrar en detalles que el lector conocerá sobradamente, observemos únicamente que la forma de relegar a un segundo plano los sistemas de ecuaciones lineales para centrarse en las estructuras algebraicas derivadas de ellos consiste en centrar la atención en los *conjuntos de soluciones* de los sistemas, los cuales forman variedades afines, interpretables geométricamente como puntos, rectas, planos y generalizaciones a dimensiones superiores.

Todas estas observaciones y matices tienen sus equivalentes para el caso de la geometría algebraica. Pese a lo que su “definición” pudiera hacer pensar, se trata de una teoría algebraica muchísimo más profunda, rica y sofisticada que el álgebra lineal, que aparece en cuanto centramos la atención en los conjuntos de soluciones de los sistemas de ecuaciones más que en los sistemas en sí. Dichos conjuntos forman variedades algebraicas, interpretables geométricamente como puntos, curvas, superficies y generalizaciones a dimensiones superiores.

Quizá la geometría algebraica debería llamarse más propiamente "álgebra no lineal" o, tal vez, "álgebra geométrica", para enfatizar así que no es realmente geometría sino que —al igual que el álgebra lineal— consiste en una serie de técnicas y conceptos algebraicos que en un contexto concreto tienen una interpretación geométrica natural, pero que son aplicables en muchos otros contextos, con lo cual podemos pensar geométricamente y aplicar ideas geométricas en casos donde la geometría sólo está presente como una mera analogía, mientras que todas las demostraciones son algebraicas y, a veces, muy distantes de cualquier interpretación geométrica directa.

Todo esto hace que si alguien quiere entender realmente la geometría algebraica tiene ante sí un doble objetivo: por una parte debe entender la conexión directa que existe entre el álgebra de la geometría algebraica y la geometría subyacente en el caso en que dicha geometría existe realmente como algo independiente del álgebra. Nos referimos al caso clásico en que los coeficientes de las ecuaciones son números complejos. Entonces las variedades algebraicas en el sentido la geometría algebraica son variedades diferenciales complejas en el sentido de la geometría diferencial, y todos los conceptos definibles algebraicamente se corresponden de forma natural con sus análogos geométricos y topológicos.

Por otra parte, es necesario entender que las técnicas algebraicas trascienden el caso clásico y son aplicables, como el álgebra lineal, cuando no es posible hablar de curvas y superficies en otro sentido que no sea el de la geometría algebraica.

Por ejemplo, veremos que es posible definir la noción de dimensión de una variedad algebraica mediante conceptos puramente algebraicos. En el caso clásico, esta dimensión algebraica coincide con la dimensión en el sentido de la geometría diferencial, pero es esencial que sigue teniendo sentido —por ejemplo— para variedades definidas mediante ecuaciones con coeficientes en un cuerpo finito, donde la geometría diferencial no tiene nada que decir. Del mismo modo, la geometría algebraica nos permite hablar de variedades tangentes, de derivadas y diferenciales, de ceros y polos de funciones, etc. sin necesidad de ninguna estructura topológica o diferencial subyacente. Esto la convierte en una herramienta muy valiosa para la teoría algebraica de números.

No debemos deducir de aquí que el único interés de la geometría algebraica es su generalidad, de modo que en el contexto clásico no aporta nada frente a la geometría diferencial. Al contrario, cuando una variedad diferencial compleja es algebraica (es decir, puede definirse mediante polinomios) entonces posee muchas propiedades globales de las que la geometría diferencial no puede dar cuenta. Por ejemplo, puede probarse que toda superficie de Riemann compacta puede representarse como una curva algebraica (las superficies de Riemann tienen dimensión real 2 pero dimensión compleja 1, por eso son curvas). A partir de aquí es posible desarrollar una rica teoría global sobre las funciones meromorfas sobre las superficies de Riemann compactas.

Lo dicho hasta aquí debería bastar para que el lector se haga una primera idea de la enorme sofisticación y riqueza conceptual de la geometría algebraica: una visión a la vez profunda y global de esta disciplina involucraría necesariamente una base de geometría afín y proyectiva (álgebra lineal), otras técnicas algebraicas más sofisticadas (álgebra conmutativa), topología algebraica, geometría diferencial, teoría de funciones de variable compleja, técnicas procedentes de la teoría algebraica de números (valoraciones, dominios de Dedekind, etc.), así como teorías que se han desarrollado específicamente para formalizar la geometría algebraica (haces y esquemas), las cuales involucran a su vez la teoría de categorías y cohomología de grupos.

Evidentemente, un libro que pretendiera mostrar todas estas facetas de la geometría algebraica y a la vez profundizara mínimamente en sus resultados debería ser muchísimo más voluminoso que éste, de modo que aquí se vuelve obligado hacer una declaración de intenciones:

La finalidad de este libro es presentar la geometría algebraica de la forma más natural posible a un lector con ciertos conocimientos de teoría algebraica de números a modo de introducción a la teoría de funciones algebraicas en general y, más concretamente, a la teoría de funciones elípticas. Podríamos expresar esto diciendo que vamos a dar el paso de una teoría de números "plana" a una teoría de números "curva", similar al paso del análisis "plano" en $\mathbb{R}^n$ al análisis "curvo" de la geometría diferencial.

Hemos evitado los enfoques demasiado técnicos, como son el del álgebra conmutativa o el de la teoría de esquemas, y en su lugar hemos destacado el aparato algebraico procedente de la teoría algebraica de números. Así mismo hemos incidido en el lenguaje geométrico, tanto en el de la geometría proyectiva como en el de la geometría diferencial, mostrando la equivalencia entre los conceptos algebraicos y los diferenciales (o topológicos) en el contexto clásico. Aunque en los primeros capítulos tratamos con variedades de dimensión arbitraria, a partir de la mitad del libro aproximadamente nos restringimos al estudio de curvas (variedades que en el caso clásico tienen dimensión compleja 1 y son, por consiguiente, superficies de Riemann). Entendemos que para un estudio sistemático de las variedades de dimensión arbitraria es recomendable estar primeramente familiarizado con la teoría de curvas. No obstante, en el apéndice volvemos brevemente al caso de variedades de dimensión arbitraria, pero únicamente para probar un teorema muy importante en la teoría de curvas elípticas, cuya prueba requiere trabajar con una superficie.

En resumen, confiamos en que el lector que siga este libro termine con una visión clara de las posibilidades que ofrece la geometría algebraica y del modo en que en ella se combinan el álgebra, la geometría y el análisis matemático.

Capítulo I

Preliminares

Aunque suponemos que el lector cuenta con una cierta base tanto algebraica como analítica, en este primer capítulo recogeremos los conceptos y resultados más especializados que vamos a necesitar posteriormente y que nos obligarían a hacer largas digresiones si quisiéramos introducirlos en el momento en que se pueda apreciar su importancia y utilidad.

1.1 Anillos noetherianos

La propiedad de Noether es una condición de finitud sobre anillos y módulos equiparable a la dimensión finita en los espacios vectoriales. En esta sección daremos algunos criterios sencillos para garantizar que un anillo o un módulo dado es noetheriano. Recordemos las definiciones:

Definición 1.1 Sea A un anillo y M un A-módulo. Se dice que M es *noetheriano* si todos sus submódulos son finitamente generados.

Un anillo A es *noetheriano* si lo es como A-módulo, es decir, si todos sus ideales son finitamente generados. En particular todo dominio de ideales principales es noetheriano.

Las caracterizaciones siguientes suelen ser útiles:

Teorema 1.2 *Sea A un anillo y M un A-módulo. Las siguientes afirmaciones son equivalentes:*

a) M es noetheriano.

b) Toda sucesión creciente de submódulos

$$M_0 \subset M_1 \subset M_2 \subset M_3 \subset \cdots$$

es finalmente constante.

c) Toda familia no vacía de submódulos de M tiene un elemento maximal respecto a la inclusión.

DEMOSTRACIÓN: a) $\Rightarrow$ b) La unión de todos los módulos M_i es un submódulo de M, luego tiene un generador finito, que estará contenido en alguno de los módulos M_{i_0}. Entonces $M = M_{i_0}$ y por lo tanto $M = M_i$ para todo $i \geq i_0$.

b) $\Rightarrow$ c) Si existiera una familia de submódulos sin maximal podríamos tomar un módulo cualquiera M_0, que al no ser maximal estaría estrictamente contenido en otro módulo M_1 de la familia, que estaría contenido en otro M_2 y así formaríamos una cadena ascendente infinita, en contradicción con b).

c) $\Rightarrow$ a) Si N es un submódulo de M que no es finitamente generado entonces tomamos $m_0 \in N$ y se cumple $N \neq (m_0)$, luego existe un m_1 en $N \setminus (m_0)$ y $N \neq (m_0, m_1)$, luego existe un m_2 en $N \setminus (m_0, m_1)$ y $N \neq (m_0, m_1, m_2)$. De este modo construimos una familia de submódulos

$$(m_0) \subset (m_0, m_1) \subset (m_0, m_1, m_2) \subset \cdots$$

que no tiene maximal. ■

Los teoremas siguientes justificarán de forma inmediata que todos los anillos y módulos que consideremos en lo sucesivo serán noetherianos:

Teorema 1.3 *Si A es un anillo y M es un A-módulo noetheriano, entonces todo submódulo y todo módulo cociente de M es noetheriano.*

DEMOSTRACIÓN: Sea N un submódulo de M. Entonces todo submódulo de N es también un submódulo de M, luego es finitamente generado y así N es noetheriano. Todo submódulo de M/N es de la forma R/N, donde $N \subset R \subset M$ y del hecho de que R es finitamente generado se sigue claramente que R/N también lo es. ■

También se cumple un recíproco:

Teorema 1.4 *Sea A un anillo, M un A-módulo y N un submódulo de M. Si N y M/N son noetherianos entonces M también lo es.*

DEMOSTRACIÓN: A cada submódulo L de M le asociamos el par de módulos $\big(L \cap N, (L+N)/N\big)$. Notemos que si $E \subset F$ son dos submódulos de M y sus pares asociados son iguales entonces $E = F$. En efecto, si $x \in F$, como $(E+N)/N = (F+N)/N$, existen $u \in N$ y $v \in E$ tales que $x = u + v$. Entonces $u \in F \cap N = E \cap N$, luego $x \in E$.

A una sucesión ascendente de submódulos de M le corresponden dos sucesiones ascendentes de submódulos de N y de M/N respectivamente. Como éstas han de ser finalmente constantes, la dada también lo ha de ser, luego M es noetheriano. ■

Teorema 1.5 *Sea A un anillo y M un A-módulo. Si E y F son submódulos noetherianos de M, entonces $E + F$ también es noetheriano.*

DEMOSTRACIÓN: Tenemos que E es noetheriano y $(E+F)/E \cong F/(E \cap F)$ también lo es, luego $E + F$ es noetheriano. ■

Teorema 1.6 *Si A es un anillo noetheriano, entonces todo A-módulo finitamente generado es noetheriano.*

Demostración: Si M admite un generador con m elementos, entonces existe un epimorfismo de anillos $f : A^m \longrightarrow M$ (pues A^m es un módulo libre de rango m y podemos extender a un epimorfismo una biyección entre una base de A^m y un generador de M). Aplicando m veces el teorema anterior concluimos que A^m es un módulo noetheriano y M es isomorfo a un cociente de A^m, luego M es noetheriano. ■

El teorema siguiente es, como veremos más adelante, uno de los pilares de la geometría algebraica:

Teorema 1.7 (Teorema de Hilbert) *Si A es un anillo noetheriano entonces $A[X_1, \ldots, X_n]$ también lo es.*

Demostración: Basta probarlo para una indeterminada. Sea $\mathfrak{a}$ un ideal de $A[X]$. Sea $\mathfrak{b}_i$ el conjunto de los coeficientes directores de los polinomios de $\mathfrak{a}$ de grado i (más el 0).

Es claro que $\mathfrak{b}_i$ es un ideal de A, así como que $\mathfrak{b}_0 \subset \mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \cdots$ (para ver que un elemento de $\mathfrak{b}_i$ está en $\mathfrak{b}_{i+1}$ basta multiplicar por X el polinomio que justifica que está en $\mathfrak{b}_i$). Como A es noetheriano, los ideales $\mathfrak{b}_i$ son iguales a partir de un $\mathfrak{b}_r$.

Sea $\mathfrak{b}_i = (b_{i1}, \ldots, b_{in})$ para $i = 0, \ldots, r$ (no es restricción suponer que el número de generadores es el mismo para todos los ideales, pues siempre podemos añadir generadores redundantes). Podemos suponer que los $b_{ij} \neq 0$.

Sea p_{ij} un polinomio en $\mathfrak{a}$ de grado i cuyo coeficiente de grado i sea b_{ij}. Vamos a probar que $\mathfrak{a} = (p_{ij} \mid i = 0, \ldots, r,\ j = 1, \ldots, n)$. Claramente este ideal está contenido en $\mathfrak{a}$.

Sea $f \in \mathfrak{a}$ un polinomio de grado d. Veremos que está en el ideal generado por los p_{ij} por inducción sobre d. El coeficiente director de f está en $\mathfrak{b}_d$. Si $d > r$ notamos que los coeficientes directores de $X^{d-r}p_{r1}, \ldots, X^{d-r}p_{rn}$ son los números $b_{r1}, \ldots, b_{rn}$, que generan $\mathfrak{b}_d = \mathfrak{b}_r$. Por consiguiente existen elementos $c_1, \ldots, c_n$ en A tales que el polinomio $f - c_1X^{d-r}p_{r1} - \cdots - c_nX^{d-r}p_{rn}$ tiene grado menor que d y está en $\mathfrak{a}$, luego por hipótesis de inducción f está en el ideal generado por los p_{ij}.

Si $d \leq r$ obtenemos un polinomio $f - c_1p_{d1} - \cdots - c_np_{dn}$ de grado menor que d y contenido en $\mathfrak{a}$, con lo que se concluye igualmente. ■

Teorema 1.8 *Si A es un anillo noetheriano y $B = A[b_1, \ldots, b_n]$ es un anillo finitamente generado sobre A, entonces B es noetheriano.*

(Porque B es isomorfo a un cociente de $A[X_1, \ldots, X_n]$).

1.2 Extensiones enteras

Los enteros algebraicos sobre un anillo son el equivalente a los elementos algebraicos sobre un cuerpo. La integridad aparece como una condición técnica necesaria en aquellos contextos en los que trabajamos con anillos y no podemos permitirnos pasar a sus cuerpos de cocientes.

Definición 1.9 Sea D un dominio íntegro y K un cuerpo que contenga a D. Un elemento $\alpha \in K$ es *entero* sobre D si es raíz de un polinomio mónico con coeficientes en D.

Veamos una caracterización de la integridad:

Teorema 1.10 *Sea D un dominio íntegro y K un cuerpo que contenga a D. Un elemento $\alpha \in K$ es entero sobre D si y sólo si existe un D-módulo finitamente generado no nulo $M \subset K$ tal que $\alpha M \subset M$.*

Demostración: Si α es entero entonces $\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_1\alpha + d_0 = 0$, para ciertos $d_i \in D$. Basta considerar el módulo $M = \left\langle 1, \alpha, \ldots, \alpha^{n-1} \right\rangle_D$.

Dado un módulo $M = \langle v_1, \ldots, v_n \rangle_D$ tal que $\alpha M \subset M$, existen elementos d_{ij} en D tales que

$$\alpha v_i = d_{i1}v_1 + \cdots + d_{in}v_n, \qquad \text{para } i = 1, \ldots, n.$$

Esto equivale a la ecuación vectorial $\alpha v = vA$, donde $v = (v_i)$ y $A = (d_{ij})$, o sea, α es un valor propio de la matriz A, luego es raíz de su polinomio característico, que claramente es mónico y con coeficientes en D. ■

Con la ayuda de este teorema podemos probar:

Teorema 1.11 *Sea D un dominio íntegro y K un cuerpo que contenga a D. Entonces el conjunto E de todos los elementos de K enteros sobre D es un subanillo de K.*

Demostración: Sean α, $\beta \in E$. Sean M y N dos D-módulos no nulos finitamente generados tales que $\alpha M \subset M$ y $\beta N \subset N$. Entonces es fácil ver que MN es un D-módulo no nulo finitamente generado y $(\alpha \pm \beta)MN \subset MN$, $\alpha\beta MN \subset MN$. Por lo tanto $\alpha \pm \beta \in E$ y $\alpha\beta \in E$. ■

Definición 1.12 Sea E/D una *extensión* de dominios íntegros, es decir, D y E son dominios íntegros tales que D es un subanillo de E. Diremos que la extensión es *entera* si todo elemento de E es entero sobre D.

Vamos a probar que las extensiones enteras de dominios íntegros se comportan como las extensiones algebraicas de cuerpos. El teorema anterior implica que si adjuntamos a un anillo un conjunto de elementos enteros obtenemos una extensión entera. Ahora probamos que si adjuntamos un número finito de elementos obtenemos además una extensión finitamente generada.

Teorema 1.13 *Sean $D \subset E$ dominios íntegros tales que $E = D[a_1, \ldots, a_n]$ con los a_i enteros sobre D. Entonces E es un D-módulo finitamente generado.*

Demostración: Si tenemos una cadena $D \subset F \subset E$ de dominios íntegros de modo que E es un F-módulo finitamente generado y F es un D-módulo finitamente generado, entonces E es un D-módulo finitamente generado. Basta observar que si $E = \langle e_1, \ldots, e_n \rangle_F$ y $F = \langle f_1, \ldots, f_m \rangle_D$ entonces $E = \langle e_i f_j \rangle_D$.

De aquí se sigue que basta probar el teorema para una sola adjunción. Supongamos que $E = D[a]$ y que a es raíz de un polinomio mónico $p(X) \in D[X]$ de grado n. Todo elemento de E es de la forma $q(a)$ con $q(X) \in D[X]$.

Podemos dividir $q(X) = p(X)c(X) + r(X)$ con $\operatorname{grad} r(X) < n$, y entonces resulta que $q(a) = r(a)$. De aquí se sigue que $E = \left\langle 1, a, \ldots, a^{n-1} \right\rangle$. ■

De aquí deducimos la transitividad de la integridad:

Teorema 1.14 *Si F/E y E/D son extensiones enteras entonces F/D también lo es.*

Demostración: Sea $\alpha \in F$. Entonces $\alpha^n + e_{n-1}\alpha^{n-1} + \cdots + e_1\alpha + e_0 = 0$ para ciertos $e_i \in E$. Sea $E' = D[e_0, \ldots, e_{n-1}]$. Por el teorema anterior E' es un D-módulo finitamente generado y $E'[\alpha]$ es un E'-módulo finitamente generado. Es fácil ver entonces que $E'[\alpha]$ es un D-módulo finitamente generado. Además es obvio que $\alpha E'[\alpha] \subset E'[\alpha]$, luego α es entero sobre D. ■

Definición 1.15 Si D es un dominio íntegro contenido en un cuerpo K, el conjunto E de todos los elementos de K enteros sobre D se llama la *clausura entera* de D en K. El teorema 1.11 prueba que se trata de un dominio íntegro. Es la mayor extensión entera de D contenida en K.

Un dominio íntegro D contenido en un cuerpo K es *íntegramente cerrado* en K si todo elemento de K entero sobre D está en D o, equivalentemente, si D coincide con su clausura entera en K. Por el teorema anterior la clausura entera de un dominio íntegro en un cuerpo es íntegramente cerrada en éste.

Un dominio integro D es *íntegramente cerrado* si es íntegramente cerrado en su cuerpo de cocientes.

Teorema 1.16 *Todo dominio de factorización única es íntegramente cerrado.*

Demostración: Sea D un dominio de factorización única. Si no es íntegramente cerrado es que hay un elemento α/β en su cuerpo de cocientes que es entero sobre D y no pertenece a D. Entonces existe un primo π que divide a β pero no divide a α. Sea

$$(\alpha/\beta)^n + d_{n-1}(\alpha/\beta)^{n-1} + \cdots + d_1(\alpha/\beta) + d_0 = 0, \qquad \text{para ciertos } d_i \in D.$$

Multiplicando por β^n queda $\alpha^n + d_{n-1}\beta\alpha^{n-1} + \cdots + d_1\beta^{n-1}\alpha + d_0\beta^n = 0$, de donde se sigue que $\pi \mid \alpha$, contradicción. ■

Si E/D es una extensión de dominios íntegros podemos identificar el cuerpo de cocientes K de D con un subcuerpo del cuerpo de cocientes L de E, con lo que tenemos una extensión de cuerpos L/K. Vamos a estudiar la relación entre ambas extensiones. Por lo pronto, cuando digamos que E/D es una extensión *finita, separable, normal, etc.* nos referiremos a que lo es la extensión L/K de los cuerpos de cocientes.

Veamos ahora que el polinomio mínimo de un elemento algebraico determina si éste es o no entero.

Teorema 1.17 *Sea D un dominio íntegro y K su cuerpo de cocientes. Sea L/K una extensión finita. Entonces un elemento $\alpha \in L$ es entero sobre D si y sólo si su polinomio mínimo sobre K tiene coeficientes enteros sobre D. En particular la norma y la traza de un entero sobre D son enteras sobre D.*

DEMOSTRACIÓN: Es obvio que un K-monomorfismo de L en una clausura algebraica de L envía elementos enteros a elementos enteros, luego los conjugados de los enteros son enteros. Los coeficientes del polinomio mínimo de α dependen polinómicamente de los conjugados de α, luego si α es entero dichos coeficientes también lo son. La norma y la traza son dos de estos coeficientes. ■

Si en el teorema anterior suponemos además que D es íntegramente cerrado, entonces resulta que un elemento algebraico sobre K es entero si y sólo si su polinomio mínimo sobre K está en $D[X]$, y en particular tenemos que la norma y la traza de un entero están en D.

Teorema 1.18 *Sea D un dominio íntegro y α un elemento algebraico sobre su cuerpo de cocientes. Entonces existe un $d \in D$ no nulo tal que $d\alpha$ es entero sobre D.*

DEMOSTRACIÓN: Por hipótesis $d_n\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_1\alpha + d_0 = 0$ para ciertos $d_i \in D$ con $d_n \neq 0$. Multiplicando por d_n^{n-1} queda

$$(d_n\alpha)^n + d_{n-1}(d_n\alpha)^{n-1} + \cdots + d_1(d_n\alpha) + d_0 = 0,$$

luego $d_n\alpha$ es entero sobre D. ■

Teorema 1.19 *Sea D un dominio íntegro noetheriano íntegramente cerrado, sea K su cuerpo de cocientes y L una extensión finita separable de K. Entonces la clausura entera de D en L es un D-módulo finitamente generado.*

DEMOSTRACIÓN: Basta probar que la clausura entera de D en L está contenida en un D-módulo finitamente generado, pues tal módulo será noetheriano y en consecuencia la clausura entera será finitamente generada.

Sea $w_1, \ldots, w_n$ una K-base de L. Por el teorema anterior podemos suponer que los w_i son enteros sobre D. Sea $T : L \longrightarrow K$ la traza de la extensión. La matriz $\bigl(T(w_iw_j)\bigr)$ tiene determinante no nulo, pues en caso contrario existirían elementos $c_1, \ldots, c_n \in K$ no todos nulos tales que

$$0 = \sum_{j=1}^{n} c_jT(w_iw_j) = T\Big(w_i \sum_{j=1}^{n} c_jw_j\Big), \qquad \text{para } i = 1, \ldots, n.$$

Sea $\alpha = \sum_{j=1}^{n} c_j w_j$. Tenemos que $T(w_i\alpha) = 0$ para todo i. Para cada $\beta \in K$ sea $\beta\alpha^{-1} = \sum_{j=1}^{n} d_j w_j$, con $d_j \in K$. Entonces

$$T(\beta) = T\Big(\sum_{j=1}^{n} d_j \alpha w_j\Big) = \sum_{j=1}^{n} d_j T(\alpha w_j) = 0,$$

o sea, $T = 0$, lo cual es imposible en una extensión separable.

De aquí que existen elementos $z_1, \ldots, z_n \in L$ tales que

$$T(z_i w_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

(Las coordenadas de z_i en la base $w_1, \ldots, w_n$ han de satisfacer un sistema de ecuaciones lineales cuya matriz es $\big(T(w_i w_j)\big)$).

Sea $c \neq 0$ un elemento de D tal que cz_i es entero sobre D para $i = 1, \ldots, n$. Si x es cualquier elemento de L entero sobre D, entonces xcz_i es entero sobre D, luego lo mismo le sucede a $T(xcz_i)$ para cada i. Si $x = \sum_{j=1}^{n} b_j w_j$, con $b_j \in K$, entonces

$$T(xcz_i) = \sum_{j=1}^{n} cb_j T(z_i w_j) = cb_i \in K,$$

y como D es íntegramente cerrado, de hecho $cb_i \in D$ y

$$x = \sum_{j=1}^{n} b_j w_j = \sum_{j=1}^{n} (cb_j)(c^{-1}w_j) \in \big\langle c^{-1}w_1, \ldots, c^{-1}w_n \big\rangle_D .$$

Así pues, el módulo $\big\langle c^{-1}w_1, \ldots, c^{-1}w_n \big\rangle_D$ contiene a la clausura entera de D en L. ■

1.3 El lema de Nakayama

Presentamos ahora un teorema muy simple por lo que a su prueba se refiere, pero que tiene numerosas consecuencias a las que apelaremos en el punto crucial de muchos argumentos. Puede decirse que gran parte de la "magia algebraica" de la geometría algebraica está condensada en el modesto lema de Nakayama:

Teorema 1.20 (Lema de Nakayama) *Sea D un dominio íntegro, $\mathfrak{a}$ un ideal de D no nulo y M un D-módulo finitamente generado tal que $\mathfrak{a}M = M$. Supongamos que si $a \in 1 + \mathfrak{a}$ cumple $aM = 0$, entonces $M = 0$. En tal caso $M = 0$.*

Demostración: Sea $M = \langle v_1, \ldots, v_n \rangle$. Entonces $v_i \in \mathfrak{a}M$, luego podemos expresar $v_i = a_{i1}v_1 + \cdots + a_{in}v_n$, para ciertos $a_{ij} \in \mathfrak{a}$. Pasando v_i al segundo

miembro obtenemos un sistema de ecuaciones lineales con matriz $A = (a_{ij} - \delta_{ij})$, donde
$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Si $|A| \neq 0$, la matriz inversa de A no tiene por qué tener sus coeficientes en D, pero, teniendo en cuenta la fórmula con que se calcula, sí que los tiene la matriz $B = |A|A^{-1}$, de modo que $BA = |A|I_n$. Es fácil ver entonces que $|A|v_i = 0$, lo cual es cierto también si $|A| = 0$. Por consiguiente, $|A|M = 0$, pero es claro que $|A| \in 1 + \mathfrak{a}$, luego por hipótesis $M = 0$. ■

Teorema 1.21 *Sea D un dominio íntegro y E una extensión de D finitamente generada como D-módulo. Sea $\mathfrak{a} \neq 1$ un ideal en D. Entonces $\mathfrak{a}E \neq 1$.*

Demostración: Como $1 \in E$, es claro que $aE = 0$ sólo se cumple si $a = 0$, pero $0 \notin 1+\mathfrak{a}$. Así pues, la hipótesis del teorema anterior se cumple trivialmente y concluimos que $\mathfrak{a}E \neq 1$, pues de lo contrario sería $E = 0$. ■

Teorema 1.22 *Sea D un dominio íntegro, $\mathfrak{a}$ un ideal de D tal que todo elemento de $1+\mathfrak{a}$ es inversible y M un D-módulo finitamente generado. Entonces, $m_1, \ldots, m_n \in M$ generan M si y sólo si sus clases módulo $\mathfrak{a}M$ generan $M/\mathfrak{a}M$.*

Demostración: Una implicación es obvia. Sea $M' = \langle m_1, \ldots, m_n \rangle$. Por hipótesis $M' + \mathfrak{a}M = M$. Basta probar que $M/M' = 0$. Aplicaremos 1.20. Ciertamente, $\mathfrak{a}(M/M') = M/M'$. Hemos de ver que si $a \in 1 + \mathfrak{a}$ y $aM/M' = 0$, entonces $M/M' = 0$, pero es que un tal a es una unidad, luego $aM/M' = M/M'$. ■

Para la última consecuencia del lema de Nakayama necesitamos un caso particular del llamado teorema de la intersección de Krull:

Teorema 1.23 *Sea D un anillo noetheriano y $\mathfrak{a}$ un ideal de D. Sea $\mathfrak{b} = \bigcap\limits_{r \geq 1} \mathfrak{a}^r$. Entonces $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$.*

Demostración: Por el teorema 1.2, existe un ideal $\mathfrak{c}$ en D maximal entre los ideales que cumplen $\mathfrak{b} \cap \mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Basta probar que $\mathfrak{a}^r \subset \mathfrak{c}$ para cierto $r \geq 1$, pues entonces $\mathfrak{b} = \mathfrak{b} \cap \mathfrak{a}^r \subset \mathfrak{b} \cap \mathfrak{c} = \mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$.

A su vez es suficiente probar que para cada $a \in \mathfrak{a}$ existe un $m \geq 1$ tal que $a^m \in \mathfrak{c}$, pues en tal caso, si $\mathfrak{a} = (a_1, \ldots, a_k)$, podemos tomar un mismo m tal que $a_i^m \in \mathfrak{c}$ para todo i, y entonces $r = mk$ cumple lo pedido, ya que en un producto de mk generadores de $\mathfrak{a}$ ha de haber uno que se repita m veces.

Fijado, $a \in \mathfrak{a}$, sea $\mathfrak{d}_m = \{d \in D \mid a^m d \in \mathfrak{c}\}$. De nuevo por el teorema 1.2, existe un $m \geq 1$ tal que $\mathfrak{d}_m = \mathfrak{d}_n$ para todo $n \geq m$. Vamos a probar que $((a^m) + \mathfrak{c}) \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. La maximalidad de $\mathfrak{c}$ implicará entonces que $a^m \in \mathfrak{c}$ y el teorema quedará probado.

Una inclusión es obvia. Tomemos $x = ua^m + c \in ((a^m) + \mathfrak{c}) \cap \mathfrak{b}$ y veamos que $x \in \mathfrak{a}\mathfrak{b}$. Tenemos que $ax = ua^{m+1} + ac \in \mathfrak{a}\mathfrak{b} = \mathfrak{b} \cap \mathfrak{c}$, luego $ua^{m+1} \in \mathfrak{c}$ y por la elección de m también $ua^m \in \mathfrak{c}$. Así pues, $x \in \mathfrak{c} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. ■

Teorema 1.24 *Sea D un dominio íntegro noetheriano y $\mathfrak{a}$ un ideal de D tal que todo elemento de $1+\mathfrak{a}$ sea unitario. Entonces* $\bigcap\limits_{r\geq 1}(\mathfrak{b}+\mathfrak{a}^r)=\mathfrak{b}$ *para todo ideal $\mathfrak{b}$ de A.*

Demostración: En el caso $\mathfrak{b}=0$ aplicamos el lema de Nakayama al módulo $M=\bigcap\limits_{r\geq 1}\mathfrak{a}^r$. La hipótesis $\mathfrak{a}M=M$ se cumple por el teorema anterior.

En el caso general tomamos $B=A/\mathfrak{b}$, que sigue siendo un anillo noetheriano y $\overline{\mathfrak{a}}=(\mathfrak{a}+\mathfrak{b})/\mathfrak{b}$, que es un ideal de B tal que los elementos de $1+\overline{\mathfrak{a}}$ son unidades. Entonces $\overline{\mathfrak{a}}^r=(\mathfrak{b}+\mathfrak{a}^r)/\mathfrak{b}$, y el caso anterior nos da que $\bigcap\limits_{r\geq 1}(\overline{\mathfrak{a}}^r)=0$, de donde se sigue el teorema. ∎

1.4 Extensiones trascendentes

Estudiamos ahora las nociones de independencia algebraica y base de trascendencia, que son fundamentales en la geometría algebraica, y están ligadas esencialmente a la noción de dimensión. La idea básica es que una variedad (curva, superficie, etc.) tiene dimensión n si sus puntos están casi completamente determinados por n coordenadas independientes. Por ejemplo, un punto de una circunferencia en el plano está casi determinado por una de sus coordenadas. Decimos "casi" porque puede haber más de un punto con una misma coordenada, pero a lo sumo hay dos. Esta idea de "coordenadas independientes" se caracterizará algebraicamente a través de las nociones que introducimos seguidamente.

En añadidura, los resultados que veremos aquí nos permitirán probar el resultado fundamental de la geometría algebraica: el teorema de los ceros de Hilbert.

Definición 1.25 Sea K/k una extensión de cuerpos. Un conjunto $S\subset K$ es *algebraicamente dependiente* sobre k si existen elementos $s_1,\ldots,s_n\in S$ distintos dos a dos y un polinomio $f\in k[X_1,\ldots,X_n]$ no nulo tal que $f(s_1,\ldots,s_n)=0$. En caso contrario se dice que S es *algebraicamente independiente* sobre k.

Una *base de trascendencia* de K sobre k es un conjunto $S\subset K$ algebraicamente independiente sobre k y maximal respecto de la inclusión.

Es claro que todos los elementos de un conjunto algebraicamente independiente sobre un cuerpo k son trascendentes sobre k. Por ello, si K/k es una extensión algebraica, el conjunto vacío es una base de trascendencia de K sobre k. En general, el lema de Zorn garantiza que toda extensión de cuerpos tiene una base de trascendencia. De hecho, todo conjunto algebraicamente independiente está contenido en una base de trascendencia.

Notemos que si en la definición de dependencia e independencia algebraica exigimos que los polinomios tengan grado 1 obtenemos la definición de dependencia e independencia lineal sobre k. Por consiguiente un conjunto algebraicamente independiente sobre un cuerpo k es linealmente independiente sobre k, pero el recíproco no es cierto. Basta pensar en las potencias de x en un cuerpo de funciones racionales $k(X)$.

Las propiedades básicas de las bases de trascendencia se siguen del resultado siguiente:

Teorema 1.26 *Sea K/k una extensión de cuerpos y $S \subset K$ un conjunto algebraicamente independiente sobre k. Entonces un elemento $u \in K \setminus k(S)$ es trascendente sobre $k(S)$ si y sólo si $S \cup \{u\}$ es algebraicamente independiente.*

Demostración: Supongamos que u es trascendente sobre $k(S)$ y supongamos que $f(s_1, \ldots, s_n, u) = 0$, donde f es un polinomio con coeficientes en k y $s_1, \ldots, s_n \in S$. Podemos expresar esta ecuación en la forma

$$\sum_i g_i(s_1, \ldots, s_n)u^i = 0,$$

para ciertos polinomios g_i con coeficientes en k. El hecho de que u sea trascendente sobre $k(S)$ implica que $g_i(s_1, \ldots, s_n) = 0$ para todo i, y como S es algebraicamente independiente los coeficientes de cada g_i son nulos, pero éstos son los coeficientes de f, luego $f = 0$.

Supongamos ahora que $S \cup \{u\}$ es algebraicamente independiente y supongamos que $f(u) = 0$, donde $f \in k(S)[X]$. Entonces

$$f(u) = \sum_i \frac{g_i(s_1, \ldots, s_n)}{h_i(s_1, \ldots, s_n)} u^i = 0,$$

donde g_i y h_i son polinomios con coeficientes en k. Multiplicando por el producto de los denominadores obtenemos una ecuación similar pero en la que los coeficientes son polinomios. De la hipótesis se sigue fácilmente que todos los coeficientes han de ser nulos, de donde también $g_i = 0$ para todo i, es decir, $f(X)$ es el polinomio nulo, luego u es trascendente sobre $k(S)$. ■

Como consecuencia inmediata tenemos:

Teorema 1.27 *Sea K/k una extensión de cuerpos y $S \subset K$ un conjunto algebraicamente independiente. Entonces S es una base de trascendencia si y sólo si la extensión $K/k(S)$ es algebraica.*

También es fácil probar lo siguiente:

Teorema 1.28 *Sea K/k una extensión de cuerpos y $S \subset K$ un conjunto arbitrario tal que la extensión $K/k(S)$ sea algebraica. Entonces S contiene una base de trascendencia de K/k.*

Demostración: Sea $T \subset S$ un conjunto algebraicamente independiente maximal respecto a la inclusión. Por el teorema 1.26 resulta que todo elemento de $S \setminus T$ es algebraico sobre $k(T)$, de donde se sigue inmediatamente que K es algebraico sobre $k(T)$, luego T es una base de trascendencia. ■

El resultado más importante sobre bases de trascendencia es el siguiente:

Teorema 1.29 *Sea K/k una extensión de cuerpos. Entonces todas las bases de trascendencia de K sobre k tienen el mismo cardinal.*

Demostración: Supongamos en primer lugar que la extensión tiene una base de trascendencia finita $S = \{s_1, \ldots, s_n\}$ y sea T cualquier otra base de trascendencia. No puede ocurrir que todo elemento de T sea algebraico sobre $k(s_2, \ldots, s_n)$, pues entonces K sería algebraico sobre este cuerpo, y en particular lo sería s_1, lo cual es imposible. Por lo tanto existe $t_1 \in T$ trascendente sobre $k(s_2, \ldots, s_n)$. Por el teorema 1.26 tenemos que el conjunto $\{t_1, s_2, \ldots, s_n\}$ es algebraicamente independiente sobre K. Más aún, s_1 es algebraico sobre este conjunto, o de lo contrario podríamos añadirlo y tendríamos un conjunto algebraicamente independiente que contendría estrictamente a S. De aquí se sigue fácilmente que K es algebraico sobre $k(t_1, s_2 \ldots, s_n)$, lo que implica que $\{t_1, s_2, \ldots, s_n\}$ es una base de trascendencia. Repitiendo el proceso podemos llegar a una base de trascendencia $\{t_1, \ldots, t_n\}$ formada por elementos de T. Por maximalidad $T = \{t_1, \ldots, t_n\}$ luego, efectivamente, T tiene también n elementos.

Supongamos ahora que K/k tiene una base de trascendencia infinita S. Por la parte ya probada, cualquier otra base de trascendencia T es también infinita. Cada $s \in S$ es algebraico sobre $k(T)$, luego es algebraico sobre $k(T_s)$, para un cierto conjunto finito $T_s \subset T$. Entonces K es algebraico sobre la adjunción a k de $\bigcup\limits_{s \in S} T_s$, luego este conjunto es una base de trascendencia de K/k. Como está contenido en T ha de ser igual a T, luego

$$|T| = \Big|\bigcup_{s \in S} T_s\Big| \leq \sum_{s \in S} |T_s| \leq \aleph_0 |S| = |S|.$$

Por simetría se da también la desigualdad opuesta. ■

Definición 1.30 Llamaremos *grado de trascendencia* de una extensión de cuerpos K/k al cardinal de cualquiera de sus bases de trascendencia. Lo representaremos por $\operatorname{gt}(K/k)$.

Así, las extensiones algebraicas son las extensiones con grado de trascendencia igual a 0.

Una extensión de cuerpos K/k es *puramente trascendente* si $K = k(S)$, donde S es un conjunto algebraicamente independiente sobre k (y por consiguiente una base de trascendencia). Es inmediato que entonces K es k-isomorfo al cuerpo de las funciones racionales sobre k con $|S|$ indeterminadas. El teorema 1.26 prueba que toda extensión se descompone en una extensión puramente trascendente seguida de una extensión algebraica.

Ejercicio: Probar que el grado de trascendencia de una cadena de extensiones es la suma de los grados de trascendencia de las extensiones intermedias.

Veamos ahora que la parte algebraica de una extensión finitamente generada de un cuerpo perfecto puede tomarse separable eligiendo adecuadamente la base de trascendencia. Para ello necesitamos un refinamiento del teorema del elemento primitivo:

Teorema 1.31 *Si $K = k(\alpha, \beta)$ es una extensión finita de cuerpos y α es separable sobre k, entonces K/k es simple.*

Demostración: Sea M una extensión de K en la que se escindan los polinomios mínimos de α y β. Claramente podemos suponer que k es infinito, con lo que podemos tomar $\gamma \in k$ tal que

$$\gamma \neq \frac{\beta' - \beta}{\alpha' - \alpha},$$

para todo par β' y α' de k-conjugados de β y α respectivamente ($\alpha' \neq \alpha$). Veamos que $\sigma = \gamma\alpha + \beta$ es un elemento primitivo. Ciertamente $E = k(\sigma) \subset K$. Sea $g(X) = \operatorname{pol\,mín}(\beta, k)$ y sea $h(X) = g(\sigma - \gamma X) \in E[X]$. Claramente

$$h(\alpha) = g(\sigma - \gamma\alpha) = g(\beta) = 0.$$

Más aún, si $\alpha' \neq \alpha$ es un k-conjugado de α, tenemos que

$$\sigma - \gamma\alpha' = \gamma\alpha + \beta - \gamma\alpha' = \gamma(\alpha - \alpha') + \beta \neq \beta'$$

para todo k-conjugado β' de β. Por consiguiente $h(\alpha') \neq 0$. Así, si $f = \operatorname{pol\,mín}(\alpha, k)$ tenemos que α es la única raíz común de f y h en M. Como g se escinde en $M[X]$, lo mismo le sucede a h, luego $X - \alpha$ es el máximo común divisor de f y h en $M[X]$. Ahora bien, el máximo común divisor en $E[X]$ de ambos polinomios debe dividir a $X - \alpha$ en $M[X]$, luego $\alpha \in E$ y $\beta = \sigma - \gamma\alpha \in E$. Esto nos permite concluir que $K = E = k(\sigma)$. ■

Teorema 1.32 *Sea k un cuerpo perfecto y K/k una extensión finitamente generada. Entonces K tiene una base de trascendencia S tal que la extensión $K/k(S)$ es separable.*

Demostración: Podemos suponer que k tiene característica prima p. Sea $K = k(t_1, \ldots, t_n)$. Por el teorema 1.28 el conjunto $\{t_1, \ldots, t_n\}$ contiene una base de trascendencia de K/k. Digamos que es la formada por $\{t_1, \ldots, t_d\}$.

Sea $f(X_1, \ldots, X_{d+1})$ un polinomio irreducible tal que $f(t_1, \ldots, t_{d+1}) = 0$. Alguna de las derivadas parciales de f ha de ser no nula, pues en caso contrario p dividiría a los exponentes de todas las variables que aparecen en f, luego podríamos expresar $f = g^p$ y f no sería irreducible.

Si la derivada de f respecto de X_j es no nula, entonces los elementos t_i, para $i = 1, \ldots, d+1$, $i \neq j$, son algebraicamente independientes sobre k. En efecto, es claro que la condición sobre la derivada justifica que t_j es algebraico sobre $k(t_1, \ldots, t_{j-1}, t_{j+1}, \ldots, t_{d+1})$. Si estos generadores fueran algebraicamente dependientes, eliminando uno o más de ellos obtendríamos una base de trascendencia de K/k con menos de d elementos. Así pues, reordenando los generadores podemos suponer que t_{d+1} es separable sobre $k(t_1, \ldots, t_d)$. Por el teorema anterior existe un y tal que $k(t_1, \ldots, t_{d+2}) = k(t_1, \ldots, t_d, y)$. Repitiendo este proceso llegamos a que $K = k(s_1, \ldots, s_d, y)$, donde los d primeros generadores forman una base de trascendencia S de K/k y el último es separable sobre $k(S)$. ■

Usaremos este teorema para demostrar el teorema de los ceros de Hilbert. Éste será inmediato tras haber probado lo siguiente:

Teorema 1.33 *Sea k un cuerpo algebraicamente cerrado y $F_i \in k[X_1, \ldots, X_n]$ un conjunto finito de polinomios. Si el sistema de ecuaciones $F_i = 0$ tiene solución en una extensión finitamente generada de k, entonces tienen solución en k.*

DEMOSTRACIÓN: Sea K la extensión donde el sistema tiene solución. Por 1.32 tenemos que $K = k(t_1, \ldots, t_r, \alpha)$, donde $t_1, \ldots, t_r$ es una base de trascendencia de K/k. Sea $p(t_1, \ldots, t_r, X) \in k(t_1, \ldots, t_r)[X]$ el polinomio mínimo de α. Sea $F_i(\xi_1, \ldots, \xi_n) = 0$, con $\xi_j \in K$. Cada ξ_j será de la forma $\xi_j = c_j(t_1, \ldots, t_r, \alpha)$, con $c_j(t_1, \ldots, t_r, X) \in k(t_1, \ldots, t_r)[X]$. Entonces

$$F_i(c_1(t_1, \ldots, t_r, X), \ldots, c_n(t_1, \ldots, t_r, X)) = p(t_1, \ldots, t_r, X)q_i(t_1, \ldots, t_r, X),$$

para un cierto polinomio q_i.

Tomemos $(\alpha_1, \ldots, \alpha_r) \in k^r$ de modo que no anule al denominador de ningún coeficiente de p, q_i, $c_1, \ldots, c_n$ ni al coeficiente director de p (es decir, que no anule a su producto, lo cual es posible porque un polinomio que se anule en todo punto ha de ser nulo). Tomemos $\beta \in k$ tal que $p(\alpha_1, \ldots, \alpha_r, \beta) = 0$ y definamos $\lambda_i = c_i(\alpha_1, \ldots, \alpha_r, \tau)$. Es claro entonces que $(\lambda_1, \ldots, \lambda_n)$ es una solución del sistema de ecuaciones. ■

Ahora ya podemos probar el teorema de los ceros. Aquí lo enunciamos en su forma más basta, de modo que no es fácil advertir su importancia. En el capítulo siguiente, cuando dispongamos del lenguaje básico de la geometría algebraica, podremos obtener como consecuencia sencilla una versión mucho más refinada. De momento diremos tan sólo que viene a decir que los cuerpos algebraicamente cerrados cumplen algo más de lo que indica la definición: ésta exige en principio que todo polinomio no constante de una variable tenga al menos una raíz. Ahora probamos que cualquier sistema de ecuaciones polinómicas de varias variables tiene una raíz supuesto que se cumpla una generalización obviamente necesaria de “no ser constante”.

Teorema 1.34 (Teorema de los ceros de Hilbert) *Sea k un cuerpo algebraicamente cerrado y $F_1, \ldots, F_m \in k[X_1, \ldots, X_n]$. Si $(F_1, \ldots, F_m) \neq 1$, entonces el sistema de ecuaciones $F_i = 0$ tiene solución en k.*

DEMOSTRACIÓN: Sea M un ideal maximal que contenga a $(F_1, \ldots, F_m)$ y sea $K = k[X_1, \ldots, X_n]/M$. Es claro que las clases de las indeterminadas son una solución del sistema en K (visto como extensión de k), luego por el teorema anterior existe una solución en k. ■

1.5 Anillos de series formales de potencias

En esta sección veremos cómo trabajar con series de potencias en ausencia de una topología que dé sentido a su convergencia. La idea es que las series de potencias pueden ser definidas y manipuladas formalmente, exactamente igual que los polinomios.

Definición 1.35 Si A es un dominio íntegro, llamaremos anillo de las *series formales de potencias* con n indeterminadas $X_1, \ldots, X_n$ sobre A al conjunto $A[[X_1, \ldots, X_n]]$ formado por todas las sucesiones $\{F_m\}_{m=0}^{\infty}$ en $A[X_1, \ldots, X_n]$ tales que F_m es una forma de grado m o la forma nula. En lugar de $\{F_m\}_{m=0}^{\infty}$ escribiremos

$$\sum_{m=0}^{\infty} F_m = F_0 + F_1 + F_2 + \cdots$$

o, más detalladamente,

$$\sum_{i_1,\ldots,i_n}^{\infty} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

donde $(i_1, \ldots, i_m)$ recorre las n-tuplas de números naturales y $a_{i_1,\ldots,i_n} \in k$.

Es fácil ver que $A[[X_1, \ldots, X_n]]$ adquiere estructura de anillo conmutativo y unitario con las operaciones dadas por

$$\sum_{m=0}^{\infty} F_m + \sum_{m=0}^{\infty} G_m = \sum_{m=0}^{\infty} (F_m + G_m),$$

$$\Big(\sum_{m=0}^{\infty} F_m\Big)\Big(\sum_{m=0}^{\infty} G_m\Big) = \sum_{m=0}^{\infty} \Big(\sum_{i+j=m}^{\infty} F_i G_j\Big).$$

Podemos identificar al anillo de polinomios $A[X_1, \ldots, X_n]$ con el subanillo de $A[[X_1, \ldots, X_n]]$ formado por las series de términos finalmente nulos. También es claro que podemos ver a $A[[X_1, \ldots, X_{n-1}]]$ como subanillo de $A[[X_1, \ldots, X_n]]$. Más aún, es fácil definir un isomorfismo

$$A[[X_1, \ldots, X_n]] \cong A[[X_1, \ldots, X_{n-1}]][[X_n]].$$

La forma no nula de menor grado de una serie de potencias (no nula) se llama *término inicial* de la serie. Es claro que el término inicial de un producto es el producto de los términos iniciales, de donde se sigue en particular que los anillos de series de potencias son dominios íntegros.

A partir de aquí nos limitaremos a estudiar los anillos de series de potencias sobre un cuerpo k.

Llamaremos *orden* de una serie de potencias no nula F al grado de su término inicial. Lo representaremos por $v(F)$. Convenimos en que el orden de la serie nula es $v(0) = +\infty$, de modo que —con los convenios aritméticos obvios— se cumplen trivialmente las propiedades siguientes:

$$v(F + G) \geq \text{mín}\{v(F), v(G)\}, \qquad v(FG) = v(F) + v(G).$$

A la hora de trabajar con un anillo es conveniente conocer sus unidades:

Teorema 1.36 *Una serie formal de potencias $F \in k[[X_1, \ldots, X_n]]$ es una unidad si y sólo si su término independiente es no nulo (es decir, si $v(F) = 0$).*

Demostración: Si F es una unidad existe una serie G tal que $FG = 1$. De aquí se sigue que las formas de grado 0 verifican $F_0G_0 = 1$, luego $F_0 \neq 0$.

Recíprocamente, si $F_0 \neq 0$ podemos definir recursivamente formas $G_0, G_1, \ldots$ de modo que

$$F_0G_0 = 1,\ F_1G_0 + F_0G_1 = 0,\ F_2G_0 + F_1G_1 + F_0G_2 = 0, \ldots$$

Es claro que cada G_m es una forma de grado m (o la forma nula) y la suma G de todas estas formas cumple $FG = 1$. ■

Como consecuencia vemos que $k[[X_1, \ldots, X_n]]$ tiene un único ideal maximal

$$\mathfrak{m} = (X_1, \ldots, X_n),$$

que no es sino el ideal formado por las formas F que cumplen $v(F) > 0$.

Definiendo el *valor absoluto* de una serie de potencias F como $|F| = 2^{-v(F)}$ (con el convenio de que $|0| = 0$), las propiedades anteriores se traducen en

$$|F + G| \leq \max\{|F|, |G|\}, \qquad |FG| = |F||G|.$$

En estos términos, el teorema 1.36 afirma que las unidades de $k[[X_1, \ldots, X_n]]$ son las series con valor absoluto igual a 1.

A su vez, el valor absoluto nos permite definir una distancia (en el sentido topológico usual) en $k[[X_1, \ldots, X_n]]$, a saber, la dada por

$$d(F, G) = |F - G|.$$

En lo sucesivo consideraremos a $k[[X_1, \ldots, X_n]]$ como espacio topológico con la topología inducida por esta distancia. Los argumentos usuales en topología se pueden aplicar en este contexto general para demostrar que la suma, el producto y la aplicación $\epsilon \mapsto \epsilon^{-1}$ (definida sobre el grupo de unidades) son continuas. Por ejemplo, la continuidad de la última aplicación se sigue de que

$$|\epsilon^{-1} - \delta^{-1}| = \left|\frac{\delta - \epsilon}{\epsilon\delta}\right| = |\delta - \epsilon|.$$

En la práctica es más cómodo trabajar directamente con v, sin necesidad de pasar por el valor absoluto. Por ejemplo, es claro que una serie está más próxima a la serie nula cuanto mayor es su orden y, más en general, dos series están más próximas entre sí cuanto mayor es el grado del primer monomio en que difieren.

Observemos ahora que toda serie formal de potencias cumple

$$\sum_{m=0}^{\infty} F_m = \lim_N \sum_{m=0}^{N} F_m,$$

pues

$$v\Big(\sum_{m=0}^{\infty} F_m - \sum_{m=0}^{N} F_m\Big) > N.$$

Esto significa que una serie es el límite de sí misma cuando se la considera como serie en el sentido topológico usual (como sucesión de polinomios). En particular tenemos que $k[X_1,\ldots,X_n]$ es denso en $k[[X_1,\ldots,X_n]]$. Más en general, el teorema siguiente afirma que una serie de series formales de potencias converge si y sólo si su término general tiende a 0:

Teorema 1.37 *Si $\{G_r\}_{r=0}^{+\infty}$ es una sucesión en $k[[X_1,\ldots,X_n]]$, entonces la serie $\sum\limits_r G_r$ converge si y sólo si $\lim\limits_r v(G_r) = +\infty$.*

Demostración: Si la serie converge, entonces

$$G_t = \sum_{r=0}^{t} G_r - \sum_{r=0}^{t-1} G_r.$$

Tomando límites y usando la continuidad de la suma obtenemos que

$$\lim_t G_t = \sum_{r=0}^{\infty} G_r - \sum_{r=0}^{\infty} G_r = 0,$$

luego $\lim\limits_t |G_t| = 0$ y $\lim\limits_r v(G_r) = +\infty$.

Para probar el recíproco, digamos que

$$\sum_{r=0}^{t} G_r = \sum_{m=0}^{\infty} F_m^t.$$

La hipótesis afirma que para cada $m \geq 0$ existe un $r(m) \geq 0$ tal que si $r \geq r(m)$ entonces G_r no tiene formas de grado $\leq m$, luego la sucesión $\{F_m^t\}_t$ toma un valor constante F_m para $t \geq r(m)$. Notemos que F_m es una forma de grado m o bien la forma nula, luego podemos definir la serie

$$G = \sum_{m=0}^{\infty} F_m \in k[[X_1,\ldots,X_n]].$$

Más aún, la igualdad $F_s^t = F_s$ se da para todo $t \geq r(m)$ y todo $s \leq m$, de donde se sigue que

$$v\Big(G - \sum_{r=0}^{t} G_r\Big) \geq m,$$

y esto prueba que

$$G = \lim_t \sum_{r=0}^{t} G_r.$$

■

Nota Si $k \subset K$, es claro que la topología de $k[[X_1, \ldots, X_n]]$ es la restricción de la de $K[[X_1, \ldots, X_n]]$. Más aún, si D es un dominio íntegro y k es su cuerpo de cocientes, es fácil ver que $D[[X_1, \ldots, X_n]]$ es completo con la topología inducida.

■

El teorema 1.36 nos da la estructura de los anillos $k[[X]]$. En efecto, toda serie de potencias (no nula) en una indeterminada es de la forma

$$F = \sum_{m=r}^{\infty} a_m X^m, \qquad a_r \neq 0,$$

con lo que $F = \epsilon X^r$, donde

$$\epsilon = \sum_{m=0}^{\infty} a_{m+r} X^m$$

es una unidad de $k[[X]]$. La expresión es única porque necesariamente $r = v(F)$.

A su vez esto implica que $k[[X]]$ es un dominio euclídeo con la norma dada por la aplicación v, ya que trivialmente $v(FG) \geq v(F)$ (si $F \neq 0 \neq G$) y dados un dividendo $D = \epsilon X^r$ y un divisor $d = \delta X^s$ ambos no nulos, la división euclídea es

$$\begin{array}{ll} D = d(\epsilon\delta^{-1}X^{r-s}) + 0 & \text{si } r \leq s, \\ D = d \cdot 0 + D & \text{si } s < r. \end{array}$$

Así pues, $k[[X]]$ es un dominio de ideales principales y, como sólo tiene un ideal maximal $\mathfrak{m} = (X)$, es un dominio de factorización única con un único primo X. Resumimos lo que hemos demostrado:

Teorema 1.38 *Si k es un cuerpo, entonces $k[[X]]$ es un dominio de ideales principales con un único ideal maximal $\mathfrak{m} = (X)$. Sus únicos ideales son*

$$0 \cdots \subset \mathfrak{m}^3 \subset \mathfrak{m}^2 \subset \mathfrak{m} \subset 1.$$

Es conocido que los anillos de polinomios en una indeterminada son dominios de ideales principales, mientras que esto es falso en el caso de varias indeterminadas, pero todos ellos son dominios de factorización única. Vamos a probar que lo mismo sucede con los anillos de series formales de potencias. Por simplicidad supondremos que el cuerpo de constantes k es infinito, si bien esta hipótesis se puede suprimir, aunque para nosotros no supone ninguna restricción.

Necesitamos un resultado auxiliar. Diremos que una $F \in k[[X_1, \ldots, X_n]]$ no nula es *regular* en X_n si su término inicial contiene un monomio cX_n^m con $c \in k$, $c \neq 0$.

Teorema 1.39 *Si k es un cuerpo infinito y $F \in k[[X_1, \ldots, X_n]]$ es una serie no nula, existe un automorfismo $\phi : k[[X_1, \ldots, X_n]] \longrightarrow k[[X_1, \ldots, X_n]]$ tal que $\phi(F)$ es regular en X_n.*

Demostración: Sea F_m el término inicial de F. Entonces tenemos que $F_m(X_1, \ldots, X_{n-1}, 1)$ es un polinomio no nulo. Como el cuerpo k es infinito existe $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ tal que $F_m(a_1, \ldots, a_{n-1}, 1) \neq 0$.

La sustitución $X_i \mapsto X_i + a_i X_n$ $(i = 1, \ldots, n-1)$, $X_n \mapsto X_n$ define un automorfismo del anillo de polinomios $k[X_1, \ldots, X_n]$, que claramente se extiende a un automorfismo ϕ del anillo de series formales.

La forma inicial de $\phi(F)$ es $F'_m = F_m(X_1 + a_1 X_n, \ldots, X_{n-1} + a_{n-1} X_n, X_n)$, luego $F'_m(0, \ldots, 0, 1) = F_m(a_1, \ldots, a_{n-1}, 1) \neq 0$, y éste es el coeficiente de X_n en F'_m, luego $\phi(F)$ es regular en X_n. ■

Insistimos en que la hipótesis sobre el cuerpo k en los teoremas siguientes puede ser eliminada sin más que generalizar el teorema anterior. El teorema siguiente nos permitirá aplicar razonamientos inductivos sobre el número de indeterminadas:

Teorema 1.40 (Teorema de preparación de Weierstrass) *Consideremos una serie de potencias $F \in k[[X_1, \ldots, X_n]]$ regular respecto de X_n y tal que $v(F) = m \geq 1$. Para cada serie $G \in k[[X_1, \ldots, X_n]]$ existen $U \in k[[X_1, \ldots, X_n]]$ y $R_i \in k[[X_1, \ldots, X_{n-1}]]$ (para $0 \leq i \leq m-1$) unívocamente determinados por G y F tales que*

$$G = UF + \sum_{i=0}^{m-1} R_i X_n^i.$$

Demostración: Para cada serie $P \in k[[X_1, \ldots, X_n]]$ llamamos $r(P)$ a la suma de todos los monomios de P que no son múltiplos de X_n^m. De este modo, existe una serie $h(P) \in k[[X_1, \ldots, X_n]]$ tal que

$$P = r(P) + X_n^m h(P). \tag{1.1}$$

Es claro que $r(P)$ es un polinomio en X_n de grado $< m$ con coeficientes en $k[[X_1, \ldots, X_{n-1}]]$. También es inmediato que r y h son aplicaciones k-lineales de $k[[X_1, \ldots, X_n]]$ en sí mismo.

El hecho de que F sea regular en X_n se traduce en que $v(h(F)) = 0$, luego $h(F)$ es una unidad de $k[[X_1, \ldots, X_n]]$. Por su parte, la serie $r(F)$, vista como polinomio en X_n con coeficientes en $k[[X_1, \ldots, X_{n-1}]]$, tiene sus coeficientes en el ideal maximal $\mathfrak{m} = (X_1, \ldots, X_{n-1})$ (o, de lo contrario, F tendría un monomio cX^r con $r < m$).

El teorema equivale a la existencia de una serie $U \in k[[X_1, \ldots, X_n]]$ tal que

$$h(G) = h(UF), \tag{1.2}$$

pues en tal caso $h(G - UF) = 0$ y (1.1) nos da que $G - UF = r(G - UF)$ es un polinomio en X_n de grado $< m$. Recíprocamente, si se cumple el teorema entonces $h(G - UF) = 0$, luego U cumple (1.2) por la linealidad de h. Más aún, si probamos que U está unívocamente determinado, también lo estarán los R_i.

Para cualquier serie U, tenemos que $UF = U\,r(F) + X_n^m U\,h(F)$, luego (1.2) equivale a

$$h(G) = h(U\,r(F)) + U\,h(F). \tag{1.3}$$

Como $h(F)$ es una unidad, vamos a expresar esta condición en términos de $V = U\,h(F)$. Llamamos $M = -r(F)h(F)^{-1}$, de modo que $U\,r(F) = -MV$ y la condición (1.3) es equivalente a

$$h(G) = -h(MV) + V. \tag{1.4}$$

Así pues, basta probar que hay una única serie V que cumple esta condición. Llamemos ahora $s(P) = h(MP)$, con lo que tenemos otra aplicación k-lineal en $k[[X_1, \ldots, X_n]]$. La condición (1.4) es equivalente a

$$V = H + s(V), \tag{1.5}$$

donde hemos definido $H = h(G)$. En definitiva, basta probar que existe una única serie de potencias V que cumple esta última condición.

Para probar la unicidad observamos que si V cumple (1.5) entonces, la linealidad de s nos da $V = H + s(H) + s^2(V)$ y, en general,

$$V = H + s(H) + s^2(H) + \cdots + s^r(H) + s^{r+1}(V).$$

Notemos que si una serie P, vista como serie en X_n con coeficientes en $k[[X_1, \ldots, X_{n-1}]]$, tiene todos sus coeficientes en el ideal $\mathfrak{m}^r$, para cierto $r \geq 0$, entonces $s(P)$ tiene sus coeficientes en $\mathfrak{m}^{r+1}$. En efecto, los coeficientes de M están en $\mathfrak{m}$, luego los de MP están en $\mathfrak{m}^{r+1}$ y los coeficientes de $h(MP)$ son parte de los de MP. En particular las sucesiones $s^r(H)$ y $s^{r+1}(V)$ tienden a cero, luego la serie

$$V = H + s(H) + s^2(H) + \cdots \tag{1.6}$$

converge y V es el único que puede cumplir (1.5). Falta probar que ciertamente lo cumple. Para ello hacemos $V = H + s(H) + \cdots + s^r(H) + V_r$.

Por la linealidad de s vemos que

$$V - H - s(V) = V_r - s^{r+1}(H) - s(V_r),$$

y las tres sucesiones de la derecha tienden a 0 con r, luego concluimos que $V - H - s(V) = 0$. ■

Teorema 1.41 *Si k es un cuerpo infinito, el anillo de series formales de potencias $k[[X_1, \ldots, X_n]]$ es noetheriano.*

Demostración: Razonamos por inducción sobre n. El caso $n = 1$ es obvio, puesto que $k[[X]]$ es un dominio de ideales principales. Sea $\mathfrak{a}$ un ideal en $k[[X_1, \ldots, X_n]]$ y vamos a ver que tiene un generador finito. Podemos suponer que $\mathfrak{a} \neq 0, 1$ y, usando el teorema 1.39, que $\mathfrak{a}$ contiene una serie F (necesariamente con $v(F) = m \geq 1$) regular en X_n.

Llamemos $A = k[[X_1, \ldots, X_{n-1}]]$, que es un anillo noetheriano por hipótesis de inducción. El teorema anterior implica que

$$\mathfrak{a} = (F) + (\mathfrak{a} \cap \langle 1, X_n, \ldots, X_n^{m-1} \rangle_A).$$

Ahora bien, $\langle 1, X_n, \ldots, X_n^{m-1} \rangle_A$ es un A-módulo finitamente generado y, por la propiedad de noether, también lo es el submódulo $\mathfrak{a} \cap \langle 1, X_n, \ldots, X_n^{m-1} \rangle_A$. Así, un generador finito de este módulo forma, junto con F, un generador finito de $\mathfrak{a}$. ■

Ahora, para probar que los anillos $k[[X_1, \ldots, X_n]]$ son dominios de factorización única basta demostrar que en ellos los elementos irreducibles son primos. Para ello necesitamos una variante del teorema de Weierstrass:

Teorema 1.42 *Sea $F \in k[[X_1, \ldots, X_n]]$ una serie de potencias regular en X_n tal que $m = v(F) \geq 1$. Entonces existen una unidad $E \in k[[X_1, \ldots, X_n]]$ y series $R_i \in k[[X_1, \ldots, X_{n-1}]]$ (para $0 \leq i \leq m-1$), ninguna de las cuales es una unidad, tales que*

$$F = E(X_n^m + R_{m-1}X_n^{m-1} + \cdots + R_1X_n + R_0).$$

Además, tanto E como las R_i están unívocamente determinadas por F.

Demostración: Aplicamos el teorema de Weierstrass a $G = -X_n^m$, de modo que

$$-UF = X_n^m + R_{m-1}X_n^{m-1} + \cdots + R_1X_n + R_0.$$

Si algún R_i fuera una unidad, el miembro izquierdo tendría términos de grado $< m$, lo cual es imposible. Por otra parte UF contiene el monomio X_n^m, lo que implica que U es una unidad. Basta tomar $E = -U^{-1}$. La unicidad se sigue inmediatamente de la del teorema de Weierstrass. ■

Teorema 1.43 *Si k es un cuerpo infinito, entonces $k[[X_1, \ldots, X_n]]$ es un dominio de factorización única.*

Demostración: Razonamos por inducción sobre n. El caso $n = 1$ lo tenemos probado, pues $k[[X]]$ es un dominio de ideales principales. Puesto que $k[[X_1, \ldots, X_n]]$ es noetheriano, basta tomar una serie $F \in k[[X_1, \ldots, X_n]]$ irreducible y demostrar que es prima. Para ello suponemos que F divide a un producto GH, es decir, que $DF = GH$, y hemos de probar que F divide a G o a H.

El teorema 1.39 nos permite suponer que la serie $DFGH$ es regular en X_n, pero entonces también lo son las cuatro series D, F, G, H. Sean D', F', G', H' los polinomios en $k[[X_1, \ldots, X_{n-1}]][X_n]$ asociados a las series respectivas por el teorema anterior (convenimos que el polinomio asociado a una unidad es 1). Es claro que $D'F'$ y $G'H'$ cumplen el teorema anterior para las series DF y GH, luego por la unicidad $D'F' = G'H'$. Basta probar que F' divide a G' o a H'. Equivalentemente, podemos suponer que D, F, G, $H \in k[[X_1, \ldots, X_{n-1}]][X_n]$.

Veamos que F es irreducible en $k[[X_1, \ldots, X_{n-1}]][X_n]$. En efecto, si $U \mid F$ en este anillo y no es una unidad, entonces tiene grado $r \geq 1$ y su coeficiente director es una unidad en $k[[X_1, \ldots, X_{n-1}]]$, ya que el coeficiente director de F es 1. Por consiguiente U contiene un monomio cX_n^r con $c \neq 0$.

La aplicación $k[[X_1,\ldots,X_{n-1}]] \longrightarrow k$ que a cada serie le asigna su término independiente es un homomorfismo de anillos que induce a su vez un homomorfismo $k[[X_1,\ldots,X_{n-1}]][X_n] \longrightarrow k[X_n]$. La imagen de U divide a la imagen de F, que es X_n^m, luego la imagen de U es exactamente cX_n^r. En particular esto implica que U no tiene término independiente, luego tampoco es una unidad en $k[[X_1,\ldots,X_n]]$.

Así pues, si F se descompusiera en $k[[X_1,\ldots,X_{n-1}]][X_n]$ como producto de dos factores no unitarios, lo mismo le sucedería en $k[[X_1,\ldots,X_n]]$ y no sería irreducible. Concluimos que F es irreducible en $k[[X_1,\ldots,X_{n-1}]][X_n]$. Por hipótesis de inducción $k[[X_1,\ldots,X_{n-1}]]$ es un dominio de factorización única, luego también lo es $k[[X_1,\ldots,X_{n-1}]][X_n]$, luego F es primo en este anillo, en el cual $F \mid GH$. Concluimos que $F \mid G$ o $F \mid H$ en $k[[X_1,\ldots,X_{n-1}]][X_n]$ y, por consiguiente, también en $k[[X_1,\ldots,X_n]]$. ■

Para terminar vamos a estudiar las derivadas parciales de las series formales de potencias.

En el anillo de polinomios $k[X_1,\ldots,X_n]$ tenemos definidas la aplicaciones lineales

$$\frac{\partial}{\partial X_i} : k[X_1,\ldots,X_n] \longrightarrow k[X_1,\ldots,X_n],$$

que cumplen las propiedades usuales de las derivadas. Las derivadas de una constante son nulas, las derivadas de una forma de grado $n > 0$ son formas de grado $n-1$ o tal vez la forma nula (esto sólo puede ocurrir si k tiene característica prima). En cualquier caso, la derivada de una forma de grado n tiene siempre grado $\geq n-1$ (entendiendo que el grado de 0 es $+\infty$).

Esto nos permite definir

$$\frac{\partial}{\partial X_i} : k[[X_1,\ldots,X_n]] \longrightarrow k[[X_1,\ldots,X_n]]$$

mediante

$$\frac{\partial F}{\partial X_i} = \sum_{m=1}^{\infty} \frac{\partial F_m}{\partial X_i},$$

de modo que

$$v\Big(\frac{\partial F}{\partial X_i}\Big) \geq v(F) - 1.$$

Esta desigualdad implica que las derivadas parciales son aplicaciones continuas. A su vez, de aquí se sigue que todas las propiedades de las derivadas parciales sobre polinomios valen también sobre series de potencias. Por ejemplo, para probar la fórmula del producto tomamos dos series F y G y las expresamos como límites de sus sumas parciales:

$$F = \lim_m F^{(m)}, \qquad G = \lim_m G^{(m)},$$

con lo que

$$\frac{\partial FG}{\partial X_i} = \lim_m \frac{\partial F^{(m)}G^{(m)}}{\partial X_i} = \lim_m \Big(\frac{\partial F^{(m)}}{\partial X_i} G^{(m)} + F^{(m)} \frac{\partial F^{(m)}}{\partial X_i}\Big) = \frac{\partial F}{\partial X_i} G + F \frac{\partial G}{\partial X_i}.$$

Igualmente se demuestra la fórmula para derivar un cociente F/G (donde G ha de ser una unidad) o la versión siguiente de la regla de la cadena:

Teorema 1.44 *Dados un polinomio $P(Y_1,\ldots,Y_m)\in k[Y_1,\ldots,Y_m]$ y m series formales de potencias $F_1,\ldots,F_m\in k[[X_1,\ldots,X_n]]$, se cumple que*

$$\frac{\partial P(F_1,\ldots,F_m)}{\partial X_i}=\sum_{r=1}^m \frac{\partial P}{\partial Y_r}(F_1,\ldots,F_m)\frac{\partial F_r}{\partial X_i}.$$

Si el cuerpo de constantes tiene característica 0, los coeficientes de una serie formal de potencias pueden recuperarse a partir de sus derivadas mediante la fórmula de Taylor:

Teorema 1.45 *Sea k un cuerpo de característica 0 y $F\in k[[X_1,\ldots,X_n]]$. Entonces*

$$F=\sum_{m=1}^\infty \sum_{r_1+\cdots+r_n=m}\frac{1}{r_1!\cdots r_n!}\left.\frac{\partial^m F}{\partial X_1^{r_1}\cdots\partial X_n^{r_n}}\right|_0 X_1^{r_1}\cdots X_n^{r_n},$$

donde la notación de parciales sucesivas tiene la interpretación obvia y la evaluación en 0 se una serie representa a su término independiente.

DEMOSTRACIÓN: Basta probar que la expresión tras el primer sumatorio es F_m (la forma de grado m de F). Ahora bien, es claro que

$$\left.\frac{\partial^m F}{\partial X_1^{r_1}\cdots\partial X_n^{r_n}}\right|_0=\frac{\partial^m F_m}{\partial X_1^{r_1}\cdots\partial X_n^{r_n}},$$

luego la expresión tras el primer sumatorio es el polinomio de Taylor de la forma F_m, luego es F_m. ■

1.6 Funciones holomorfas de varias variables

Pasamos ahora a ocuparnos de los preliminares analíticos. Suponemos al lector familiarizado con la teoría de funciones holomorfas de una variable, así como con el cálculo diferencial real de varias variables. En esta sección demostraremos los resultados que vamos a necesitar sobre funciones holomorfas de varias variables. Los hechos básicos son "híbridos" sencillos de ambas teorías. Identificamos cada punto

$$z=(z_1,\ldots,z_n)=(x_1+iy_1,\ldots,x_n+iy_n)\in\mathbb{C}^n$$

con el punto $(x_1,y_1,\ldots,x_n,y_n)\in\mathbb{R}^{2n}$.

Definición 1.46 Sea U abierto en $\mathbb{C}^n$. Una función $f:U\subset\mathbb{C}^n\longrightarrow\mathbb{C}^m$ es *holomorfa* si es diferenciable (como aplicación de un abierto de $\mathbb{R}^{2n}$ en $\mathbb{R}^{2m}$) y para cada $p\in U$, la diferencial $df_p:\mathbb{C}^n\longrightarrow\mathbb{C}^m$ es $\mathbb{C}$-lineal. Una biyección holomorfa con inversa holomorfa entre dos abiertos de $\mathbb{C}^n$ se llama *transformación conforme.*

Es claro que la composición de funciones holomorfas es una función holomorfa. Así mismo es evidente que una función con imagen en $\mathbb{C}^m$ es holomorfa si y sólo si lo son sus m funciones coordenadas. Por consiguiente, no perdemos generalidad si estudiamos la holomorfía de funciones $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}$.

La $\mathbb{C}$-linealidad de la diferencial en un punto $p \in U$ significa explícitamente que han de existir números complejos $\Delta_k = \alpha_k + i\beta_k$ tales que, para todo $z \in \mathbb{C}^n$,

$$df_p(z) = \sum_{k=1}^n \Delta_k z_k = \sum_{k=1}^n \big((\alpha_k x_k - \beta_k y_k) + i(\alpha_k y_k + \beta_k x_k)\big).$$

Si comparamos con

$$\sum_{k=1}^n \left(\left.\frac{\partial \operatorname{Re} f}{\partial x_k}\right|_p x_k + \left.\frac{\partial \operatorname{Re} f}{\partial y_k}\right|_p y_k + i\left.\frac{\partial \operatorname{Im} f}{\partial x_k}\right|_p x_k + i\left.\frac{\partial \operatorname{Im} f}{\partial y_k}\right|_p y_k \right),$$

que es otra expresión para $df_p(z_1, \ldots, z_n)$, vista como aplicación de $\mathbb{R}^{2n}$ en $\mathbb{R}^2$, concluimos que

$$\alpha_k = \left.\frac{\partial \operatorname{Re} f}{\partial x_k}\right|_p = \left.\frac{\partial \operatorname{Im} f}{\partial y_k}\right|_p, \quad \beta_k = -\left.\frac{\partial \operatorname{Re} f}{\partial y_k}\right|_p = \left.\frac{\partial \operatorname{Im} f}{\partial x_k}\right|_p.$$

Recíprocamente, basta con que se den las igualdades anteriores entre las derivadas parciales (en todo $p \in U$) para que los Δ_k definidos por las ecuaciones anteriores justifiquen que df_p es $\mathbb{C}$-lineal. En resumen:

Teorema 1.47 *Una función $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}$, definida en un abierto U, es holomorfa si y sólo si es diferenciable y verifica las llamadas* ecuaciones de Cauchy-Riemann:

$$\left.\frac{\partial \operatorname{Re} f}{\partial x_k}\right|_p = \left.\frac{\partial \operatorname{Im} f}{\partial y_k}\right|_p, \quad \left.\frac{\partial \operatorname{Re} f}{\partial y_k}\right|_p = -\left.\frac{\partial \operatorname{Im} f}{\partial x_k}\right|_p, \quad k = 1, \ldots, n.$$

En las condiciones de este teorema definimos

$$\left.\frac{\partial f}{\partial z_k}\right|_p = \left.\frac{\partial \operatorname{Re} f}{\partial x_k}\right|_p + i\left.\frac{\partial \operatorname{Im} f}{\partial x_k}\right|_p = -i\left(\left.\frac{\partial \operatorname{Re} f}{\partial y_k}\right|_p + i\left.\frac{\partial \operatorname{Im} f}{\partial y_k}\right|_p\right),$$

con lo que podemos expresar la diferencial de f en la forma

$$df_p(z) = \left.\frac{\partial f}{\partial z_1}\right|_p z_1 + \cdots + \left.\frac{\partial f}{\partial z_n}\right|_p z_n.$$

Teniendo en cuenta que las diferenciales dz_k son simplemente las proyecciones, como en el caso real podemos expresar esta igualdad como una ecuación funcional:

$$df = \frac{\partial f}{\partial z_1}\, dz_1 + \cdots + \frac{\partial f}{\partial z_n}\, dz_n.$$

En el caso general de una función $f : U \subset \mathbb{C}^m \longrightarrow \mathbb{C}^n$ concluimos que df es la aplicación lineal cuya matriz en las bases canónicas es la matriz jacobiana compleja

$$Jf = \begin{pmatrix} \frac{\partial f_1}{\partial z_1} & \cdots & \frac{\partial f_m}{\partial z_1} \\ \vdots & & \vdots \\ \frac{\partial f_1}{\partial z_n} & \cdots & \frac{\partial f_m}{\partial z_n} \end{pmatrix}$$

Aplicando que la matriz de una composición de aplicaciones lineales es el producto de las matrices obtenemos la regla de la cadena para derivadas parciales complejas.

La interpretación de las derivadas parciales es la misma que en el caso de funciones de variable real: si $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}$ es holomorfa y $p \in U$, existe un entorno de p_k donde está definida la función

$$f_k(z) = f(p_1, \ldots, \overset{(k)}{z}, \ldots, p_n)$$

y es holomorfa como función de una variable (porque es diferenciable y cumple las ecuaciones de Cauchy-Riemann). La derivada parcial respecto de z_k en p_k es la derivada $f_k'(p_k)$.

Es una simple rutina comprobar que las reglas básicas del cálculo de derivadas parciales de funciones de variable real son válidas también en el caso complejo. Por ejemplo, la función $z_1 z_2$ es holomorfa y

$$d(z_1 z_2) = z_2\, dz_1 + z_1\, dz_2.$$

Combinando esto con la regla de la cadena obtenemos la regla usual para la derivada parcial de un producto. Similarmente ocurre con sumas y cocientes.

Si $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}$ es una función holomorfa y $p \in U$, por las fórmulas integrales de Cauchy para funciones de una variable, existe un $\delta > 0$ y un abierto V en $\mathbb{C}^{n-1}$ tal que $p \in V \times D(p_n, 2\delta) \subset U$ y, para todo $z \in V \times D(p_n, 2\delta)$ tal que $|z_n - p_n| < \delta/2$, se cumple que

$$\frac{\partial f}{\partial z_n} = \frac{1}{2\pi i} \int_{|\zeta - p_n| = \delta} \frac{f(z_1, \ldots, z_{n-1}, \zeta)}{(\zeta - z_n)^2}\, d\zeta.$$

El integrando es una función continua en las $n+1$ variables, luego podemos concluir que las derivadas parciales de las funciones holomorfas son continuas. Ahora bien, el integrando es también una función holomorfa, luego sus derivadas parciales son continuas (respecto de las $n+1$ variables). Las derivadas de esta expresión respecto a x_k e y_k pueden calcularse derivando el integrando, con lo que son funciones continuas. Así pues, las derivadas parciales de f son diferenciables. Además, como el integrando verifica las ecuaciones de Cauchy-Riemann, lo mismo vale para para las derivadas parciales (complejas) de f. En conclusión:

Teorema 1.48 *Las derivadas parciales de las funciones holomorfas son funciones holomorfas. En particular las funciones holomorfas son infinitamente derivables.*

El teorema siguiente nos proporciona una relación más precisa entre la diferencial de una aplicación holomorfa como aplicación real y como aplicación compleja:

Teorema 1.49 *Si $f : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ es una aplicación $\mathbb{C}$-lineal, también es una aplicación $\mathbb{R}$-lineal, y el determinante de f como aplicación $\mathbb{R}$-lineal es el módulo al cuadrado de su determinante como aplicación $\mathbb{C}$-lineal.*

Demostración: Si (e_k) es la base canónica de $\mathbb{C}^n$, entonces una $\mathbb{R}$-base de $\mathbb{C}^n$ la forman los vectores e_k, ie_k. Si $f(e_k) = (a_{kj} + ib_{kj})$, entonces tenemos que $f(ie_k) = (-b_{kj} + ia_{kj})$, con lo que la matriz de f como aplicación $\mathbb{C}$-lineal es $A = (a_{kj} + ib_{kj})$ y la matriz de $\mathbb{C}$ como aplicación $\mathbb{R}$-lineal es[1]

$$B = \left(\begin{array}{c|c} a_{kj} & b_{kj} \\ \hline -b_{kj} & a_{kj} \end{array}\right).$$

Para calcular su determinante podemos considerarla como matriz compleja:

$$\left|\begin{array}{c|c} a_{kj} & b_{kj} \\ \hline -b_{kj} & a_{kj} \end{array}\right| = \left|\begin{array}{c|c} a_{kj} + ib_{kj} & b_{kj} \\ \hline -b_{kj} + ia_{kj} & a_{kj} \end{array}\right| = \left|\begin{array}{c|c} a_{kj} + ib_{kj} & b_{kj} \\ \hline 0 & a_{kj} - ib_{kj} \end{array}\right|,$$

con lo que $\det B = (\det A)(\det \overline{A}) = (\det A)(\overline{\det A}) = |\det A|^2$. ■

En particular, el determinante jacobiano de una transformación conforme entre dos abiertos de $\mathbb{C}^n$ es mayor que 0 en todo punto o, dicho de otro modo, las transformaciones conformes conservan la orientación.

Veamos ahora que las funciones holomorfas admiten desarrollos en series de potencias.

Ante todo, diremos que una serie formal $F \in \mathbb{C}[[Z_1, \ldots, Z_n]]$ es *convergente* en un punto $(z_1, \ldots, z_n) \in \mathbb{C}^n$ si la serie que resulta de evaluar sus monomios en $(z_1, \ldots, z_n)$ converge absolutamente en $\mathbb{C}$ con cualquier ordenación de sus términos. Al exigir convergencia absoluta, la ordenación es irrelevante.

Es claro que esta definición coincide con la usual en el caso de series de una variable (aquí hay que tener presente que las series de potencias de una variable convergen absolutamente en su disco de convergencia).

Diremos que una serie de potencias es *convergente* si converge en todos los puntos de un entorno de $(0, \ldots, 0)$. El *dominio de convergencia* de la serie es la unión de todos los entornos (abiertos) de 0 donde converge.

Teorema 1.50 *Una serie de potencias convergente converge casi uniformemente en su dominio a una función holomorfa.*

[1] Entenderemos que las matrices divididas en bloques representan a las matrices que resultan de intercalar las filas y las columnas de cada bloque.

DEMOSTRACIÓN: Sea $F(Z_1, \ldots, Z_n) \in \mathbb{C}[[Z_1, \ldots, Z_n]]$ una serie convergente. Por la propia definición de convergencia (donde exigimos convergencia absoluta), tenemos que si F converge en un punto $(z_1, \ldots, z_n)$ con $z_i \neq 0$ para todo i, entonces también converge en $(r_1, \ldots, r_n) = (|z_1|, \ldots, |z_n|)$ y, por el criterio de mayoración de Weierstrass, la serie converge uniformemente sobre el compacto formado por todos los puntos que cumplen $|z_i| \leq r_i$. Es fácil ver que todo subconjunto compacto del dominio puede cubrirse por un número finito de compactos de esta forma, lo que nos da la convergencia casi uniforme.

En particular tenemos que F es un límite casi uniforme de funciones continuas, luego es una función continua en su dominio.

Si $(z_1, \ldots, z_n)$ es un punto de dicho dominio, la función $F(z_1, \ldots, z_{n-1}, Z_n)$ viene dada por una serie de potencias de una variable convergente en un entorno de 0, luego es una función holomorfa y su derivada es el límite de las derivadas de sus sumas parciales, es decir, la suma de la serie formal $\partial F/\partial Z_n$.

Lo mismo es válido si fijamos otras coordenadas, y así podemos concluir que las derivadas parciales (formales) de F son convergentes (al menos en el mismo dominio que F) y sus sumas son las derivadas parciales correspondientes de (la suma de) F.

En particular, las derivadas parciales de F funciones continuas (porque vienen dadas por series convergentes), luego (la suma de) F es una función diferenciable.

Finalmente, como al fijar $n-1$ variables en F obtengamos una función holomorfa de una variable, tenemos que F satisface las ecuaciones de Cauchy-Riemann, luego es una función holomorfa. ■

Recíprocamente, toda función F holomorfa en un entorno de $(0, \ldots, 0)$ se puede expresar como suma de una serie de potencias. Un *polidisco* en $\mathbb{C}^n$ es un conjunto de la forma

$$D(z; r_1, \ldots r_n) = \{w \in \mathbb{C}^n \mid |w_i - z_i| < r_i, \quad i = 1, \ldots, n\}.$$

Tomamos un polidisco $D = D(0; r_1, \ldots, r_n)$ cuya clausura esté contenida en el dominio de F y, para cada punto $(z_1, \ldots, z_n) \in D$, consideramos la integral:

$$\int_{|\zeta_1|=r_1, \ldots, |\zeta_n|=r_n} \frac{F(\zeta_1, \ldots, \zeta_n)}{(\zeta_1 - z_1) \cdots (\zeta_n - z_n)} \, d\zeta_1 \cdots d\zeta_n.$$

Esta integral se define análogamente a las integrales curvilíneas de una variable, de modo que, tras un cambio de variables, se reduce a dos integrales (una parte real y otra imaginaria) sobre un cubo $[0, 1]^n$. Puesto que estamos integrando una función continua sobre un conjunto compacto, podemos descomponer la integral en n integrales sucesivas. Si consideramos todo el integrando salvo el término $\zeta_n - z_n$ como una función holomorfa de la variable ζ_n, la fórmula integral de Cauchy para funciones de una variable nos da que la integral coincide con

$$2\pi i \int_{|\zeta_1|=r_1, \ldots, |\zeta_{n-1}|=r_{n-1}} \frac{F(\zeta_1, \ldots, \zeta_{n-1}, z_n)}{(\zeta_1 - z_1) \cdots (\zeta_{n-1} - z_{n-1})} \, d\zeta_1 \cdots d\zeta_{n-1}.$$

Repitiendo el razonamiento llegamos a que

$$F(z_1,\ldots,z_n) = \frac{1}{(2\pi i)^n}\int_{|\zeta_1|=r_1,\ldots,|\zeta_n|=r_n} \frac{F(\zeta_1,\ldots,\zeta_n)}{(\zeta_1-z_1)\cdots(\zeta_n-z_n)}\,d\zeta_1\cdots d\zeta_n.$$

Ésta es la versión para varias variables de la fórmula integral de Cauchy. Ahora sumamos la serie geométrica de razón z_i/ζ_i y la dividimos entre ζ_i. El resultado es

$$\frac{1}{\zeta_i - z_i} = \sum_{m_i=0}^{\infty}\frac{z_i^{m_i}}{\zeta_i^{m_i+1}},$$

donde la serie converge absolutamente siempre que $|z_i| < |\zeta_i|$. Por la fórmula del producto de Cauchy tenemos la convergencia absoluta de

$$\frac{1}{(\zeta_1-z_1)\cdots(\zeta_n-z_n)} = \sum_{m_1,\ldots,m_n}\frac{z_1^{m_1}\cdots z_n^{m_n}}{\zeta_1^{m_1+1}\cdots\zeta_n^{m_n+1}}.$$

El criterio de mayoración de Weierstrass implica que esta serie converge uniformemente sobre el producto de las circunferencias $|\zeta_i| = r_i$, y esto sigue siendo cierto si multiplicamos cada sumando por $F(\zeta_1,\ldots,\zeta_n)$ (ya que F está acotada sobre el producto). Esto significa que si sustituimos esta expresión en la fórmula integral de Cauchy, podemos intercambiar la integral con el sumatorio, lo que nos lleva a que

$$F(z_1,\ldots,z_n) = \sum_{m_1,\ldots,m_n} a_{m_1,\ldots,m_n} z_1^{m_1}\cdots z_n^{m_n},$$

donde

$$a_{m_1,\ldots,m_n} = \frac{1}{(2\pi i)^n}\int_{|\zeta_1|=r_1,\ldots,|\zeta_n|=r_n}\frac{F(\zeta_1,\ldots,\zeta_n)}{\zeta_1^{m_1+1}\cdots\zeta_n^{m_n+1}}\,d\zeta_1\cdots d\zeta_n.$$

Con esto tenemos probada la mayor parte del teorema siguiente:

Teorema 1.51 *Si F es una función holomorfa en un entorno de la clausura de un polidisco D de centro 0, entonces F admite en D un único desarrollo en serie de potencias*

$$F(z_1,\ldots,z_n) = \sum_{m=1}^{\infty}\sum_{r_1+\cdots+r_n=m}\frac{1}{r_1!\cdots r_n!}\left.\frac{\partial^m F}{\partial Z_1^{r_1}\cdots\partial Z_n^{r_n}}\right|_0 Z_1^{r_1}\cdots Z_n^{r_n}.$$

DEMOSTRACIÓN: Hemos probado que F admite un desarrollo en serie de potencias para ciertos coeficientes. El teorema 1.45 afirma que dichos coeficientes son necesariamente los que indica el enunciado si interpretamos las derivadas formalmente (es decir, considerando que F no es la función holomorfa dada sino la serie de potencias). Ahora bien, sabemos que las derivadas formales de la serie de potencias convergen a las derivadas de la función F, y al evaluarlas en 0 obtenemos el valor en 0 de las derivadas de (la función) F, luego el desarrollo de F es necesariamente el que indica el enunciado. ■

Definición 1.52 Llamaremos $\mathbb{C}\{Z_1,\ldots,Z_n\}$ al subconjunto de $\mathbb{C}[[Z_1,\ldots,Z_n]]$ formado por las series que convergen en un entorno de 0. Obviamente se trata de un subanillo, pues la suma de dos series convergentes converge a la suma de las sumas de las series, e igualmente con el producto.

Más aún, si $F \in \mathbb{C}\{Z_1,\ldots,Z_n\}$ es una unidad en $\mathbb{C}[[Z_1,\ldots,Z_n]]$, también es una unidad en $\mathbb{C}\{Z_1,\ldots,Z_n\}$. En efecto, sabemos que su término independiente no es nulo, luego su suma no se anula en $(0,\ldots,0)$, luego la función $1/F$ es holomorfa en un entorno de $(0,\ldots,0)$ y admite un desarrollo en serie, es decir, existe una serie convergente G tal que $FG=1$. En principio este producto se refiere a las funciones suma, pero entonces el producto formal converge a la constante 1 y, por la unicidad de los desarrollos, $FG=1$ en $\mathbb{C}[[Z_1,\ldots,Z_n]]$. En otras palabras, la inversa de una serie convergente (cuando existe) es también una serie convergente.

Equivalentemente, el anillo $\mathbb{C}\{Z_1,\ldots,Z_n\}$ tiene a $\mathfrak{m}=(Z_1,\ldots,Z_n)$ como único ideal maximal. Notemos que para comprobar la convergencia de una serie podemos sustituir sus coeficientes por sus valores absolutos y estudiarla sobre puntos con coordenadas reales positivas. Teniendo esto en cuenta, es fácil ver que $\mathbb{C}\{Z_1,\ldots,Z_n\}\cong\mathbb{C}\{Z_1,\ldots,Z_{n-1}\}\{Z_n\}$.

El mismo argumento empleado para $\mathbb{C}[[Z]]$ prueba que $\mathbb{C}\{Z\}$ es un dominio de ideales principales. Más aún, el teorema de preparación de Weierstrass y todas sus consecuencias son válidas para $\mathbb{C}\{Z_1,\ldots,Z_n\}$ con las mismas pruebas. El único punto donde hay que añadir algunas comprobaciones adicionales es en la prueba del propio teorema 1.40:

En primer lugar, es evidente que si P es una serie convergente, las series $r(P)$ y $h(P)$ son también convergentes. Más aún, si llamamos $\bar{P}$ a la serie que resulta de sustituir los coeficientes de P por sus valores absolutos, tenemos que sobre números reales positivos, $\overline{h(P)}$ está mayorada por $\bar{P}$. Por consiguiente, $\overline{s(P)}$ está mayorada por $\bar{M}\bar{P}$, y $\overline{s^n(P)}$ está mayorada por $\bar{M}^n\bar{P}$.

Esto garantiza la convergencia de la serie V dada por (1.6), pues $\bar{V}$ está mayorada por la serie

$$(\bar{M}+\bar{M}^2+\bar{M}^3+\cdots)\bar{H},$$

que converge en un entorno de 0, ya que $\bar{M}(0)=0$, luego en un entorno de 0 se cumple que $\bar{M}(r_1,\ldots,r_n)<1$, y la suma es una serie geométrica. De la convergencia de V se sigue la de todas las series que proporciona el teorema.

De aquí se sigue inmediatamente que $\mathbb{C}\{Z_1,\ldots,Z_n\}$ es noetheriano, la versión de 1.42 para series convergentes y el hecho de que $\mathbb{C}\{Z_1,\ldots,Z_n\}$ es un dominio de factorización única.

Veamos ahora un resultado técnico que necesitaremos más adelante. Para cada punto $a\in\mathbb{C}^n$, llamamos $\mathcal{H}_a$ al conjunto de las clases de equivalencia de funciones holomorfas en un entorno de a, donde dos funciones están relacionadas si coinciden en un entorno de a. Si $h\in\mathcal{H}_a$, entonces $h(z+a)$ es holomorfa en un entorno de 0, luego el teorema 1.51 nos da una serie de Taylor en $\mathbb{C}\{Z_1,\ldots,Z_n\}$. Claramente, así tenemos un isomorfismo $\mathcal{H}_a\cong\mathbb{C}\{Z_1,\ldots,Z_n\}$ que prueba, en particular, que $\mathcal{H}_a$ es un dominio de factorización única.

Teorema 1.53 *Si f y g son funciones holomorfas en un punto $a \in \mathbb{C}^n$ primas entre sí como elementos de $\mathcal{H}_a$, entonces existe un entorno U de a en el que ambas son holomorfas y primas entre sí como elementos de $\mathcal{H}_b$, para todo $b \in U$.*

DEMOSTRACIÓN: Notemos que podemos suponer $a = 0$. En efecto, la aplicación $\phi : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ dada por $\phi(z) = z + a$ es una transformación conforme que induce isomorfismos $\mathcal{H}_b \cong \mathcal{H}_{b+a}$. Así, $\phi \circ f$ y $\phi \circ g$ son primas entre sí en $\mathcal{H}_0$ y, si el teorema se cumple para ellas, entonces son primas entre sí en todos los anillos $\mathcal{H}_b$, donde b recorre un entorno de 0, luego f y g son primas entre sí en todos los anillos $\mathcal{H}_{a+b}$, es decir, en los anillos $\mathcal{H}_b$, donde ahora b recorre un entorno de a.

Supongamos, pues, que $a = 0$. El resultado es trivial si alguna de las funciones es una unidad en $\mathcal{H}_0$, pues entonces lo es también en $\mathcal{H}_b$, para todo b en un entorno de 0. Supongamos que no son unidades.

La prueba del teorema 1.39 muestra que es posible encontrar una misma transformación lineal $\phi : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ que haga que las funciones $f' = \phi \circ f$ y $g' = \phi \circ g$ tengan series de Taylor regulares en Z_n. Estas funciones siguen siendo primas entre sí en $\mathcal{H}_0$ y, si existe un entorno U que cumple el teorema para ellas, es claro que $\phi[U]$ es un entorno de 0 que cumple el teorema para f y g, ya que para cada $u \in U$ tenemos que f' y g' son primas entre sí en $\mathcal{H}_u$, luego f y g son primas entre sí en $\mathcal{H}_{\phi(u)}$.

Por consiguiente, podemos suponer que las series de Taylor de f y g en 0 son regulares en Z_n, con lo que el teorema 1.42 nos da que, salvo unidades, dichas series son polinomios mónicos en Z_n con coeficientes en $\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}$. Puesto que las unidades lo son también en todos los puntos de un entorno de 0, podemos eliminarlas.

Sea d el máximo común divisor de f y g en $\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}[Z_n]$, un polinomio que podemos tomar mónico y que será una unidad en $\mathbb{C}\{Z_1, \ldots, Z_n\}$. Entonces d es también el máximo común divisor de f y g en el anillo de polinomios sobre el cuerpo de cocientes de $\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}$, donde podemos aplicar la relación de Bezout. Después de quitar denominadores, se convierte en una relación de la forma

$$uf + vg = dr,$$

donde u, v son funciones holomorfas en un entorno de 0 con series de Taylor en $\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}[Z_n]$ y r es una función holomorfa no nula cuya serie de Taylor pertenece a $\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}$. Sea U un entorno de 0 donde estén definidas todas estas funciones y donde d siga siendo una unidad.

Si $b \in U$, podemos considerar las cinco funciones como elementos de $\mathcal{H}_b$, que se identifican con series de $\mathbb{C}\{Z_1, \ldots, Z_n\}$ componiéndolas primero con la traslación $z + b$. Esta composición hace que las series de Taylor sean otras, pero sigue siendo cierto que las series de u, v, f, g, d son polinomios (mónicos en el caso de f, g y d) de $\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}[Z_n]$ y la de r está en $\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}$. Si ahora identificamos las funciones con estas nuevas series alrededor de b, siguen cumpliendo la relación $uf + vg = dr$.

Supongamos que f y g tienen un divisor común (no unitario) c en $\mathcal{H}_b$, que será también un divisor de r. Notemos que todo primo $p \in \mathbb{C}\{Z_1, \ldots, Z_{n-1}\}$ es también primo en el anillo $\mathbb{C}\{Z_1, \ldots, Z_n\} \cong \mathbb{C}\{Z_1, \ldots, Z_{n-1}\}\{Z_n\}$, ya que

$$\mathbb{C}\{Z_1, \ldots, Z_n\}/(p) \cong (\mathbb{C}\{Z_1, \ldots, Z_{n-1}\}/(p))\{Z_n\}$$

es un dominio íntegro. Por consiguiente, eliminando una unidad, podemos suponer que $c \in \mathbb{C}\{Z_1, \ldots, Z_{n-1}\}$. Más aún, c no puede ser una unidad de este anillo. Esto hace que un múltiplo de c no pueda tener un monomio Z_n^m, pero f lo tiene, lo que nos da una contradicción. ■

Definición 1.54 Una *serie de Laurent* es una serie de la forma

$$\sum_{m_1,\ldots,m_n\in\mathbb{Z}} a_{m_1,\ldots,m_n} z_1^{m_1} \cdots z_n^{m_n}, \qquad a_{m_1,\ldots,m_n} \in \mathbb{C}.$$

Su *dominio de convergencia* es la unión de todos los abiertos donde converge absolutamente.

Hay que entender que la convergencia de una serie de Laurent sólo está definida para puntos $z \in \mathbb{C}^n$ tales que $z_i \neq 0$ para todo i. Observemos que una serie de Laurent se descompone en suma de 2^n series:

$$\sum_{\epsilon_1,\ldots,\epsilon_n} \sum_{m_1,\ldots,m_n} a_{\epsilon_1 m_1,\ldots,\epsilon_n m_n} z_1^{\epsilon_1 m_1} \cdots z_n^{\epsilon_n m_n},$$

donde $\epsilon_i = \pm 1$ y m_i recorre los números naturales si $\epsilon_i = 1$ y los números naturales no nulos si $\epsilon_i = -1$.

Si llamamos

$$S_\epsilon(z) = \sum_{m_1,\ldots,m_n} a_{\epsilon_1 m_1,\ldots,\epsilon_n m_n} z_1^{m_1} \cdots z_n^{m_n},$$

tenemos que la serie de Laurent converge en un punto $z \in \mathbb{C}^n$ (de coordenadas no nulas) si y sólo si cada serie de potencias S_ϵ converge en $z^\epsilon = (z_1^{\epsilon_1}, \ldots, z_n^{\epsilon_n})$, y el tal caso la suma de la serie es igual a

$$\sum_\epsilon S_\epsilon(z^\epsilon).$$

Teniendo en cuenta que las funciones $z \mapsto z^\epsilon$ son transformaciones conformes, es claro que una serie de Laurent converge casi uniformemente a una función holomorfa en su dominio de convergencia.

Ahora vamos a demostrar que toda función holomorfa en un *polidisco reducido*

$$D'(0; r_1, \ldots, r_n) = \{z \in \mathbb{C}^n \mid 0 < |z_i| < r_i,\ i = 1, \ldots, n\}$$

admite un desarrollo en serie de Laurent:

Teorema 1.55 *Sea f una función holomorfa en un polidisco $D'(0; r_1, \ldots, r_n)$, entonces f admite un desarrollo en serie absolutamente convergente de la forma*

$$f(z) = \sum_{m_1,\ldots,m_n \in \mathbb{Z}} a_{m_1,\ldots,m_n} z_1^{m_1} \cdots z_n^{m_n},$$

donde necesariamente

$$a_{m_1,\ldots,m_n} = \frac{1}{(2\pi i)^n} \int_{|z_1|=r_1',\ldots,|z_n|=r_n'} \frac{f(\zeta_1,\ldots,\zeta_n)}{\zeta_1^{m_1+1} \cdots \zeta_n^{m_n+1}} \, d\zeta_1 \cdots d\zeta_n,$$

para cualesquiera $0 < r_i' < r_i$.

Demostración: Por simplificar la notación vamos a tomar $n = 2$, aunque el argumento es completamente general. Fijemos radios $r_i' < |z_i| < r_i'' < r_i$ y llamemos C_i' (resp. C_i'') a la circunferencia de centro 0 y radio r_i' (resp. r_i''). Consideramos la integral

$$\int_{(C_1'-C_1'')\times(C_2'-C_2'')} \frac{f(\zeta_1,\zeta_2)}{(\zeta_1 - z_1)(\zeta_2 - z_2)} \, d\zeta_1 d\zeta_2.$$

Descomponiéndola en dos integrales sucesivas y aplicando sucesivamente el teorema de Cauchy para funciones de una variable (comparar con el razonamiento previo al teorema 1.51), concluimos que

$$\begin{aligned}
f(z_1,z_2) &= \frac{1}{(2\pi i)^2} \int_{(C_1'-C_1'')\times(C_2'-C_2'')} \frac{f(\zeta_1,\zeta_2)}{(\zeta_1 - z_1)(\zeta_2 - z_2)} \, d\zeta_1 d\zeta_2 \\
&= \frac{1}{(2\pi i)^2} \int_{C_1'\times C_2'} \frac{f(\zeta_1,\zeta_2)}{(\zeta_1 - z_1)(\zeta_2 - z_2)} \, d\zeta_1 d\zeta_2 \\
&+ \frac{1}{(2\pi i)^2} \int_{C_1''\times C_2''} \frac{f(\zeta_1,\zeta_2)}{(\zeta_1 - z_1)(\zeta_2 - z_2)} \, d\zeta_1 d\zeta_2 \\
&- \frac{1}{(2\pi i)^2} \int_{C_1'\times C_2''} \frac{f(\zeta_1,\zeta_2)}{(\zeta_1 - z_1)(\zeta_2 - z_2)} \, d\zeta_1 d\zeta_2 \\
&- \frac{1}{(2\pi i)^2} \int_{C_1''\times C_2'} \frac{f(\zeta_1,\zeta_2)}{(\zeta_1 - z_1)(\zeta_2 - z_2)} \, d\zeta_1 d\zeta_2.
\end{aligned}$$

Los cuatro integrandos se desarrollan de forma similar como series de potencias. Veamos, por ejemplo, el caso del último. Para $|\zeta_1| = r_1''$ se cumple que

$$\frac{1}{\zeta_1 - z_1} = \sum_{m_1=0}^{\infty} \frac{z_1^{m_1}}{\zeta_1^{m_1+1}},$$

mientras que para $|\zeta_2| = r_2'$ tenemos que

$$-\frac{1}{\zeta_2 - z_2} = \sum_{m_2=0}^{\infty} \frac{\zeta_2^{m_2}}{z_2^{m_2+1}}.$$

La fórmula del producto de Cauchy nos da entonces la convergencia absoluta de

$$-\frac{1}{(\zeta_1 - z_1)(\zeta_2 - z_2)} = \sum_{m_1,m_2=0}^{\infty} \frac{z_1^{m_1}}{\zeta_1^{m_1+1}} \frac{\zeta_2^{m_2}}{z_2^{m_2+1}} = \sum_{m_1 \geq 0, m_2 < 0} \frac{z_1^{m_1} z_2^{m_2}}{\zeta_1^{m_1+1} \zeta_2^{m_2+1}}.$$

El cuarto término de la descomposición precedente se convierte así en

$$\frac{1}{(2\pi i)^2} \int_{|\zeta_1|=r_1'', |\zeta_2|=r_2'} \sum_{m_1 \geq 0, m_2 < 0} \frac{f(\zeta_1, \zeta_2)}{\zeta_1^{m_1+1} \zeta_2^{m_2+1}} \, z_1^{m_1} z_2^{m_2}.$$

El teorema de mayoración de Weierstrass implica que la serie converge uniformemente sobre el producto de las dos circunferencias (pues podemos mayorarla por el producto de una cota de f por las series geométricas de razones $|z_1|/r_1''$ y $r_2'/|z_2|$, respectivamente). Esto nos permite intercambiar la serie con la integral, con lo que resulta:

$$\frac{1}{(2\pi i)^2} \sum_{m_1 \geq 0, m_2 < 0} \left(\int_{|\zeta_1|=r_1'', |\zeta_2|=r_2'} \frac{f(\zeta_1, \zeta_2)}{\zeta_1^{m_1+1} \zeta_2^{m_2+1}} \right) z_1^{m_1} z_2^{m_2}.$$

Descomponiendo la integral en dos integrales sucesivas y aplicando las propiedades de las integrales de funciones holomorfas de una variable vemos que la integral no se modifica si cambiamos los radios por los radios r_1' y r_2' del enunciado. Al agrupar los cuatro términos queda el desarrollo del enunciado.

Veamos ahora que si f admite un desarrollo en serie de Laurent, entonces los coeficientes a_m son necesariamente los dados por el teorema. En efecto, consideramos la integral:

$$\int_{|z_1|=r_1', \ldots, |z_n|=r_n'} \frac{f(\zeta_1, \ldots, \zeta_n)}{\zeta_1^{m_1} \cdots \zeta_n^{m_n}} \, d\zeta_1 \cdots d\zeta_n.$$

El desarrollo de f puede descomponerse en suma de un número finito de series de potencias (agrupamos todos los monomios con exponentes del mismo signo y cambiamos z_i por $1/z_i$ para los exponentes negativos), de donde se deduce que la serie converge uniformemente en compactos. Esto nos permite intercambiar la serie con la integral, con lo que ésta es igual a

$$\sum_{s \in \mathbb{Z}^n} a_s \int_{|z_1|=r_1', \ldots, |z_n|=r_n'} \zeta_1^{s_1 - m_1 + 1} \cdots \zeta_n^{s_n - m_n + 1} d\zeta_1 \cdots d\zeta_n.$$

Como las variables están separadas, la integral se descompone en un producto de n integrales de una variable, y todas son nulas excepto las correspondientes a $s_i = m_i$. Resulta que

$$\int_{|z_1|=r_1', \ldots, |z_n|=r_n'} \frac{f(\zeta_1, \ldots, \zeta_n)}{\zeta_1^{m_1} \cdots \zeta_n^{m_n}} \, d\zeta_1 \cdots d\zeta_n = (2\pi i)^n a_m,$$

luego a_m es necesariamente el dado en el enunciado. ■

Para terminar vamos a demostrar las versiones complejas del teorema de la función inversa y el teorema de la función implícita. El teorema de la función implícita del análisis real se traduce inmediatamente a su análogo complejo:

Teorema 1.56 *Sea $f : U \subset \mathbb{C}^{m+n} \longrightarrow \mathbb{C}^n$ una función holomorfa en el abierto U y sea $(w_0, z_0) \in U$ tal que $f(w_0, z_0) = 0$. Supongamos que*

$$\begin{vmatrix} \left.\frac{\partial f_1}{\partial z_1}\right|_{(w_0,z_0)} & \cdots & \left.\frac{\partial f_n}{\partial z_1}\right|_{(w_0,z_0)} \\ \vdots & & \vdots \\ \left.\frac{\partial f_1}{\partial z_n}\right|_{(w_0,z_0)} & \cdots & \left.\frac{\partial f_n}{\partial z_n}\right|_{(w_0,z_0)} \end{vmatrix} \neq 0.$$

Entonces existen abiertos $(w_0, z_0) \in W \subset U$, $w_0 \in X \subset \mathbb{C}^m$ y una función holomorfa $g : X \longrightarrow \mathbb{C}^n$ de modo que

$$\{(w, z) \in W \mid f(w, z) = 0\} = \{(w, g(w)) \mid w \in X\}.$$

DEMOSTRACIÓN: Si reformulamos las hipótesis del teorema en términos del análisis real, tenemos una función $f : U \subset \mathbb{R}^{2m+2n} \longrightarrow \mathbb{R}^{2n}$ de clase C^∞ y un punto $(u_1, v_1, \ldots, u_m, v_m, x_1, y_1, \ldots, x_n, y_n)$ que cumple $f(u, v, x, y) = 0$. Además, el determinante formado por las derivadas de las $2n$ últimas funciones coordenadas de f respecto de las variables x_i e y_i (en dicho punto) es no nulo, pues es el cuadrado del módulo del determinante del enunciado (la relación entre ambos determinantes es la misma que entre los considerados en el teorema 1.49). Esto nos permite aplicar el teorema de la función implícita real, según el cual existen abiertos W y X y una función g de clase C^∞ que cumplen el enunciado salvo en lo tocante a la holomorfía de g. El teorema quedará probado si demostramos que g cumple las ecuaciones de Cauchy-Riemann.

Para ello basta derivar la función $f(w, g(w))$ —que es idénticamente nula en el abierto X— mediante la regla de la cadena. Por simplicidad llamaremos $z = x + iy = g(w)$:

$$\sum_{i=1}^n \frac{\partial \operatorname{Re} f_k}{\partial x_i} \frac{\partial x_i}{\partial u_j} + \sum_{i=1}^n \frac{\partial \operatorname{Re} f_k}{\partial y_i} \frac{\partial y_i}{\partial u_j} + \frac{\partial \operatorname{Re} f_k}{\partial u_j} = 0,$$

$$\sum_{i=1}^n \frac{\partial \operatorname{Im} f_k}{\partial x_i} \frac{\partial x_i}{\partial u_j} + \sum_{i=1}^n \frac{\partial \operatorname{Im} f_k}{\partial y_i} \frac{\partial y_i}{\partial u_j} + \frac{\partial \operatorname{Im} f_k}{\partial u_j} = 0.$$

Cuando k varía entre 1 y n tenemos un sistema de $2n$ ecuaciones lineales con $2n$ incógnitas cuya matriz de coeficientes tiene determinante no nulo. Más concretamente, es de la forma

$$\left|\begin{array}{c|c} A & B \\ \hline -B & A \end{array}\right|,$$

donde

$$A' = \left(\frac{\partial \operatorname{Re} f_k}{\partial x_i}\right), \quad B = \left(\frac{\partial \operatorname{Re} f_k}{\partial y_i}\right).$$

Esto nos permite despejar $\dfrac{\partial x_i}{\partial u_j}$ como cociente de dos determinantes: el denominador es el determinante anterior, y el numerador tiene la forma

$$\left|\begin{array}{c|c} A' & B \\ \hline -B' & A \end{array}\right|,$$

donde A' y B' resultan de sustituir la columna i-ésima en A y en B respectivamente por la columna formada por las derivadas

$$-\frac{\partial \operatorname{Re} f_k}{\partial u_j} \quad \text{y} \quad -\frac{\partial \operatorname{Re} f_k}{\partial v_j}, \quad k = 1, \ldots, n.$$

La derivada $\dfrac{\partial y_i}{\partial v_j}$ tiene una expresión casi idéntica, con la única diferencia de que ahora el numerador es el determinante

$$\left| \begin{array}{c|c} A & B' \\ \hline -B & A' \end{array} \right|.$$

Mediante manipulaciones sencillas se concluye que

$$\left| \begin{array}{c|c} A' & B \\ \hline -B' & A \end{array} \right| = \left| \begin{array}{c|c} A & B' \\ \hline -B & A' \end{array} \right|,$$

con lo que

$$\frac{\partial x_i}{\partial u_j} = \frac{\partial y_i}{\partial v_j}.$$

Similarmente se comprueban las otras ecuaciones de Cauchy-Riemann. ■

Ahora es fácil probar el teorema de la función inversa:

Teorema 1.57 *Sea $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}^n$ una función holomorfa en el abierto U y sea $z_0 \in U$ tal que la matriz jacobiana $Jf(z_0)$ tenga determinante no nulo. Entonces existen abiertos $z_0 \in U_0 \subset U$ y $f(z_0) \in V \subset \mathbb{C}^n$ de modo que $f|_{U_0} : U_0 \longrightarrow V$ es una transformación conforme.*

Demostración: Basta aplicar el teorema de la función implícita a la función $h : \mathbb{C}^n \times U \longrightarrow \mathbb{C}^n$ dada por $h(w, z) = w - f(z)$ y al punto $(f(z_0), z_0)$. Esto nos da una función holomorfa $g : V \longrightarrow U_0$ tal que $h(w, g(w)) = 0$, es decir, $f(g(w)) = w$, para todo $w \in V$.

Por el teorema de la función inversa real sabemos también que f es biyectiva en un entorno de z_0, luego g ha de ser su inversa, y acabamos de ver que es holomorfa. ■

Terminamos con una ligera generalización del teorema de la función implícita.

Teorema 1.58 *Sea $f : U \subset \mathbb{C}^n \longrightarrow \mathbb{C}^m$ una función holomorfa en el abierto U. Sea $z_0 \in U$ tal que $f(z_0) = 0$ y la matriz jacobiana $Jf(z)$ tenga rango constante r en un entorno de z_0. Entonces podemos dividir adecuadamente las coordenadas de $\mathbb{C}^n = \mathbb{C}^{n-r} \times \mathbb{C}^r$ de modo que existen abiertos*

$$z_0 = (z_1^0, z_2^0) \in W \subset U, \qquad z_1^0 \in X \subset \mathbb{C}^{n-r}$$

y una función holomorfa $g : X \longrightarrow \mathbb{C}^r$ de modo que

$$\{(z_1, z_2) \in W \mid f(z_1, z_2) = 0\} = \{(z_1, g(z_1)) \mid z_1 \in X\}.$$

Demostración: Reordenando las variables y las funciones coordenadas de f, podemos suponer que el determinante de las r primeras filas y columnas de $Jf(z)$ es distinto de 0 en z_0. Por continuidad sigue siendo no nulo en un entorno de z_0. Sea $f' : U \longrightarrow \mathbb{C}^r$ la función formada por las r primeras funciones coordenadas de f. Podemos aplicarle el teorema de la función implícita, lo cual nos da abiertos como los del enunciado y una función $g : X \longrightarrow \mathbb{C}^r$ que cumple el enunciado para f' en lugar de f. Podemos suponer que el determinante formado por las primeras r filas de Jf' no se anula en W. Basta probar que

$$\{z \in W \mid f(z) = 0\} = \{z \in W \mid f'(z) = 0\}.$$

Una inclusión es obvia. Sea $F_i : X \longrightarrow \mathbb{C}$ dada por $F_i(z) = f_i(z, g(z))$. Sabemos que $F_i = 0$ para $i = 1, \ldots, r$ y basta probar que lo mismo es cierto para índices mayores. También sabemos que $F_i(z_1^0) = 0$ para todo i, luego es suficiente ver que las derivadas parciales de las funciones F_i son nulas en X, ya que entonces las funciones F_i serán constantes.

Si $(z_1, \ldots, z_{n-r}) \in X$, entonces $z = (z_1, \ldots, z_{n-r}, g(z_1, \ldots, z_{n-r})) \in W$ luego las r primeras columnas de $Jf(z)$ son linealmente independientes y, por otra parte, sabemos que el rango es r, luego las columnas restantes son combinación lineal de las primeras. Digamos que

$$\frac{\partial f_i}{\partial z_k} = \sum_{l=1}^{r} a_{il} \frac{\partial f_l}{\partial z_k}, \quad i = r+1, \ldots, m.$$

En principio, los coeficientes a_{ij} son funciones de z, pero sólo nos van a interesar sobre el z que hemos fijado. Por otra parte, ara $i > r$ y $1 \leq j \leq n-r$ se cumple que

$$\frac{\partial F_i}{\partial z_j} = \frac{\partial f_i}{\partial z_j} + \sum_{k=n-r+1}^{n} \frac{\partial f_i}{\partial z_k} \frac{\partial z_k}{\partial z_j},$$

donde las funciones z_k de la derecha son las funciones coordenadas de g y las parciales respecto de f_i están evaluadas en $(z_1, \ldots, z_{n-r}, g(z_1, \ldots, z_{n-r}))$. Por lo tanto

$$\frac{\partial F_i}{\partial z_j} = \sum_{l=1}^{r} a_{il} \frac{\partial f_l}{\partial z_j} + \sum_{k=n-r+1}^{n} \sum_{l=1}^{r} a_{il} \frac{\partial f_l}{\partial z_k} \frac{\partial z_k}{\partial z_j}$$

$$= \sum_{l=1}^{r} a_{il} \left(\frac{\partial f_l}{\partial z_j} + \sum_{k=n-r+1}^{n} \frac{\partial f_l}{\partial z_k} \frac{\partial z_k}{\partial z_j} \right) = \sum_{l=1}^{r} a_{il} \frac{\partial F_l}{\partial z_j} = 0.$$

■

1.7 Variedades analíticas

Para terminar recogemos los resultados fundamentales que vamos a necesitar sobre variedades diferenciales complejas. Muchos de ellos los obtendremos como consecuencia de hechos análogos sobre variedades reales, que supondremos conocidos.

Definición 1.59 Una *carta compleja* en un espacio topológico V es un par (U, z), donde U es un abierto en V y z es un homeomorfismo entre U y un abierto de $\mathbb{C}^n$.

Un *atlas analítico* en V es un conjunto de cartas cuyos dominios cubran V y que sean compatibles dos a dos, en el sentido de que si (U, z) y (U', z') son cartas del atlas y $U \cap U' \neq \varnothing$, entonces la aplicación $z^{-1} \circ z'$ es una transformación conforme entre $z[U \cap U']$ y $z'[U \cap U']$.

Notemos que todas las cartas de un atlas analítico han de tener imagen en abiertos de $\mathbb{C}^n$ para un mismo n (pues si $m \neq n$ los abiertos de $\mathbb{C}^m$ no son conformemente equivalentes a los de $\mathbb{C}^n$).

Es fácil ver que si a un atlas analítico le añadimos todas las cartas compatibles con sus elementos, obtenemos de nuevo un atlas (es decir, las cartas añadidas no sólo son compatibles con las del atlas dado, sino también entre sí). Además, el atlas así obtenido es maximal respecto a la inclusión, en el sentido de que no está contenido en otro atlas mayor.

Una *estructura analítica* en un espacio topológico V es un atlas analítico en V maximal respecto de la inclusión. Una *variedad analítica* es un par $(V, \mathcal{A})$, donde V es un espacio topológico (de Hausdorff) y $\mathcal{A}$ es una estructura analítica en V.

Acabamos de ver que un atlas analítico en un espacio topológico V determina una única estructura analítica en V, pero dos atlas diferentes pueden determinar la misma estructura analítica.

Si las cartas de una variedad analítica V toman imágenes en abiertos de $\mathbb{C}^n$, diremos que V tiene *dimensión (compleja) n*.

Una aplicación $f : V \longrightarrow W$ entre variedades analíticas es *holomorfa* si para cada $p \in V$ y cada par de cartas z alrededor de p y z' alrededor de $f(p)$, se cumple que la función $z^{-1} \circ f \circ z'$ es holomorfa en su dominio. Diremos que f es una *transformación conforme* si es biyectiva y tanto f como f^{-1} son holomorfas (y en tal caso diremos que las variedades son *conformemente equivalentes.*)

Es fácil ver que para que una función sea holomorfa basta con que cumpla la definición para un par de cartas z y z' alrededor de cada punto p y de su imagen (es decir, si lo cumple para dos dadas, lo cumple para dos cualesquiera).

Por otra parte, todo abierto de una variedad analítica V hereda de forma natural una estructura analítica (formada por las restricciones de las cartas que cortan al abierto), por lo que podemos hablar de funciones holomorfas en un abierto de una variedad, y entonces una función es holomorfa si y sólo si lo es en un entorno de cada punto.

Funciones holomorfas y meromorfas Si V es una variedad analítica, llamaremos $\mathcal{H}(V)$ al conjunto de las funciones holomorfas $V \longrightarrow \mathbb{C}$. Es fácil ver que tiene estructura de anillo con la suma y el producto definidos puntualmente. Las funciones constantes forman un subcuerpo isomorfo a $\mathbb{C}$, por lo que $\mathcal{H}(V)$ es, de hecho, una $\mathbb{C}$-álgebra.

Teorema 1.60 *Si V es una variedad analítica conexa y $\alpha \in \mathcal{H}(V)$ se anula en un abierto no vacío, entonces $\alpha = 0$. Como consecuencia, $\mathcal{H}(V)$ es un dominio íntegro. Si además V es compacta, entonces $\mathcal{H}(V) = \mathbb{C}$.*

DEMOSTRACIÓN: Sea U la unión de todos los abiertos de V donde α se anula. Queremos ver que $U = V$. En caso contrario, como V es conexa, tiene que haber un punto p en la frontera de U. Podemos tomar un entorno de U conformemente equivalente a una bola abierta en $\mathbb{C}^n$ de modo que p se corresponda con su centro. Puesto que p tiene puntos de U arbitrariamente próximos, podemos tomar un punto $q \in U$ y una carta $z : W \longrightarrow E$, donde E es la esfera

$$E = \{z \in \mathbb{C}^n \mid |z_1|^2 + \cdots + |z_n|^2 < 1\}.$$

de modo que p, $q \in W$ y $z(q) = 0$. Así, α se corresponde con una función holomorfa $\alpha' \in \mathcal{H}(E)$ que se anula en un entorno de 0 pero que no se anula en ningún entorno de un cierto punto $p' = z(p)$. Vamos a probar que $\alpha' = 0$, con lo que tendremos una contradicción. Equivalentemente, basta probar el teorema en el caso en que $V = E$ y α se anula en un entorno de 0.

Si $D \subset \mathbb{C}$ es el disco unidad y $q \in E$ es un punto arbitrario, la aplicación $D \longrightarrow E$ dada por $\lambda \mapsto \lambda q/\|q\|$ es holomorfa, y al componerla con α obtenemos una aplicación holomorfa en D que se anula en un entorno de 0, luego es nula por el principio de prolongación analítica, luego $\alpha(q) = 0$.

La segunda afirmación del teorema se cumple porque si $\alpha, \beta \in \mathcal{H}(V)$ cumplen $\alpha\beta = 0$ y $\alpha \neq 0$, entonces el conjunto U de puntos donde α no se anula es un abierto no vacío y $\beta|_U = 0$, luego $\beta = 0$.

Si además V es compacta, dada $\alpha \in \mathcal{H}(V)$ existe un punto $p \in V$ tal que $|\alpha|$ toma su valor máximo. Basta probar que α es constante en un entorno de p, lo cual reduce el problema de nuevo al caso en que $V = E$ y $p = 0$. Consideramos igualmente un punto $q \in E$ y la misma aplicación $D \longrightarrow E$, que convierte ahora α en una función holomorfa en D cuyo módulo es máximo en 0. Por el principio del módulo máximo, ha de ser constante, luego $\alpha(0) = \alpha(q)$. ■

Acabamos de ver que en una variedad analítica compacta y conexa no hay funciones holomorfas no triviales, por lo que necesitamos el concepto más general de función meromorfa, que viene a ser una "función holomorfa con singularidades". Más precisamente, en el caso de variedades de dimensión 1, las funciones meromorfas son las funciones holomorfas cuyas singularidades son aisladas y a lo sumo son polos, pero no singularidades esenciales. No vamos a entrar aquí en una clasificación de las singularidades en dimensión superior, sino que generalizaremos la noción de función meromorfa a partir del hecho de que las funciones meromorfas de una variable son localmente cocientes de funciones holomorfas.

Así, si U es un abierto conexo en una variedad analítica, podemos considerar el cuerpo de cocientes $\mathcal{K}(U)$ del anillo $\mathcal{H}(U)$. A sus elementos los llamaremos *fracciones holomorfas* en U. Diremos que una fracción $\alpha \in \mathcal{K}(U)$ es *holomorfa* en un punto $p \in U$ si $\alpha = \beta/\gamma$, donde β, $\gamma \in \mathcal{H}(U)$ y $\gamma(p) \neq 0$. En tal caso definimos $\bar{\alpha}(p) = \beta(p)/\gamma(p)$. Es claro que este valor no depende de la representación de α como fracción.

También es obvio que el conjunto de puntos donde α es holomorfa es un abierto $U_0 \subset U$ (denso, por el teorema anterior), así como que $\bar{\alpha}$ es realmente una función holomorfa en U_0. Más aún, si α, $\alpha' \in \mathcal{K}(U)$ cumplen que $\bar{\alpha}$ y $\bar{\alpha}'$ coinciden en un abierto de U, entonces $\alpha = \alpha'$. En efecto, sea p un punto donde ambas funciones coinciden, y sean $\alpha = \beta/\gamma$, $\alpha' = \beta'/\gamma'$, de modo que $\gamma(p) \neq 0 \neq \gamma'(p)$. Entonces las funciones β/γ y β'/γ' están definidas en un entorno de p y son iguales, luego $\beta\gamma' - \gamma\beta' \in \mathcal{H}(U)$ se anula en un entorno de p, luego $\beta\gamma' - \gamma\beta' = 0$ en $\mathcal{H}(U)$, luego $\alpha = \alpha'$.

En particular, cada $\alpha \in \mathcal{K}(U)$ está completamente determinada por $\bar{\alpha}$, por lo que en lo sucesivo identificaremos la fracción α con la función holomorfa que define y omitiremos la barra.

Observemos también que si $U \subset U'$ son abiertos conexos en una variedad analítica, podemos definir un monomorfismo de cuerpos $\mathcal{K}(U') \longrightarrow \mathcal{K}(U)$ mediante $\alpha = \beta/\gamma \mapsto \alpha|_U = \beta|_U/\gamma|_U$. Es evidente que no depende de la representación de α como fracción, así como que el dominio de $\alpha|_U$ es la intersección con U del dominio de α y que, considerada como función holomorfa sobre este dominio, es la restricción de α considerada como función holomorfa.

Con esto estamos en condiciones de definir las funciones meromorfas sobre una variedad analítica:

Definición 1.61 Si V es una variedad analítica, una *función meromorfa* en V es una función $f : U \longrightarrow \mathbb{C}$ definida sobre un abierto denso de V tal que todo punto de V tiene un entorno abierto conexo W tal que $f|_{U\cap W} \in \mathcal{K}(W)$. Llamaremos $\mathcal{M}(V)$ al conjunto de todas las funciones meromorfas en V.

Es claro que las funciones meromorfas son holomorfas en su dominio. El conjunto $\mathcal{M}(V)$ tiene estructura de anillo con las operaciones definidas como sigue: dadas dos funciones meromorfas $f : U \longrightarrow \mathbb{C}$ y $f' : U' \longrightarrow \mathbb{C}$, cubrimos V con abiertos conexos W_i tales que $f|_{U\cap W_i}$, $f'|_{U'\cap W_i} \in \mathcal{K}(W_i)$ y consideramos las funciones $f|_{U\cap W_i} + f'|_{U'\cap W_i} \in \mathcal{K}(W_i)$. Llamamos U'' a la unión de sus dominios y definimos $f + f' : U'' \longrightarrow \mathbb{C}$ como la función que extiende a todas las sumas. El producto se define análogamente.

Si V es una variedad analítica conexa, entonces $\mathcal{M}(V)$ es un cuerpo, pues si $f \in \mathcal{M}(V)$ no es nula, podemos cubrir V con abiertos conexos W_i tales que $f|_{W_i} \in \mathcal{K}(W_i)$, y ha de ser $f|_{W_i} \neq 0$, pues en caso contrario f sería una función holomorfa que se anularía en un abierto, luego sería nula. Por consiguiente, podemos considerar las fracciones holomorfas $f|_{W_i}^{-1} \in \mathcal{K}(W_i)$, que claramente definen una función meromorfa f^{-1} con la propiedad de que $ff^{-1} = 1$.

Vamos a probar un teorema sobre la estructura del cuerpo $\mathcal{M}(V)$, para lo cual necesitamos un resultado previo:

Teorema 1.62 *Sea f una función holomorfa en (un entorno de) el polidisco cerrado $|z_i| \leq 1$, $i = 1, \ldots, n$ y sea M el máximo de f en dicho polidisco. Supon-*

gamos que f y todas sus derivadas de orden menor que h se anulan en 0*. Entonces, para todo z en el polidisco abierto, se cumple que* $|f(z)| \leq M \max_i |z_i|^h$.

Demostración: Para cada $z \in \mathbb{C}^n$ llamaremos $|z| = \max_i |z_i|$. Fijemos un z tal que $0 < |z| < 1$ y para cada $t \in \mathbb{C}$ definamos $g(t) = f(tz)$, que es una función holomorfa en un entorno del disco $|t| \leq |z|^{-1}$.

La hipótesis sobre las derivadas de f implica que su serie de Taylor no tiene términos de grado menor que h, luego a la serie de Taylor de g le sucede lo mismo, es decir, la función $g(t)/t^h$ es holomorfa en un entorno del disco cerrado. Por el principio del módulo máximo, $|g(t)/t^h|$ es menor o igual que el valor que toma esta función en la frontera del disco, que a su vez es menor o igual que $M/|z|^{-h}$, es decir, tenemos que $|g(t)/t^h| \leq M|z|^h$. Haciendo $t = 1$ queda $f(z) \leq M|z|^h$, como había que probar. ■

Otro hecho elemental que necesitaremos a continuación es el siguiente: el número de monomios de grado $\leq m$ en n indeterminadas es

$$M_n^m = \binom{m+n}{n}.$$

En efecto, podemos dividir tales monomios en dos grupos: los que contienen alguna indeterminada X_n, que son M_n^{m-1}, y los que no contienen ninguna, que son M_{n-1}^m, luego $M_n^m = M_n^{m-1} + M_{n-1}^m$. Basta razonar por inducción sobre $m + n$.

Teorema 1.63 *Si V es una variedad analítica compacta, entonces el grado de trascendencia de $\mathcal{M}(V)$ sobre $\mathbb{C}$ es menor o igual que* $\dim X$.

Demostración: Sea $n = \dim V$ y tomemos funciones $f_1, \ldots, f_{n+1} \in \mathcal{M}(V)$. Hemos de probar que existe un polinomio no nulo $F \in \mathbb{C}[T_1, \ldots, T_{n+1}]$ tal que $F(f_1, \ldots, f_{n+1}) = 0$.

Para cada punto $x \in V$ vamos a elegir tres entornos $x \in W_x \subset V_x \subset U_x$. En primer lugar elegimos U_x tal que $f_i = P_{i,x}/Q_{i,x}$, donde $P_{i,x}$, $Q_{i,x} \in \mathcal{H}(U_x)$ son funciones primas entre sí en todos los puntos de U_x. La existencia de U_x nos la da el teorema 1.53. Tomamos V_x tal que su clausura esté contenida en U_x y que sea el dominio de una carta con imagen en el polidisco $|z_i| < 1$. El tercer entorno W_x es la antiimagen del polidisco $|z_i| < 1/2$.

Consideremos dos puntos x, $y \in V$ tales que $U_x \cap U_y \neq \varnothing$. En dicha intersección tenemos que

$$\frac{P_{i,x}}{Q_{i,x}} = \frac{P_{i,y}}{Q_{i,y}},$$

y ambas fracciones son primas entre sí en cada punto de $U_x \cap U_y$, por lo que $Q_{i,x}/Q_{i,y}$ ha de ser una unidad en cada punto, es decir, $Q_{i,x} = Q_{i,y}\phi_{i,x,y}$, para una cierta función holomorfa $\phi_{i,x,y} \in \mathcal{H}(U_x \cap U_y)$ que no se anula en ningún punto.

Podemos tomar un número finito de puntos $\xi_1, \ldots, \xi_r \in V$ tales que los abiertos W_{ξ_j} cubran V. Definimos

$$\phi_{j,k} = \prod_{i=1}^{n+1} \phi_{i,\xi_j,\xi_k}, \qquad C = \max_{j,k} \max_{V_{\xi_j} \cap V_{\xi_k}} |\phi_{j,k}|.$$

Notemos que $C \geq 1$, pues $\phi_{j,k}\phi_{k,j} = 1$.

Consideremos un polinomio arbitrario $F(T_1, \ldots, T_{n+1})$ de grado m y pongamos que

$$F(f_1, \ldots, f_{n+1}) = \frac{R_x}{Q_x^m} \qquad \text{en } V_x, \tag{1.7}$$

donde

$$Q_x = \prod_{i=1}^{n+1} Q_{i,x}.$$

Observemos que $R_{\xi_j} = \phi_{j,k}^m R_{\xi_k}$ en $V_{\xi_j} \cap V_{\xi_k}$. Vamos a probar que, para cada $h > 0$, podemos encontrar un polinomio no nulo F para el cual las funciones R_{ξ_j} tengan nulas todas las derivadas de orden menor que h en ξ_j.

Observemos que la aplicación que a cada polinomio F le asigna la función R_{ξ_j} es lineal, como también lo es la que a F le asigna una derivada parcial fija de R_{ξ_j} en ξ_j. Consideremos, pues, la aplicación lineal que a cada polinomio F de grado $\leq m$ le asigna el vector formado por todas las derivadas parciales de orden $< h$ de todas las funciones R_{ξ_j} en ξ_j (incluyendo la derivada de orden 0, igual a $R_{\xi_j}(\xi_j)$). Si escogemos m y h de modo que

$$\binom{n+m+1}{n+1} > r\binom{n+h-1}{n}, \tag{1.8}$$

la aplicación tendrá un núcleo no trivial, pues el miembro izquierdo es la dimensión del espacio de polinomios y el miembro derecho es el número de derivadas parciales. (Notemos que el número de derivadas parciales de orden $\leq m$ de una función de n variables es el mismo que el de monomios de grado $\leq m$ en n indeterminadas). Basta tomar un polinomio F en dicho núcleo.

Así podemos aplicar el teorema anterior a las funciones R_{ξ_j}. Para ello llamamos

$$M = \max_j \max_{x \in V_{\xi_j}} |R_{\xi_j}(x)|,$$

con lo que, para todo $x \in W_{\xi_j}$, se cumple que

$$|R_{\xi_j}(x)| \leq \frac{M}{2^h}.$$

El máximo M se alcanzará en un punto $x_0 \in V_{\xi_j}$. Entonces $x_0 \in W_{\xi_k}$, para cierto k, luego

$$M = |R_{\xi_j}(x_0)| = |R_{\xi_k}(x_0)||\phi_{k,j}(x_0)|^m \leq \frac{M}{2^h} C^m.$$

Vamos a ver que podemos elegir h y m de modo que $C^m/2^h < 1$, lo que obliga a que $M = 0$, lo que a su vez implica que cada R_{ξ_j} es nula en V_{ξ_j} y, como estos abiertos cubren V, concluimos que $F(f_1, \ldots, f_{n+1})$ por (1.7).

Pongamos $C = 2^\lambda$, donde $\lambda \geq 0$, porque $C \geq 1$. Lo que queremos es que $\lambda m \leq h$. Ahora bien, el miembro izquierdo de (1.8) es un polinomio de grado $n+1$ en m, digamos $P(m)$, mientras que el miembro derecho es un polinomio de grado n en h, digamos $Q(h)$. Fijemos un natural $l > \lambda$ y hagamos $h = lm$. El polinomio $Q(lm)$ tiene también grado n en m, luego sólo hemos de tomar un m suficientemente grande para que $P(m) > Q(lm)$, lo cual siempre es posible. ■

Complexificaciones Es claro que toda variedad analítica de dimensión n es también una variedad diferencial (real de clase C^∞) de dimensión $2n$. El teorema 1.49 implica que las variedades analíticas son siempre variedades diferenciales orientables.

Para definir espacios tangentes y diferenciales complejas conviene recordar la estructura de producto tensorial: si W es un espacio topológico real, llamaremos *complexificación* de V al producto tensorial $\mathbb{C} \otimes_{\mathbb{R}} W$, que es un espacio vectorial complejo de la misma dimensión, cuyos elementos se expresan de forma única como $1 \otimes v + i \otimes w$, con v, $w \in W$. Simplificando la notación, escribiremos

$$\mathbb{C} \otimes_R W = \{v + iw \mid v,\ w \in W\}.$$

Si $v_1, \ldots, v_n$ es una base de W, entonces también es una base de $\mathbb{C} \otimes_{\mathbb{R}} W$ como $\mathbb{C}$-espacio vectorial, mientras que $v_1, \ldots, v_n, iv_1, \ldots, iv_n$ es una base de éste como $\mathbb{R}$-espacio vectorial.

Por ejemplo, si V es una variedad analítica y $C^\infty(V, \mathbb{R})$ es el espacio de todas las funciones (infinitamente) diferenciables de V en $\mathbb{R}$, entonces la complexificación $C^\infty(V, \mathbb{C}) = \mathbb{C} \otimes_{\mathbb{R}} C^\infty(V)$ es claramente el espacio de todas las funciones diferenciables de V en $\mathbb{C}$.

Si $p \in V$, representaremos por $C_p^\infty(V, \mathbb{C})$ al conjunto de todas las funciones complejas diferenciables definidas en un entorno de V. No podemos considerarlo la complexificación de su análogo real $C_p^\infty(V, \mathbb{R})$ porque no tenemos una estructura de espacio vectorial, pero en cualquier caso sus elementos son de la forma $f_1 + if_2$, con $f_1, f_2 \in C_p^\infty(V, \mathbb{R})$.

Llamaremos $T_p(V, \mathbb{R})$ al espacio tangente a V en p como variedad real, mientras que $T_p(V, \mathbb{C})$ será su complexificación. De este modo, si V tiene dimensión compleja n, su dimensión real es $2n$, luego $T_p(V, \mathbb{R})$ tiene también dimensión $2n$ y $T_p(V, \mathbb{C})$ tiene dimensión compleja $2n$. Si (U, z) es una carta analítica de V alrededor de p y llamamos $z_k = x_k + iy_k$ a las funciones coordenadas, entonces una base de $T_p(V, \mathbb{C})$ está formada por las derivaciones

$$\left.\frac{\partial}{\partial x_k}\right|_p, \quad \left.\frac{\partial}{\partial y_k}\right|_p, \qquad k = 1, \ldots, n. \tag{1.9}$$

Para cada $v = v_1 + iv_2 \in T_p(V, \mathbb{C})$ y cada $f = f_1 + if_2 \in C_p^\infty(V, \mathbb{C})$, podemos definir
$$v(f) = v_1(f_1) - v_2(f_2) + i(v_1(f_2) + v_2(f_1)) \in \mathbb{C},$$
de modo que podemos ver a los elementos de v como derivaciones de $C_p^\infty(V)$, es decir, se cumple $v(\alpha f_1 + \beta g) = \alpha v(f) + \beta v(g)$ y
$$v(fg) = v(f)g(p) + v(g)f(p).$$

Ahora conviene observar un hecho general sobre complexificaciones y espacios duales: si W es un espacio vectorial real, entonces $(\mathbb{C} \otimes_{\mathbb{R}} W)^* \cong \mathbb{C} \otimes_{\mathbb{R}} W^*$.

En efecto, cada $\phi = \phi_1 + i\phi_2 \in \mathbb{C} \otimes_{\mathbb{R}} W^*$ se identifica con la aplicación de $(\mathbb{C} \otimes_{\mathbb{R}} W)^*$ dada por
$$\phi(v_1 + iv_2) = \phi_1(v_1) - \phi_2(v_2) + i(\phi_1(v_2) + \phi_2(v_1)). \tag{1.10}$$

Así, volviendo a la variedad analítica V, tenemos que $T_p(V, \mathbb{C})^*$ puede verse como la complexificación de $T_p(V, \mathbb{R})$, luego tiene por base a
$$dx_1|_p, \ldots, dx_n|_p, dy_1|_p, \ldots, dy_n|_p. \tag{1.11}$$

En general, para cada función $f = f_1 + if_2 \in C_p^\infty(V, \mathbb{C})$, definimos la diferencial
$$df_p = df_1|_p + idf_2|_p \in T_p(V, \mathbb{C})^*.$$

Vista como elemento de $T_p(V, \mathbb{C})^*$ según la identificación (1.10), su acción es
$$df_p(v) = (df_1|_p + idf_2|_p)(v_1 + iv_2) = df_1|_p(v_1) - df_2|_p(v_2) + i(df_1|_p(v_2) + df_2|_p(v_1))$$
$$= v_1(f_1) - v_2(f_2) + i(v_2(f_1) + v_1(f_2)) = v(f).$$

Es claro que (1.11) es la base dual de (1.9), de donde se sigue que , para cada $v \in T_p(V, \mathbb{C})$, su expresión en coordenadas es
$$v = \sum_{k=1}^n \left(v(x_k) \left.\frac{\partial}{\partial x_k}\right|_p + v(y_k) \left.\frac{\partial}{\partial y_k}\right|_p \right).$$

Una base alternativa que nos será más útil para estudiar las aplicaciones holomorfas es
$$dz_k|_p = dx_k|_p + idy_k|_p, \quad d\bar{z}_k|_p = dx_k|_p - idy_k|_p. \tag{1.12}$$

La base dual de (1.12) resulta ser la formada por las derivaciones
$$\left.\frac{\partial}{\partial z_k}\right|_p = \frac{1}{2}\left(\left.\frac{\partial}{\partial x_k}\right|_p - i \left.\frac{\partial}{\partial y_k}\right|_p \right), \quad \left.\frac{\partial}{\partial \bar{z}_k}\right|_p = \frac{1}{2}\left(\left.\frac{\partial}{\partial x_k}\right|_p + i \left.\frac{\partial}{\partial y_k}\right|_p \right).$$

De este modo, para cada $v \in T_p(V,\mathbb{C})$ se cumple

$$v = \sum_{k=1}^{n} \left(v(z_k) \left.\frac{\partial}{\partial z_k}\right|_p + v(\bar{z}_k) \left.\frac{\partial}{\partial \bar{z}_k}\right|_p \right). \tag{1.13}$$

Así mismo, si $f \in C_p^\infty(V,\mathbb{C})$ se cumple

$$df_p = \sum_{k=1}^{n} \left(\left.\frac{\partial f}{\partial z_k}\right|_p dz_k|_p + \left.\frac{\partial f}{\partial \bar{z}_k}\right|_p d\bar{z}_k|_p \right). \tag{1.14}$$

El espacio tangente holomorfo Llamaremos $\mathcal{H}_p(V)$ al conjunto de las funciones holomorfas en un entorno de p (donde dos de ellas se identifican si coinciden en un entorno de p).

Teorema 1.64 *Una función $f \in C_p^\infty(V,\mathbb{R})$ definida sobre una variedad analítica de dimensión n es holomorfa (en un entorno de p) si y sólo existe una carta z alrededor de p tal que*

$$\frac{\partial f}{\partial \bar{z}_k} = 0, \quad k = 1,\ldots,n.$$

Además en tal caso esta relación se cumple para cualquier carta alrededor de p.

DEMOSTRACIÓN: La condición equivale a que

$$\frac{\partial f}{\partial x_k} + i\frac{\partial f}{\partial y_k} = \frac{\partial \operatorname{Re} f}{\partial x_k} - \frac{\partial \operatorname{Im} f}{\partial y_k} + i\frac{\partial \operatorname{Im} f}{\partial x_k} + i\frac{\partial \operatorname{Re} f}{\partial y_k} = 0,$$

es decir,

$$\frac{\partial \operatorname{Re} f}{\partial x_k} = \frac{\partial \operatorname{Im} f}{\partial y_k}, \quad \frac{\partial \operatorname{Im} f}{\partial x_k} = -\frac{\partial \operatorname{Re} f}{\partial y_k},$$

o también:

$$\frac{\partial \operatorname{Re}(z^{-1} \circ f)}{\partial x_k} = \frac{\partial \operatorname{Im}(z^{-1} \circ f)}{\partial y_k}, \quad \frac{\partial \operatorname{Im}(z^{-1} \circ f)}{\partial x_k} = -\frac{\partial \operatorname{Re}(z^{-1} \circ f)}{\partial y_k}.$$

Así pues, la condición del enunciado se cumple si y sólo si la función $z^{-1} \circ f$ satisface las ecuaciones de Cauchy-Riemann, es decir, si y sólo si es holomorfa, pero, por definición, f es holomorfa (en el dominio de z) si y sólo si lo es $z^{-1} \circ f$.

■

Un desarrollo análogo al de la prueba anterior muestra que si $f \in \mathcal{H}_p(V)$, entonces

$$\left.\frac{\partial f}{\partial z_k}\right|_p = \left.\frac{\partial z^{-1} \circ f}{\partial z_k}\right|_{z(p)}.$$

Además la igualdad (1.14) se reduce ahora a

$$df_p = \sum_{k=1}^{n} \left.\frac{\partial f}{\partial z_k}\right|_p dz_k|_p \tag{1.15}$$

Diremos que una función $f : V \longrightarrow \mathbb{C}$ es *antiholomorfa* si su conjugada $\overline{f}$ (la composición con la conjugación compleja) es holomorfa. Es inmediato comprobar las relaciones

$$\left.\frac{\partial \overline{f}}{\partial z_k}\right|_p = \left.\frac{\partial f}{\partial \overline{z}_k}\right|_p, \qquad \left.\frac{\partial \overline{f}}{\partial \overline{z}_k}\right|_p = \left.\frac{\partial f}{\partial z_k}\right|_p,$$

de donde se sigue que una función f es antiholomorfa si y sólo si sus derivadas respecto a las coordenadas z_k son nulas. Esto nos permite definir:

$$T_p^h V = \langle \partial_{z_1}|_p, \ldots, \partial_{z_n}|_p \rangle, \quad T_p^a V = \langle \partial_{\bar{z}_1}|_p, \ldots, \partial_{\bar{z}_n}|_p \rangle, \tag{1.16}$$

sin que la definición dependa del sistema de coordenadas, pues el *espacio tangente holomorfo* $T_p^h V$ está formado por las derivaciones que se anulan sobre las funciones antiholomorfas y el *espacio tangente antiholomorfo* $T_p^a V$ está formado por las derivaciones que se anulan sobre las funciones holomorfas. Obviamente tenemos la relación

$$T_p(V, \mathbb{C}) = T_p^h V \oplus T_p^a V.$$

El espacio $T_p^h V$ tiene dimensión n sobre $\mathbb{C}$ y dimensión $2n$ sobre $\mathbb{R}$. Éste es el espacio tangente natural cuando nos restringimos a tratar con funciones holomorfas, por lo que lo representaremos simplemente por $T_p V$.

Notemos que para derivaciones holomorfas $v \in T_p V$, la relación (1.13) se reduce a

$$v = \sum_{k=1}^n v(z_k) \left.\frac{\partial}{\partial z_k}\right|_p.$$

Teniendo en cuenta (1.15) y (1.16), es claro que si $f \in \mathcal{H}_p(V)$, entonces $d_p f$ se anula sobre las derivaciones antiholomorfas, luego podemos considerar que $df_p \in T_p^* V$. Fijada una carta z alrededor de p, las diferenciales $dz_k|_p$ constituyen una base de $T_p^* V$.

Diferenciales entre variedades Sea $\phi : V \longrightarrow W$ una aplicación holomorfa entre variedades analíticas. La diferencial $d\phi_p : T_p(V, \mathbb{R}) \longrightarrow T_p(W, \mathbb{R})$ se extiende a una aplicación $\mathbb{C}$-lineal $d\phi_p : T_p(V, \mathbb{C}) \longrightarrow T_p(W, \mathbb{C})$ mediante

$$d\phi_p(v_1 + iv_2) = d\phi_p(v_1) + i d\phi_p(v_2).$$

Se comprueba inmediatamente que si $v \in T_p(V, \mathbb{C})$ entonces

$$d\phi_p(v)(f) = v(\phi \circ f),$$

de donde a su vez se sigue que $d\phi_p$ transforma derivaciones holomorfas en derivaciones holomorfas, luego se restringe a una aplicación lineal

$$d\phi_p : T_p V \longrightarrow T_p W.$$

Es fácil ver que se cumple la regla de la cadena: $d(\phi \circ \psi)_p = d\phi_p \circ d\psi_{\phi(p)}$.

Fijadas cartas z alrededor de p y w alrededor de $\phi(p)$, la matriz de $d\phi_p$ en las bases $\partial_{z_i}|_p$ y $\partial_{w_j}|_p$ tiene por coeficientes

$$d\phi_p(\partial z_i|_p)(w_j) = \left.\frac{\partial z^{-1} \circ \phi \circ w_j}{\partial z_i}\right|_{z(p)}.$$

Así pues, la matriz jacobiana de $d\phi_p$ respecto a unas cartas dadas z y w es la misma que la de su lectura $z^{-1} \circ \phi \circ w$ respecto a dichas cartas.

Observemos que si $\phi : V \longrightarrow W$ es una aplicación holomorfa de un abierto de $\mathbb{C}^n$ a un abierto de $\mathbb{C}^m$ y $p \in V$, tenemos definidas dos diferenciales $d\phi_p$, una es la aplicación $d\phi_p : T_pV \longrightarrow T_pW$ que acabamos de introducir y la otra es la diferencial usual en análisis real vista como aplicación $\mathbb{C}$-lineal

$$d\phi_p : \mathbb{C}^n \longrightarrow \mathbb{C}^m.$$

Las observaciones del párrafo precedente muestran que ambas se corresponden a través del isomorfismo $T_pV \cong \mathbb{C}^n$ que hace corresponder la base $\partial_{z_i}|_p$ (correspondiente a la carta identidad en V) con la base canónica de $\mathbb{C}^n$, y del isomorfismo correspondiente para W.

El teorema de la función inversa Demostramos ahora la versión compleja del teorema de la función inversa junto con algunas aplicaciones, que son una traducción trivial de propiedades análogas reales.

Teorema 1.65 (Teorema de la función inversa) *Sea $\phi : V \longrightarrow W$ una función holomorfa entre variedades y sea $p \in V$ un punto tal que la diferencial $d\phi_p : T_p(V) \longrightarrow T_{\phi(p)}(W)$ es un isomorfismo. Entonces existe un entorno U de p en V tal que $\phi[U]$ es abierto en W y $\phi|_U : U \longrightarrow \phi[U]$ es una transformación conforme.*

Demostración: Notemos que ambas variedades han de tener la misma dimensión n. Sea (U', z) una carta alrededor de p y (U'', w) una carta alrededor de $\phi(p)$ de modo que $f[U'] \subset U''$. Entonces $z^{-1} \circ f \circ w$ es una aplicación diferenciable entre dos abiertos de $\mathbb{C}^n$ cuya diferencial en $z(p)$ es un isomorfismo.

Por el teorema 1.57 existe un entorno G de $z(p)$ tal que $(z^{-1} \circ \phi \circ w)[G]$ es abierto en $\mathbb{C}^n$ y la restricción de $z^{-1} \circ \phi \circ w$ es conforme. Basta tomar $U = z^{-1}[G]$. ■

En la mayor parte de los casos no vamos a trabajar con variedades analíticas abstractas, sino con subvariedades de $\mathbb{C}^n$ o del espacio proyectivo $\mathrm{P}^n(\mathbb{C})$. La definición de subvariedad, que damos a continuación, incluye la condición natural para garantizar que el espacio tangente de la subvariedad en un punto puede considerarse como subespacio del espacio tangente de la variedad en el mismo punto. Geométricamente esto expresa que la subvariedad no tiene "picos".

Definición 1.66 Diremos que una variedad analítica W es una *subvariedad* de una variedad analítica V si $W \subset V$, la topología de W es la inducida desde V, la inclusión $i : W \longrightarrow V$ es holomorfa y, para cada $p \in W$, la diferencial $di_p : T_pW \longrightarrow T_pV$ es inyectiva.

En estas condiciones podemos identificar a T_pW con un subespacio de T_pV. Es claro que un abierto U en una variedad analítica V es una subvariedad (con la estructura diferencial que resulta de restringir las cartas) pues la inclusión es holomorfa (su lectura en una carta de V y su restricción a U es la identidad) y la diferencial de la inclusión es inyectiva (su matriz jacobiana en las cartas indicadas es la identidad). De hecho, podemos identificar $T_pU = T_pV$.

Ahora vamos a relacionar la geometría de una variedad y la de sus subvariedades, para lo cual necesitamos algunos resultados algebraicos sobre diferenciales:

Definición 1.67 Sea V una variedad analítica. Diremos que un conjunto de funciones $z_1, \ldots, z_m \in \mathcal{H}_p(V)$ es *independiente* en p si $dz_1|_p, \ldots, dz_m|_p$ son linealmente independientes en $T_p^*(V)$.

Obviamente, las funciones coordenadas de una carta son siempre funciones independientes. Recíprocamente tenemos el teorema siguiente:

Teorema 1.68 *Sea V una variedad analítica de dimensión n y $w_1, \ldots, w_n$ un conjunto de n funciones independientes en un punto $p \in V$. Entonces $w_1, \ldots, w_n$ forman un sistema de coordenadas alrededor de p.*

DEMOSTRACIÓN: Sea U un entorno de p en el que estén definidas todas las funciones w_i. Definimos $w : U \longrightarrow \mathbb{C}^n$ mediante $w(q) = (w_1(q), \ldots, w_n(q))$. Claramente w es holomorfa.

Llamemos $z_1, \ldots, z_n$ a las proyecciones en $\mathbb{C}^n$, es decir, a las funciones coordenadas correspondientes a la carta identidad. Consideremos la codiferencial $dw_p^* : T_{w(p)}^*(\mathbb{C}^n) \longrightarrow T_p^*(V)$. Tenemos que

$$dw_p^*(dz_i|_{w(p)}) = dw|_p \circ dz_i|_{w(p)} = dw_i|_p.$$

Así pues, dw_p^* transforma la base $dz_i|_{w(p)}$ de $T_{w(p)}^*(\mathbb{C}^n)$ en la base $dw_i|_p$ de $T_p^*(V)$. Por consiguiente dw_p^* es un isomorfismo, luego también lo es dw_p. Por el teorema de la función inversa 1.65, la función w se restringe a una transformación conforme en un entorno de p, es decir, a una carta. ■

Un poco más en general tenemos:

Teorema 1.69 *Sea V una variedad analítica de dimensión n y $w_1, \ldots, w_m$ un conjunto de $m \leq n$ funciones independientes en un punto $p \in V$. Entonces $w_1, \ldots, w_m$ forman parte de un sistema de coordenadas alrededor de p.*

DEMOSTRACIÓN: Sea z una carta alrededor de p. Entonces $dw_1|_p, \ldots, dw_m|_p$ puede completarse hasta una base de $T_p^*(V)$ mediante algunas de las diferenciales $dz_i|_p$. Digamos que $dw_1|_p, \ldots, dw_m|_p, dz_{m+1}|_p, \ldots, dz_n|_p$ forman dicha base. Por el teorema anterior $w_1, \ldots, w_m, z_{m+1}, \ldots, z_n$ forman un sistema de coordenadas alrededor de p. ■

Con esto podemos probar un resultado notable sobre subvariedades:

Teorema 1.70 *Sea $\phi : V \longrightarrow W$ una aplicación entre variedades y supongamos que W es una subvariedad de X. Entonces ϕ es holomorfa si y sólo si lo es como aplicación $\phi : V \longrightarrow X$.*

DEMOSTRACIÓN: Una implicación es obvia. Supongamos que $\phi : V \longrightarrow X$ es diferenciable y tomemos un punto $p \in V$. Sea (U, z) una carta en X alrededor de $\phi(p)$. Consideremos la inclusión $i : W \longrightarrow X$. Como $di|_{\phi(p)}$ es inyectiva, tenemos que $di^*_{\phi(p)}$ es suprayectiva, luego las formas

$$di^*_{\phi(p)}(dz_i|_{\phi(p)}) = di|_{\phi(p)} \circ dz_i|_{\phi(p)} = d(z_i|_{U\cap W})|_{\phi(p)}$$

son un sistema generador de $T^*_{\phi(p)}(W)$. Eliminando algunos de ellos obtenemos una base. Si llamamos m a la dimensión de X y n a la de W, tenemos que n de las funciones $z_i|_{U\cap W}$ son independientes en $\phi(p)$, luego por 1.68 forman un sistema coordenado (de W) alrededor de $\phi(p)$. En otras palabras, si llamamos $\pi : \mathbb{C}^m \longrightarrow \mathbb{C}^n$ a una cierta proyección (es decir, una aplicación que elimina las componentes adecuadas), la composición $z \circ \pi$ se restringe a una carta en W alrededor de $\phi(p)$. La lectura de ϕ (como aplicación de V en W) respecto a una carta cualquiera w alrededor de p y la carta $z \circ \pi$ alrededor de $\phi(p)$ es $w^{-1} \circ \phi \circ z \circ \pi$. Las tres primeras funciones forman una función holomorfa, pues son una lectura de ϕ como aplicación en X, y al componer con π seguimos teniendo una función holomorfa. Así pues, ϕ es holomorfa en un entorno de p, y esto vale para todo $p \in V$. ■

De aquí se sigue a su vez otro hecho relevante:

Teorema 1.71 *Sea V una variedad analítica y $W \subset V$. Entonces W admite a lo sumo una estructura analítica que lo convierte en subvariedad de V.*

DEMOSTRACIÓN: Sean W y W' el mismo conjunto W con dos estructuras diferenciales que lo conviertan en subvariedad de V. Entonces la identidad en W es holomorfa como aplicación $W \longrightarrow V$, luego también lo es como aplicación $W \longrightarrow W'$, e igualmente al revés, luego la identidad es una transformación conforme, lo que significa que ambas estructuras analíticas son la misma. ■

Una prueba alternativa es la siguiente: si $W \subset V$ es una subvariedad, $p \in W$ y $z : U \longrightarrow U' \subset \mathbb{C}^n$ es una carta en W alrededor de p, entonces $z^{-1} : U' \longrightarrow V$ es un homeomorfismo en su imagen, es holomorfa como aplicación en U y, por consiguiente, también holomorfa como aplicación en V. Además, $dz^{-1}|_q$ ha de ser inyectiva, para todo punto $q \in U'$.

Recíprocamente, si U' es un abierto en $\mathbb{C}^n$ y $\phi : U' \longrightarrow W$ es un homeomorfismo en un abierto U de W, holomorfa como aplicación en V y $d\phi_q$ es inyectiva en todo punto, entonces también es holomorfa como aplicación en W y por el teorema de la función inversa es una transformación conforme, luego ϕ^{-1} es una carta de W.

En resumen, si W es una subvariedad de V, entonces las cartas de W son necesariamente las inversas de los homeomorfismos entre abiertos de $\mathbb{C}^n$ y abiertos de W que son holomorfos como aplicaciones en V y cuya diferencial tiene rango n en cada punto. Todo esto no depende de la estructura analítica de W, luego no hay más que una estructura analítica posible en W.

Definición 1.72 Un subconjunto W de una variedad analítica V es *analítico* alrededor de un punto $p \in W$ (o que p es un *punto analítico* de W respecto de V) si p tiene un entorno en W que admite estructura de subvariedad de V.

Teorema 1.73 *Un subconjunto W de una variedad analítica V es analítico alrededor de un punto p si y sólo si existe un homeomorfismo $z : U \longrightarrow U'$ entre un abierto $U \subset W$, $p \in U$, y un abierto $U' \subset \mathbb{C}^n$ tal que $z^{-1} : U' \longrightarrow V$ sea holomorfa y dz_q^{-1} sea inyectiva para todo $q \in U'$.*

DEMOSTRACIÓN: Una implicación ya está probada. Si existe z en estas condiciones, entonces U es una variedad analítica con z como única carta. Además es una subvariedad de V, pues la lectura de la inclusión $i : U \longrightarrow V$ respecto a z y una carta w en V alrededor de un punto $q \in U$ es $z^{-1} \circ w$, que es composición de dos funciones holomorfas, luego i es holomorfa. Además di_q es composición del isomorfismo $dz_q : T_qU \longrightarrow T_{z(q)}U'$ con el monomorfismo $dz_{z(q)}^{-1} : T_{z(q)}U' \longrightarrow T_qV$, luego es inyectiva. ■

Así hemos reducido el problema de si un subconjunto W de una variedad V admite o no estructura de subvariedad a un problema local. El teorema siguiente muestra que el carácter analítico local en cada punto equivale al carácter analítico global del conjunto:

Teorema 1.74 *Un subconjunto W de una variedad analítica V admite estructura de subvariedad de V si y sólo si es analítico alrededor de cada uno de sus puntos.*

DEMOSTRACIÓN: Una implicación es obvia. Si W es analítico alrededor de cada uno de sus puntos, entonces alrededor de cada punto $p \in W$ existe un abierto con una carta respecto a la única estructura analítica posible en el abierto. Basta ver que dos cartas cualesquiera son compatibles entre sí. Si $z_i : U_i \longrightarrow U_i'$ son dos cartas de dos abiertos en W con $U_1 \cap U_2 \neq \varnothing$, entonces las restricciones $z_i|_{U_1 \cap U_2}$ son dos cartas para las dos estructuras analíticas que hereda la intersección. Por la unicidad han de ser compatibles, pero esto implica que z_1 y z_2 son compatibles. ■

Veamos otra aplicación de 1.68:

Teorema 1.75 *Sea W una subvariedad de dimensión m una variedad analítica V de dimensión n y sea $z : U \longrightarrow \mathbb{C}^n$ una carta de V alrededor de un punto $p \in W$. Entonces, de entre las funciones coordenadas $z_1, \ldots, z_n$, es posible seleccionar m de ellas tales que las restricciones $z_i|_{U \cap W}$ forman una carta de W alrededor de p.*

DEMOSTRACIÓN: Sea $i : W \longrightarrow V$ la inclusión, de modo que la diferencial $di_p : T_pW \longrightarrow T_pV$ es inyectiva. La aplicación dual $di_p^* : T_p^*V \longrightarrow T_p^*W$ es suprayectiva y transforma cada $dz_i|_p$ en $d(z_i|_{U \cap W})_p$, luego m de estas diferenciales forman una base de T_p^*W, luego las correspondientes m funciones $z_i|_{U \cap W}$ son independientes, luego forman una carta de W. ■

En particular, si aplicamos el teorema anterior al caso $V = \mathbb{C}^n$ y a la carta z formada por la identidad en $\mathbb{C}^n$, vemos que, reordenando oportunamente las coordenadas, vemos que una carta de W alrededor de p la forman las funciones coordenadas $z_1, \ldots, z_d$. Si llamamos $\phi : U' \longrightarrow W$ a su inversa, vemos que $W \cap U$ es la gráfica de ϕ, es decir:

$$W \cap U = \{z \in U \mid (z_1, \ldots, z_d) \in U' \text{ y } (z_{d+1}, \ldots, z_n) = \phi(z_1, \ldots, z_d)\}.$$

Así pues, toda subvariedad analítica de $\mathbb{C}^n$ es localmente la gráfica de una función holomorfa.

1.8 Toros complejos

Aunque, tal y como hemos comentado en la sección anterior, la mayoría de las variedades analíticas que vamos a estudiar serán subvariedades de espacios afines y proyectivos, aquí vamos a introducir uno de los ejemplos más sencillos de variedades abstractas:

Definición 1.76 Sea V un espacio vectorial complejo de dimensión g. Es claro que todos los isomorfismos $V \longrightarrow \mathbb{C}^g$ determinan una misma estructura analítica en V. Un *retículo* en V es un subgrupo R generado por $2g$ vectores linealmente independientes sobre $\mathbb{R}$. Un *toro complejo* de dimensión (compleja) g es un grupo de la forma $T = V/R$, donde R es un retículo en V.

Podemos considerar un isomorfismo de $\mathbb{R}$-espacios vectoriales $\phi : V \longrightarrow \mathbb{R}^{2g}$ que transforme un generador de R en la base canónica de $\mathbb{R}^{2g}$, con lo que R se corresponde con $\mathbb{Z}^{2g}$, y ϕ induce un isomorfismo de grupos

$$T \cong \mathbb{R}^{2g}/\mathbb{Z}^{2g} \cong (\mathbb{R}/\mathbb{Z})^{2g}.$$

A su vez, si $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ es la circunferencia unidad, el homomorfismo $\mathbb{R} \longrightarrow S^1$ dado por $t \mapsto e^{2\pi i t}$ induce un isomorfismo de grupos $\mathbb{R}/\mathbb{Z} \cong S^1$, luego tenemos que $T \cong (S^1)^{2g}$.

Más aún, S^1 es una subvariedad (real) de $\mathbb{C} = \mathbb{R}^2$, luego todo toro complejo T de dimensión g admite una estructura de variedad diferencial real compacta de dimensión $2g$. Vamos a ver que esta estructura no depende de la elección del isomorfismo $T \cong (S^1)^{2g}$, así como que de ella se puede extraer de forma natural una estructura analítica, con lo que los toros complejos serán también variedades analíticas compactas.

En la cadena de espacios $T = V/R \cong \mathbb{R}^{2g}/\mathbb{Z}^{2g} \cong (\mathbb{R}/\mathbb{Z})^{2g} \cong (S^1)^{2g}$ consideramos las estructuras diferenciales inducidas desde el último de ellos (las que convierten a los isomorfismos en difeomorfismos).

Fijado $z_0 = e^{2\pi i t_0} \in S$, la restricción de $f(t) = e^{2\pi i t}$ a $]t_0 - \pi, t_0 + \pi[$ es la inversa de una carta alrededor de z_0, y el diagrama siguiente es conmutativo:

$$\begin{tikzcd} \mathbb{R}/\mathbb{Z} \arrow[r, "\bar{f}"] & S^1 \\ \mathbb{R} \arrow[u, "p"] \arrow[ur, "f"'] & \end{tikzcd}$$

donde p es la proyección. Por lo tanto, la restricción de p a $]t_0 - \pi, t_0 + \pi[$ es la inversa de una carta alrededor de $[t_0]$.

Fijado un punto $P_0 \in T$, la inversa de una carta alrededor de su imagen

$$([t_1^0], \ldots, [t_{2g}^0]) \in (\mathbb{R}/\mathbb{Z})^{2g}$$

es la restricción a $U = \prod\limits_{k=1}^{2g} \left]t_k^0 - \pi, t_k^0 + \pi\right[$ del producto de las proyecciones de cada factor.

La inversa de la carta correspondiente alrededor de $[(t_1^0, \ldots, t_{2g}^0)] \in \mathbb{R}^{2g}/\mathbb{Z}^{2g}$ es la restricción a U de la proyección $p : \mathbb{R}^{2g} \longrightarrow \mathbb{R}^{2g}/\mathbb{Z}^{2g}$.

Ahora notamos que si $x = (t_1^0 - \pi, \ldots, t_{2g}^0 - \pi) \in \mathbb{R}^{2g}$, entonces

$$U = \{x + \alpha_1 e_1 + \cdots + \alpha_{2g} e_{2g} \mid 0 < \alpha_k < 2\pi\},$$

donde los vectores e_k son la base canónica de $\mathbb{R}^{2k}$.

Sea $R = \langle w_1, \ldots, w_{2g} \rangle_{\mathbb{Z}}$ y sea $\phi : V \longrightarrow \mathbb{R}^{2g}$ el $\mathbb{R}$-isomorfismo dado por $\phi(w_k) = e_k$. Sea $z \in V$ tal que $\phi(z) = x$ y sea

$$U' = \{z + \alpha_1 w_1 + \cdots + \alpha_{2g} w_{2g} \mid 0 < \alpha_k < 2\pi\} \subset V.$$

Claramente, $\phi[U'] = U$, y el diagrama siguiente es conmutativo:

$$\begin{tikzcd} V/R \arrow[r, "\bar{\phi}"] & \mathbb{R}^{2g}/\mathbb{Z}^{2g} \\ V \arrow[u, "p"] \arrow[r, "\phi"'] & \mathbb{R}^{2g} \arrow[u, "p"'] \end{tikzcd}$$

Por consiguiente, la restricción de la proyección p al abierto U' es la inversa de una carta alrededor del punto de partida P_0. Más aún, el razonamiento precedente prueba que la restricción de p a un entorno suficientemente pequeño de cualquier punto de V es la inversa de una carta. Las cartas de esta forma constituyen un atlas de V/R que no depende de los isomorfismos que hemos considerado. Es fácil ver que si componemos la inversa de una de estas cartas con otra de ellas obtenemos una traslación en V, que es una función holomorfa, luego el atlas que hemos obtenido es en realidad un atlas analítico de T. El teorema siguiente resume lo que hemos probado:

Teorema 1.77 *Si $T = V/R$ es un toro complejo de dimensión g, entonces T admite una estructura analítica tomando como cartas las inversas de las restricciones de la proyección $p : V \longrightarrow T$ a abiertos suficientemente pequeños (para que sean inyectivas). Así, T resulta ser una variedad analítica compacta de dimensión (compleja) g. Como variedad real, T es difeomorfo a un producto de $2g$ circunferencias S^1 (y el difeomorfismo puede tomarse de modo que además sea un isomorfismo de grupos).*

Es claro que la estructura de grupo de T es compatible con la estructura diferencial, es decir, que las aplicaciones $+ : T \times T \longrightarrow T$ y $- : T \longrightarrow T$ son holomorfas. Esto se expresa diciendo que los toros complejos son grupos de Lie complejos.

Pronto veremos que, aunque dos toros complejos de la misma dimensión son difeomorfos como variedades reales, esto no significa que sean conformemente equivalentes como variedades complejas.

Para el resto de la sección nos restringiremos al caso $g = 1$.

Teorema 1.78 *Sean R y S dos retículos en $\mathbb{C}$ y $\phi : \mathbb{C}/R \longrightarrow \mathbb{C}/S$ una aplicación holomorfa. Entonces existen constantes α, $\beta \in \mathbb{C}$ tales que el diagrama siguiente es conmutativo:*

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\tilde{\phi}"] \arrow[d, "p_R"'] & \mathbb{C} \arrow[d, "p_S"] \\
\mathbb{C}/R \arrow[r, "\phi"'] & \mathbb{C}/S
\end{tikzcd}$$

donde $\tilde{\phi}$ viene dada por $\tilde{\phi}(z) = \alpha z + \beta$.

Demostración: Es fácil ver que la proyección $p_S : \mathbb{C} \longrightarrow \mathbb{C}/S$ es lo que en topología se conoce como un cubrimiento, es decir, una aplicación es decir, una aplicación continua y suprayectiva tal que cada punto $[z] \in \mathbb{C}/S$ tiene un entorno abierto V tal que p_S se restringe a un homeomorfismo $p_S|_U : U \longrightarrow V$ sobre cada componente conexa U de $p_S^{-1}[V]$. En efecto, basta tomar un entorno conexo U de z donde $p_S|_U$ sea inyectiva y $V = p_S[U]$. Entonces $p_S^{-1}[V]$ es la unión disjunta de los trasladados $s + U$, para cada $s \in S$.

Sea $f : \mathbb{C} \longrightarrow \mathbb{C}/S$ dada por $f = p_R \circ \phi$. Un teorema básico de la topología algebraica (el criterio de elevación[2]) afirma que, como p_S es un cubrimiento de un espacio topológico y su dominio $\mathbb{C}$ es localmente compacto y simplemente conexo, la aplicación continua (arbitraria) f se eleva a $\mathbb{C}$, es decir, existe una aplicación continua $\tilde{\phi} : \mathbb{C} \longrightarrow \mathbb{C}$ tal que $\tilde{\phi} \circ p_S = f$. En concreto, esto significa que $\phi([z]) = [\tilde{\phi}(z)]$.

El hecho de que p_R y p_S sean localmente conformes implica que $\tilde{\phi}$ es holomorfa. Para cada $\omega \in R$, la aplicación $\tilde{\phi}(z+\omega) - \tilde{\phi}(z)$ toma valores en S. Como $\mathbb{C}$ es conexo y S es discreto, ha de ser constante, y su derivada será nula. Así pues, $\tilde{\phi}'(z + \omega) = \tilde{\phi}'(z)$, para todo $z \in \mathbb{C}$ y todo $\omega \in R$.

[2] Teorema 8.15 en mi libro de *Topología algebraica.* Ver la observación posterior.

Esto nos permite definir $\tilde{\phi}' : \mathbb{C}/R \longrightarrow \mathbb{C}$ mediante $\tilde{\phi}'([z]) = \tilde{\phi}'(z)$ y de nuevo por la conformidad local de p_R tenemos que se trata de una aplicación holomorfa. Concluimos que $\tilde{\phi}'$ es constante, ya que de no serlo su imagen sería abierta en $\mathbb{C}$, pero también compacta, lo cual es absurdo.

Sea, pues, $\alpha \in \mathbb{C}$ tal que $\phi'(z) = \alpha$ para todo $z \in \mathbb{C}$. Obviamente entonces, existe $\beta \in \mathbb{C}$ tal que $\phi(z) = \alpha z + \beta$ para todo $z \in \mathbb{C}$. ■

De aquí se deducen varias consecuencias, pero antes conviene introducir algunas definiciones.

Definición 1.79 Un *homomorfismo analítico* $\phi : \mathbb{C}/R \longrightarrow \mathbb{C}/S$ entre dos toros complejos es un homomorfismo de grupos que además es una aplicación holomorfa entre las dos superficies de Riemann. Un *isomorfismo analítico* es un homomorfismo analítico biyectivo (en particular una transformación conforme).

Si en el teorema anterior suponemos que $\phi(0) = 0$, entonces se ha de cumplir que $\tilde{\phi}(\beta) \in S$, y en tal caso $\tilde{\phi}(z) = \alpha z$ induce también la aplicación ϕ, es decir, podemos suponer $\beta = 0$, con lo que resulta que ϕ es un homomorfismo analítico:

Teorema 1.80 *Si $\phi : \mathbb{C}/R \longrightarrow \mathbb{C}/S$ es una aplicación holomorfa entre dos toros complejos que cumple $\phi(0) = 0$, entonces ϕ es un homomorfismo analítico, inducido por la multiplicación por un cierto $\alpha \in \mathbb{C}$.*

En particular, una transformación conforme $\phi : \mathbb{C}/R \longrightarrow \mathbb{C}/S$ entre dos toros complejos que cumpla $\phi(0) = 0$ es un isomorfismo analítico. Ahora bien, si $\phi(0) = [\beta]$, podemos considerar la aplicación $\psi : \mathbb{C}/S \longrightarrow \mathbb{C}/S$ dada por $\psi([z]) = [z-\beta]$. Es claro que está bien definida y es una transformación conforme del toro en sí mismo. Por consiguiente, $\phi \circ \psi$ es también una transformación conforme y conserva el 0, luego es un isomorfismo analítico. Con esto hemos probado:

Teorema 1.81 *Dos toros complejos son conformemente equivalentes si y sólo si son conformemente isomorfos.*

Si $\phi : \mathbb{C}/R \longrightarrow \mathbb{C}/S$ es un isomorfismo analítico entre dos toros complejos, el número α que lo representa en $\mathbb{C}$ ha de cumplir $\alpha R = S$ y, recíprocamente, todo $\alpha \in \mathbb{C}$ que cumpla $\alpha R = S$ induce un isomorfismo analítico entre los toros. Esto nos lleva a la definición siguiente:

Definición 1.82 Dos retículos R y S en $\mathbb{C}$ son *linealmente equivalentes* si existe un número complejo α tal que $\alpha R = S$.

Geométricamente, esto significa que uno puede obtenerse de otro mediante una rotación y una homotecia. Los teoremas anteriores muestran que dos toros $\mathbb{C}/R$ y $\mathbb{C}/S$ son conformemente equivalentes (o analíticamente isomorfos) si y sólo si los retículos R y S son linealmente equivalentes.

Explícitamente, si $R = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}}$ y $S = \langle \omega_1', \omega_2' \rangle_{\mathbb{Z}}$, tenemos que R y S son equivalentes si y sólo si existe un $\alpha \in \mathbb{C}^*$ tal que $\langle \alpha\omega_1', \alpha\omega_2' \rangle_{\mathbb{Z}} = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}}$, lo que a su vez equivale a que existan enteros a, b, c, d tales que

$$\alpha\omega_1' = d\omega_1 + c\omega_2, \quad \alpha\omega_2' = b\omega_1 + a\omega_2, \qquad ad - bc = \pm 1.$$

Esto equivale a que

$$\frac{\omega_2'}{\omega_1'} = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1}, \qquad a, b, c, d \in \mathbb{Z}, \quad ad - bc = \pm 1.$$

Si llamamos $\tau = \omega_2/\omega_1$ y $\tau' = \omega_2'/\omega_1'$, concluimos que R y S son linealmente equivalentes si y sólo si existen números a, b, c, d tales que

$$\tau' = \frac{a\tau + b}{c\tau + d}, \qquad a, b, c, d \in \mathbb{Z}, \quad ad - bc = \pm 1.$$

Observemos que

$$\operatorname{Im}\tau' = \frac{\operatorname{Im}((a\tau + b)(c\bar{\tau} + d)))}{|c\tau + d|^2} = \frac{bc\operatorname{Im}\bar{\tau} + ad\operatorname{Im}\tau}{|c\tau + d|^2} = \frac{ad - bc}{|c\tau + d|^2}\operatorname{Im}\tau.$$

El hecho de que ω_1 y ω_2 sean linealmente independientes sobre $\mathbb{R}$ equivale a que $\operatorname{Im}\tau \neq 0$ y, eligiendo el orden, podemos exigir que $\operatorname{Im}\tau > 0$. Igualmente podemos suponer que $\operatorname{Im}\tau' > 0$, con lo que $ad - bc$ ha de tomar el signo positivo. Con esto hemos probado el teorema siguiente:

Teorema 1.83 *Sean $R = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}}$ y $S = \langle \omega_2', \omega_2' \rangle_{\mathbb{Z}}$ dos retículos en $\mathbb{C}$ con bases elegidas de modo que $\tau = \omega_2/\omega_1$ y $\tau' = \omega_2'/\omega_1'$ tengan parte imaginaria positiva. Entonces R y S son linealmente equivalentes si y sólo si existen números enteros a, b, c, d tales que*

$$\tau' = \frac{a\tau + b}{c\tau + d}, \qquad ad - bc = 1.$$

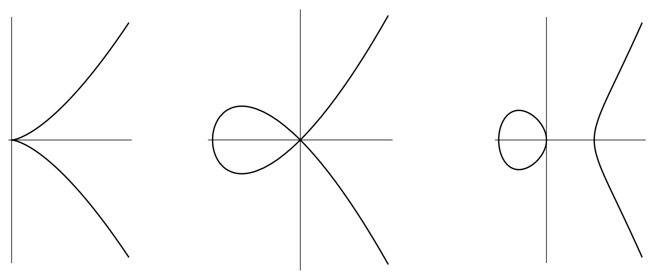
Ahora es claro que existen infinitos retículos no equivalentes dos a dos, luego hay infinitos toros complejos —de dimensión 1— no conformemente equivalentes dos a dos.

Capítulo II

Variedades algebraicas

La geometría algebraica estudia los sistemas de ecuaciones polinómicas sobre un cuerpo k o, equivalentemente, los subconjuntos de k^n donde se anula un conjunto dado de polinomios. A estos conjuntos los llamaremos subconjuntos algebraicos de k^n.

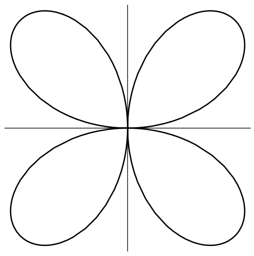
Antes de dar definiciones más precisas conviene observar algunos ejemplos en $\mathbb{R}^2$. Es claro que si $F(X) \in \mathbb{R}[X]$, entonces la gráfica de F es el conjunto de soluciones de la ecuación $Y - F(X) = 0$, luego las gráficas de los polinomios son conjuntos algebraicos. También lo son las secciones cónicas (elipses, hipérbolas y parábolas), pues toda cónica puede expresarse como el conjunto de las soluciones de un polinomio de segundo grado en dos variables. Con polinomios de tercer grado encontramos ciertos fenómenos notables.



$Y^2 = X^3$ $\qquad$ $Y^2 = X^2(X+1)$ $\qquad$ $Y^2 = X(X^2-1)$

Estos ejemplos (junto con los de las gráficas de polinomios y las secciones cónicas) sugieren que los conjuntos algebraicos definidos por un polinomio en $\mathbb{R}^2$ son “curvas” en un sentido que deberemos precisar, pero que en una primera aproximación podríamos concretar diciendo que localmente son homeomorfos a segmentos de recta.

La primera figura muestra que las curvas algebraicas pueden tener “picos”. La segunda muestra que pueden cortarse a sí mismas, con lo que en realidad hay puntos alrededor de los cuales no podemos decir que las curvas sean localmente rectas. La tercera muestra que las curvas algebraicas no tienen por qué ser conexas. A medida que aumentamos el grado podemos obtener curvas más complejas. Veamos un último ejemplo en grado 6:



$$(X^2 + Y^2)^3 - 4X^2Y^2 = 0$$

2.1 Variedades afines

A la hora de estudiar los conjuntos algebraicos, a menudo resulta útil "moverlos" hasta una posición adecuada (por ejemplo, en la que un punto que nos interese pase a ser el $(0, 0)$, etc.) Sin embargo, desde un punto de vista teórico resulta más conveniente aún "movernos nosotros" en lugar de mover el conjunto, es decir, cambiar de sistema de referencia. Ello nos lleva a recordar primeramente los conceptos básicos de la geometría afín.

Definición 2.1 Llamaremos *espacio afín n-dimensional* de un cuerpo k al conjunto $A^n(k) = k^n$. A sus elementos los llamaremos *puntos.* Cuando k se sobrentienda escribiremos simplemente A^n. Escribiremos k^n cuando queramos referirnos a k^n como espacio vectorial.

La diferencia entre A^n y k^n es que en A^n "olvidamos" la estructura vectorial de k^n, de modo que ningún punto desempeña un papel destacado (al contrario de lo que ocurre en k^n con el vector 0). Esto no significa que despreciemos la estructura vectorial, sino que nos permitimos la posibilidad de asociar una estructura vectorial a cada punto, de modo que el vector 0 sea en cada momento el punto que más convenga. Más concretamente, si P y Q son puntos de A^n, llamaremos $\overrightarrow{PQ} = Q - P \in k^n$. De este modo, fijado un punto $O \in A^n$, obtenemos una estructura vectorial al identificar cada punto $P \in A^n$ con el vector $\overrightarrow{OP}$.

Un *sistema de referencia afín* en A^n es una $n+1$-tupla $(O; P_1, \ldots, P_n)$ tal que los vectores $\overrightarrow{OP_i}$ forman una base de k^n. Las *coordenadas* de un punto $P \in A^n$ en dicho sistema de referencia son las coordenadas del vector $\overrightarrow{OP}$ en la base $\overrightarrow{OP_i}$. Cuando no haya confusión escribiremos O en lugar de $(O; P_1, \ldots, P_n)$.

Así, si las coordenadas de P son $(a_1, \ldots, a_n)$, tenemos que

$$P = O + \overrightarrow{OP} = O + a_1\overrightarrow{OP_1} + \cdots + a_n\overrightarrow{OP_n}.$$

En particular vemos que un punto está completamente determinado por sus coordenadas en un sistema de referencia dado. En la mayoría de las ocasiones sobrentenderemos que hemos fijado un sistema de referencia e identificaremos cada punto con la n-tupla de sus coordenadas.

Es fácil ver que si tenemos dos sistemas de referencia afines O y O', entonces las coordenadas de un punto arbitrario P en ambos sistemas, digamos $(X_1, \ldots, X_n)$ y $(X_1', \ldots, X_n')$ están relacionadas por un sistema de ecuaciones lineales:

$$\begin{array}{rcl} X_1' & = & b_1 + a_{11}X_1 + \cdots + a_{1n}X_n, \\ \cdots & & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ X_n' & = & b_n + a_{n1}X_1 + \cdots + a_{nn}X_n. \end{array} \tag{2.1}$$

Cualquier sistema de ecuaciones de este tipo cuya matriz de coeficientes (a_{ij}) sea regular se corresponde con un cambio de sistema de referencia.

A partir de aquí conviene "olvidar" que los puntos de A^n son, conjuntistamente, n-tuplas y pensar que cada punto P tiene determinadas unas coordenadas en cada sistema de referencia de A^n. Las componentes de P son simplemente sus coordenadas en el sistema de referencia formado por $O = (0, \ldots, 0)$ y los vectores de la base canónica de k^n, pero este sistema de referencia particular no tiene ningún significado especial en la teoría.

Definición 2.2 Si $F \in k[X_1, \ldots, X_n]$ es un polinomio y un punto $P \in A^n$ tiene coordenadas $(a_1, \ldots, a_n)$ en un sistema de referencia dado, escribiremos $F(P)$ para referirnos a $F(a_1, \ldots, a_n)$. Por supuesto, esta notación depende del sistema de referencia. Si $S \subset k[X_1, \ldots, X_n]$ es un conjunto de polinomios, llamaremos

$$V(S) = \{P \in A^n \mid F(P) = 0 \text{ para todo } F \in S\}.$$

Diremos que un conjunto $C \subset A^n$ es *algebraico* si $C = V(S)$ para cierto conjunto $S \subset k[X_1, \ldots, X_n]$.

Observemos que $V(S)$ depende del sistema de referencia con el que se evalúan los polinomios, pero no sucede lo mismo con el carácter algebraico de un conjunto: Si $C = V(S)$ es un conjunto algebraico respecto a un sistema de referencia O y consideramos otro sistema O', a cada polinomio $F \in S$ le podemos asignar —mediante un cambio de variables lineal de tipo (2.1)— otro polinomio F' de modo que F se anula en las coordenadas de un punto P respecto a O si y sólo si F' lo hace en sus coordenadas respecto de O'. Si llamamos S' al conjunto de los polinomios así obtenidos resulta que $C = V_O(S) = V_{O'}(S')$, luego T también es algebraico respecto del sistema O'.

El conjunto vacío es algebraico, pues $\varnothing = V(1)$.

En la práctica es costumbre referirse a un conjunto algebraico mediante las ecuaciones que lo definen, de modo que, por ejemplo, en lugar de escribir $V = V(X^2 + Y^2 - 1, X + Y + Z - 3)$ podemos decir que V es el conjunto algebraico determinado por las ecuaciones

$$X^2 + Y^2 = 1, \qquad X + Y + Z = 3.$$

Los subconjuntos algebraicos de A^2 definidos por una única ecuación se llaman *curvas afines planas.* Las curvas planas se clasifican en *rectas, cónicas, cúbicas, cuárticas,* etc. según el grado del polinomio que las define.[1]

Es claro que un mismo conjunto algebraico puede definirse mediante distintos sistemas de ecuaciones. Por ejemplo, una misma circunferencia en $A^3(\mathbb{R})$ puede definirse como la intersección de un cilindro y un plano, o de una esfera y un plano, o de dos esferas, etc. Una forma de evitar que nuestros resultados dependan de las ecuaciones particulares con las que definimos un conjunto algebraico es considerar simultáneamente todas las ecuaciones posibles.

En primer lugar observamos que si $S \subset k[X_1, \ldots, X_n]$ e I es el ideal generado por S, entonces $V(S) = V(I)$, luego todo conjunto algebraico está determinado por un ideal. Esto nos lleva a tratar con conjuntos algebraicos definidos por infinitas ecuaciones. Ahora bien, puesto que el anillo $k[X_1, \ldots, X_n]$ es noetheriano (teorema 1.7), todo ideal es finitamente generado, luego en realidad todo conjunto algebraico está determinado por un número finito de polinomios.[2] Considerar infinitas ecuaciones es sólo un recurso teórico para evitar una elección arbitraria de ecuaciones.

Dado un conjunto algebraico $C = V(S)$, la pregunta obligada es si, al sustituir el conjunto S por el ideal $I = (S)$, obtenemos el conjunto de todas las ecuaciones polinómicas satisfechas por C. Precisemos esto:

Definición 2.3 Si $C \subset A^n$ es un conjunto algebraico, fijado un sistema de referencia afín, definimos el ideal

$$I(C) = \{F \in k[X_1, \ldots, X_n] \mid F(P) = 0 \text{ para todo } P \in C\}.$$

Hemos de entender que $I(\varnothing) = k[X_1, \ldots, X_n]$.

Así, los polinomios de $I(C)$ determinan todas las ecuaciones satisfechas por el conjunto C. Nos estábamos preguntando si $I(V(I)) = I$, para todo ideal I. Similarmente, cabe preguntarse si $V(I(C)) = C$, para todo conjunto algebraico C, o —más en general— si las correspondencias $C \leftrightarrow I$ que acabamos de definir son biyectivas y mutuamente inversas.

Esto no es cierto en general. En principio tenemos que $I \subset I(V(I))$ y $C = V(I(C))$. Sin embargo, la primera inclusión no tiene por qué ser una igualdad, como muestra el ejemplo siguiente:

Ejemplo Consideremos la “curva” en $A^2(\mathbb{R})$ dada por $X^2+Y^2 = 0$. Nada más lejos de nuestras expectativas sobre las curvas algebraicas que el hecho de que una de ellas pueda reducirse al punto $(0, 0)$. Resulta que el conjunto algebraico

[1]Esta definición es provisional. En la nota de la página 62 añadiremos una restricción natural a la definición de curva. La idea es que el conjunto algebraico determinado por $(X - Y)(X^2 + Y^2 - 1) = 0$ no sea una curva, sino la unión de dos curvas: una recta y una circunferencia.

[2]Este hecho que aquí comentamos al paso fue en su momento un notable descubrimiento de Hilbert.

$C = \{(0,0)\}$ está definido por el conjunto $S = \{X^2 + Y^2\}$, o también por el ideal $I = (X^2 + Y^2) \subset \mathbb{R}[X, Y]$, pero los polinomios de este ideal no son todos los que se anulan en C, pues no contiene a los polinomios X e Y, lo cuales, pese a ello, se anulan en C. Así, $I(V(I)) \neq I$.

Estas patologías se deben a que $\mathbb{R}$ no es algebraicamente cerrado. Si consideramos a $X^2 + Y^2$ como polinomio en $\mathbb{C}[X, Y]$ vemos que

$$X^2 + Y^2 = (X + iY)(X - iY),$$

luego $V(X^2 + Y^2) \subset A^2(\mathbb{C})$ es la unión de dos rectas que se cortan en $(0,0)$. Pronto será evidente que el ideal $I = (X^2+Y^2) \subset \mathbb{C}[X, Y]$ sí que consta de todos los polinomios que se anulan en C, entre los cuales no está X, pues ciertamente X no se anula en $(i, 1) \in C$. ■

Aun si consideramos cuerpos algebraicamente cerrados, hay otra cuestión que debemos tener en cuenta.

Definición 2.4 Llamaremos *radical* de un ideal I de un anillo conmutativo y unitario A al ideal

$$\operatorname{Rad} I = \{a \in A \mid a^n \in I \text{ para un natural } n > 0\}.$$

Es fácil ver que, efectivamente, se trata de un ideal de A, pues si $a^m \in I$ y $b^m \in I$ entonces $(a + b)^{m+n} \in I$. Además $I \subset \operatorname{Rad} I$ y si $I \neq A$ entonces $\operatorname{Rad} I \neq A$.

Un ideal I es *radical* si $I = \operatorname{Rad} I$ o, equivalentemente, si cuando $a^n \in I$ entonces $a \in I$. Es claro que $\operatorname{Rad} I$ cumple esta propiedad, luego $\operatorname{Rad} I$ es el menor ideal radical que contiene a I. Todo ideal primo es radical.

Es evidente que todo ideal $I(X)$ es radical. El teorema siguiente muestra que cuando el cuerpo base es algebraicamente cerrado, la restricción de la correspondencia entre ideales y conjuntos algebraicos se vuelve biyectiva al restringirla a ideales radicales. (A este teorema se le suele llamar también "Teorema de los ceros de Hilbert". Nosotros reservaremos este nombre para el teorema 1.34.)

Teorema 2.5 *Sea k un cuerpo algebraicamente cerrado e I un ideal del anillo de polinomios $k[X_1, \ldots, X_n]$. Entonces $I(V(I)) = \operatorname{Rad} I$.*

Demostración: Una inclusión es obvia. Digamos que $I = (F_1, \ldots, F_m)$. Tomemos $G \in I(V(I))$, es decir, G se anula en todos los puntos donde se anulan los polinomios F_i. Añadamos una indeterminada T y consideremos los polinomios

$$F_1, \ldots, F_m, TG - 1 \in k[X_1, \ldots, X_n, T].$$

Por hipótesis no tienen soluciones en común, luego por el teorema de los ceros de Hilbert 1.34 existen polinomios $H_1, \ldots, H_m, H \in k[X_1, \ldots, X_n, T]$ tales que

$$H_1F_1 + \cdots + H_mF_m + H(TG - 1) = 1.$$

Ahora sustituimos $T = 1/Y$ y, multiplicando por una potencia adecuada de Y, obtenemos una ecuación de la forma

$$H_1'F_1 + \cdots + H_m'F_m + H'(G - Y) = Y^N,$$

para ciertos polinomios $H_1', \ldots, H_m', H' \in k[X_1, \ldots, X_n, Y]$. Finalmente sustituimos $Y = G$ y queda que $G^N \in (F_1, \ldots, F_m)$. ∎

En particular, si el ideal I es radical tenemos que $I(V(I)) = I$, luego la aplicación $I \mapsto V(I)$ biyecta los ideales radicales con los conjuntos algebraicos. Su inversa es $C \mapsto I(C)$. Claramente ambas correspondencias invierten las inclusiones.

Nota En lo sucesivo, y si no se indica lo contrario, sobrentenderemos que el cuerpo base k es algebraicamente cerrado. Esto no significa que no podamos aplicar los resultados que obtengamos a otros casos naturales, como $k = \mathbb{R}$. No obstante, los resultados para cuerpos no algebraicamente cerrados serán "reflejos" más o menos débiles de la teoría abstracta sobre cuerpos algebraicamente cerrados.

Ahora estamos en condiciones de introducir ciertos matices en la teoría. Por ejemplo, según las definiciones que hemos dado, la curva plana de ecuación $XY = 0$ es una cónica, pero es más descriptivo decir que se trata de la unión de las rectas $X = 0$ e $Y = 0$. En general, tenemos lo siguiente:

Teorema 2.6 *La intersección de conjuntos algebraicos es un conjunto algebraico. La unión de un número finito de conjuntos algebraicos es un conjunto algebraico.*

Demostración: Es inmediato comprobar que

$$\bigcap_{i\in I} V(S_i) = V(\bigcup_{i\in I} S_i).$$

Por otra parte, si F y G son polinomios, es claro que $V(FG) = V(F) \cup V(G)$. Así mismo, todo conjunto algebraico es intersección de un número finito de conjuntos $V(F_i)$, de donde se sigue fácilmente que la unión de dos conjuntos algebraicos es un conjunto algebraico. De hecho, es fácil concluir que

$$V(I_1) \cup \cdots \cup V(I_n) = V(I_1 \cdots I_n).$$

∎

Esto hace que un conjunto algebraico pueda ser muy heterogéneo, como la unión de una esfera, un plano y una recta. Sin embargo, vamos a ver que en tal caso es posible "separar" teóricamente la esfera, el plano y la recta a partir de su unión. Para ello introducimos el concepto que da título a esta sección:

Definición 2.7 Un conjunto algebraico C es *reducible* si existen conjuntos algebraicos C_1, C_2 distintos de C y tales que $C = C_1 \cup C_2$. En caso contrario diremos que C es *irreducible.* A los conjuntos algebraicos irreducibles los llamaremos también *variedades afines.*

El teorema siguiente muestra que todo conjunto algebraico está formado por una unión finita de variedades, por lo que limitarnos a estudiar variedades no supone una restricción importante. Al contrario, es imprescindible si no queremos perdernos en la confusión que produce una mezcla finita caótica de variedades:

Teorema 2.8 *Todo conjunto algebraico C se descompone de forma única en unión de variedades $C = V_1 \cup \cdots \cup V_n$ tales que $V_i \not\subset V_j$ para $i \neq j$.*

Demostración: Sea A el conjunto de todos los conjuntos algebraicos en A^n que no pueden descomponerse en unión finita de variedades. Hemos de probar que es vacío. Si contiene un conjunto C, entonces C no es irreducible, luego $C = C_1 \cup Y_1$, donde ambos conjuntos están contenidos estrictamente en C. Al menos uno de ellos no ha de poder descomponerse en unión de variedades. Digamos que $C_1 \in A$. Entonces $C_1 = C_2 \cup Y_2$, etc. Continuando este proceso obtenemos una sucesión de conjuntos algebraicos

$$C \supset C_1 \supset C_2 \supset C_3 \supset \cdots$$

Al considerar sus ideales obtenemos una sucesión estrictamente creciente de ideales de $k[X_1, \ldots, X_n]$, lo cual es imposible porque este anillo es noetheriano.

Así pues, todo conjunto C admite una descomposición en las condiciones del enunciado (si una de las variedades está contenida en otra, la eliminamos).

Para probar la unicidad observamos que si

$$V_1 \cup \cdots \cup V_n = W_1 \cup \cdots \cup W_m$$

son dos descomposiciones en las condiciones del enunciado, entonces

$$V_i = (W_1 \cap V_i) \cup \cdots \cup (W_m \cap V_i),$$

y al ser irreducible ha de ser $V_i \subset W_j$, para cierto j. Similarmente $W_j \subset V_r$, para cierto r, pero entonces $V_i \subset V_r$, luego $i = r$ y así $V_i = W_j$. Ahora es fácil ver que las dos descomposiciones son la misma. ■

Comprobar que un conjunto algebraico es irreducible suele ser una tarea delicada. El resultado fundamental es el siguiente:

Teorema 2.9 *Un conjunto algebraico $C \neq \varnothing$ es irreducible si y sólo si $I(C)$ es un ideal primo.*

Demostración: Si $I(C)$ no es primo, tomemos $F_1F_2 \in I(C)$ de modo que $F_i \notin I(C)$. Entonces $C = (C \cap V(F_1)) \cup (C \cap V(F_2))$. Los conjuntos $C \cap V(F_i)$ son algebraicos y están contenidos estrictamente en C, pues si $C \subset V(F_i)$ entonces $F_i \in I(C)$. Así pues, C no es irreducible.

Recíprocamente, si $C = C_1 \cup C_2$ es una descomposición de C, entonces existen polinomios $F_i \in I(C_i) \setminus I(C)$, los cuales cumplen, por otra parte, que $F_1F_2 \in I(C)$, luego $I(C)$ no es primo. ■

Las variedades más simples son los puntos. Puesto que la correspondencia entre ideales y conjuntos algebraicos invierte las inclusiones y los puntos no contienen variedades menores, vemos que los puntos se corresponden con los ideales maximales (notemos que un ideal radical maximal es lo mismo que un ideal maximal).

Ejemplo Sea $V = V(F) \subset A^2$ una curva plana y sea $F = F_1^{r_1} \cdots F_m^{r_m}$ la descomposición de F en factores irreducibles. Entonces

$$V = V(F_1) \cup \cdots \cup V(F_m)$$

es la descomposición de V en variedades irreducibles. En efecto, cada conjunto $V_i = V(F_i)$ es irreducible, pues el ideal $I_i = (F_i)$ es primo, luego es radical, luego $I(V_i) = \operatorname{rad}(F_i) = (F_i)$, y podemos aplicar el teorema anterior.

Además, no puede ocurrir que $V_i \subset V_j$ para $i \neq j$, pues entonces $(F_j) \subset (F_i)$, luego $F_i \mid F_j$ y $F_i = F_j$.

Concluimos que una curva plana es irreducible si y sólo si la ecuación que la define es irreducible o, a lo sumo, potencia de un polinomio irreducible. En cualquier caso, una curva plana irreducible siempre puede definirse mediante una ecuación irreducible. ■

Nota En lo sucesivo, cuando hablemos de una curva plana (una recta, una cónica, una cúbica, etc.) sobrentenderemos que es irreducible salvo que indiquemos explícitamente lo contrario.

Teorema 2.10 *Los conjuntos definidos por una ecuación $Y = G(X_1, \ldots, X_n)$ (es decir, las gráficas de los polinomios) son irreducibles.*

Demostración: Basta probar que el polinomio $F = Y - G(X_1, \ldots, X_n)$ es irreducible, pues entonces $I(V(F)) = \operatorname{rad}(F) = (F)$ será un ideal primo. Si $F = F_1F_2$, entonces uno de los factores ha de tener grado en Y igual a 1, digamos $F_1 = S(X_1, \ldots, X_n)Y + T(X_1, \ldots, X_n)$. Por consiguiente $F_2 = F_2(X_1, \ldots, X_n)$, con lo que, igualando coeficientes,

$$1 = S(X_1, \ldots, X_n)F_2(X_1, \ldots, X_n),$$

luego F_2 es constante. ■

Ejemplo Los conjuntos algebraicos dados por

$$Y^2 = X^3, \quad Y^2 = X^2(X+1), \quad Y^2 = X(X^2-1) \quad \text{y} \quad X^2 + Y^2 = 1$$

son irreducibles, es decir, son curvas planas. (Ver las figuras de la página 55).

Según el ejemplo anterior, basta probar que los polinomios correspondientes son irreducibles. Para los tres últimos podemos aplicar el criterio de irreducibilidad de Eisenstein. Por ejemplo, el polinomio $Y^2 - X^2(X+1) \in k[X][Y]$

cumple que todos sus coeficientes menos el director son divisibles entre el primo $X+1$ y el término independiente no es divisible entre $(X+1)^2$.

Para $Y^2 - X(X^2-1)$ usamos el primo X y para Y^2+X^2-1 el primo $X+1$.

Supongamos ahora que $Y^2 - X^3 = F_1F_2$. Es fácil ver que si el grado en Y de uno de los factores es 2, el otro ha de ser constante. Supongamos, pues, que

$$F_1 = G_1(X)Y + H_1(X), \qquad F_2 = G_2(X)Y + H_2(X).$$

Multiplicando e igualando coeficientes queda que

$$G_1G_2 = 1, \quad G_1H_2 + H_1G_2 = 0, \quad H_1H_2 = -X^3.$$

De la primera igualdad obtenemos que G_1 y G_2 son constantes, de la segunda que $H_1 = aH_2$, para cierto $a \in k$, y de la tercera que $aH_2^2 = -X^3$, lo cual es imposible. Por lo tanto $Y^2 - X^3$ es irreducible. ■

Seguidamente estudiamos las aplicaciones que conectan adecuadamente dos variedades afines. Éstas son, naturalmente, las aplicaciones definidas a través de polinomios.

Definición 2.11 Sean $V \subset A^m(k)$ y $W \subset A^n(k)$ dos variedades afines. Una aplicación $\phi : V \longrightarrow W$ es *polinómica* si, fijados sistemas de referencia afines, existen polinomios $F_1, \ldots, F_n \in k[X_1, \ldots, X_m]$ tales que para todo $P \in V$ se cumple que $\phi(P) = (F_1(P), \ldots, F_n(P))$. (Entiéndase: las coordenadas de $\phi(P)$ son las imágenes por los F_i de las coordenadas de P.)

Un *isomorfismo* entre variedades es una aplicación polinómica biyectiva cuya inversa sea también polinómica.[3]

Es fácil ver que el carácter polinómico de una aplicación no depende de los sistemas de referencia considerados. También es fácil comprobar que la composición de aplicaciones polinómicas es una aplicación polinómica.

Ejemplo La parábola $Y = X^2$ es isomorfa a la recta A^1. Un isomorfismo es el dado por $\phi(t) = (t, t^2)$. ■

Llamaremos $k[V]$ al conjunto de las funciones polinómicas $V \longrightarrow k$. Aquí estamos considerando a $k = A^1$ como una variedad. Es claro que $k[V]$ es un anillo con las operaciones definidas puntualmente (aquí consideramos a k como cuerpo y no meramente como espacio afín). Además contiene una copia de k (formada por las funciones constantes).

Notemos que la definición de $k[V]$ no depende de la elección de un sistema de referencia en A^n. Ahora bien, si fijamos uno, podemos obtener una representación en coordenadas de cada función de $k[V]$. Concretamente, cada polinomio $F \in k[X_1, \ldots, X_m]$ define una función polinómica $f \in k[V]$ dada por $f(P) = F(P)$ (entendiendo que el segundo miembro es F actuando sobre las

[3] En el ejercicio de la página 119 se muestra un ejemplo de aplicación polinómica biyectiva con inversa no polinómica.

coordenadas de P). La aplicación $F \mapsto f$ es un epimorfismo de anillos y su núcleo es $I(V)$. Por consiguiente tenemos la representación

$$k[V] \cong k[X_1, \ldots, X_n]/I(V). \tag{2.2}$$

En la práctica consideraremos a (2.2) como una igualdad, si bien hemos de recordar que sólo tiene sentido cuando hemos fijado un sistema de referencia en A^n. Representaremos por x_i a la clase de X_i en $k[X_1, \ldots, X_n]/I(V)$. Observemos que las funciones x_i son las que asignan a cada punto $P \in V$ sus coordenadas en el sistema de referencia fijado.

Se cumple que $k[V] = k[x_1, \ldots, x_n]$. Más concretamente, cada función $f \in k[V]$ tiene una representación coordenada (no necesariamente única) de la forma $f = F(x_1, \ldots, x_n)$, donde $F \in k[X_1, \ldots, X_n]$ es cualquier polinomio que cumpla $f = [F]$. Si $P \in V$ tiene coordenadas $(a_1, \ldots, a_n)$, entonces $f(P) = F(a_1, \ldots, a_n)$.

Como $I(V)$ es un ideal primo, la representación (2.2) muestra que $k[V]$ es un dominio íntegro.

Ejemplo Sea $V = V(X - Y^2)$. Entonces $k[V] = k[x, y]$, y es fácil ver que x e y son trascendentes sobre k, pero no son algebraicamente independientes, sino que $x = y^2$. Por lo tanto $k[V] = k[y]$ es isomorfo al anillo de polinomios $k[Y]$. Alternativamente, podemos llamar $y = \sqrt{x}$ y entonces $k[V] = k[x][\sqrt{x}]$.

Cada punto $x \in k$ se corresponde con dos puntos $(x, \sqrt{x})$ y $(x, -\sqrt{x})$ en V (salvo el 0, para el que los dos puntos son el mismo), de modo que la función $\sqrt{x}$, que en k ha de verse como una "función multiforme" —que asocia dos imágenes a cada punto— es en V una función uniforme que asocia a cada uno de los dos puntos correspondientes a x en V una de las dos raíces cuadradas de x en k. ■

Vamos a probar que $k[V]$ determina a V salvo isomorfismo. En primer lugar observemos que si $P \in V$ entonces $I(P)$ es un ideal maximal de $k[X_1, \ldots, X_m]$ que contiene a $I(V)$, luego $I_V(P) = I(P)/I(V)$ es un ideal maximal de $k[V]$. Recíprocamente, todo ideal maximal de $k[V]$ ha de ser de esta forma. Por lo tanto, los puntos de V se corresponden biunívocamente con los ideales maximales de $k[V]$.

Notemos que, en principio, la definición $I_V(P) = I(P)/I(V)$ depende de la representación coordenada $k[V] \cong k[X_1, \ldots, X_n]/I(V)$ en un sistema de referencia, pero, a través del isomorfismo, el ideal maximal $I_V(P)$ se corresponde con el conjunto de las funciones de $k[V]$ que se anulan en P, lo cual no depende de ningún sistema de referencia. Por lo tanto hemos probado:

Teorema 2.12 *Si V es una variedad afín, los ideales maximales de $k[V]$ son de la forma $I_V(P) = \{f \in k[V] \mid f(P) = 0\}$, para cierto $P \in V$, de modo que la correspondencia $P \leftrightarrow I_V(P)$ es una biyección entre V y el conjunto de todos los ideales maximales de $k[V]$.*

Observemos ahora que si $\phi : V \longrightarrow W$ es una aplicación polinómica entonces la aplicación $\overline{\phi} : k[W] \longrightarrow k[V]$ dada por $\overline{\phi}(f) = \phi \circ f$ es un homomorfismo de anillos. Además, si $P \in V$, se cumple

$$I_W(\phi(P)) = \overline{\phi}^{-1}[I_V(P)].$$

En efecto, si $f \in I_W(\phi(P))$, entonces se cumple que $\overline{\phi}(f)(P) = f(\phi(P)) = 0$, luego $\overline{\phi}(f) \in I_V(P)$. Esto prueba una inclusión y, por la maximalidad, tenemos la igualdad.

En particular vemos que si $\overline{\phi} = \overline{\psi}$ entonces $\phi = \psi$. Otro hecho inmediato es que $\overline{\phi}$ transforma cada función constante de $k[W]$ en la constante correspondiente de $k[V]$. Expresaremos esto diciendo que $\overline{\phi}$ es un *k-homomorfismo.*

Teorema 2.13 *Sean $V \subset A^m$ y $W \subset A^n$ dos variedades afines sobre un cuerpo k. Entonces la correspondencia $\phi \mapsto \overline{\phi}$ es una biyección entre las aplicaciones polinómicas $\phi : V \longrightarrow W$ y los k-homomorfismos de anillos $\overline{\phi} : k[W] \longrightarrow k[V]$.*

Demostración: Ya hemos probado que la correspondencia es inyectiva. Sólo falta ver que es suprayectiva. Fijamos sistemas de referencia en A^m y A^n, con lo que podemos identificar las funciones de $k[V]$ y $k[W]$ con clases de polinomios.

Consideremos un k-homomorfismo $\alpha : k[W] \longrightarrow k[V]$. Sea $\alpha(x_i) = [F_i]$. Los polinomios F_i determinan una función polinómica $\phi : A^m \longrightarrow A^n$, así como el homomorfismo de anillos $\phi^* : k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_m]$ definido mediante $G \mapsto G(F_1, \ldots, F_n)$.

Se cumple que $\phi^*[I(W)] \subset I(V)$, pues si $G \in I(W)$, entonces la clase de $\phi^*(G)$ módulo $I(V)$ es

$$G([F_1], \ldots, [F_n]) = G(\alpha(x_1), \ldots, \alpha(x_n)) = \alpha([G]) = \alpha(0) = 0.$$

Por lo tanto $\phi[V] \subset W$, pues si $P \in V$ y $G \in I(W)$, entonces $G(\phi(P)) = \phi^*(G)(P) = 0$, luego $\phi(P) \in V(I(W)) = W$. Así pues, ϕ se restringe a una función polinómica de V en W, y es fácil ver que cumple $\overline{\phi} = \alpha$. ∎

Es claro que, bajo la biyección de este teorema, los isomorfismos entre variedades se corresponden con k-isomorfismos de anillos. Así pues, dos variedades son isomorfas si y sólo si sus anillos de funciones polinómicas son k-isomorfos.

Terminamos la sección introduciendo una clase de funciones más generales que las polinómicas y que serán fundamentales en la teoría. Se trata de las aplicaciones racionales. De momento definimos únicamente las funciones racionales de una variedad en k, si bien más adelante generalizaremos la definición a aplicaciones entre variedades cualesquiera.

Definición 2.14 Sea $V \subset A^n(k)$ una variedad afín. Llamaremos cuerpo de las *funciones racionales* de V al cuerpo de cocientes de $k[V]$. Lo representaremos por $k(V)$. Notemos que esta definición no depende de la elección de un sistema de referencia en A^n.

Diremos que una función racional $\alpha \in k(V)$ es *regular* o que *está definida* en un punto $P \in V$ si $\alpha = f/g$ con $g(P) \neq 0$, y en tal caso definimos $\alpha(P) = f(P)/g(P)$. Observemos que puede haber representaciones de α para las que el denominador se anule y otras para las que no se anule. No obstante, si α es regular en P, el valor $\alpha(P)$ no depende de la representación con la que se calcula. Se dice que α es *singular* en un punto P, o que P es una *singularidad* de α si α no es regular en P.

Ejemplo Si $V = V(X^2 + Y^2 - 1)$, entonces, como elementos de $k(V)$ tenemos la igualdad

$$\frac{1+y}{x} = \frac{x}{1-y},$$

luego esta función racional es regular en $(0, -1)$, a pesar de lo que parece indicar la expresión izquierda. No es difícil ver que $(0, 1)$ es su única singularidad. ■

Veamos que podemos identificar los elementos de $k(V)$ con las funciones que determinan, en el sentido de que si f/g y f'/g' coinciden sobre el conjunto de puntos regulares para ambas, entonces $f/g = f'/g'$.

En efecto, fijado un sistema de referencia, sea $f = [F]$, $g = [G]$, $f' = [F']$ y $g' = [G']$. Sea $H = FG' - GF'$. Entonces tenemos que $HGG' \in I(V)$, pero $G, G' \notin I(V)$, pues $g, g' \neq 0$. Como $I(V)$ es primo, ha de ser $H \in I(V)$, luego $fg' - gf' = 0$, es decir, $f/g = f'/g'$.

Esto justifica el nombre de "funciones racionales" para los elementos de $k(V)$.

Para cada punto $P \in V$ definimos el *anillo local* $\mathcal{O}_P(V)$ como el anillo de las funciones racionales de V regulares en P. Claramente $k[V] \subset \mathcal{O}_P(V) \subset k(V)$.

Teorema 2.15 *Sea V una variedad afín. El conjunto de las singularidades de una función racional sobre V es algebraico. Además*

$$k[V] = \bigcap_{P \in V} \mathcal{O}_P(V),$$

es decir, $k[V]$ es el conjunto de las funciones racionales sin singularidades.

Demostración: La primera afirmación sería inmediata si no fuera por que no podemos usar siempre la misma representación de una función racional como cociente de polinomios para determinar sus singularidades. En general, fijado un sistema de referencia y una función racional $\alpha \in k(V)$, definimos

$$I_\alpha = \{G \in k[X_1, \ldots, X_n] \mid [G]\alpha \in k[V]\}.$$

Claramente I_α es un ideal de $k[X_1, \ldots, X_n]$ que contiene a $I(V)$ y los puntos de $V(I_\alpha)$ son exactamente las singularidades de α.

Para probar la segunda afirmación observamos que si α no tiene singularidades entonces $V(I_\alpha) = \varnothing$, luego, por el teorema de los ceros, $1 \in I_\alpha$, luego $\alpha = [1]\alpha \in k[V]$. ■

Ejemplo Si V es la parábola $X = Y^2$, entonces $k(V) = k(x)(\sqrt{x})$ es una extensión cuadrática del cuerpo $k(x)$, el cual es isomorfo al cuerpo de funciones racionales $k(X)$. Así, un ejemplo de función racional en V podría ser

$$\alpha = \frac{x\sqrt{x}}{\sqrt{x} - 1},$$

cuya única singularidad es $(1, 1)$. ■

2.2 Variedades proyectivas

Los resultados más importantes de la geometría algebraica son "globales", de modo que dejan de cumplirse si quitamos puntos a las variedades. Ya hemos visto que esto sucede, por ejemplo, si nos "olvidamos" de las soluciones imaginarias de una ecuación polinómica real. Ahora veremos que por el mero hecho de tratar con variedades afines ya estamos "olvidando puntos". Nos referimos a los puntos infinitos en el sentido de la geometría proyectiva. Resulta que el marco natural de la geometría algebraica no es el espacio afín, sino el espacio proyectivo. Por ejemplo, probaremos más adelante que dos curvas planas se cortan al menos en un punto. Este resultado es falso para curvas afines —basta pensar en un par de rectas paralelas—, pero en el plano proyectivo dos rectas paralelas se cortan en un punto infinito. Al considerar rectas afines estamos eliminando un punto de cada recta, de modo que en el caso de dos rectas paralelas estamos eliminando precisamente el punto que requiere el teorema sobre la intersección de curvas planas.

Recordemos la teoría básica sobre los espacios proyectivos:

Definición 2.16 Llamaremos *espacio proyectivo* n-dimensional de un cuerpo k al conjunto $\mathrm{P}^n(k)$ de todos los subespacios vectoriales de dimensión 1 en k^{n+1}. Cuando no haya confusión escribiremos simplemente P^n.

Un *sistema de referencia proyectivo* en P^n es una $n + 2$-tupla de puntos $(P_0, \ldots, P_{n+1}) \in \mathrm{P}^n$ tales que $P_i = \langle v_i \rangle$, los vectores $v_1, \ldots, v_{n+1}$ son linealmente independientes en k^{n+1} y $v_0 = v_1 + \cdots + v_{n+1}$. Notemos que si elegimos otros v_i' (para los mismos P_i) que cumplan la definición, existirá necesariamente un $\lambda \in \mathbb{C}$ no nulo tal que $v_i' = \lambda v_i$, para todo $i = 0, \ldots, n + 1$.

Fijado un sistema de referencia proyectivo, todo punto $P = \langle v \rangle \in \mathrm{P}^n$ cumple que $v = a_1 v_1 + \cdots + a_{n+1} v_{n+1}$, para cierta $n + 1$-tupla $(a_1, \ldots, a_{n+1}) \in k^{n+1}$, no nula, unívocamente determinada por P (y el sistema de referencia) salvo un factor constante. Diremos que $(a_1, \ldots, a_{n+1})$ es un vector de *coordenadas homogéneas* de P en el sistema de referencia dado.

De este modo, todo $(a_1, \ldots, a_{n+1}) \in k^{n+1}$ no nulo es un vector de coordenadas homogéneas de un único punto de P^n, y dos vectores de coordenadas corresponden al mismo punto si y sólo si se diferencian en un factor constante. Cuando se sobrentienda un sistema de referencia prefijado, identificaremos a cada punto de P^n con su clase de coordenadas homogéneas.

Si consideramos otro sistema de referencia proyectivo $(P_0', \ldots, P_{n+1}')$, la relación entre las coordenadas homogéneas de un mismo punto P respecto a ambos sistemas de referencia es de la forma

$$\begin{array}{rcllll} X_1' & = & a_{11}X_1+ & \cdots & + a_{1n+1}X_{n+1}, \\ \vdots & & \vdots & & \vdots \\ X_{n+1}' & = & a_{n+1\,1}X_1+ & \cdots & + a_{n+1n+1}X_{n+1}, \end{array} \tag{2.3}$$

y cualquier relación de esta forma en la que la matriz de coeficientes (a_{ij}) sea regular se corresponde con un cambio de sistema de referencia.

Un *hiperplano proyectivo* en P^n es un conjunto de la forma

$$H = \{\langle v\rangle \mid v \in W\},$$

donde W es un subespacio de k^{n+1} de dimensión n. Si respecto a la base $v_1, \ldots, v_{n+1}$ asociada a un sistema de referencia proyectivo el subespacio W está formado por los vectores cuyas coordenadas satisfacen la ecuación

$$a_1X_1 + \cdots + a_{n+1}X_{n+1} = 0,$$

entonces H está formado por los puntos de P^n cuyas coordenadas homogéneas en el sistema de referencia dado satisfacen esta misma ecuación. Así mismo, toda ecuación de este tipo (con algún coeficiente no nulo) determina un hiperplano proyectivo en un sistema de referencia dado y, fijado un hiperplano H, siempre podemos elegir un sistema de referencia proyectivo respecto al cual la ecuación de H sea $X_i = 0$.

Fijemos un hiperplano proyectivo arbitrario H_∞ en P^n, al que llamaremos *hiperplano del infinito,* y tomemos un sistema de referencia respecto al cual la ecuación de H_∞ sea $X_i = 0$ (por concretar tomemos $i = n + 1$, pero todo es válido para un i arbitrario). Entonces los puntos de $\mathrm{P}^n \setminus H$ tienen coordenadas homogéneas $(X_1, \ldots, X_{n+1})$ con $X_{n+1} \neq 0$, luego dividiendo entre X_{n+1} vemos que tienen un único vector de coordenadas homogéneas de la forma $(X_1, \ldots, X_n, 1)$. Esto nos permite identificar los puntos de $\mathrm{P}^n \setminus H_\infty$ con k^n y, por consiguiente, considerar a $\mathrm{P}^n \setminus H_\infty$ como un espacio afín n-dimensional.

Fijado un sistema de referencia, el espacio proyectivo P^n está cubierto por los $n+1$ espacios afines A_i formados por los puntos de P^n cuya i-ésima coordenada homogénea es no nula. Cuando consideremos $A^n \subset \mathrm{P}^n$ sin más especificación, se entenderá que A^n es el espacio afín A_{n+1}.

Definimos los conjuntos algebraicos proyectivos de forma paralela e independiente de lo visto en la sección anterior en el caso afín y a continuación veremos la relación que existe entre ambos casos.

Definición 2.17 Si $S \subset k[X_1, \ldots, X_{n+1}]$, llamaremos

$$V(S) = \{P \in \mathrm{P}^n(k) \mid F(P) = 0 \text{ para todo } F \in S\},$$

donde $F(P) = 0$ ha de entenderse como que $F(a_1, \ldots, a_{n+1}) = 0$ para todo vector de coordenadas homogéneas $(a_1, \ldots, a_{n+1})$ de P (en un sistema de referencia dado). Un conjunto $C \subset \mathrm{P}^n(k)$ es *algebraico* si es de la forma $C = V(S)$, para cierto $S \subset k[X_1, \ldots, X_{n+1}]$. El carácter algebraico de un conjunto no depende del sistema de referencia en el que se compruebe.

Como en el caso afín, en los ejemplos concretos determinaremos los conjuntos algebraicos indicando las ecuaciones que los definen.

Recordemos que una *forma* de grado n es un polinomio cuyos monomios tienen todos grado n. Todo polinomio F se descompone de forma única como $F = F_0 + F_1 + F_2 + \cdots$, donde F_i es una forma de grado i. Observemos ahora que $F(P) = 0$ si y sólo si $F_i(P) = 0$ para todo i. En efecto, si $a = (a_1, \ldots, a_{n+1})$ es un vector de coordenadas homogéneas de P y $\lambda \in k$ es no nulo, entonces

$$F(\lambda a) = \sum_i F_i(a)\lambda^i = 0 \quad \text{para todo } \lambda \in k^*.$$

Esto sólo es posible si todos los coeficientes de este polinomio (en λ) son nulos, como queríamos probar. (Aquí usamos que k es infinito.)

Teniendo en cuenta, además, que los anillos de polinomios son noetherianos, vemos que un conjunto algebraico $C = V(S)$ es el conjunto de ceros del ideal generado por S, o también el conjunto de ceros de un número finito de polinomios, o también el conjunto de ceros de un número finito de formas.

Para cada conjunto $C \subset \mathrm{P}^n$, definimos el ideal

$$I(C) = \{F \in k[X_1, \ldots, X_{n+1}] \mid F(P) = 0 \text{ para todo } P \in C\}.$$

Un ideal $I \subset k[X_1, \ldots, X_{n+1}]$ es *homogéneo* si cuando $F \in I$ se descompone en suma de formas $F = F_0 + F_1 + \cdots$, entonces $F_i \in I$ para todo i. Hemos visto que los ideales $I(C)$ son homogéneos.

Teorema 2.18 *Un ideal $I \subset k[X_1, \ldots, X_{n+1}]$ es homogéneo si y sólo si está generado por un conjunto (finito) de formas.*

DEMOSTRACIÓN: Supongamos que $I = (F^1, \ldots, F^r)$, donde cada F^i es una forma. Sea $F \in I$. Entonces $F = \sum_i A^i F^i$, para ciertos polinomios A^i. La forma de menor grado en que se descompone F ha de ser $F_m = \sum_i A^i_{m-d_i} F^i$, donde d_i es el grado de F^i. Por lo tanto $F_m \in I$. Ahora $F - F_m \in I$ y, repitiendo el argumento, llegamos a que todas las formas de F están en I. La otra implicación es obvia. ■

Los resultados proyectivos análogos a los que hemos obtenido en la sección anterior para el espacio afín se siguen fácilmente de éstos a través del concepto de cono de un conjunto. Usaremos I_p, V_p, I_a, V_a para distinguir las correspondencias proyectivas de las afines. Recordemos que P^n está formado por los subespacios de dimensión 1 de k^{n+1}. Si $C \subset \mathrm{P}^n$ es un conjunto algebraico, definimos el *cono* de V como el conjunto $Cn(C)$ de los elementos (en k^{n+1}) de los elementos de C. De este modo, si a través de un sistema de referencia identificamos $A^{n+1} = k^{n+1}$, las coordenadas afines de los puntos de $Cn(C)$ son 0 y las coordenadas homogéneas de los puntos de C.

Así, si $C \subset \mathrm{P}^n$, $C \neq \varnothing$, se cumple $I_a(Cn(C)) = I_p(C)$, y si I es un ideal homogéneo de $k[X_1, \ldots, X_{n+1}]$ tal que $V_p(I) \neq \varnothing$, entonces $Cn(V_p(I)) = V_a(I)$. Veamos una aplicación. (Recordemos que estamos suponiendo que los cuerpos con los que trabajamos son algebraicamente cerrados.)

Teorema 2.19 *Sea I un ideal homogéneo en $k[X_1, \ldots, X_{n+1}]$. Entonces*

a) $V_p(I) = \varnothing$ si y sólo si existe un natural N tal que I contiene a todas las formas de grado $\geq N$.

b) Si $V_p(I) \neq \varnothing$ entonces $I_p(V_p(I)) = \operatorname{Rad} I$.

DEMOSTRACIÓN: a) $V_p(I) = \varnothing$ si y sólo si $V_a(I) \subset \{0\}$, lo que a su vez equivale a que $(X_1, \ldots, X_{n+1}) = I_a(\{0\}) \subset I_a(V_a(I)) = \operatorname{Rad} I$. A su vez, es fácil ver que esto equivale a que $(X_1, \ldots, X_{n+1})^N \subset I$ para algún N.

b) $I_p(V_p(I)) = I_a(Cn(V_p(I)) = I_a(V_a(I)) = \operatorname{Rad} I$. ■

Observemos que los únicos ideales homogéneos radicales que cumplen a) son 1 y $(X_1, \ldots, X_{n+1})$, luego tenemos que V_p e I_p biyectan los conjuntos algebraicos proyectivos con los ideales homogéneos radicales distintos de $(X_1, \ldots, X_{n+1})$. (Podemos admitir a 1 en la biyección entendiendo que $\varnothing = V_p(1)$ es algebraico.)

Definición 2.20 Un conjunto algebraico $C \subset \mathrm{P}^n$ es *reducible* si existen conjuntos algebraicos C_1, C_2 distintos de C y tales que $C = C_1 \cup C_2$. En caso contrario diremos que C es *irreducible*. A los conjuntos algebraicos irreducibles los llamaremos también *variedades proyectivas.*

Dejamos al lector la comprobación de que el teorema 2.6 es válido igualmente para conjuntos algebraicos proyectivos, así como que todo conjunto algebraico se descompone de forma única en unión de un número finito de variedades proyectivas no contenidas unas en otras. Así mismo, un conjunto algebraico $V \neq \varnothing$ es irreducible si y sólo si $I(V)$ es un ideal primo. El argumento es el mismo que en el caso afín, usando además lo siguiente:

Teorema 2.21 *Un ideal homogéneo $I \subsetneq k[X_1, \ldots, X_n]$ es primo si y sólo si para todo par de formas F, G tales que $FG \in I$, o bien $F \in I$ o bien $G \in I$.*

DEMOSTRACIÓN: Supongamos que $F \notin I$ y $G \notin I$. Sea F_m la forma de menor grado de F que no está en I y sea G_n la forma de menor grado de G que no está en I. Entonces

$$(FG)_{mn} = \sum_{u+v=m+n} F_u G_v \in I.$$

Por la elección de m y n, todos los sumandos tienen un factor en I salvo $F_m G_n$, luego $F_m G_n \in I$, en contradicción con la hipótesis. ■

Notemos que los puntos no se corresponden con ideales maximales, pues $I_p(P) = I_a(Cn(P))$ y $Cn(P)$ es una recta que pasa por 0, luego $I_a(Cn(P))$ es un ideal primo, aunque no maximal. Por ejemplo, está contenido estrictamente en el ideal maximal $I_a(0) = (X_1, \ldots, X_{n+1})$.

Como en el caso afín, definimos una *curva proyectiva plana* como un conjunto algebraico de P^2 (irreducible salvo que indiquemos lo contrario) definido por una única ecuación. Así mismo podemos dividir las curvas planas en *rectas, cónicas, cúbicas,* etc. según su grado.

Ahora nos ocupamos la relación entre la geometría afín y la proyectiva. Para ello nos apoyaremos en las siguientes correspondencias entre polinomios y formas:

Definición 2.22 Para cada forma $F \in k[X_1, \ldots, X_{n+1}]$ definimos el polinomio $F_* = F(X_1, \ldots, X_n, 1) \in k[X_1, \ldots, X_n]$. Recíprocamente, si $f \in k[X_1, \ldots, X_n]$ se expresa como $f = f_0 + f_1 + \cdots + f_d$, donde f_i es una forma de grado i, definimos la forma

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + f_d \in k[X_1, \ldots, X_{n+1}].$$

Al paso de f a f^* y de F a F_* lo llamaremos *homogeneizar* un polinomio y *deshomogeneizar* una forma, respectivamente.

El teorema siguiente recoge las propiedades básicas. La prueba es una comprobación rutinaria.

Teorema 2.23 *Sean F y G formas y f y g polinomios. Entonces*

a) $(FG)_* = F_* G_*, \quad (fg)^* = f^* g^*$.

b) $(f^*)_* = f$ *y, si r es la mayor potencia de X_{n+1} que divide a F, entonces* $X_{n+1}^r (F_*)^* = F$.

c) $(F+G)_* = F_* + G_*, \quad X_{n+1}^t (f+g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$, *donde* $r = \operatorname{grad} g$, $s = \operatorname{grad} f$ *y* $t = r + s - \operatorname{grad}(f+g)$.

Consideremos ahora a A^n como subconjunto de P^n, es decir, $A^n = \mathrm{P}^n \setminus H_\infty$, donde H_∞ es el hiperplano del infinito. Sea $X \subset A^n$ un conjunto algebraico. Sea $I = I(X) \subset k[X_1, \ldots, X_n]$. Definimos I^* como el ideal de $k[X_1, \ldots, X_{n+1}]$ generado por las formas f^*, para cada $f \in I$. Definimos la *clausura proyectiva* de X como $X^* = V(I^*) \subset \mathrm{P}^n$.

Recíprocamente, sea ahora $X \subset \mathrm{P}^n$ un conjunto algebraico proyectivo, sea $I = I(X) \subset k[X_1, \ldots, X_{n+1}]$, sea I_* el ideal de $k[X_1, \ldots, X_n]$ generado por los polinomios F_*, para toda forma $F \in I$. Definimos $X_* = V(I_*) \subset A^n$.

En principio estas definiciones dependen del sistema de referencia considerado, pero el teorema siguiente muestra que no es así. Tan sólo dependen de la elección del hiperplano H_∞.

Teorema 2.24 *Se cumplen las propiedades siguientes:*

a) *Si* $C \subset \mathrm{P}^n$, *entonces* $C_* = C \cap A^n$.

b) *Si* $C \subset A^n$, *entonces* $C = C^* \cap A^n$ *y* $(C^*)_* = C$.

c) *Si* $C \subset D \subset A^n$, *entonces* $C^* \subset D^* \subset \mathrm{P}^n$. *Si* $C \subset D \subset \mathrm{P}^n$, *entonces* $C_* \subset D_* \subset A^n$.

d) *Si* $C \subset A^n$, *entonces* C^* *es el menor conjunto algebraico de* P^n *que contiene a* C.

e) *Si* $C \subset A^n$ *es irreducible, entonces* C^* *es irreducible en* P^n.

f) *Si* $C = \bigcup\limits_i V_i \subset A^n$ *es la descomposición de* C *en componentes irreducibles, entonces* $C^* = \bigcup\limits_i V_i^* \subset \mathrm{P}^n$ *es la correspondiente descomposición de* C^*.

g) *Si* $C \subsetneq A^n$, *entonces ninguna componente irreducible de* C^* *está contenida en, o contiene a,* H_∞.

h) *Si* $C \subset \mathrm{P}^n$ *y ninguna componente de* C *está contenida en, o contiene a,* H_∞, *entonces* $C_* \subsetneq A^n$ *y* $(C_*)^* = C$.

Demostración: Observemos que si F es una forma en $k[X_1, \ldots, X_{n+1}]$ y $P \in A^n$, entonces $F(P) = 0$ si y sólo si $F_*(P) = 0$ (donde $F(P)$ es F actuando sobre las coordenadas homogéneas de P y $F_*(P)$ es F_* actuando sobre las coordenadas afines de P).

a) Teniendo esto en cuenta, $P \in C_*$ si y sólo si $F_*(P) = 0$ para toda forma $F \in I(C)$, si y sólo si $P \in A^n$ y $F(P) = 0$ para toda forma $F \in I(C)$, si y sólo si $P \in A^n \cap V(I(C)) = A^n \cap C$.

La primera parte de b) se prueba análogamente (usando que $f(P) = 0$ si y sólo si $f^*(P) = 0$). La segunda es inmediata: $(C^*)_* = C^* \cap A^n = C$. La propiedad c) también es trivial.

d) Sea D un conjunto algebraico tal que $C \subset D \subset \mathrm{P}^n$. Si $F \in I(D)$, entonces $F_* \in I(C)$, luego $F = X_{n+1}^r (F_*)^* \in I(C)^*$. Así pues, $I(D) \subset I(C)^*$, luego $C^* \subset V(I(D)) = D$.

e) Tenemos que $I = V(C)$ es un ideal primo. Observemos que si $F \in I^*$ entonces $F_* \in I$. En efecto, $F = \sum p_i f_i^*$, con $f_i \in I$, luego $F_* = \sum p_{i*} f_i \in I$. Por lo tanto, si $FG \in I^*$, tenemos que $F_* G_* \in I$, luego $F_* \in I$ o $G_* \in I$, y entonces $F = X_{n+1}^r (F_*)^* \in I^*$ o $G \in I^*$. Por consiguiente I^* es primo y $I(C^*) = I(V(I^*)) = I^*$, luego C^* es irreducible.

f) se sigue inmediatamente de c), d), e).

g) De a) y f) se sigue que ninguna componente de C^* está contenida en H_∞. No perdemos generalidad si suponemos que C es irreducible. Si $H_\infty \subset C^*$, entonces $I(C)^* \subset I(C^*) \subset I(H_\infty) = (X_{n+1})$, pero si $0 \neq F \in I(C)$, entonces $F^* \in I(C)^*$, pero $F^* \notin (X_{n+1})$.

h) También podemos suponer que C es irreducible. Basta demostrar que $C \subset (C_*)^*$, pues entonces $C_* \subset C \subset (C_*)^*$ y aplicamos d). A su vez, basta ver que $I(C_*)^* \subset I(C)$. Tomemos $f \in I(C_*) = I(V(I(C)_*)) = \operatorname{Rad} I(C)_*$. Entonces $f^N \in I(C)_*$, para cierto N. Usando el teorema anterior concluimos que $X_{n+1}^r (f^N)^* \in I(C)$, para cierto r, pero $I(C)$ es primo y $X_{n+1} \notin I(C)$, ya que $C \not\subset H_\infty$. Así pues, $f^* \in I(V)$. ■

Respecto a g) y h), conviene observar que la única variedad proyectiva que contiene a H_∞ es P^n, pues si $H_\infty \subset V$, entonces $I(V) \subset (X_{n+1})$, pero esto es imposible, pues si $F \in I(V)$, entonces $F = X_{n+1}^r G$, donde $G \notin (X_{n+1})$ y $r \geq 1$, lo cual contradice que $I(V)$ sea primo.

En particular, las variedades afines se corresponden biunívocamente con las variedades proyectivas no contenidas en el hiperplano infinito.

Ejemplo Un error muy frecuente es creer que $(f_1, \ldots, f_n)^* = (f_1^*, \ldots, f_n^*)$. Para ver que esto es falso en general basta considerar $V = V(Y - X^2, Y + X^2)$, que claramente es el punto $(0, 0)$, luego su clausura proyectiva es $(0, 0, 1)$. Sin embargo, $V(YZ - X^2, YZ + X^2) = \{(0, 0, 1), (0, 1, 0)\}$. ■

Ejercicio: Demostrar que si $F \in k[X_1, \ldots, X_n]$, entonces $V(F)^* = V(F^*)$.

Ejemplo En la práctica —cuando no haya confusión— identificaremos cada variedad afín con su clausura proyectiva. Así, por ejemplo, si decimos que la parábola $Y = X^2 + 1$ tiene un punto en el infinito hay que entender que su clausura proyectiva, dada por $YZ = X^2 + Z^2$, corta a la recta infinita $Z = 0$ en un único punto. Ciertamente, éste es $(0, 1, 0)$.

Si ahora consideramos como recta infinita la recta $Y = 0$, la parte finita de la curva pasa a ser $Z = X^2 + Z^2$, que es una elipse. Como curva en $\mathbb{R}^2$ tiene todos sus puntos finitos, si bien en $\mathbb{C}^2$ corta a la recta del infinito en dos puntos imaginarios. ■

Ejemplo Más en general, una cónica (no necesariamente irreducible) en P^2 está determinada por una forma cuadrática $F(X, Y, Z) = 0$. Esta ecuación puede expresarse matricialmente como $(X, Y, Z)A(X, Y, Z)^t = 0$, donde A es una matriz simétrica. Es conocido que toda matriz simétrica de rango r sobre un cuerpo de característica distinta de 2 es congruente con una matriz con todos sus coeficientes nulos salvo r unos en la diagonal. Congruente quiere decir que existe una matriz regular M tal que MAM^t tiene la forma indicada. Esto se traduce en que el cambio de coordenadas determinado por M transforma una cónica arbitraria en otra cuya ecuación es una de las siguientes:

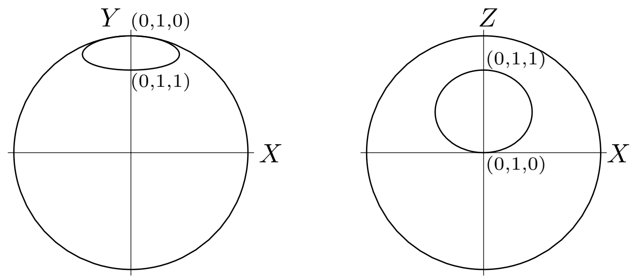
$$X^2 = 0, \qquad X^2 + Y^2 = 0, \qquad X^2 + Y^2 + Z^2 = 0.$$

Las dos primeras son claramente reducibles, mientras que la última es irreducible (ha de serlo, pues existen cónicas irreducibles). Así pues, todas las cónicas (irreducibles) admiten en un cierto sistema de referencia la ecuación $X^2 + Y^2 + Z^2 = 0$. ■

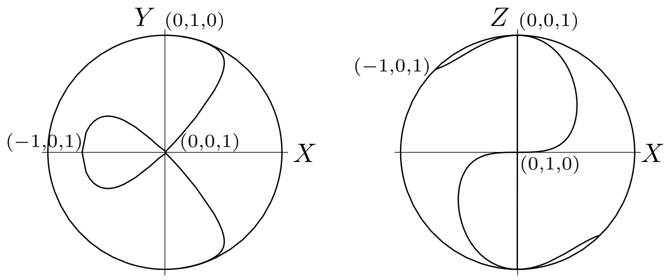
Ejemplo Veamos otra prueba de la irreducibilidad de la curva V dada por $Y^2 = X^3$ (comparar con el ejemplo de la página 62). Tenemos que su clausura proyectiva V^* es $Y^2Z = X^3$ y deshomogeneizando respecto de Y obtenemos el polinomio $Z - X^3$. Como $Z = X^3$ es irreducible (por ser una gráfica), concluimos que su clausura proyectiva también es irreducible, pero ésta es V^*, luego V también es irreducible. ■

Ejemplo Una forma de visualizar el plano proyectivo completo $\mathrm{P}^2(\mathbb{R})$ es la siguiente: identificamos cada punto con la terna de coordenadas homogéneas $(X, Y, Z) \in \mathbb{R}^3$ de norma euclídea 1 y $Z \geq 0$. Esto nos da un único punto de la semiesfera unidad, excepto para los puntos infinitos (con $Z = 0$) para los que tenemos dos posibilidades (dos puntos antípodas en el ecuador de la esfera). Después podemos proyectar ortogonalmente esta terna sobre el plano XY, con lo que tenemos una correspondencia entre el plano proyectivo y el círculo unidad, biyectiva salvo por que cada punto infinito se corresponde con dos puntos opuestos de la circunferencia unidad.

Por ejemplo, las dos figuras siguientes muestran la curva $Y = X^2 + 1$, de modo que se ve claramente que la diferencia entre una parábola y una elipse es simplemente una cuestión de punto de vista (proyectivo). La parábola corresponde al punto de vista de la izquierda, donde uno de los puntos está en la circunferencia unidad, mientras que la elipse corresponde al punto de vista de la derecha.



Las figuras siguientes muestran dos vistas de la curva “alfa” $Y^2 = X^2(X+1)$ (ver la figura de la página 55).



Su clausura proyectiva es $Y^2Z = X^2(X + Z)$. Las dos ramas infinitas de la “alfa” se unen en el punto infinito $(0, 1, 0)$, que se vuelve finito si tomamos como recta infinita $Y = 0$. La parte finita es entonces la curva $Z = X^3 + ZX^2$, que también puede verse como la gráfica de la función

$$Z = \frac{X^3}{1 - X^2}.$$

Ahora hay dos puntos infinitos, que son el $(0, 0, 1)$ y el $(-1, 0, 1)$ (que se corresponden con las asíntotas de la función anterior). ■

Para definir el cuerpo de funciones racionales de una variedad proyectiva conviene probar primero lo siguiente:

Teorema 2.25 *Sea I un ideal homogéneo de $k[X_1, \ldots, X_{n+1}]$ y consideremos el anillo $A = k[X_1, \ldots, X_{n+1}]/I$. Entonces todo $f \in A$ se expresa de forma única como $f = f_0 + \cdots + f_m$, donde f_i es la clase de una forma de grado i.*

DEMOSTRACIÓN: Sólo hay que probar la unicidad. Si $f = g_0 + \cdots + g_r$ es otra descomposición, sean $f_i = [F_i]$, $g_i = [G_i]$. Entonces $\sum(F_i - G_i) \in I$ y, al ser homogéneo, $F_i - G_i \in I$, lo que prueba que $f_i = g_i$. ■

En particular, en un cociente A de este tipo podemos llamar *formas* de grado i a las clases de formas de grado i, de modo que una misma clase no puede ser una forma de dos grados distintos.

Sea $V \subset \mathrm{P}^n(k)$ una variedad proyectiva. Fijado un sistema de referencia proyectivo, definimos $k_h[V] = k[X_1, \ldots, X_{n+1}]/I(V)$. Se trata de un dominio íntegro, pero sus clases no determinan funciones sobre V y mucho menos los elementos de su cuerpo de cocientes. Ahora bien, si $f = [F]$ y $g = [G]$ son dos formas del mismo grado en $k_h[V]$, entonces F/G determina una función sobre los puntos de V donde G no se anula, pues $F(P)/G(P)$ no depende de las coordenadas homogéneas de P con que calculemos el cociente. Así mismo, esta función tampoco se altera si cambiamos F o G por formas equivalentes (con tal de que el denominador no se anule). En otras palabras, que la función F/G depende únicamente de las clases f y g. Más aún, depende únicamente del elemento f/g del cuerpo de cocientes de $k_h[V]$.

Definición 2.26 Sea $V \subset \mathrm{P}^n(k)$ una variedad proyectiva. Definimos el *cuerpo de funciones racionales* de V como el subcuerpo $k(V)$ del cuerpo de cocientes de $k_h[V]$ formado por los cocientes de formas del mismo grado (más el 0).

Si $\alpha \in k(V)$ y $P \in V$, diremos que α es *regular* o que está definida en P si $\alpha = f/g$, con $f, g \in k_h[V]$ y $g(P) \neq 0$. (Notemos que $g(P)$ no está bien definido, pero la condición $g(P) \neq 0$ sí lo está.) En tal caso, el valor $\alpha(P) = f(P)/g(P)$ está bien definido. En caso contrario diremos que α es *singular* en P o que P es una *singularidad* de α. Si $P \in V$, definimos el *anillo local* $\mathcal{O}_P(V)$ como el conjunto de las funciones de $k(V)$ regulares en P.

El mismo argumento que en el caso afín prueba que los elementos de $k(V)$ pueden identificarse con las funciones que definen. En principio, la definición de $k(V)$ depende de la elección de un sistema de referencia proyectivo. No obstante, ahora es fácil ver que sus elementos (considerados como funciones) no dependen de dicha elección.

El teorema siguiente muestra que al tomar la clausura proyectiva de una variedad afín el cuerpo de funciones racionales que obtenemos es esencialmente el mismo de la variedad de partida.

Teorema 2.27 *Sea V una variedad afín y sea V^* su clausura proyectiva. Entonces la restricción a V determina un k-isomorfismo de $k(V^*)$ en $k(V)$. Para cada punto $P \in V$, el anillo $\mathcal{O}_P(V^*)$ se transforma en $\mathcal{O}_P(V)$.*

Demostración: Fijado un sistema de referencia proyectivo, una función racional f de V^* está determinada por dos formas F y G del mismo grado. Claramente, su restricción a V viene dada (en términos de las coordenadas afines de los puntos de V) por F_*/G_*, luego ciertamente dicha restricción es una función racional sobre V. Es fácil ver que esta aplicación no depende de la elección de F y G. Así mismo es claro que se trata de un homomorfismo. Basta ver que es suprayectivo, pero es que si $[F]/[G]$ es cualquier función racional en V y, digamos, $\operatorname{grad} F = \operatorname{grad} G + r$, entonces las formas F^* y $X_{n+1}^r G^*$ determinan una función racional de V^* cuya restricción a V es $[F]/[G]$. Si $\operatorname{grad} F < \operatorname{grad} G$ multiplicamos F^* por la potencia adecuada de X_{n+1}. ■

Ejemplo Sea V la parábola $X = Y^2$ y sea V^* su clausura proyectiva, determinada por la ecuación $XZ = Y^2$. Sabemos que $k(V^*) \cong k(V) \cong k(x)(\sqrt{x})$. La función racional

$$\alpha = \frac{x\sqrt{x}}{\sqrt{x}-1},$$

(donde $\sqrt{x} = y$), se corresponde con la función racional

$$\alpha^* = \frac{xy}{yz - z^2}.$$

■

2.3 Variedades cuasiproyectivas

Si bien los resultados globales de la geometría algebraica se aplican a las variedades proyectivas, las variedades afines son una herramienta muy útil para obtener resultados locales. Más en general, conviene introducir una noción más general de variedad que incluya tanto las variedades afines, como las proyectivas, como los conjuntos que resultan de eliminar un conjunto algebraico en una variedad. Esto nos permitirá descartar, por ejemplo, las singularidades de una función racional. Para ello necesitamos definir una topología en los espacios proyectivos:

Definición 2.28 Llamaremos *topología de Zariski* en P^n a la topología que tiene por cerrados a los conjuntos algebraicos. En lo sucesivo consideraremos a todos los subconjuntos de P^n como espacios topológicos con esta topología.

El teorema 2.6 prueba que, efectivamente, los conjuntos algebraicos determinan una topología. Ahora, bien, hemos de tener presente en todo momento que no cumple la propiedad de Hausdorff. Concretamente, si $V \subset \mathrm{P}^n$ es una variedad y U_1, U_2 son abiertos en V no vacíos, entonces $U_1 \cap U_2 \neq \varnothing$, pues en caso contrario podríamos descomponer V en unión de dos subconjuntos algebraicos propios: $V = (V \setminus U_1) \cup (V \setminus U_2)$. Así pues, ningún par de puntos en una variedad puede tener entornos disjuntos. Más aún, con esto hemos probado que todo abierto no vacío en una variedad corta a cualquier otro abierto no vacío, es decir, es denso.

Llamaremos *variedades cuasiproyectivas* (o, simplemente, variedades) a los subconjuntos abiertos de las variedades proyectivas.

En particular, todas las variedades proyectivas son variedades. Más concretamente, las variedades proyectivas son las variedades cerradas (en P^n). En efecto, si V es una variedad cerrada, entonces es abierto en una variedad proyectiva W y, al ser denso y cerrado, de hecho $V = W$.

Más aún, si V es una variedad, entonces $\overline{V}$ es una variedad (proyectiva). En efecto, V es abierto en una variedad proyectiva W, pero entonces es denso en W, el cual es cerrado en P^n, luego $W = \overline{V}$.

Dicho de otro modo: hemos definido una variedad V como un abierto en una variedad proyectiva. Ahora acabamos de ver que la única variedad proyectiva en la cual V es abierto es $\overline{V}$.

Las variedades afines también son variedades. En efecto, en primer lugar observamos que A^n puede identificarse con un abierto en P^n, luego los espacios afines son variedades. En general, si V es una variedad afín entonces V^* es una variedad proyectiva y $V = V^* \cap A^n$ es abierto en V^*, luego V es una variedad en el sentido que acabamos de introducir. Más aún, tenemos que $V^* = \overline{V}$.

Observemos que si C es un conjunto algebraico en A^n, entonces $C = C^* \cap A^n$ y C^* es cerrado en P^n, luego C es cerrado en A^n. Recíprocamente, todo cerrado en A^n es algebraico. Así pues, podemos definir directamente la topología de Zariski en A^n como la que tiene por cerrados a los conjuntos algebraicos, sin hacer referencia a ninguna inmersión de A^n en P^n.

Trivialmente, todo abierto en una variedad es una variedad. Un cerrado C en una variedad V es una variedad si y sólo si no se puede descomponer como unión de dos subconjuntos cerrados propios. En efecto, tenemos que

$$C = V \cap \overline{C} = A \cap \overline{V} \cap \overline{C} = A \cap \overline{C},$$

donde A es abierto en P^n, luego C es abierto en $\overline{C}$. Por lo tanto C es una variedad si y sólo si lo es $\overline{C}$, es decir, si y sólo si $\overline{C}$ es irreducible, y es fácil comprobar que $\overline{C}$ es unión de cerrados si y sólo si lo es C.

Conviene tener presente que una variedad en sentido general es "casi lo mismo" que una variedad proyectiva: si una variedad proyectiva "típica" es una esfera, una variedad cuasiproyectiva típica puede ser una esfera menos una circunferencia y menos tres puntos. La esfera completa se recupera al tomar la clausura de la variedad.

El hecho de que los anillos de polinomios son noetherianos (el teorema de Hilbert) se traduce en que las variedades satisfacen la propiedad de compacidad (salvo por que no son espacios de Hausdorff):

Teorema 2.29 *Todo cubrimiento por abiertos de una variedad admite un subcubrimiento finito.*

DEMOSTRACIÓN: Equivalentemente, hemos de probar que si una familia $\{C_i\}_{i\in I}$ de cerrados en una variedad $V \subset \mathrm{P}^n$ tiene intersección vacía, entonces una subfamilia finita tiene también intersección vacía. Más en general, probaremos que existe un conjunto finito $I_0 \subset I$ tal que

$$\bigcap_{i\in I} C_i = \bigcap_{i\in I_0} C_i.$$

Cambiando cada C_i por su clausura en P^n, podemos suponer que los C_i son cerrados en P^n. Sea $I_i = I(C_i)$ y sea I el ideal de $k[X_1,\ldots,X_{n+1}]$ generado por la unión de los I_i. Por el teorema de Hilbert I es un ideal finitamente generado, digamos $I = (F_1,\ldots,F_r)$, y las formas F_j pueden obtenerse como suma de múltiplos de un número finito de formas de un número finito de ideales I_i, digamos con $i \in I_0$. Así, si $P \in \bigcap\limits_{i\in I_0} C_i$ tenemos que $F_j(P) = 0$, para $j = 1,\ldots,r$. Si $F \in I_i$, entonces F se expresa como suma de múltiplos de las formas F_j, luego $F(P) = 0$, luego $P \in V(I_i) = C_i$. Así $P \in \bigcap\limits_{i\in I} C_i$. ■

El teorema 2.27 nos permite identificar las funciones racionales de una variedad afín con las de su clausura proyectiva. Generalizaremos este hecho definiendo las funciones racionales de una variedad arbitraria como las de su clausura:

Definición 2.30 Si V es una variedad, definimos el cuerpo de las *funciones racionales* en V como $k(V) = k(\overline{V})$. Para cada punto $P \in V$ definimos el anillo local $\mathcal{O}_P(V) = \mathcal{O}_P(\overline{V})$. El anillo de las *funciones regulares* en V es

$$k[V] = \bigcap_{P\in V} \mathcal{O}_P(V).$$

Si V es una variedad afín o proyectiva, estos conceptos coinciden con los que ya teníamos definidos. En realidad, para que estas definiciones resulten razonables, es necesario justificar que podemos considerar a los elementos de $k[V]$ como funciones sobre V (en principio son funciones en $\overline{V}$). Esto es consecuencia inmediata del teorema siguiente:

Teorema 2.31 *Si V es una variedad y $\alpha \in k[V]$ una función que se anule en todo punto de V. Entonces $\alpha = 0$.*

DEMOSTRACIÓN: Supongamos que existe $P \in \overline{V}$ tal que $\alpha(P) \neq 0$. Entonces $\alpha = f/g$, donde f y g son formas del mismo grado tales que $f(P) \neq 0 \neq g(P)$. El conjunto $W = \{Q \in \overline{V} \mid f(Q) \neq 0 \neq g(Q)\}$ es abierto, luego corta a V, y α no se anula en los puntos de la intersección. ■

Para terminar de perfilar el comportamiento de las funciones racionales sobre una variedad generalizamos el teorema 2.15.

Teorema 2.32 *El conjunto de las singularidades de una función racional sobre una variedad es un conjunto cerrado.*

DEMOSTRACIÓN: Sea V una variedad. Toda función racional sobre V se extiende (por definición) a una función sobre $\overline{V}$ y el conjunto de singularidades en V es la intersección con V del conjunto de singularidades de la extensión. Por lo tanto podemos trabajar con $\overline{V}$, es decir, suponer que V es cerrada. El espacio P^n está cubierto por $n+1$ espacios afines abiertos A_i. Si C es el conjunto de las singularidades de una función racional en V, entonces $C \cap A_i$ es el conjunto de las singularidades de su restricción a $V \cap A_i$, que es cerrado en A_i por el teorema 2.15. Por lo tanto, $\mathrm{P}^n \setminus C$, que es la unión de los conjuntos $A_i \setminus (C \cap A_i)$, es abierto, y C es cerrado. ■

Así pues, si V es una variedad, cada función racional de V es regular en un abierto U, de modo que $k(V)$ es la unión de los anillos $k[U]$, donde U recorre los abiertos de V. Similarmente, si $P \in V$, el anillo $\mathcal{O}_P(V)$ es la unión de los anillos $k[U]$, donde U varía en los entornos de P.

Nos ocupamos ahora de las aplicaciones entre variedades. Debido a que la topología de Zariski no es de Hausdorff, las aplicaciones continuas no tienen un comportamiento muy satisfactorio. Sin embargo, si a la continuidad le añadimos un requisito más, obtenemos el concepto de aplicación regular, y veremos que las aplicaciones regulares entre variedades se comportan como las aplicaciones continuas entre espacios de Hausdorff.

Definición 2.33 Una aplicación $\phi : V \longrightarrow W$ entre dos variedades es *regular* si es continua y para todo abierto U de W tal que $\phi[V] \cap U \neq \varnothing$ y toda función $\alpha \in k[U]$, se cumple que $\overline{\phi}(\alpha) = \phi \circ \alpha \in k[\phi^{-1}[U]]$. La aplicación ϕ es un *isomorfismo* si es biyectiva y tanto ϕ como ϕ^{-1} son regulares.

Notemos que una definición alternativa es la siguiente: ϕ es regular si es continua y para todo $P \in V$ y toda $\alpha \in \mathcal{O}_{\phi(P)}(W)$ se cumple que $\overline{\phi}(\alpha) \in \mathcal{O}_P(V)$.

Ejemplo Sea A una matriz regular de dimensión $n+1$ y —fijado un sistema de referencia— sea $\phi : \mathrm{P}^n \longrightarrow \mathrm{P}^n$ la aplicación dada por $\phi(X) = XA$. Claramente ϕ está bien definida (no depende de la elección de coordenadas homogéneas y nunca da el vector nulo) y se cumple que es regular. En efecto, si $C \subset \mathrm{P}^n$ es un conjunto algebraico, tenemos que $X \in \phi^{-1}[C] \leftrightarrow XA \in C \leftrightarrow F(XA) = 0$, para toda forma $F \in I(C)$. Así pues, $\phi^{-1}[C]$ es el conjunto algebraico determinado por las formas $F(XA)$, donde $F \in I(C)$. Esto prueba que ϕ es continua. Similarmente, si $P \in \mathrm{P}^n$ tiene coordenadas a, una función $\alpha \in \mathcal{O}_{\phi(P)}(\mathrm{P}^n)$ es de la forma $\alpha = F(X)/G(X)$, donde F y G son formas del mismo grado y $G(aA) \neq 0$, y $\bar{\phi}(\alpha) = F(XA)/G(XA)$ también es un cociente de formas del mismo grado y el denominador no se anula en a. Por consiguiente $\bar{\phi}(\alpha) \in \mathcal{O}_P(\mathrm{P}^n)$.

Las aplicaciones ϕ de este tipo se llaman *transformaciones proyectivas* de P^n. Es claro que son biyectivas, y que la inversa de una transformación proyectiva es de nuevo una transformación proyectiva. Por lo tanto las transformaciones proyectivas son isomorfismos de P^n en sí mismo. De hecho, forman un grupo con la composición.

Se dice que dos variedades de P^n son *proyectivamente equivalentes* si una es la imagen de la otra por una transformación proyectiva. En particular esto implica que son isomorfas. Es fácil ver que dos variedades son proyectivamente equivalentes si y sólo si pueden definirse con las mismas ecuaciones respecto de dos sistemas de referencia.

Por ejemplo, en la página 73 hemos visto que todas las cónicas (sobre un cuerpo de característica distinta de 2) son proyectivamente equivalentes, y en particular isomorfas. ■

Es fácil ver que la composición de aplicaciones regulares es regular, así como que la regularidad es una propiedad local, es decir, una aplicación es regular si y sólo si lo es su restricción a un entorno abierto de cada punto. Toda aplicación regular $\phi : V \longrightarrow W$ induce un k-homomorfismo de anillos $\overline{\phi} : k[W] \longrightarrow k[V]$. Si ϕ es un isomorfismo entonces $\overline{\phi}$ también lo es. Ahora probamos que la regularidad generaliza la noción de aplicación polinómica.

Teorema 2.34 *Si V y W son variedades afines, una aplicación $\phi : V \longrightarrow W$ es regular si y sólo si es polinómica.*

Demostración: Si ϕ es polinómica, fijados dos sistemas de referencia, $\phi(P) = (F_1(P), \ldots, F_n(P))$, para ciertos polinomios F_i. Si $C \subset W$ es un subconjunto algebraico de W, entonces $P \in \phi^{-1}[C]$ si y sólo si $\phi(P) \in C$, si y sólo si $F(\phi(P)) = 0$, para toda $F \in I(C)$. Las funciones $\phi \circ F$ son polinomios, y C es el conjunto de ceros de todos ellos. Por lo tanto C es algebraico. Esto prueba la continuidad de ϕ.

Si U es abierto en W y $\alpha \in k[U]$, entonces α es una función racional definida en todos los puntos de U. Digamos que $\alpha = [F]/[G]$, donde F, G son polinomios. Sea $\overline{\alpha} = [\phi \circ F]/[\phi \circ G] \in k(V)$. Vamos a ver que $\overline{\alpha}$ está definida en $\phi^{-1}[U]$ y que sobre sus puntos $\overline{\alpha} = \phi \circ \alpha$. Esto probará que $\overline{\phi}(\alpha) = \overline{\alpha}$.

En efecto, si $P \in \phi^{-1}[U]$, entonces α está definida en $\phi(P)$, luego podemos expresar $\alpha = [F']/[G']$, con $G'(\phi(P)) \neq 0$. Así, $FG' - GF' \in I(W)$, luego $(\phi \circ F)(\phi \circ G') - (\phi \circ G)(\phi \circ F') \in I(V)$, y por consiguiente $\overline{\alpha} = [\phi \circ F']/[\phi \circ G']$ está definida en P y $\overline{\alpha}(P) = \alpha(\phi(P))$.

Sea ahora $\phi : V \longrightarrow W$ una función regular. Por el teorema 2.13, existe una función polinómica $\psi : V \longrightarrow W$ tal que $\overline{\phi} = \overline{\psi}$. De aquí se sigue que $\phi = \psi$, pues, al igual que ψ, la función ϕ cumple $\overline{\phi}^{-1}[I_V(P)] = I_W(\phi(P))$. ■

Si V es una variedad, hemos llamado a $k[V]$ el anillo de las funciones regulares en V. Este nombre es consistente con la definición general que hemos dado de función regular. En efecto:

Teorema 2.35 *Si V es una variedad, entonces el anillo $k[V]$ está formado por todas las funciones regulares $\alpha : V \longrightarrow A^1$.*

Demostración: Si α es regular, como la identidad $I : A^1 \longrightarrow A^1$ cumple $I \in k[A^1]$, la definición de función regular nos da que $\alpha = \alpha \circ I \in k[V]$.

Recíprocamente, si $\alpha \in k[V]$, basta probar la regularidad de su restricción a un entorno de cada punto $P \in V$. Dado P, tenemos que $\alpha = [F]/[G]$, donde F y G son formas del mismo grado con $G(P) \neq 0$. Sea

$$U = \{Q \in V \mid G(Q) \neq 0\}.$$

Basta probar que α es regular en U. Para puntos $Q \in U$, tenemos que $\alpha(Q) = F(Q)/G(Q)$. La continuidad de α es clara, pues es fácil ver que los únicos cerrados no vacíos en A^1 distintos de todo A^1 son los conjuntos finitos, con lo que basta ver que si $a \in A^1$ entonces $\alpha^{-1}[a]$ es cerrado, pero

$$\alpha^{-1}[a] = \{Q \in U \mid F(Q) - aG(Q) = 0\}.$$

Por otra parte, si $\alpha(Q) = a$ y $\beta \in \mathcal{O}_a(A^1)$, entonces $\beta = F'/G'$, donde F' y G' son polinomios tales que $G'(a) \neq 0$. La composición $\alpha \circ \beta$ es claramente una función racional cuyo denominador no se anula en Q, luego $\alpha \circ \beta \in \mathcal{O}_Q(U)$.

■

Veamos una última propiedad adicional de interés:

Teorema 2.36 *Las inclusiones entre variedades son aplicaciones regulares. Una aplicación $\phi : V \longrightarrow W$ con $W \subset \mathrm{P}^n$ es regular si y sólo si lo es como aplicación $\phi : V \longrightarrow \mathrm{P}^n$.*

Demostración: Sea $i : V \longrightarrow W$ una aplicación de inclusión. Obviamente es continua. Tomemos $\alpha \in \mathcal{O}_P(W)$. Hemos de probar que $\alpha|_V \in \mathcal{O}_P(V)$, pero $\alpha = [F]/[G]$, donde F y G son formas del mismo grado y $G(P) \neq 0$. La restricción a V admite esta misma representación considerando las clases módulo $I(V)$ en lugar de módulo $I(W)$, lo cual prueba que $\alpha|_V \in \mathcal{O}_P(V)$.

Respecto a la segunda afirmación, si ϕ es regular como aplicación en W, lo es como aplicación en P^n porque la inclusión $W \longrightarrow \mathrm{P}^n$ es regular. Supongamos ahora que ϕ es regular como aplicación en P^n. Entonces es continua, y también lo es como aplicación en W. Sea $P \in V$ y tomemos $\alpha \in \mathcal{O}_{\phi(P)}(W)$. Entonces $\alpha = [F]/[G]$ es un cociente de dos clases de formas módulo $I(W)$. Dichas formas determinan una función racional $\beta \in \mathcal{O}_{\phi(P)}(\mathrm{P}^n)$ que coincide con α en un entorno de $\phi(P)$ en W (donde $G \neq 0$). Por consiguiente $\phi \circ \alpha$ coincide con $\phi \circ \beta$ en un entorno de P en V. Por hipótesis $\phi \circ \beta \in \mathcal{O}_P(V)$, luego lo mismo vale para $\overline{\phi}(\alpha) = \phi \circ \alpha$. Esto prueba que ϕ es regular como aplicación en W.

■

En este punto conviene generalizar levemente los conceptos de variedad afín y proyectiva:

Definición 2.37 Llamaremos *variedades afines (proyectivas)* a las variedades isomorfas a variedades afines (proyectivas).

Así, cuando digamos que $V \subset A^n$ es una variedad afín deberá entenderse que es una variedad afín en el sentido usual (una variedad cerrada en A^n), mientras que si hablamos de una variedad afín V se entenderá en este sentido general. El interés de este concepto se debe a que, como veremos enseguida, todo punto de una variedad tiene una base de entornos formada por variedades afines en este sentido.

Si V es una variedad afín, llamaremos *abiertos principales* de V a los conjuntos $V_\alpha = \{P \in V \mid \alpha(P) \neq 0\}$, donde $\alpha \in k[V]$ es una función regular no nula.

A continuación vemos que los abiertos principales son realmente abiertos:

Teorema 2.38 *Sea V una variedad afín y $\alpha \in k[V]$, $\alpha \neq 0$. Entonces el abierto principal V_α es una variedad abierta en V. Se cumple que*

$$k[V_\alpha] = k[V][1/\alpha] = \{\beta/\alpha^n \mid \beta \in k[V],\ n \in \mathbb{Z}\}.$$

Además V_α es una variedad afín.

DEMOSTRACIÓN: No perdemos generalidad si suponemos que $V \subset A^n$. Ciertamente V_α es una variedad, pues, si $P \in V_\alpha$, entonces $\alpha = [F]/[G]$, donde F y G son polinomios tales que $F(P) \neq 0 \neq G(P)$. Por lo tanto el conjunto

$$W = \{Q \in V \mid F(Q) \neq 0 \neq G(Q)\}$$

es un entorno de P contenido en V_α.

En principio, $k[V_\alpha] \subset k(\overline{V}_\alpha) = k(\overline{V})$, pero por 2.27 podemos identificar a $k[V_\alpha]$ con el anillo de las restricciones a V de sus elementos, de modo que $k[V_\alpha] \subset k(V)$. Tomemos $\gamma \in k[V_\alpha]$. En la demostración del teorema 2.15 hemos visto que el conjunto de las singularidades de γ es $V(I_\gamma)$, donde

$$I_\gamma = \{G \in k[X_1, \ldots, X_n] \mid [G]\gamma \in k[V]\}.$$

Si $\alpha = [F]$, tenemos que γ está definida en los puntos donde F no se anula, luego $V(I_\gamma) \subset V(F)$, luego $I(V(F)) \subset \operatorname{Rad} I_\gamma$. Por consiguiente $F^N \in I_\gamma$, para cierto N, es decir, $\alpha^N\gamma = \beta \in k[V]$. Esto prueba la inclusión $k[V_\alpha] \subset k[V][1/\alpha]$. La otra es obvia.

Falta probar que V_α es isomorfa a una variedad afín. Para ello consideramos el ideal I' de $k[X_1, \ldots, X_{n+1}]$ generado por $I(V)$ y por el polinomio $X_{n+1}F - 1$. Definimos $\psi : k[X_1, \ldots, X_{n+1}] \longrightarrow k[V_\alpha]$ mediante $\psi(X_i) = [X_i]$ para $i \leq n$ y $\psi(X_{n+1}) = 1/\alpha$. Según lo que acabamos de probar, ψ es un epimorfismo de anillos. Es claro que su núcleo contiene a I', luego induce un epimorfismo $\overline{\psi} : k[X_1, \ldots, X_{n+1}]/I' \longrightarrow k[V_\alpha]$.

Llamemos A al subanillo del cociente formado por las clases con un representante en $k[X_1, \ldots, X_n]$. Entonces $\bar{\psi}$ se restringe a un isomorfismo $A \longrightarrow k[V]$.

Sólo hay que comprobar la inyectividad: si $\bar{\psi}([G]) = 0$, entonces $G \in I(V_\alpha)$, luego $GF \in I(V)$, pero $F \notin I(V)$ (porque $\alpha = [F] \neq 0$), luego $G \in I(V) \subset I'$ y así $[G] = 0$.

El dominio de $\overline{\psi}$ es la adjunción a A de la clase $[X_{n+1}]$, la imagen es $k[V][1/\alpha]$ y $\overline{\psi}([X_{n+1}]) = 1/\alpha$. Es fácil ver entonces que $\overline{\psi}$ es un isomorfismo.

En particular concluimos que I' es un ideal primo, luego define una variedad afín $V' = V(I') \subset A^{n+1}$, de modo que $\overline{\psi} : k[V'] \longrightarrow k[V_\alpha]$. La proyección $A^{n+1} \longrightarrow A^n$ en las n primeras componentes es claramente una aplicación regular, que se restringe a una aplicación regular $\phi : V' \longrightarrow V_\alpha$. Esta aplicación es biyectiva pues, si $P \in V_\alpha$, su única antiimagen se obtiene completando sus coordenadas con $1/F(P)$. Falta probar que ϕ^{-1} es regular.

Para ello consideramos $V' \subset \mathrm{P}^{n+1}$. Según hemos visto,

$$\begin{aligned}\phi^{-1}(a_1,\ldots,a_n) &= (a_1,\ldots,a_n,F^{-1}(a_1,\ldots,a_n),1)\\ &= (a_1F(a_1,\ldots,a_n),\ldots,a_nF(a_1,\ldots,a_n),1,F(a_1,\ldots,a_n)).\end{aligned}$$

Ahora consideramos a V' contenido en el espacio afín determinado por $X_{n+1} \neq 0$, con lo que la expresión para ϕ^{-1} es

$$\phi^{-1}(a_1,\ldots,a_n) = (a_1F(a_1,\ldots,a_n),\ldots,a_nF(a_1,\ldots,a_n),F(a_1,\ldots,a_n)).$$

Vemos que es una aplicación polinómica, luego es regular. ■

Con esto podemos probar lo que habíamos anunciado:

Teorema 2.39 *Todo punto de una variedad tiene una base de entornos (abiertos) formada por variedades afines.*

DEMOSTRACIÓN: Sea $V \subset \mathrm{P}^n$ una variedad, $P \in V$ y U un entorno (abierto) de P. Sea A^n un espacio afín que contenga a P. No perdemos generalidad si sustituimos V por $\overline{V} \cap A^n$, con lo que V es una variedad afín. Como $P \notin V \setminus U$, y éste es un subconjunto algebraico de A^n, existe un polinomio $F \in I(V \setminus U)$ tal que $F(P) \neq 0$. Sea $\alpha = [F] \in k[V]$. Entonces $P \in V_\alpha \subset U$ y, por el teorema anterior, V_α cumple lo pedido. ■

2.4 Producto de variedades

Es claro que podemos considerar como variedad afín a cualquier producto de variedades afines sin más que identificar $A^m \times A^n$ con A^{m+n} de forma natural. De todos modos, debemos advertir que la topología de Zariski en el producto obtenida por esta identificación no es la topología producto. El caso es que nos gustaría generalizar esto a variedades cualesquiera, no necesariamente afines. Para ello introducimos el concepto siguiente:

Definición 2.40 Sean m y n números naturales no nulos. Llamemos $N = (m+1)(n+1) - 1$. Fijamos un sistema de referencia en $\mathrm{P}^N(k)$ y consideramos las coordenadas homogéneas de cada punto como una matriz (X_{ij}) de orden $(m+1)\times(n+1)$. Definimos la *variedad de Segre* $m\times n$ como el subconjunto $S_{m,n}$ de P^N formado por los puntos que satisfacen las ecuaciones

$$X_{i,j}X_{k,l} = X_{k,j}X_{i,l}.$$

Notemos que estas ecuaciones expresan que todas las submatrices 2×2 de la matriz de coordenadas de los puntos de $S_{m,n}$ tienen determinante nulo, es decir, que $S_{m,n}$ está formado por los puntos cuya matriz de coordenadas homogéneas tiene rango 1.

La definición que hemos dado depende del sistema de referencia, pero es claro que dos variedades de Segre $m\times n$ son isomorfas. La propia definición muestra que $S_{m,n}$ es un conjunto algebraico. Para justificar su nombre hemos de probar que es irreducible, pero de momento pospondremos la prueba.

Para comprender el interés de las variedades de Segre, definimos la *inyección de Segre* $i_{m,n}:\mathrm{P}^m\times\mathrm{P}^n\longrightarrow S_{m,n}$ mediante

$$i_{m,n}(a_1,\ldots,a_{m+1},b_1,\ldots,b_{n+1}) = (a_ib_j)_{ij}.$$

Es claro que $i_{m,n}$ no depende de la elección de las coordenadas homogéneas de cada par de puntos, así como que su imagen está en $S_{m,n}$. Además es biyectiva, pues si $P\in S_{m,n}$, su única antiimagen es el par (Q,R) cuyas coordenadas homogéneas son cualquier fila y cualquier columna, respectivamente, de la matriz de coordenadas de P.

Consideremos ahora el espacio afín A^N determinado por $X_{m+1,n+1}\neq 0$. Es claro que $S_{m,n}\cap A^N = i[A^m\times A^n]$, donde A^m es el espacio afín determinado por $X_{m+1}\neq 0$ y A^n el determinado por $X_{n+1}\neq 0$. Así, podemos definir una aplicación $\phi: A^{m+n}\longrightarrow S_{m,n}\cap A^N$ mediante

$$\phi(a_1,\ldots,a_m,b_1,\ldots,b_n) = (a_ib_j), \qquad a_{m+1}=a_{n+1}=1.$$

Es fácil ver que ϕ es un isomorfismo (es polinómica con inversa polinómica).

Esto significa que si identificamos a $\mathrm{P}^m\times\mathrm{P}^n$ con $S_{m,n}$ a través de la inyección de Segre, entonces $A^m\times A^n$ se identifica con una variedad afín isomorfa a A^{m+n}. El isomorfismo transforma el par de puntos de coordenadas afines $((X_i),(Y_j))$ en el punto de coordenadas afines (X_i,Y_j).

Un subconjunto $X\subset\mathrm{P}^m\times\mathrm{P}^n$, identificado con un subconjunto de $S_{m,n}$, es algebraico si y sólo si las coordenadas homogéneas (X_i,Y_j) de sus puntos son las que satisfacen un sistema de ecuaciones de tipo $F(X_iY_j)=0$, donde $F(T_{ij})$ es una forma, digamos de grado d. El polinomio $F(X_iY_j)$ tiene la propiedad de ser *bihomogéneo* de grado d, es decir, la suma de los grados de las variables X_i en cada monomio es igual a la suma de los grados de las variables Y_j en cada monomio y ambas son iguales a d. Es claro entonces que los subconjuntos algebraicos de $\mathrm{P}^m\times\mathrm{P}^n$ son los determinados (en un sistema de referencia de cada factor) por un conjunto de polinomios bihomogéneos de un mismo grado d en ambos grupos de variables.

Ahora bien, los polinomios bihomogéneos de grados (d_1, d_2), es decir, los polinomios que cumplen que la suma de los grados de las variables X_i en cada monomio es igual a d_1 y la suma de los grados de las variables Y_i en cada monomio es igual a d_2, también definen conjuntos algebraicos. En efecto, si $d_1 < d_2$ y $r = d_2 - d_1$, una ecuación $F(X_i, Y_j) = 0$ equivale a las ecuaciones bihomogéneas de grado d_2 dadas por

$$X_1^r F(X_i, Y_j) = 0, \ldots, X_{m+1}^r F(X_i, Y_j) = 0.$$

En conclusión:

> *Al identificar* $\mathrm{P}^m \times \mathrm{P}^n$ *con la variedad de Segre, sus subconjuntos algebraicos son los determinados por un sistema de ecuaciones bihomogéneas, de grados en* X *e* Y *no necesariamente iguales.*

Ahora es claro que un conjunto es algebraico en $\mathrm{P}^m \times \mathrm{P}^n$ respecto a una elección de sistemas de referencia en los factores si y sólo si lo es respecto a cualquier otra elección.

En lo sucesivo identificaremos $\mathrm{P}^m \times \mathrm{P}^n = S_{m,n}$. Nos falta probar que $\mathrm{P}^m \times \mathrm{P}^n$ es irreducible. Para ello observamos primero lo siguiente:

Teorema 2.41 *Si* $V \subset \mathrm{P}^m$ *es una variedad proyectiva y* $Q \in \mathrm{P}^n$*, entonces* $V \times \{Q\}$ *es una variedad proyectiva isomorfa a* V*.*

Demostración: En general, el producto de conjuntos algebraicos es un conjunto algebraico, pues está definido por la unión de las ecuaciones que definen a los factores. Una descomposición $V \times \{Q\} = (V_1 \times \{Q\}) \cup (V_2 \times \{Q\})$ en conjuntos algebraicos daría lugar a una descomposición $V = V_1 \cup V_2$, y es claro que V_1 y V_2 también serían algebraicos. Por consiguiente $V \times \{Q\}$ es una variedad proyectiva.

Veamos que la aplicación $\phi(P) = (P, Q)$ es un isomorfismo. Para probar que es regular basta ver que lo es restringida a un entorno de cada punto. No perdemos generalidad si estudiamos la restricción al espacio A^m definido por $X_{m+1} \neq 0$. También podemos suponer que Q cumple $Y_{m+1} = 1$. Así la expresión en coordenadas afines de la restricción de ϕ es $\phi(X_1, \ldots, X_m) = (X_i Y_j)$, donde $X_{m+1} = 1$ e Y_j son las coordenadas de Q (constantes). Vemos que se trata de una aplicación polinómica, luego regular.

Para probar la regularidad de la inversa razonamos de forma similar, restringiéndonos a $A^N \cap (V \times \{Q\})$. Ahora la expresión coordenada de la restricción de ϕ^{-1} es simplemente una proyección. ■

Ahora ya podemos probar la irreducibilidad de $\mathrm{P}^m \times \mathrm{P}^n$. De hecho probamos algo más general:

Teorema 2.42 *Si* $V \subset \mathrm{P}^m$ *y* $W \subset \mathrm{P}^n$ *son variedades proyectivas, entonces* $V \times W$ *es una variedad proyectiva.*

Demostración: Como ya hemos comentado en la prueba del teorema anterior, $V \times W$ es algebraico. El problema es demostrar que es irreducible. Supongamos que $V \times W = Z_1 \cup Z_2$, donde ambos conjuntos son cerrados. Definimos

$$U_i = \{Q \in W \mid V \times \{Q\} \not\subset Z_i\}.$$

Como $V \times \{Q\}$ es irreducible, ha de ser $U_1 \cap U_2 = \varnothing$. Si probamos que los U_i son abiertos, puesto que W es una variedad, esto sólo será posible si uno de los dos es vacío, digamos $U_1 = \varnothing$, lo que implica que $V \times W \subset Z_1$, como queremos probar. Veamos, pues, que U_1 es abierto (lo mismo vale para U_2).

Si $Q \in U_1$, entonces existe un $P \in V$ tal que $F(P, Q) \neq 0$, donde F es una de las formas que definen a Z_1. Entonces $G(X) = F(P, X)$ es una forma tal que

$$Q \in \{X \in W \mid G(X) \neq 0\} \subset U_1.$$

Esto prueba que U_1 es un entorno de Q, luego es abierto. ■

A partir de aquí ya es fácil obtener los resultados básicos sobre productos. Por ejemplo, el producto de variedades es una variedad, ya que

$$(\overline{V} \times \overline{W}) \setminus (V \times W) = ((\overline{V} \setminus V) \times \overline{W}) \cup (\overline{V} \times (\overline{W} \setminus W))$$

es cerrado por el teorema anterior, luego $V \times W$ es abierto en $\overline{V} \times \overline{W}$. Además el producto de variedades afines es una variedad afín. Veamos algunos hechos más:

Teorema 2.43 *Sean V, W, V', W' y Z variedades. Entonces*

a) Las proyecciones de $V \times W$ en cada factor son aplicaciones regulares.

b) Si $\phi : Z \longrightarrow V$ y $\psi : Z \longrightarrow W$ son aplicaciones regulares, entonces la aplicación $(\phi, \psi) : Z \longrightarrow V \times W$ dada por $(\phi, \psi)(P) = (\phi(P), \psi(P))$ es regular.

c) Si $\phi : V \longrightarrow V'$ y $\psi : W \longrightarrow W'$ son aplicaciones regulares, entonces la aplicación $\phi \times \psi : V \times W \longrightarrow V' \times W'$ dada por $(\phi \times \psi)(P, Q) = (\phi(P), \psi(Q))$ es regular.

d) La diagonal $\Delta_X = \{(P, P) \mid P \in V\}$ es cerrada en $V \times V$. La aplicación $\delta_X : X \longrightarrow \Delta_X$ dada por $\delta_X(P) = (P, P)$ es un isomorfismo.

Demostración: La prueba de a) es sencilla (al restringirse a espacios afines, las expresiones coordenadas de las proyecciones son proyecciones, luego aplicaciones polinómicas).

b) Por 2.36 no perdemos generalidad si suponemos que $V = \mathrm{P}^m$, $W = \mathrm{P}^n$. Para probar que (ϕ, ψ) es regular, basta probar que lo es restringida a cualquier cubrimiento abierto de Z. Puesto que $\mathrm{P}^m \times \mathrm{P}^n$ puede cubrirse con productos de espacios afines, podemos suponer que $V = A^m$ y $W = A^n$. Puesto que todo punto de Z tiene un entorno afín, podemos suponer que Z es una variedad afín.

Entonces ϕ y ψ son aplicaciones polinómicas, y es claro que (ϕ, ψ) también lo es.

c) se sigue de b) aplicado a las composiciones de las proyecciones seguidas de ϕ y ψ.

d) La diagonal Δ_X es la intersección con $X \times X$ de la diagonal de $\mathrm{P}^n \times \mathrm{P}^n$, que claramente es cerrada. La aplicación δ_X es regular por b) y su inversa es regular porque es la proyección. ■

De aquí deducimos una consecuencia de gran utilidad:

Teorema 2.44 *Si $\phi, \psi : V \longrightarrow W$ son aplicaciones regulares entre variedades, entonces $\{P \in V \mid \phi(P) = \psi(P)\}$ es cerrado en V. En particular, si ϕ y ψ coinciden en un conjunto denso, entonces $\phi = \psi$.*

DEMOSTRACIÓN: El conjunto en cuestión es $(\phi, \psi)^{-1}[\Delta_W]$. ■

Como aplicación podemos probar lo siguiente:

Teorema 2.45 *Sea $\phi : V \longrightarrow W$ una aplicación regular entre variedades. Si ϕ es densa (es decir, si $\phi[V]$ es denso en W), entonces $\overline{\phi} : k[W] \longrightarrow k[V]$ es un monomorfismo de anillos. Si W es afín el recíproco es cierto.*

DEMOSTRACIÓN: Si α, $\beta \in k[W]$ y $\overline{\phi}(\alpha) = \overline{\phi}(\beta)$, es decir, si $\phi \circ \alpha = \phi \circ \beta$, entonces α y β coinciden en $\phi[V]$, luego $\alpha = \beta$ por el teorema anterior.

Supongamos ahora que $\phi[V]$ no es denso en W y que W es afín. Tomemos $P \in W \setminus \overline{\phi[V]}$. Entonces existe un polinomio $F \in I(\overline{\phi[V]})$ tal que $F(P) \neq 0$, luego $f = [F] \in k[W]$ (aquí usamos que W es afín) cumple que $\overline{\phi}(f) = 0$, pero $f \neq 0$. Por lo tanto $\overline{\phi}$ no es inyectiva. ■

Para terminar con los productos de variedades probaremos un resultado del que deduciremos una propiedad importante de las aplicaciones regulares: la imagen de una variedad proyectiva por una aplicación regular es cerrada.

Teorema 2.46 *Sea V una variedad proyectiva y W una variedad arbitraria. Entonces la proyección $p : V \times W \longrightarrow W$ es cerrada, es decir, la imagen de un cerrado en $V \times W$ es cerrada en W.*

DEMOSTRACIÓN: Podemos suponer que V es cerrado en P^m. Entonces $V \times W = (V \times \mathrm{P}^n) \cap (\mathrm{P}^m \times W)$ es cerrado en $\mathrm{P}^m \times W$. Si C es cerrado en $V \times W$, también lo es $\mathrm{P}^m \times W$, luego podemos suponer que $V = \mathrm{P}^m$. Por 2.39 podemos cubrir W por abiertos afines. Si A es uno de ellos, entonces $C \cap (\mathrm{P}^m \times A)$ es cerrado en $\mathrm{P}^m \times A$. Si probamos el teorema para $W = A$, tendremos que $p[C \cap (\mathrm{P}^m \times A)]$ será cerrado en A, y es claro que entonces $p[C]$ será cerrado en W, como queremos demostrar. Por consiguiente, basta probar el teorema para el caso en que W es una variedad afín. Podemos suponer que W es cerrado en un espacio afín A^n. Como $\mathrm{P}^m \times W = (\mathrm{P}^m \times \overline{W}) \cap (\mathrm{P}^m \times A^n)$ es cerrado en $\mathrm{P}^m \times A^n$, podemos suponer que $W = A^n$.

En resumen, basta probar el teorema en el caso $p : \mathrm{P}^m \times A^n \longrightarrow A^n$. Fijemos sistemas de referencia en P^m y P^n de modo que A^n venga dado por la condición $Y_{n+1} \neq 0$. El conjunto C está formado por los puntos de $\mathrm{P}^m \times \mathrm{P}^n$ cuyas coordenadas homogéneas satisfacen un conjunto de ecuaciones de la forma $F_r(X_i, Y_j) = 0$, $r = 1, \ldots, t$, donde las F_r son formas bihomogéneas, y además $Y_{n+1} \neq 0$. Si sustituimos $Y_{n+1} = 1$ en cada forma F_r obtenemos polinomios homogéneos únicamente en las variables X_i tales que los puntos de C son exactamente los de coordenadas homogéneas $(X_1, \ldots, X_{m+1})$ y coordenadas afines $(Y_1, \ldots, Y_n)$ que cumplen el sistema de ecuaciones $F_r(X_i, Y_j) = 0$.

Un punto $P \in A^n$, de coordenadas (Y_j) está en $p[C]$ si y sólo si el sistema de ecuaciones $F_r(X_i, Y_j) = 0$ tiene solución no nula en las X_i. Según el teorema 2.19, esto sucede si y sólo si

$$(X_1, \ldots, X_{m+1})^s \not\subset (F_1(X_i, Y_j), \ldots, F_t(X_i, Y_j)), \tag{2.4}$$

para todo natural s. (Tengamos presente que las coordenadas Y_j son fijas, luego cada $F_r(X_i, Y_j)$ es una forma en las X_i.) Llamemos C_s al conjunto de los puntos $P \in A^n$, de coordenadas (Y_i), tales que esta condición se cumple para s. Según acabamos de ver, $p[C]$ es la intersección de todos los C_s, luego basta probar que cada uno de ellos es cerrado.

Sea $G_k \in k[X_1, \ldots, X_{m+1}]$ una enumeración de los monomios de grado s con coeficiente 1 (son un número finito). La inclusión

$$(X_1, \ldots, X_{m+1})^s \subset (F_1(X_i, Y_j), \ldots, F_t(X_i, Y_j)) \tag{2.5}$$

equivale a que cada G_k se exprese en la forma

$$G_k(x) = \sum_r p_{kr}(X_i) F_r(X_i, Y_j),$$

para ciertos polinomios $p_{kr}(X_i)$. Comparando las componentes homogéneas de grado s, podemos exigir que cada p_{kr} sea una forma de grado $s - d_r$, donde d_r es el grado (en las X_i) de F_r y $p_{kr} = 0$ si $d_r > s$.

Sea $N_k^r(X_i)$ una enumeración de los monomios de grado $s - d_r$ con coeficiente 1. La inclusión (2.5) equivale a que las formas $N_k^r(X_i) F_r(X_i, Y_j)$ generan el espacio vectorial de las formas de grado s. Si llamamos D a la dimensión de este espacio, la inclusión (2.5) equivale a que la matriz formada por los coeficientes de los monomios $G_{k'}$ en las formas $N_k^r(x) F_r(x, y)$ tenga rango D, o también a que exista un determinante $D \times D$ formado por estos coeficientes que sea distinto de 0. Por consiguiente, la condición (2.4) equivale a que todos estos determinantes sean nulos, pero tales determinantes dependen polinómicamente de las coordenadas (Y_i), luego, efectivamente, los puntos de C_s son los aquellos cuyas coordenadas afines (Y_i) satisfacen un sistema de ecuaciones polinómicas. ■

Como aplicación tenemos:

Teorema 2.47 *Sea $\phi : V \longrightarrow W$ una aplicación regular entre variedades y supongamos que V es proyectiva. Entonces $\phi[V]$ es cerrado en W.*

Demostración: Sea $G \subset V \times W$ la gráfica de ϕ (conjuntistamente $G = \phi$). Entonces $G = (\phi \times i)^{-1}(\Delta_W)$, donde $i : W \longrightarrow W$ es la identidad. Por lo tanto G es cerrado en $V \times W$ y por el teorema anterior su proyección en W es cerrada, pero ésta es $\phi[V]$. ■

Ahora podemos mostrar una diferencia esencial entre las variedades afines y las proyectivas. Hemos visto que una variedad afín V está determinada salvo isomorfismo por su anillo de funciones regulares $k[V]$. La situación es radicalmente distinta para variedades proyectivas:

Teorema 2.48 *Sea V una variedad proyectiva sobre un cuerpo k. Entonces $k[V] = k$.*

Demostración: Si $\alpha \in k[V]$, entonces $\alpha : V \longrightarrow A^1$, y en particular $\alpha : V \longrightarrow \mathrm{P}^1$. Por el teorema anterior $\alpha[V]$ es cerrado en P^1. Ahora bien, $\alpha[V] \subset A^1$, y no puede ser $\alpha[V] = A^1$, pues no sería cerrado en P^1.

Por otra parte, es fácil ver que los únicos cerrados en A^1 distintos de A^1 son los conjuntos finitos. Más aún, $\phi[V]$ no puede contener más de un punto, pues si $\phi[V] = \{a_1, \ldots, a_r\}$, entonces los cerrados $\phi^{-1}[a_i]$ contradirían la irreducibilidad de V. Por consiguiente ϕ es constante. ■

Esto a su vez puede generalizarse:

Teorema 2.49 *Sea $\phi : V \longrightarrow W$ una aplicación regular de una variedad proyectiva en una variedad afín. Entonces ϕ es constante.*

Demostración: Podemos suponer que W es abierto en A^m, y a su vez podemos suponer que $\phi : V \longrightarrow A^m$. Basta aplicar el teorema anterior a las composiciones de ϕ con las proyecciones en los factores de $A^m = k^m$. ■

2.5 Aplicaciones racionales

Ahora estamos en condiciones de definir las aplicaciones más generales que aparecen de forma natural en la teoría básica sobre variedades algebraicas. Se trata de las aplicaciones racionales, que hasta ahora tenemos definidas únicamente en el caso $\alpha : V \longrightarrow A^1$, y constituyen el cuerpo de funciones racionales $k(V)$ de la variedad V. La definición general debe extender a ésta.

En principio podríamos definir una aplicación racional $\phi : V \longrightarrow W$ entre dos variedades como una aplicación regular $\phi : U \longrightarrow W$, donde U es un abierto en V, pero hemos de hacer una matización: diremos que ϕ es *equivalente* a otra aplicación regular $\phi' : U' \longrightarrow W$ si ϕ y ϕ' coinciden en $U \cap U'$. En virtud del teorema 2.44 tenemos una relación de equivalencia, pues los abiertos no vacíos son densos. La clase de equivalencia de ϕ define una función regular en la unión de los dominios de sus elementos, con la propiedad de que no puede extenderse a una aplicación regular en un abierto mayor.

Definición 2.50 Una *aplicación racional* $\phi : V \longrightarrow W$ entre dos variedades es una aplicación regular definida en un subconjunto abierto de V que no puede extenderse a una aplicación regular en ningún abierto mayor. Los puntos donde ϕ no está definida se llaman *singularidades* de ϕ. También se dice que son los puntos donde ϕ es *singular.*

Hemos visto que toda aplicación regular definida en un abierto de una variedad V se extiende a una única aplicación racional en V. El considerar las extensiones máximas es necesario para que las singularidades estén bien definidas. Observemos que el conjunto de singularidades de una función racional es cerrado por definición.

Veamos ahora que si V es una variedad, entonces $k(V)$ es precisamente el conjunto de las funciones racionales $\alpha : V \longrightarrow A^1$.

Si $\alpha \in k(V)$ y C es el conjunto de sus singularidades (en el sentido que ya teníamos definido, es decir, el conjunto de puntos de V donde α no está definida), entonces C es cerrado en V y la restricción de α a $U = V \setminus C$ es una función regular. Lo único que hemos de justificar es que C es también el conjunto de los singularidades de α en el sentido de la definición anterior, es decir, que $\alpha|_U$ no puede extenderse a una función regular en un entorno de un punto $P \in U$. Si existiera tal entorno W, entonces, $\alpha \in k[W]$, luego $\alpha = [F]/[G]$, donde F y G son formas del mismo grado, $G(P) \neq 0$ y las clases se toman módulo $I(\overline{W}) = I(\overline{V})$, pero entonces α estaría definida en P en el sentido usual para funciones de $k(V)$.

Recíprocamente, si $\alpha : V \longrightarrow A^1$ es racional, entonces existe un abierto U en V tal que $\alpha|_U \in k[U]$, es decir, $\alpha|_U = \beta|_U$, para una cierta $\beta \in k(V)$. Como α y β son racionales en el sentido de la definición anterior y coinciden en un abierto, necesariamente $\alpha = \beta \in k(V)$.

A partir de aquí podemos caracterizar las aplicaciones racionales en varios casos de interés. Por ejemplo:

Teorema 2.51 *Las funciones racionales $\phi : V \longrightarrow A^n$ en una variedad V son las funciones (definidas sobre un abierto de V) de la forma*

$$\phi(P) = (\alpha_1(P), \ldots, \alpha_n(P)),$$

donde $\alpha_i \in k(V)$. Más concretamente, un punto $P \in V$ es una singularidad de ϕ si y sólo si es una singularidad de alguna de las funciones coordenadas α_i.

DEMOSTRACIÓN: Sea U el conjunto de los puntos de V donde ϕ está definida. Entonces $\phi|_U : U \longrightarrow A^n$ es una aplicación regular, luego también lo son las proyecciones $\alpha_i = \phi|_U \circ p_i : U \longrightarrow A^1$. Por consiguiente $\alpha_i \in k(U) = k(V)$.

Recíprocamente, si ϕ cumple que $\alpha_i \in k(V)$ y U es la intersección de los dominios de las funciones α_i, entonces $\phi|_U$ es regular por el teorema 2.43, luego ϕ es racional, y es fácil ver que su dominio es exactamente U. ■

Consideremos ahora una función racional $\phi : V \longrightarrow \mathrm{P}^n$ y sea $P \in V$. Fijados sistemas de coordenadas, pongamos que la coordenada X_{n+1} de $\phi(P)$ es no nula, es decir, que $\phi(P) \in A^n$, donde A^n es el espacio afín determinado por la condición $X_{n+1} \neq 0$. La restricción de ϕ al abierto $U = \phi^{-1}[A^n]$ es una aplicación regular, en particular racional, con imagen en A^n, luego por el teorema anterior, ϕ es de la forma

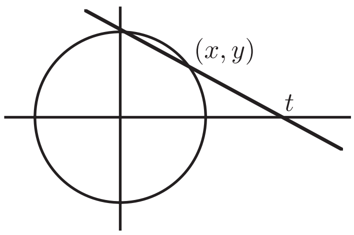
$$\phi(Q) = (\alpha_1(Q), \ldots, \alpha_n(Q)), \qquad \alpha_i \in k(V).$$

En un entorno de P, cada α_i admite la expresión $\alpha_1 = [F_i]/[F_{n+1}]$, donde las F_i son formas del mismo grado. Por consiguiente, las coordenadas homogéneas de la imagen de un punto Q son de la forma

$$\phi(Q) = (F_1(Q), \ldots, F_{n+1}(Q)),$$

para ciertas formas F_i del mismo grado. No obstante, hemos de tener presente que esta expresión es local, es decir, tenemos una expresión de este tipo válida en un entorno de cada punto P. Recíprocamente, si una función ϕ puede ser definida localmente por expresiones de este tipo, será racional, y será regular en aquellos puntos en los que exista una expresión de este tipo cuyas coordenadas no se anulen simultáneamente.

Ejemplo Sea $V = V(X^2+Y^2-1)$ la circunferencia unidad. Si la consideramos como variedad real, es conocido que la proyección estereográfica proporciona una biyección entre $V \setminus \{(0,1)\}$ y la recta afín. Las fórmulas son



$$(x,y) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right),$$

$$t = \frac{x}{1-y} = \frac{1+y}{x}.$$

Si consideramos a V como variedad compleja (junto con la recta afín compleja) la situación no es tan simple, pues pues los puntos $t = \pm i$ no tienen imagen en V. De este modo, estas aplicaciones definen biyecciones mutuamente inversas entre $V \setminus \{(0,1)\}$ y $A^1 \setminus \{\pm i\}$. Claramente son isomorfismos.

Las singularidades se deben a que las rectas que unen el punto $(0,1)$ con los puntos $(\pm i, 0)$ cortan a V en el infinito. Similarmente, el punto $(0,1)$ de V "debería" corresponderse con el punto infinito de P^1. En otras palabras: las singularidades desaparecen si consideramos variedades proyectivas. Sea, pues, $V = V(X^2+Y^2-Z^2)$. Las fórmulas de la proyección estereográfica en coordenadas homogéneas (x,y,z) para V y (t,u) para P^1 son

$$(x,y,z) = (2tu,\ t^2-u^2,\ t^2+u^2), \qquad (t,u) = (x,\ z-y) = (z+y,\ x).$$

Así vemos que los puntos $(\pm i, 1)$ se transforman en los puntos infinitos $(\pm i, 1, 0)$. Ahora es fácil comprobar que estas transformaciones mutuamente inversas son de hecho isomorfismos entre V y P^1.

Observemos que hemos de considerar las dos expresiones que determinan a (t, u) en función de (x, y, z), pues ninguna de las dos es válida globalmente. Este ejemplo también muestra cómo un punto puede ser singular para una función racional entre variedades (el punto i, por ejemplo) y dejar de serlo cuando extendemos la imagen (de la circunferencia afín a la proyectiva). ■

Ejercicio: Describir explícitamente un isomorfismo entre la recta proyectiva y la parábola $YZ = X^2$.

Es fácil generalizar el teorema 2.45. Supongamos que $\phi : V \longrightarrow W$ es una función racional (con imagen) densa entre dos variedades. Sea $U_2 \subset W$ un abierto afín y $U_1 \subset \phi^{-1}[U_2]$ un abierto afín en V, que podemos tomar tal que ϕ sea regular en U_1. Así tenemos que $\phi|_{U_1} : U_1 \longrightarrow U_2$ es regular y densa. En efecto, si $A \subset U_2$ es un abierto no vacío, entonces $A \cap \phi[V] \neq \varnothing$, luego $\phi^{-1}[A]$ es un abierto no vacío, luego $\phi^{-1}[A] \cap U_1 \neq \varnothing$, luego $A \cap \phi[U_1] \neq \varnothing$. Por 2.45 tenemos que $\overline{\phi} : k[U_2] \longrightarrow k[U_1]$ es un k-monomorfismo, luego se extiende a un k-monomorfismo entre los cuerpos de cocientes, es decir, $\overline{\phi} : k(W) \longrightarrow k(V)$.

Concretamente, si $\alpha \in k(W)$ está definida en un punto $\phi(P) \in U_2$, entonces $\alpha = \beta/\gamma$, donde $\beta, \gamma \in k[U_2]$ y $\gamma(\phi(P)) \neq 0$. Por lo tanto $\overline{\phi}(\alpha) = (\phi \circ \beta)/(\phi \circ \gamma)$ está definida en P y $\overline{\phi}(\alpha)(P) = \alpha(\phi(P))$. Así pues, $\overline{\phi}(\alpha)|_{U_1} = \phi|_{U_1} \circ \alpha$.

De aquí se sigue que $\overline{\phi}$ no depende de la elección de los abiertos U_1 y U_2, pues si los cambiamos por otros U_1' y U_2' entonces las correspondientes aplicaciones $\overline{\phi}(f)$ y $\overline{\phi}'(f)$ coinciden en $U_1 \cap U_1'$, luego son la misma función racional. Puesto que todo punto tiene un entorno afín, si A es el abierto de puntos regulares de $\alpha \in k(W)$, entonces $\overline{\phi}(\alpha)$ está definida en $\phi^{-1}[A]$ y $\overline{\phi}(\alpha) = \phi \circ \alpha$. Con esto hemos probado la mitad del teorema siguiente:

Teorema 2.52 *Sea $\phi : V \longrightarrow W$ una aplicación racional densa entre variedades sobre un cuerpo k. Entonces ϕ induce un único k-monomorfismo de cuerpos $\overline{\phi} : k(W) \longrightarrow k(V)$ determinado por la propiedad siguiente: si U es abierto en W y $\alpha \in k[U]$, entonces $\overline{\phi}(\alpha) \in k[\phi^{-1}[U]]$ y $\overline{\phi}(\alpha) = \phi \circ \alpha$. Recíprocamente, todo k-monomorfismo $h : k(W) \longrightarrow k(V)$ es de la forma $h = \overline{\phi}$, para una cierta aplicación racional densa $\phi : V \longrightarrow W$.*

DEMOSTRACIÓN: Tomamos variedades afines $V' \subset V$ y $W' \subset W$ (abiertas). Entonces $k(V') = k(V)$ y $k(W') = k(W)$. Si probamos el teorema para V' y W' tendremos una aplicación racional $\phi : V' \longrightarrow W'$ que induce a h, pero ϕ determina una única aplicación racional $\phi : V \longrightarrow W$. Alternativamente, podemos suponer que V y W son afines.

Sea $k[W] = k[x_1, \ldots, x_n]$. Entonces $h(x_i) = \alpha_i/\beta_i$, con α_i, $\beta_i \in k[V]$. Sea $\beta = \beta_1 \cdots \beta_n$. Tenemos que $h[k[W]] \subset k[V][1/\beta] = k[V_\beta]$ (ver 2.38), luego tenemos un k-monomorfismo $h : k[W] \longrightarrow k[V_\beta]$. Por el teorema 2.13 tenemos que $h = \overline{\phi}$, para una cierta aplicación regular $\phi : V_\beta \longrightarrow W$. Como h es inyectiva, el teorema 2.45 nos da que $\phi[V_\beta]$ es denso en W. La aplicación ϕ se extiende a una única aplicación racional densa $\phi : V \longrightarrow W$ que claramente induce a h. ■

Ahora podemos determinar exactamente las aplicaciones entre variedades que conservan los cuerpos de funciones racionales:

Definición 2.53 Una aplicación $\phi : V \longrightarrow W$ entre variedades es *birracional* si existen abiertos $U_1 \subset V$ y $U_2 \subset W$ tales que $\phi|_{U_1} : U_1 \longrightarrow U_2$ es un isomorfismo.

Claramente, el isomorfismo indicado (con su inverso) induce funciones racionales densas $\phi : V \longrightarrow W$ y $\phi^{-1} : W \longrightarrow V$ que claramente inducen isomorfismos (mutuamente inversos) $\overline{\phi} : k(W) \longrightarrow k(V)$ y $\overline{\phi}^{-1} : k(V) \longrightarrow k(W)$.

Informalmente, podemos decir que una aplicación birracional es una aplicación racional con inversa racional, pero hemos de tener presente que las aplicaciones birracionales no están definidas necesariamente en toda la variedad (cuando lo están son isomorfismos).

Diremos que dos variedades V y W son *birracionalmente equivalentes* si existe una aplicación birracional entre ellas. Claramente se trata de una relación de equivalencia.

Teorema 2.54 *Dos variedades son birracionalmente equivalentes si y sólo si sus cuerpos de funciones racionales son k-isomorfos.*

DEMOSTRACIÓN: Una implicación se sigue directamente de 2.52. Supongamos que $\phi : k(V) \longrightarrow k(W)$ es un k-isomorfismo entre los cuerpos de funciones racionales de dos variedades. Podemos suponer que son afines. Como en la prueba de 2.52, existe un $\beta \in k[W]$ tal que $\phi[k[V]] \subset k[W_\beta]$. Similarmente, existe $\alpha \in k[V]$ tal que $\phi^{-1}[k[W]] \subset k[V_\alpha]$. Entonces ϕ se restringe a un isomorfismo entre los anillos $k[V_{\alpha,\phi^{-1}(\beta)}]$ y $k[W_{\beta,\phi(\alpha)}]$ y, como las variedades son afines, el teorema 2.13 (ver las observaciones posteriores) nos da que son isomorfas, luego V y W son birracionalmente equivalentes. ■

Ejercicio: Refinar la prueba del teorema anterior para demostrar que dos puntos de dos variedades tienen entornos k-isomorfos si y sólo si sus anillos de funciones regulares son k-isomorfos.

Ejemplo Sea V la curva "alfa" $Y^2 = X^2(X + 1)$, (ver la página 55). Observemos que la recta $Y = tX$ que pasa por el origen con pendiente t corta a V en $(0, 0)$ y en $(t^2 - 1, t(t^2 - 1))$.

La función polinómica $\phi : A^1 \longrightarrow V$ dada por $\phi(t) = (t^2 - 1, t(t^2 - 1))$ es biyectiva salvo por que pasa dos veces por $(0, 0)$, a saber, para $t = \pm 1$. Si llamamos $V_0 = V \setminus \{(0, 0)\}$, entonces V_0 es una variedad abierta en V y la restricción $\phi : A^1 \setminus \{\pm 1\} \longrightarrow V_0$ es un isomorfismo. En efecto, su inversa es $\psi(x, y) = y/x$, que es regular, pues el denominador no se anula en V_0 (hay que comprobar además que $y/x \neq \pm 1$).

Por consiguiente, $\phi : A^1 \longrightarrow V$ es una aplicación birracional y así V es birracionalmente equivalente a una recta. Ahora no estamos en condiciones de probarlo, pero V no es isomorfa a una recta. ■

Ejercicio: Probar que ϕ se extiende a una aplicación racional $\phi : \mathrm{P}^1 \longrightarrow \overline{V}$ tal que $\phi(1, 0) = (0, 1, 0)$.

Capítulo III

Dimensión

En este capítulo asociaremos un invariante a cada variedad algebraica que se corresponde con la noción geométrica de dimensión. En la primera sección estudiamos una clase especial de aplicaciones entre variedades que —como veremos— conservarán la dimensión, en la segunda introduciremos el concepto de dimensión propiamente dicho, luego estudiaremos la dimensión desde un punto de vista local, a través de las variedades tangentes y, por último, estudiaremos con más detalle las variedades de dimensión 1, es decir, las curvas algebraicas.

3.1 Aplicaciones finitas

Consideremos en primer lugar una aplicación regular densa $\phi : V \longrightarrow W$ entre variedades afines. Según el teorema 2.45 tenemos que $\bar{\phi} : k[W] \longrightarrow k[V]$ es un monomorfismo de anillos, que nos permite considerar a $k[W]$ como un subanillo de $k[V]$.

Definición 3.1 Diremos que una aplicación regular densa $\phi : V \longrightarrow W$ entre variedades afines es *finita* si $k[V]$ es una extensión entera de $k[W]$. (Ver 1.12).

El teorema 1.14 implica que la composición de aplicaciones finitas es finita. Todo isomorfismo es trivialmente finito.

Ejemplo Sea V la hipérbola $XY = 1$ y sea $p : V \longrightarrow A^1$ la proyección $p(x, y) = x$. Ciertamente es una aplicación regular (polinómica) y es densa, pues su imagen es todo A^1 excepto el origen. Sin embargo, no es finita, pues $k[A^1] = k[X]$, $k[V] = k[x, y]$ y $\bar{p} : k[A^1] \longrightarrow k[V]$ viene dada por $\bar{p}(X)(x, y) = x$, es decir, $\bar{p}(X) = x$, con lo que podemos identificar $k[A^1] = k[x]$.

Por consiguiente, $k[V] = k[A^1][y]$, pero y no es entero sobre $k[A^1]$, ya que su polinomio mínimo es $xY - 1$. ■

Hemos dado este ejemplo para mostrar explícitamente cómo puede fallar la condición que define la finitud. Sin embargo, el resultado es obvio porque las aplicaciones finitas no sólo son densas, sino que, de hecho, son suprayectivas:

Teorema 3.2 *Toda aplicación finita entre variedades afines es suprayectiva y cada punto tiene un número finito de antiimágenes.*

DEMOSTRACIÓN: Podemos suponer que $V \subset A^n$. Fijado un sistema de referencia en V, sea $k[V] = k[x_1, \ldots, x_n]$. Tomemos un punto $P \in W$. Para probar que $\phi^{-1}[P]$ es finito basta ver que cada coordenada x_i toma un número finito de valores sobre este conjunto.

Tenemos que x_i es entero sobre $k[W]$, luego satisface una relación de la forma

$$x_i^k + a_1 x_i^{k-1} + \cdots + a_k = 0,$$

para ciertas funciones $a_i \in k[W]$. Si $Q \in \phi^{-1}[P]$ tiene coordenadas x, entonces, evaluando la igualdad anterior en Q (teniendo en cuenta que, por la identificación, $a_j(Q) = a_j(\phi(Q)) = a_j(P)$) resulta que

$$x_i^k + a_1(P) x_i^{k-1} + \cdots + a_k(P) = 0,$$

con lo que las coordenadas i-ésimas de los puntos de $\phi^{-1}[P]$ son raíces de un mismo polinomio no nulo, luego son un número finito.

Veamos ahora la suprayectividad. Sea $\mathfrak{m}_P$ el ideal de $k[W]$ formado por las funciones que se anulan en P. Concretamente, si P tiene coordenadas $(\alpha_1, \ldots, \alpha_m)$ y $k[W] = k[y_1, \ldots, y_m]$, entonces $\mathfrak{m}_P = (y_1 - \alpha_1, \ldots, y_m - \alpha_m)$.

La aplicación ϕ es regular, luego es polinómica. Consideremos polinomios $F_1, \ldots, F_m$ tales que $\phi(P) = (F_1(P), \ldots, F_m(P))$. Entonces $\phi^{-1}[P]$ es el conjunto algebraico determinado por las ecuaciones $F_i(X_1, \ldots, X_n) - \alpha_i = 0$. Así pues, $\phi^{-1}[P] = \varnothing$ equivale a que

$$(F_1 - \alpha_1, \ldots, F_m - \alpha_m) = k[X_1, \ldots, X_n].$$

En tal caso tomamos clases módulo $I(V)$ y queda que

$$(\bar{\phi}(y_1) - \alpha_1, \ldots, \bar{\phi}(y_m) - \alpha_m) = k[V].$$

Si identificamos $\bar{\phi}(y_i)$ con y_i, esto equivale a que $\mathfrak{m}_P\, k[V] = k[V]$ (o sea, el ideal generado por $\mathfrak{m}_p$ en $k[V]$ es $k[V]$). Sin embargo, el teorema 1.21 nos dice que esto es imposible. ■

El teorema siguiente nos permitirá extender la definición de aplicación finita al caso de aplicaciones entre variedades cuasiproyectivas arbitrarias.

Teorema 3.3 *Sea $\phi : V \longrightarrow W$ una aplicación regular entre variedades afines. Si todo punto $P \in W$ tiene un entorno afín U tal que $U' = \phi^{-1}[U]$ es afín y $\phi|_{U'} : U' \longrightarrow U$ es finita, entonces ϕ es finita.*

DEMOSTRACIÓN: Para cada $P \in W$, podemos tomar $\alpha \in k[W]$ tal que el abierto principal W_α esté contenido en un entorno U de P que cumpla el teorema. Entonces $\phi^{-1}[W_\alpha] = V_{\bar{\phi}(\alpha)} \subset U'$ es una subvariedad afín de V y es claro que la restricción de ϕ a $\phi^{-1}[W_\alpha]$ es finita, pues, llamando $\alpha' = \alpha|_U$, tenemos que

$$k[W_\alpha] = k[U_{\alpha'}] = k[U][1/\alpha'], \quad k[V_{\bar{\phi}(\alpha)}] = k[U'_{\bar{\phi}(\alpha')}] = k[U'][1/\alpha'].$$

Así pues, a las hipótesis del teorema podemos añadir que cada U es principal. Por consiguiente, tenemos a W cubierto por abiertos principales $\{W_\alpha\}_{\alpha\in S}$, para cierto $S \subset k[W]$. Si $\alpha = [F_\alpha]$, el ideal generado por $I(W)$ y los F_α no tiene ningún cero, luego es $k[X_1, \ldots, X_n]$. Esto se traduce en que $(S) = k[W]$. Como $k[W]$ es noetheriano, existe un número finito de funciones $\alpha_1, \ldots, \alpha_n \in S$ de modo que $(\alpha_1, \ldots, \alpha_n) = k[W]$ y, por lo tanto, los abiertos W_{α_i} cubren W.

Por 1.13 sabemos que $k[V_{\alpha_i}] = k[V][1/\alpha_i]$ es un $k[W_{\alpha_i}]$-módulo finitamente generado. Digamos que $k[V_{\alpha_i}] = \langle\omega_{i1}, \ldots, \omega_{in}\rangle_{k[W_{\alpha_i}]}$.

Podemos suponer que $\omega_{ij} \in k[V]$, pues si, en general, $\omega_{ij}/\alpha_i^{m_i}$ formaran un generador, los ω_{ij} también lo serían. Vamos a probar que $k[V] = \langle\omega_{ij}\rangle_{k[W]}$. De este modo, 1.10 implica entonces que los ω_{ij} son enteros sobre $k[W]$ y el teorema quedará probado.

Todo $\beta \in k[V]$ admite una expresión

$$\beta = \sum_j \frac{a_{ij}}{\alpha_i^{n_i}}\,\omega_{ij}, \qquad a_{ij} \in k[W],$$

para cada i. Ningún punto de W es un cero común de todas las funciones $\alpha_i^{n_i}$, de donde se sigue que $(\{\alpha_i\}_i) = k[W]$. Así pues, existen funciones $h_i \in k[W]$ tales que $\sum\limits_i \alpha_i^{n_i} h_i = 1$, luego

$$\beta = \beta\sum_i \alpha_i^{n_i} h_i = \sum_{i,j} a_{ij} h_i \omega_{ij} \in \langle\omega_{ij}\rangle_{k[W]}.$$

■

Definición 3.4 Una aplicación regular $\phi : V \longrightarrow W$ entre variedades cuasiproyectivas es *finita* si todo punto $P \in W$ tiene un entorno afín U tal que $U' = \phi^{-1}[U]$ es una subvariedad afín de V y $\phi|_{U'} : U' \longrightarrow U$ es finita.

El teorema 3.3 garantiza que esta definición coincide con la precedente para variedades afines. Además, el argumento usado al principio de la prueba muestra que si ϕ cumple esta definición entonces la cumple para entornos arbitrariamente pequeños de cada punto de W (más concretamente, la cumple para todo abierto principal de todo abierto que la cumpla). Por consiguiente:

Teorema 3.5 *Si $\phi : V \longrightarrow W$ es una aplicación finita y U es un abierto en W, entonces la restricción $\phi : \phi^{-1}[U] \longrightarrow U$ también es finita.*

El teorema 3.2 es claramente válido para aplicaciones entre variedades cuasiproyectivas. Otra propiedad sencilla es la siguiente:

Teorema 3.6 *Las aplicaciones finitas son cerradas (es decir, la imagen de un conjunto cerrado por una aplicación finita es cerrada).*

DEMOSTRACIÓN: Sea $\phi : V \longrightarrow W$ una aplicación finita y sea $C \subset V$ un conjunto cerrado. Por el teorema 2.29 podemos cubrir W por un número finito de variedades afines U tales que $U' = \phi^{-1}[U]$ es afín y la restricción de $\phi|_{U'}$ es finita. Basta probar que $\phi|_{U'}[C \cap U']$ es cerrado o, equivalentemente, podemos suponer que V y W son variedades afines. Tampoco perdemos generalidad si suponemos que C es irreducible. Es fácil ver entonces que $\overline{\phi[C]}$ es también irreducible.

La restricción $\phi|_C : C \longrightarrow \overline{\phi[C]}$ es finita, pues todo $\alpha \in k[C]$ se extiende a $\beta \in k[V]$, que es raíz de un polinomio mónico con coeficientes en $k[W]$, luego α es raíz del polinomio que resulta de restringir sus coeficientes a $\overline{\phi[C]}$. Como las aplicaciones finitas son suprayectivas, ha de ser $\phi[C] = \overline{\phi[C]}$, luego $\phi[C]$ es cerrado. ■

Ahora necesitamos un ejemplo importante de aplicación finita.

Definición 3.7 Sea E una subvariedad lineal de P^n, es decir, el conjunto de ceros de un sistema de d formas lineales $L_1, \ldots, L_d$. Es fácil ver que E es irreducible. Definimos la *proyección* de centro E como la aplicación racional $\pi : \mathrm{P}^n \longrightarrow \mathrm{P}^{d-1}$ dada por

$$\pi(x) = (L_1(x), \ldots, L_d(x)).$$

Es claro que π es regular en el abierto $\mathrm{P}^n \setminus E$. Si C es una subvariedad cerrada de P^n disjunta de E, la restricción $\pi : C \longrightarrow \mathrm{P}^{d-1}$ es una aplicación regular. Vamos a ver que $\pi : C \longrightarrow \pi[C]$ es finita.

Notemos que $U_i = \pi^{-1}[A_i^{d-1}] \cap C$ es el abierto en C determinado por la condición $L_i(x) \neq 0$, luego es una variedad afín (es la intersección con C del complementario de un hiperplano de P^n). Además los abiertos U_i cubren C, luego basta probar que las restricciones $\pi : U_i \longrightarrow A_i^{d-1} \cap \pi[C]$ son finitas. Por simplificar la notación tomamos $i = 1$.

Por el teorema 2.38, cada $\alpha \in k[U_1]$ (vista como aplicación racional en C) es de la forma

$$\alpha = \frac{G(x_1, \ldots, x_{n+1})}{L_1^m(x_1, \ldots, x_{n+1})},$$

donde G es una forma de grado m. Sea $\pi_1 : C \longrightarrow \mathrm{P}^d$ dada por

$$\pi_1(x) = (L_1^m(x), \ldots, L_d^m(x), G(x)).$$

(Notemos que estamos trabajando en tres espacios proyectivos: P^n, P^{d-1} y P^d. Usaremos $X_1, \ldots, X_{n+1}$ para coordenadas en P^n, $Y_1, \ldots, Y_{d+1}$ para coordenadas en P^d y $Z_1, \ldots, Z_d$ para coordenadas en P^{d-1}.)

La aplicación π_1 es regular, pues si $x \in C$, alguna de las formas L_i^m no se anula. Por el teorema 2.47 tenemos que $\pi_1[C]$ es una subvariedad cerrada de P^d. Digamos que viene definida por las ecuaciones $F_1 = \cdots = F_s = 0$.

Como $C \cap E = \varnothing$, las formas L_i no tienen ningún cero común en C, luego el punto $(0, \ldots, 0, 1) \in \mathrm{P}^d$ no está en $\pi_1[C]$. Esto significa que las funciones

$Y_1, \ldots, Y_d$, $F_1, \ldots, F_s$ no tienen ningún cero común en P^d. Por 2.19 existe un $N > 0$ tal que

$$(Y_1, \ldots, Y_d, Y_{d+1})^N \subset (Y_1, \ldots, Y_d, F_1, \ldots, F_s).$$

En particular Y_{d+1}^N está en el ideal de la derecha, luego

$$Y_{d+1}^N = \sum_{j=1}^{d} Y_j H_j + \sum_{j=1}^{s} F_j G_j,$$

para ciertos polinomios H_j y G_j. Llamando $H_j^{(q)}$ a la componente homogénea de grado q de H_j vemos que la forma

$$T(Y_1, \ldots, Y_{d+1}) = Y_{d+1}^N - \sum_{j=1}^{d} Y_j H_j^{(N-1)} \tag{3.1}$$

se anula sobre $\pi_1[C]$. Visto como polinomio en Y_{d+1}, tiene grado N y su coeficiente director es 1. Podemos expresarlo en la forma

$$T = Y_{d+1}^N + \sum_{j=0}^{N-1} A_{N-j}(Y_1, \ldots, Y_d) Y_{d+1}^j. \tag{3.2}$$

Sustituyendo en (3.1) la definición de π_1, vemos que $T(L_1^m, \ldots, L_d^m, G)$ se anula en C. Según (3.2), tenemos que

$$G^N + \sum_{j=0}^{N-1} A_{N-j}(L_1^m, \ldots, L_d^m) G^j = 0.$$

Dividiendo entre L_1^{mN} queda

$$\alpha^N + \sum_{j=0}^{N-1} A_{N-j}(1, L_2^m/L_1^m, \ldots, L_d^m/L_1^m)\alpha^j = 0.$$

Esto es un polinomio mónico con coeficientes en $k[A_1^{d-1} \cap \pi[C]]$. Explícitamente, los coeficientes son las imágenes por $\bar{\pi}$ de las funciones regulares

$$A_{N-j}(1, z_2/z_1, \ldots, z_d/z_1) = A_{N-j}(z_2, \ldots, z_d),$$

donde hemos pasado de las coordenadas homogéneas a las coordenadas afines.

■

Para generalizar este resultado necesitamos una nueva aplicación:

Definición 3.8 Es fácil ver que el número de $n+1$-tuplas $(i_1, \ldots, i_{n+1})$ de números naturales que cumplen $i_1 + \cdots + i_{n+1} = m$ es $N + 1 = \binom{n+m}{n}$. Por ello, podemos subindicar las coordenadas homogéneas de los puntos de P^N en la forma $(v_{i_1,\ldots,i_{n+1}})$. Si (u_i) son las coordenadas homogéneas en P^n, definimos la *inmersión de Veronese* $V_m : \mathrm{P}^n \longrightarrow \mathrm{P}^N$ como la aplicación que a cada $(u_1, \ldots, u_{n+1}) \in \mathrm{P}^n$ le asigna el punto cuya coordenada homogénea $v_{i_1,\ldots,i_{n+1}}$ es $u_1^{i_1} \cdots u_{n+1}^{i_{n+1}}$.

Se trata de una aplicación regular, pues entre las coordenadas de la imagen están las u_i^m, que no se anulan simultáneamente. Los puntos de la imagen satisfacen las ecuaciones

$$v_{i_1,\ldots,i_{n+1}} v_{j_1,\ldots,j_{n+1}} = v_{k_1,\ldots,k_{n+1}} v_{l_1,\ldots,l_{n+1}}, \tag{3.3}$$

siempre que $i_1 + j_1 = k_1 + l_1, \ldots, i_{n+1} + j_{n+1} = k_{n+1} + l_{n+1}$.

Recíprocamente, si un punto de P^N cumple estas ecuaciones está en la imagen de V_m. Para probarlo observamos que de ellas se sigue que algún $v_{0,\ldots,m,\ldots,0} \neq 0$. En efecto, tomamos una coordenada $v_{i_1,\ldots,i_{n+1}} \neq 0$. Supongamos que $i_1 \neq 0$, sea $r > 0$ tal que $ri_1 \geq m$. Así, aplicando (3.3) varias veces podemos expresar $v^r_{i_1,\ldots,i_{n+1}}$ como producto de r coordenadas entre las cuales está $v_{m,0,\ldots,0} \neq 0$. Así pues, el conjunto algebraico determinado por (3.3) está cubierto por los abiertos U_i formados por los puntos con $v_{0,\ldots,m,\ldots,0} \neq 0$ (donde la m está en la posición i). Es fácil ver que cada punto de U_1 tiene como antiimagen a

$$V_m^{-1}(v_{i_1,\ldots,i_{n+1}}) = (v_{m,0,\ldots,0}, v_{m-1,1,0,\ldots,0}, \ldots, v_{m-1,0,\ldots,0,1}).$$

Para los demás abiertos U_i tenemos una expresión similar, luego la imagen de V_m es el conjunto algebraico determinado por las ecuaciones (3.3). Se trata de una variedad, pues si se descompusiera en variedades, sus antiimágenes formarían una descomposición de P^n. Además, las expresiones que hemos obtenido para V_m^{-1} muestran que V_m^{-1} también es regular, luego es un isomorfismo. La variedad $V_m[\mathrm{P}^n]$ se llama *variedad de Veronese,* y hemos probado que es isomorfa a P^n.

El interés de la variedad de Veronese se debe a que si

$$F = \sum a_{i_1,\ldots,i_{n+1}} u_1^{i_1} \cdots u_{n+1}^{i_{n+1}}$$

es una forma de grado m y $H = V(F) \subset \mathrm{P}^n$, entonces $V_m[H]$ es la intersección con $V_m[\mathrm{P}^m]$ del hiperplano de ecuación $\sum a_{i_1,\ldots,i_{n+1}} v_{i_1,\ldots,i_{n+1}} = 0$.

Esto nos permite probar:

Teorema 3.9 *Si $F_1, \ldots, F_{r+1}$ son formas de grado m en P^n que no se anulan simultáneamente en una variedad cerrada $C \subset \mathrm{P}^n$, entonces $\phi : C \longrightarrow \mathrm{P}^r$ dada por*

$$\phi(x) = (F_1(x), \ldots, F_{r+1}(x))$$

es una aplicación finita en su imagen.

Demostración: Consideramos la inmersión de Veronese $V_m : \mathrm{P}^n \longrightarrow \mathrm{P}^N$. Sean $L_1, \ldots, L_{r+1}$ las formas lineales correspondientes con $F_1, \ldots, F_{r+1}$ en P^N y sea $\pi : V_m[C] \longrightarrow \mathrm{P}^r$ la proyección definida en 3.7. Es claro que $\phi = V_m \circ \pi$. Como V_m es un isomorfismo y π es finita, concluimos que ϕ también es finita. ■

Terminamos con dos resultados que necesitaremos más adelante:

Teorema 3.10 (Teorema de normalización de Noether) *Si V es una variedad afín, existe una aplicación finita $\phi : V \longrightarrow A^n$, para cierto n.*

Demostración: Sea $V \subset A^N$. Podemos suponer que $V \neq A^N$. Sea $\overline{V} \subset \mathrm{P}^N$ la clausura de V. Entonces $\overline{V} \neq \mathrm{P}^N$. Tomemos un punto $P \in \mathrm{P}^N \setminus A^N$ tal que $P \notin \overline{V}$ y consideramos la proyección $\phi : \overline{V} \longrightarrow \mathrm{P}^{N-1}$ (definición 3.7). Sabemos que es finita. Concretamente, si $P = (1, a_1, \ldots, a_N, 0)$, será

$$\phi(X_1, \ldots, X_{N+1}) = (a_2 X_1 - X_2, \cdots, a_N X_1 - X_N, X_{N+1}).$$

Es claro que $\phi[V] \subset A^{N-1}$. Si no se da la igualdad entonces, por continuidad y el teorema 2.47, tenemos que $\phi[\overline{V}] = \overline{\phi[V]}$. Podemos repetir el argumento para obtener una aplicación finita $\phi_1 : \overline{\phi[V]} \longrightarrow \mathrm{P}^{N-2}$. Tras un número finito de pasos se ha de dar la igualdad, y la composición de todas las aplicaciones construidas es la aplicación finita buscada. ■

Teorema 3.11 *Si $\phi : V \longrightarrow W$ es una aplicación regular densa entre variedades, entonces $\phi[V]$ contiene un abierto no vacío.*

Demostración: Si U es un abierto afín en W y U' es un abierto afín en $\phi^{-1}[U]$, es claro que $\phi|_{U'} : U' \longrightarrow U$ sigue siendo una aplicación regular densa, luego podemos suponer que V y W son variedades afines. Según 2.45, podemos identificar a $k[W]$ con un subanillo de $k[V]$ a través de $\bar{\phi}$. Sea r el grado de trascendencia de $k(V)$ sobre $k(W)$. Podemos tomar $u_1, \ldots, u_r \in k[V]$ algebraicamente independientes sobre $k(W)$.

Entonces $k[W][u_1, \ldots, u_r] \cong k[W \times A^r]$. Fijando un isomorfismo, podemos factorizar $\bar{\phi} = \bar{\psi} \circ \bar{\chi}$, donde $\bar{\psi} : k[W] \longrightarrow k[W \times A^r]$ y $\bar{\chi} : k[W \times A^r] \longrightarrow k[V]$. Estos monomorfismos inducen a su vez aplicaciones regulares $\chi : V \longrightarrow W \times A^r$ y $\psi : W \times A^r \longrightarrow W$ de modo que $\phi = \chi \circ \psi$. Por 2.45 ambas son densas. De hecho es fácil ver que ψ es simplemente la proyección.

Sea $k[V] = k[v_1, \ldots, v_m]$. Por 1.18 existen $a_1, \ldots, a_m \in k[W \times A^r]$ tales que $a_i v_i$ es entero sobre $k[W \times A^r]$. Sea $f = a_1 \cdots a_m \in k[W \times A^r]$.

Consideramos el abierto $(W \times A^r)_f$ definido en 2.38. Como las funciones a_i son inversibles en $k[(W \times A^r)_f] = k[W \times A^r][1/f]$, concluimos que las funciones v_i son enteras sobre este anillo. Por lo tanto, la restricción

$$\chi : V_{\bar{\phi}(f)} \longrightarrow (W \times A^r)_f$$

es finita, luego es suprayectiva. En particular, $(W \times A^r)_f \subset \chi[V]$, de donde a su vez $\psi[(W \times A^r)_f] \subset \phi[V]$. Basta probar que $\psi[(W \times A^r)_f]$ contiene un abierto en W. Sea $k[W] = k[x_1, \ldots, x_s]$ y $k[A^r] = k[u_1, \ldots, u_r]$. Entonces f es un polinomio en $x_1, \ldots, x_s, u_1, \ldots, u_r$. Digamos que

$$f = \sum_{i_1, \ldots, i_r} F_{i_1, \ldots, i_r}(x_1, \ldots, x_s) u_1^{i_1} \cdots u_r^{i_r}.$$

Como $f \neq 0$, algún $F_0 = F_{i_1, \ldots, i_r}$ no es idénticamente nulo en W. Sea $f_0 = [F] \in k[W]$. Se cumple que $W_{f_0} \subset \psi[(W \times A^r)_f]$, pues si $x \in W_{f_0}$

podemos tomar $u \in A^r$ tal que $f(x,u) \neq 0$, luego $(x,u) \in (W \times A^r)_f$ y así $x = \psi(x,u) \in \psi[(W \times A^r)_f]$. ■

Este resultado es útil para reducir problemas concernientes a aplicaciones entre variedades arbitrarias al caso de aplicaciones entre variedades afines. Concretamente:

Teorema 3.12 *Sea $\phi : V \longrightarrow W$ una aplicación densa entre variedades. Entonces existe un abierto afín $U \subset W$ tal que $U' = \phi^{-1}[U]$ es afín.*

DEMOSTRACIÓN: Sea U un abierto afín en W. El abierto $\phi^{-1}[U]$ no tiene por qué ser afín, pero contiene un abierto afín U', cuya imagen $\phi[U']$ será densa en U. Por el teorema anterior aplicado a $\phi|_{U'} : U' \longrightarrow U$ obtenemos que $\phi[U']$ contiene un abierto, que podemos tomar de la forma U_α, para cierta $\alpha \in k[U]$. Entonces $\phi^{-1}[U_\alpha] = U'_{\bar{\phi}(\alpha)}$ es afín. ■

3.2 La dimensión de un conjunto algebraico

Introducimos ahora el concepto central de este capítulo. Informalmente, la noción algebraica de dimensión está basada en el número de coordenadas independientes que encontramos en una variedad. Por ejemplo, en la circunferencia $X^2 + Y^2 = 1$ podemos encontrar puntos con cualquier valor de X pero, una vez fijada X, sólo hay un número finito de valores posibles para Y (a lo sumo dos). Esto se debe a que las funciones coordenadas sobre la circunferencia (es decir, como elementos de $k(V)$) son algebraicamente dependientes, pues verifican la relación $x^2 + y^2 = 1$. En general, la dimensión de una variedad será el número de coordenadas algebraicamente independientes que podamos encontrar en ella. Con precisión:

Definición 3.13 Llamaremos *dimensión* de una variedad V al grado de trascendencia sobre k de $k(V)$. La representaremos por $\dim V$. La *dimensión* de un conjunto algebraico como el máximo de las dimensiones de sus componentes irreducibles. Un conjunto algebraico tiene *dimensión pura* si todas sus componentes irreducibles tienen la misma dimensión.

Notemos que si V es un abierto en una variedad W, por definición V y W tienen el mismo cuerpo de funciones racionales, luego $\dim V = \dim W$. Por el teorema 2.54, dos variedades birracionalmente equivalentes (en particular, isomorfas) tienen la misma dimensión. Las variedades de dimensión 1 se llaman *curvas*[1] (algebraicas), las variedades de dimensión 2 se llaman *superficies* (algebraicas). Las subvariedades de A^n o P^n de dimensión $n-1$ se llaman *hipersuperficies*.

Si $W \subset V$ son conjuntos algebraicos, se llama *codimensión* de W en V a la diferencia $\dim V - \dim W$. Cuando se habla de la codimensión de un conjunto

[1] Un poco más abajo probaremos que lo que hemos llamado curvas planas son curvas de acuerdo con esta definición general.

algebraico sin especificar respecto a qué otro, se entiende que es respecto al espacio A^n o P^n que lo contiene. Así, por ejemplo, las hipersuperficies son las variedades afines o proyectivas de codimensión 1.

Vamos a calcular la dimensión de algunas variedades sencillas:

Espacios afines y proyectivos Es claro que $\dim A^n = \dim \mathrm{P}^n = n$, pues su cuerpo de funciones racionales es $k(X_1, \ldots, X_n)$.

Puntos Las variedades de dimensión 0 son los puntos. En efecto, por una parte, si P es un punto en cualquier espacio P^n, es claro que se trata de una variedad afín para la que $k[P] = k(P) = k$ (las funciones regulares han de ser constantes), luego $\dim P = 0$. Por otra parte, si V es una variedad de dimensión 0, pasando a su clausura podemos suponer que es cerrada en P^n y cortándola con un espacio afín podemos suponer que es una variedad afín (ninguna de estas operaciones altera el cuerpo de funciones racionales). Entonces resulta que $k(V)$ es algebraico sobre k, pero k es algebraicamente cerrado, luego $k(V) = k$ y también $k[V] = k$. Así pues, las funciones coordenadas son constantes y V es un punto.

El conjunto vacío Es conveniente asignar al conjunto vacío una dimensión menor que a los puntos, por lo que convendremos que $\dim \varnothing = -1$.

Variedades lineales Una variedad lineal proyectiva V es una subvariedad de P^n determinada por m formas lineales

$$\begin{aligned} a_{11}X_1 + \cdots + a_{1n+1}X_{n+1} &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}X_1 + \cdots + a_{mn+1}X_{n+1} &= 0. \end{aligned}$$

Si el rango de la matriz de coeficientes es r, podemos eliminar $m-r$ ecuaciones sin alterar V. Si $r = n+1$ entonces el sistema sólo tiene la solución trivial, con lo que $V = \varnothing$. En otro caso podemos despejar r variables en términos de las $n+1-r$ restantes, de donde se sigue fácilmente que

$$k[X_1, \ldots, X_{n+1}]/I(V) \cong k[X_1, \ldots, X_{n+1-r}].$$

Esto prueba que $I(V)$ es primo, luego V es ciertamente una variedad proyectiva. Es fácil construir un isomorfismo $V \longrightarrow \mathrm{P}^{n-r}$ (eliminando las r coordenadas homogéneas dependientes). Por lo tanto $\dim V = n - r$. Notemos que esta fórmula vale incluso en el caso en que $r = n+1$ y $V = \varnothing$.

Similarmente se tratan las variedades lineales afines, definidas por ecuaciones lineales. Si $V \subset A^n$ está definida por r ecuaciones independientes y $V \neq \varnothing$, entonces V es una variedad isomorfa a A^{n-r} y $\dim V = n - r$. Notemos que ahora hay que suponer explícitamente $V \neq \varnothing$.

Productos Si V y W son variedades, entonces

$$\dim V \times W = \dim V + \dim W.$$

En efecto, como $V \times W$ es abierto en $\overline{V} \times \overline{W}$, no perdemos generalidad si suponemos que las variedades son proyectivas. Por el mismo motivo, podemos cortarlas con espacios afines y suponer que son afines. Digamos que $V \subset A^M$, $W \subset A^N$, $\dim V = m$ y $\dim W = n$. Sean $x_1, \ldots, x_M$ las coordenadas en V e $y_1, \ldots, y_N$ las coordenadas en W. Podemos suponer que $x_1, \ldots, x_m$ son algebraicamente independientes al igual que $y_1, \ldots, y_n$.

Tenemos que $k(V \times W) = k(x_1, \ldots, x_M, y_1, \ldots, y_N)$ y es claro que todos los generadores dependen algebraicamente de $x_1, \ldots, x_m, y_1, \ldots, y_n$. Basta probar que estas coordenadas son algebraicamente independientes. Supongamos que $F(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$. Entonces, para cada punto $(a_1, \ldots, a_M) \in V$, el polinomio $F(a_1, \ldots, a_m, Y_1, \ldots, Y_n)$ anula a $y_1, \ldots, y_n$ en $k(W)$, luego ha de ser el polinomio nulo. Esto significa que cada uno de los coeficientes $a(X_1, \ldots, X_m)$ de F se anula sobre todos los puntos de V, es decir, anula a $x_1, \ldots, x_m$ en $k(V)$, luego $a(X_1, \ldots, X_m) = 0$ y, en conclusión, $F = 0$.

Conos Si V es una variedad proyectiva, $Cn(V)$ es una variedad afín y

$$\dim Cn(V) = \dim V + 1.$$

Ciertamente el cono $Cn(V)$ es una variedad, pues el ideal $I(Cn(V)) = I(V)$ es un ideal primo. Digamos que $V \subset \mathrm{P}^n$. Podemos suponer que V no está contenida en el hiperplano $X_{n+1} = 0$, de modo que $V' = V \cap A^n$ es una variedad afín de la misma dimensión (es abierta en V). Así mismo,

$$Cn(V)' = \{X \in Cn(V) \mid X_{n+1} \neq 0\}$$

es abierto en $Cn(V)$, luego tiene la misma dimensión. Basta observar que la aplicación $\phi : Cn(V)' \longrightarrow V' \times A^1$ dada por

$$\phi(X) = (X_1/X_{n+1}, \ldots, X_n/X_{n+1}, X_{n+1})$$

es un isomorfismo. Claramente es biyectiva y regular, y su inversa es

$$(X, Y) \mapsto (YX_1, \ldots, YX_n, Y),$$

que también es regular. ■

Veamos ahora algunos resultados básicos.

Teorema 3.14 *Si* $\phi : V \longrightarrow W$ *es una aplicación finita entre variedades, entonces* $\dim V = \dim W$.

DEMOSTRACIÓN: Podemos restringir ϕ a una aplicación finita entre abiertos en V y W que sean variedades afines. Por ser abiertos tendrán la misma dimensión que las variedades que los contienen, luego en definitiva podemos suponer que V y W son variedades afines. Entonces $k[V]$ es una extensión entera de $k[W]$, luego $k(V)$ es una extensión algebraica de $k(W)$, luego ambas tienen el mismo grado de trascendencia sobre k. ■

Teorema 3.15 *Sean $V \subset W$ dos variedades. Entonces* $\dim V \leq \dim W$. *Si V es cerrada y* $\dim V = \dim W$ *entonces $V = W$.*

DEMOSTRACIÓN: No perdemos generalidad si suponemos que $W \subset \mathrm{A}^n$. Si $\dim W = m$ y $x_1, \ldots, x_{m+1}$ son $m+1$ funciones coordenadas cualesquiera, tenemos que satisfacen una relación polinómica, y sus restricciones a V cumplirán la misma relación, luego serán algebraicamente dependientes en $k(V)$. Por consiguiente $\dim V \leq m$.

Supongamos ahora que V es cerrada y que $\dim V = \dim W = m$. Tenemos que $I(W) \subset I(V)$, y basta probar la otra inclusión. Sea, pues $F \in I(V)$ un polinomio y supongamos que no es nulo en W. Sea $f = [F] \in k[W]$. Sea $x_1, \ldots, x_m$ una base de trascendencia de $k(V)$ formada por funciones coordenadas. Es claro que estas funciones han de ser algebraicamente independientes en $k(W)$ y, por la hipótesis sobre las dimensiones, han de ser una base de trascendencia de $k(W)$. Por consiguiente f es raíz de un polinomio irreducible

$$a_r(x_1, \ldots, x_m)f^r + \cdots + a_1(x_1, \ldots, x_m)f + a_0(x_1, \ldots, x_m) = 0,$$

de modo que en particular $a_0 \neq 0$. Ahora bien, esta ecuación se cumple también en V, donde además $f = 0$, luego ha de ser $a_0(x_1, \ldots, x_n) = 0$ en V. Pero las funciones x_i son algebraicamente independientes en $k(V)$, luego ha de ser $a_0 = 0$, contradicción. Así pues, $F \in I(W)$. ■

Veamos ahora que las hipersuperficies son las variedades definibles mediante una sola ecuación. Más en general:

Teorema 3.16 *Un subconjunto algebraico C de A^n o P^n es definible por una sola ecuación si y sólo si tiene dimensión pura $n - 1$.*

DEMOSTRACIÓN: Supongamos que C está definido por una única ecuación (no nula) $F = 0$. No perdemos generalidad si suponemos que $C \subset A^n$. Sea $F = F_1^{r_1} \cdots F_m^{r_m}$ la descomposición de F en factores irreducibles. Es claro que

$$C = V(F) = V(F_1) \cup \cdots \cup V(F_m)$$

y basta probar el teorema para cada $V(F_i)$, es decir, podemos suponer que F es irreducible. Entonces (F) es un ideal primo, luego C es una variedad, pues $I(C) = I(V(F)) = \operatorname{rad}(F) = (F)$. Supongamos que la variable X_n aparece en el polinomio $F(X_1, \ldots, X_n)$ y veamos que $x_1, \ldots, x_{n-1}$ son algebraicamente independientes en $k(C)$. En efecto, si se cumpliera una relación $G(x_1, \ldots, x_{n-1}) = 0$, entonces $G(X_1, \ldots, X_{n-1}) \in (F)$, lo cual es imposible.

Por consiguiente $\dim C \geq n-1$ y por el teorema anterior, puesto que $C \neq A^n$, ha de ser $\dim C = n - 1$.

Para probar el recíproco podemos suponer que C es irreducible. Así mismo podemos suponer que es una variedad afín $C \subset A^n$. Como $\dim C = n - 1$, en particular $C \neq A^n$, luego $I(C) \neq 0$. Sea $F \in I(C)$ no nulo. Como $I(C)$ es primo, podemos suponer que F es irreducible. Entonces $C \subset V(F)$, pero por la parte ya probada $\dim C = n - 1 = \dim V(F)$, y por el teorema anterior concluimos que $C = V(F)$. ■

Ahora es claro que las curvas planas son las hipersuperficies de A^2 o P^2. En particular son curvas. En la prueba de este teorema hemos visto que, al igual que ocurre con las curvas planas, las hipersuperficies son las variedades definibles por una sola ecuación irreducible. El hecho de que las hipersuperficies sean las superficies con la definición más simple posible no impide que sean muy representativas, tal y como muestra el teorema siguiente:

Teorema 3.17 *Toda variedad de dimensión n es birracionalmente equivalente a una hipersuperficie de A^{n+1}.*

DEMOSTRACIÓN: Sea V una variedad de dimensión n. Por 1.32 podemos tomar una base de trascendencia $x_1, \ldots, x_n$ de $k(V)$ de manera que la extensión $k(V)/k(x_1, \ldots, x_n)$ sea separable. Por el teorema del elemento primitivo, existe $x_{n+1} \in k(V)$ tal que $k(V) = k(x_1, \ldots, x_{n+1})$. Sea $F(x_1, \ldots, x_n, X_{n+1})$ el polinomio mínimo de x_{n+1} sobre $k(x_1, \ldots, x_n)$.

El homomorfismo $k[X_1, \ldots, X_{n+1}] \longrightarrow k(V)$ dado por $X_i \mapsto x_i$ tiene por núcleo (F), luego $k[X_1, \ldots, X_{n+1}]/(F) \cong k[x_1, \ldots, x_{n+1}]$. En particular es un dominio íntegro y (F) es primo. Por consiguiente $W = I(F)$ es una subvariedad de A^{n+1} tal que $k[W] \cong k[x_1, \ldots, x_{n+1}]$, luego $k(W) \cong k(V)$ y, por 2.54, concluimos que V es birracionalmente equivalente a W. Esto implica a su vez que $\dim W = n$, luego W es una hipersuperficie de A^{n+1}. ■

En particular toda curva es birracionalmente equivalente a una curva plana.

Ya sabemos que cuando a los puntos de P^N les imponemos una restricción polinómica, pasamos a un conjunto de dimensión $N - 1$. Ahora generalizaremos esto demostrando que cada ecuación (no redundante) que añadimos a un conjunto algebraico disminuye una unidad la dimensión.

Teorema 3.18 *Sea $V \subset \mathrm{P}^N$ una variedad proyectiva de dimensión n y sea $F \in k[X_1, \ldots, X_{N+1}]$ una forma que no es idénticamente nula en V. Sea*

$$V_F = \{P \in V \mid F(P) = 0\}.$$

Entonces $\dim V_F = n - 1$.

DEMOSTRACIÓN: Observemos en general que si C es un conjunto algebraico proyectivo, no necesariamente irreducible, existe una forma G de cualquier grado m prefijado que no es idénticamente nula en ninguna componente irreducible de C. Basta tomar un punto de cada componente de C, tomar una forma lineal L que no se anule en ninguno de ellos y considerar $G = L^m$. (Para encontrar L basta tomar un punto que no sea solución de un número finito de ecuaciones lineales, o sea, fuera del conjunto algebraico definido por el producto de todas ellas.)

Llamemos $V^0 = V$, $F_0 = F$ y $V^1 = V_F$. Sea ahora F_1 una forma del mismo grado que F que no se anule en ninguna componente irreducible de V^1 y sea $V^2 = V^1_{F_1}$, etc. Por el teorema 3.15 tenemos que

$$\dim V^0 > \dim V^1 > \cdots$$

Por consiguiente $V^{n+1} = \varnothing$. Esto significa que las formas $F_0, \ldots, F_n$ no tienen ceros comunes en V. Sea $\phi : V \longrightarrow \mathrm{P}^n$ la aplicación dada por

$$\phi(P) = (F_0(P), \ldots, F_n(P)).$$

Según 3.9, la aplicación ϕ es finita en su imagen, luego

$$n = \dim V = \dim \phi[V] \leq \dim \mathrm{P}^n = n,$$

luego ϕ es suprayectiva. Ahora bien, si fuera $\dim V_F < n - 1$, en realidad $V^n = \varnothing$, luego las formas $F_0, \ldots, F_{n-1}$ no tendrían ceros comunes en V. A su vez, esto se traduciría en que el punto $(0, \ldots, 0, 1)$ no estaría en la imagen de ϕ, contradicción. ■

De aquí se sigue inmediatamente que una variedad posee subvariedades de cualquier dimensión menor que la suya. Observemos que lo que hemos probado es que al menos una componente irreducible de V_F tiene dimensión $n-1$, aunque en principio podría haber otras componentes de dimensión menor. Vamos a ver que no es así:

Teorema 3.19 *Bajo las hipótesis del teorema anterior, V_F tiene dimensión pura $n - 1$.*

Demostración: Consideramos la aplicación finita $\phi : V \longrightarrow \mathrm{P}^n$ construida en la prueba del teorema anterior y sean A^n_i los subespacios afines de P^n determinados por $X_i \neq 0$. Sea $U_i = \phi^{-1}[A^n_i]$. Así

$$U_i = \{P \in V \mid F_i(P) \neq 0\}.$$

Si $V \subset \mathrm{P}^k$, la inmersión de Veronese $V_m : \mathrm{P}^k \longrightarrow \mathrm{P}^N$ transforma U_i es una variedad isomorfa contenida en el complementario de un hiperplano de P^N, es decir, en una variedad afín. Por lo tanto U_i es afín.

Toda componente irreducible W de V_F corta a algún U_i, y entonces $W \cap U_i$ es abierto en W, luego tiene la misma dimensión. Así pues, basta probar que cada componente irreducible de $V_F \cap U_i$ tiene dimensión $n - 1$ (de hecho, basta ver que es $\geq n - 1$). Por abreviar omitiremos el subíndice $U = U_i$.

Sea $f = [F]/[F_i] \in k[U]$. De este modo,

$$C = V_F \cap U = \{P \in U \mid f(P) = 0\}.$$

Sean $f_1, \ldots, f_n \in k[U]$ las funciones $[F_j]/[F_i]$ para $j \neq i$. Notemos que $f = f_1$. Por 3.5, la aplicación ϕ se restringe a una aplicación finita $\phi : U \longrightarrow A^n$ cuyas funciones coordenadas son las f_i. Así pues, $\bar{\phi} : k[X_1, \ldots, X_n] \longrightarrow k[U]$ cumple $\phi(X_i) = f_i$.

Ahora podemos sustituir U por una variedad isomorfa $U \subset A^m$. Digamos que $f_i = [F_i]$, para ciertos polinomios $F_i \in k[Y_1, \ldots, Y_m]$ (que no tienen nada que ver con las formas F_i anteriores).

Sea W una componente irreducible de C. Basta probar que las funciones $f_i|_W$, para $i = 2, \ldots n$, son algebraicamente independientes en $k[W]$. Supongamos, por reducción al absurdo, que existe $G(X_2, \ldots, X_n) \in k[X_1, \ldots, X_n]$ no nulo tal que $G(f_2|_W, \ldots, f_n|_W) = 0$. Sea $G' = G(F_2, \ldots, F_n) \in I(W)$.

Para cada componente irreducible W' de C distinta de W, podemos tomar un polinomio de $I(W') \setminus I(W)$, y el producto de tales polinomios es un polinomio H que es idénticamente nulo en todas las componentes de C excepto en W. Así

$$G'H \in I(C) = I(V(I(U) \cup \{F_1\})) = \operatorname{Rad}(I(U) \cup \{F_1\}),$$

luego $(G'H)^l \in (I(U) \cup \{F_1\})$. Tomando clases módulo $I(U)$ concluimos que $(g'h)^l \in (f_1)$, es decir, que $f_1 \mid (g'h)^l$, para cierto $l > 0$.

Vamos a probar que $f_1 \mid h^r$, para cierto $r > 0$, lo cual implica que H se anula en C, en contradicción con la forma en que lo hemos construido.

Observemos que $k[f_1, \ldots, f_n] \subset k[U]$ es isomorfo a $k[X_1, \ldots, X_n]$ (a través de $\bar{\phi}$), luego en particular es un dominio de factorización única. Como g' en un polinomio en $f_2, \ldots, f_n$, es claro que f_1 y g' son primos entre sí. No podemos concluir directamente que $f_1 | h$ porque $h \notin k[f_1, \ldots, f_n]$, pero sabemos que es un entero algebraico sobre este anillo. Es claro que basta demostrar este hecho puramente algebraico:

> *Sea $A = k[X_1, \ldots, X_n]$ y B una extensión entera de A. Sean x, $y \in A$ primos entre sí y sea $z \in B$ tal que $x \mid yz$ en B. Entonces existe un $r > 0$ tal que $x \mid z^r$.*

En efecto, digamos que $yz = xw$, con $w \in B$. Sea

$$p(T) = T^r + b_1 T^{r-1} + \cdots + b_r$$

el polinomio mínimo de w sobre $k(X_1, \ldots, X_n)$. Como A es un dominio de factorización única, es íntegramente cerrado (teorema 1.16), luego por 1.17 tenemos que $p(T) \in A[T]$. El polinomio mínimo de $z = xw/y$ será $q(T) = (x/y)^r p(yT/x)$, es decir,

$$q(T) = T^r + \frac{xb_1}{y} T^{r-1} + \cdots + \frac{x^r b_r}{y^r} \in A[T].$$

Así pues, $x^i b_i / y^i \in A$, luego $y^i \mid x^i b_i$ en A y, como x e y son primos entre sí, de hecho $y^i \mid b_i$. Por consiguiente,

$$z^r = -x \left(\frac{b_1}{y} z^{r-1} + \frac{xb_2}{y^2} z^{r-2} + \cdots + \frac{x^{r-1} b_r}{y^r} \right),$$

luego $x \mid z^r$. ■

De aquí podemos deducir un teorema importante sobre dimensiones. Previamente demostramos unos hechos de interés en sí mismos. El primero es la generalización del teorema anterior para variedades cuasiproyectivas.

Teorema 3.20 *Sea $V \subset \mathrm{P}^N$ una variedad cuasiproyectiva de dimensión n y $F \in k[X_1, \ldots, X_{N+1}]$ una forma que no es idénticamente nula en V. Si $V_F \neq \varnothing$, entonces tiene dimensión pura $n-1$.*

DEMOSTRACIÓN: Sea $\overline{V}_F = W_1 \cup \cdots \cup W_r$ la descomposición de $\overline{V}_F$ en componentes irreducibles. Por el teorema anterior tienen dimensión $n-1$. Es claro que $V_F = \overline{V}_F \cap V$, luego

$$V_F = (W_1 \cap V) \cup \cdots \cup (W_r \cap V).$$

Cada $W_i \cap V$ es vacío o bien abierto en W_i (porque V es abierto en $\overline{V}$), luego las $W_i \cap V$ no vacías son las componentes irreducibles de V y tienen dimensión $n-1$. ■

Notemos que si $V \subset A^N$ es una variedad afín entonces las formas en $N+1$ variables se corresponden con las aplicaciones de $k[A^N]$, las cuales se corresponden a su vez con las aplicaciones de $k[V]$. Por lo tanto, un caso particular del teorema anterior se enuncia como sigue:

Teorema 3.21 *Sea V una variedad afín de dimensión n y sea $f \in k[V]$, $f \neq 0$. Si el conjunto $\{P \in V \mid f(P) = 0\}$ es no vacío, tiene dimensión pura $n-1$.*

El teorema siguiente se prueba por inducción sobre m a partir de 3.20:

Teorema 3.22 *Sea $V \subset \mathrm{P}^N$ una variedad cuasiproyectiva de dimensión n y sea C el conjunto de los puntos de V que anulan simultáneamente m formas en $N+1$ variables. Si $C \neq \varnothing$, entonces todas sus componentes irreducibles tienen dimensión $\geq n-m$.*

Las mismas consideraciones previas a 3.21 nos dan ahora:

Teorema 3.23 *Sea V una variedad afín de dimensión n y sea C el conjunto de los puntos de V donde se anulan m funciones de $k[V]$. Entonces, si $C \neq \varnothing$ todas sus componentes irreducibles tienen dimensión $\geq n-m$.*

El teorema siguiente es un primer ejemplo de un teorema global de la geometría algebraica:

Teorema 3.24 *Sean V, $W \subset \mathrm{P}^N$ dos variedades cuasiproyectivas y sea X una componente irreducible no vacía (supuesto que exista) de $V \cap W$. Entonces*

$$\operatorname{codim} X \leq \operatorname{codim} V + \operatorname{codim} W.$$

Si V y W son proyectivas y $\operatorname{codim} V + \operatorname{codim} W \leq N$, entonces $V \cap W \neq \varnothing$ y, en particular,

$$\operatorname{codim}(V \cap W) \leq \operatorname{codim} V + \operatorname{codim} W.$$

DEMOSTRACIÓN: Para la primera parte, tomando clausuras, podemos suponer que las variedades son proyectivas y, cortándolas con un espacio afín A^N que corte a X, podemos suponer que son afines: $V, W \subset A^N$. Sea $\Delta \subset A^N \times A^N$ la diagonal. La aplicación $\phi : V \cap W \longrightarrow A^N \times A^N$ dada por $\phi(P) = (P, P)$ tiene imagen $(V \times W) \cap \Delta$ y claramente es un isomorfismo. Como Δ está definido por las N funciones $x_i - y_i$, el teorema anterior nos da que

$$\dim X = \dim \phi[X] \geq \dim(V \times W) - N = \dim V + \dim W - N.$$

Por consiguiente,

$$\operatorname{codim} X \leq 2N - \dim V - \dim W = \operatorname{codim} V + \operatorname{codim} W.$$

Para la segunda parte consideramos los conos $Cn(V)$ y $Cn(W)$, que son variedades en A^{N+1} de dimensión una unidad mayor (luego de la misma codimensión). Además $Cn(V \cap W) = Cn(V) \cap Cn(W)$. Como la intersección contiene al menos al origen, podemos aplicar la parte ya probada, en virtud de la cual

$$\operatorname{codim} Cn(V \cap W) \leq \operatorname{codim} Cn\, V + \operatorname{codim} Cn\, W = \operatorname{codim} V + \operatorname{codim} W \leq N,$$

luego $\dim Cn(V \cap W) \geq 1$ y $\dim(V \cap W) \geq 0$, luego $V \cap W \neq \varnothing$. ■

Ejercicio: Ahora es claro que dos curvas en P^2 se cortan al menos en un punto. Probar que esto generaliza al teorema fundamental del álgebra mostrando que una curva $Y = F(X)$ no puede cortar al eje X $(Y = 0)$ en el punto infinito $(1, 0, 0)$.

3.3 Variedades tangentes y diferenciales

Vamos a asociar una variedad tangente a cada punto de una variedad, en correspondencia con la noción análoga en geometría diferencial. Primeramente conviene definir la diferencial de un polinomio:

Sea $F(X) \in k[X_1, \ldots, X_n]$ y $a \in k^n$. Considerando la descomposición en formas del polinomio $F'(X') = F(a + X')$ podemos expresar

$$F(X) = F(a) + F_1(X - a) + F_2(X - a) + \cdots$$

donde F_i es una forma de grado i. Derivando esta descomposición obtenemos que

$$\frac{\partial F}{\partial X_i} = \frac{\partial F_1}{\partial X_i} + \frac{\partial F_2}{\partial X_i}(X - a) + \cdots$$

luego

$$\frac{\partial F_1}{\partial X_i} = \left.\frac{\partial F}{\partial X_i}\right|_a$$

y, por consiguiente,

$$F_1(X - a) = \left.\frac{\partial F}{\partial X_1}\right|_a (X_1 - a_1) + \cdots + \left.\frac{\partial F}{\partial X_n}\right|_a (X_n - a_n).$$

Definición 3.25 La *diferencial* de un polinomio $F(X) \in k[X_1, \ldots, X_n]$ en un punto $a \in k^n$ es el polinomio

$$d_aF(X) = \left.\frac{\partial F}{\partial X_1}\right|_a X_1 + \cdots + \left.\frac{\partial F}{\partial X_n}\right|_a X_n.$$

Hemos probado que

$$F(X) = F(a) + d_aF(X-a) + F_2(X-a) + F_3(X-a) + \cdots$$

donde cada F_i es una forma de grado i.

Se comprueba inmediatamente que

$$d_a(F+G) = d_aF + d_aG, \qquad d_a(FG) = F(a)\,d_aG + G(a)\,d_aF. \tag{3.4}$$

Definición 3.26 Si $V \subset A^n$ es una variedad afín y $P \in V$. Fijado un sistema de referencia en A^n, sea $a \in k^n$ el vector de coordenadas de P. Llamaremos *variedad tangente* a V en P a la variedad lineal T_PV determinada por las ecuaciones $d_aF(X-a) = 0$, donde F recorre $I(V)$.

Las relaciones (3.4) muestran que si $I(V) = (F_1, \ldots, F_m)$, entonces

$$T_P(V) = V(d_aF_1(X-a), \ldots, d_aF_m(X-a)).$$

En principio, esta definición depende del sistema de referencia en el que calculamos las coordenadas de P y el ideal $I(V)$. Vamos a ver que en realidad no es así. Consideremos dos sistemas de referencia O y O'. Sea $X = c + X'A$ la ecuación de cambio de coordenadas, donde $c \in k^n$ y A es una matriz regular. El punto P tendrá vectores de coordenadas a y a' relacionados por $a = c + a'A$. Por otra parte, cada $F(X) \in I(V)$ se corresponde con $F'(X') = F(c+X'A) \in I(V)'$.

Hemos de probar que si un punto $Q \in A^n$ tiene coordenadas X y X', entonces

$$d_aF(X-a) = 0 \leftrightarrow d_{a'}F'(X'-a') = 0.$$

En efecto, es claro que

$$\left.\frac{\partial F'}{\partial X'_i}\right|_{a'} = \left.\frac{\partial F}{\partial X_1}\right|_a a_{i1} + \cdots + \left.\frac{\partial F}{\partial X_n}\right|_a a_{in},$$

luego si llamamos $\nabla F'(a')$ y $\nabla F(a)$ a los vectores formados por las derivadas parciales, vemos que su relación es $\nabla F'(a') = \nabla F(a)A^t$. Ahora es claro que

$$d_{a'}F'(X'-a') = (X'-a') \cdot \nabla F'(a')^t = (X-a)A^{-1}A\nabla F(a)^t = d_aF(X-a).$$

Esto prueba que la variedad tangente no depende del sistema de referencia desde el cual se calcula. ■

Ejemplos *Si $V = \{P\} \subset A^n$, entonces $T_P V = \{P\}$.*

En efecto, si P tiene coordenadas $a \in k^n$, entonces

$$I(V) = (X_1 - a_1, \ldots, X_n - a_n),$$

luego las ecuaciones de $T_P V$ se reducen a $X_i - a_i = 0$, con lo que $T_P(V) = \{P\}$.

Si $V = A^n$, entonces $T_P(V) = A^n$.

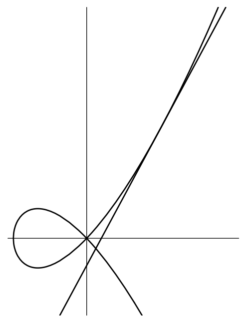
En efecto, $I(V) = (1)$ y la ecuación de $T_P V$ es $0 = 0$.

Si V es la circunferencia $X^2 + Y^2 = 1$ (y la característica del cuerpo k no es 2), entonces $T_P V$ es una recta en cada punto $P \in V$.

En efecto, la ecuación de $T_P V$ en un punto P de coordenadas (a, b) es claramente $2a(X - a) + 2b(Y - b) = 0$. Esta ecuación no puede ser idénticamente nula, ya que $(0, 0) \notin V$.

Si V y W son variedades afines, $T_{(P,Q)}(V \times W) = T_P V \times T_Q W$.

En efecto, $I(V \times W)$ está generado por los polinomios de $I(V)$ en las indeterminadas $X_1, \ldots, X_n$ y los polinomios de $I(W)$ en las indeterminadas $Y_1, \ldots, Y_m$, luego un punto (R, S) está en $T_{(P,Q)}(V \times W)$ si y sólo si R cumple las ecuaciones de $T_P V$ y S cumple las ecuaciones de $T_Q W$.



Consideremos ahora $V = V(Y^2 - X^2(X + 1))$. La ecuación para $T_P V$ en un punto P de coordenadas (a, b) es

$$-a(3a + 2)(X - a) + 2b(Y - b) = 0.$$

Esto es una recta salvo si $a(3a-2) = b = 0$. Teniendo en cuenta que $P \in V$, el único punto que cumple $b = 0$ es $(0, 0)$. Así pues, la variedad tangente a V es una recta en todos los puntos excepto en $(0, 0)$, donde $T_{(0,0)}V = A^2$. La figura muestra la tangente en el punto $(1, \sqrt{2})$. ■

Estos ejemplos sugieren que la dimensión de la variedad tangente es "por lo general" la dimensión de V, si bien esto puede fallar en los puntos "problemáticos", como es el caso del punto donde la curva "alfa" se corta a sí misma.

Hasta aquí hemos trabajado con variedades afines. Consideremos ahora una variedad proyectiva $V \subset \mathrm{P}^n$, sea $P = (a_1, \ldots, a_n, 1)$ un punto del espacio afín A^n determinado por $x_{n+1} \neq 0$ y sea $V_* = V \cap A^n$. Tomemos una forma $F \in I(V)$, de modo que $f(X_1, \ldots, X_n) = F(X_1, \ldots, X_n, 1) \in I(V_*)$. Entonces, un punto $(X_1, \ldots, X_n, 1) \in A^n$ está en $T_P V_*$ si cumple (para toda F)

$$\left.\frac{\partial f}{\partial X_1}\right|_{(a_1,\ldots,a_n)} (X_1 - a_1) + \cdots + \left.\frac{\partial f}{\partial X_n}\right|_{(a_1,\ldots,a_n)} (X_n - a_n) = 0.$$

Equivalentemente, la condición es

$$\left.\frac{\partial F}{\partial X_1}\right|_{(a_1,\ldots,a_n,1)} (X_1 - a_1 X_{n+1}) + \cdots + \left.\frac{\partial F}{\partial X_n}\right|_{(a_1,\ldots,a_n,1)} (X_n - a_n X_{n+1}) = 0.$$

Es fácil ver que si F es una forma de grado r, se cumple la relación

$$\frac{\partial F}{\partial X_1} X_1 + \cdots + \frac{\partial F}{\partial X_{n+1}} X_{n+1} = rF.$$

Como $F(a_1, \ldots, a_n, 1) = 0$, en particular

$$\left.\frac{\partial F}{\partial X_1}\right|_{(a_1,\ldots,a_n,1)} a_1 + \cdots + \left.\frac{\partial F}{\partial X_n}\right|_{(a_1,\ldots,a_n,1)} a_n = - \left.\frac{\partial F}{\partial X_{n+1}}\right|_{(a_1,\ldots,a_n,1)}.$$

Multiplicando ambos miembros por X_{n+1} y sumando esta identidad a la condición de tangencia, obtenemos que ésta equivale a

$$\left.\frac{\partial F}{\partial X_1}\right|_{(a_1,\ldots,a_n,1)} X_1 + \cdots + \left.\frac{\partial F}{\partial X_{n+1}}\right|_{(a_1,\ldots,a_n,1)} X_{n+1} = 0.$$

Esta condición es homogénea tanto en X como en P, luego podemos expresarla en la forma

$$\left.\frac{\partial F}{\partial X_1}\right|_{P} X_1 + \cdots + \left.\frac{\partial F}{\partial X_{n+1}}\right|_{P} X_{n+1} = 0. \tag{3.5}$$

Es fácil ver que esta condición no depende del sistema de referencia, de modo que podemos dar la definición siguiente:

Definición 3.27 Si $V \subset \mathrm{P}^n$ es una variedad proyectiva y $P \in V$, definimos la *variedad (proyectiva) tangente* a V en P como la variedad lineal $T_P V$ determinada por las ecuaciones (3.5), donde F varía en las formas de (un generador de) $I(V)$.

El razonamiento precedente muestra que $T_P V$ es la clausura proyectiva de la variedad tangente en P a la variedad afín V_* que resulta de cortar V con el complementario de cualquier hiperplano en el que no esté P. En particular $\dim T_P V = \dim T_P V_*$.

Definimos la *variedad tangente* en un punto de una variedad cuasiproyectiva como la variedad tangente en dicho punto de su clausura proyectiva.

Volvamos al caso de una variedad afín V y un punto $P \in V$. Entonces $T_P V$ es una variedad lineal afín, luego si fijamos a P como origen, $T_P V$ adquiere una estructura natural de espacio vectorial, caracterizada por que si a es el vector de coordenadas de P en A^n, entonces las aplicaciones $x_i - a_i$ son lineales. La dimensión de $T_P V$ como espacio vectorial es la misma que como variedad.

Observemos ahora que si $g = [G] = [G'] \in k[V]$, con G, $G' \in k[X_1, \ldots, X_n]$, entonces $G - G' \in I(V)$, luego $d_a G(X-a) - d_a G'(X-a) \in I(T_P V)$. Esto nos permite definir $d_P g = [d_a G(X-a)] \in k[T_P V]$. Se cumple que la función $d_P g$ no depende del sistema de referencia con el que se calcula: Si $g = [G]$, en otro sistema de referencia dado por $X = c + X'A$, tenemos que $g = [G']$, donde $G'(X') = G(c + X'A)$. Entonces

$$d_{a'} G'(X' - a') = (X' - a') \nabla G'(a')^t = (X - a) A^{-1} A \nabla G(a)^t = d_a G(X - a).$$

Más aún, es claro que d_Pg es una forma lineal en T_PV, pues

$$d_Pg = \left.\frac{\partial G}{\partial X_1}\right|_a d_Px_1 + \cdots + \left.\frac{\partial G}{\partial X_n}\right|_a d_Px_n$$

y $d_Px_i = x_i - a_i$. Tenemos así una aplicación $d_P : k[V] \longrightarrow T_PV^*$, donde T_PV^* es el espacio dual de T_PV. Claramente se cumple:

$$d_P(f+g) = d_Pf + d_Pg, \qquad d_P(fg) = f(P)d_Pg + g(P)d_Pf.$$

Más aún, podemos extender d_P a una aplicación lineal $d_P : \mathcal{O}_P(V) \longrightarrow T_PV^*$ mediante

$$d_P(f/g) = \frac{g(P)\,d_Pf - f(P)\,d_Pg}{g(P)^2} \in T_PV^*.$$

No es difícil probar que esta extensión está bien definida y sigue cumpliendo las relaciones usuales para la suma y el producto. De todos modos no necesitamos este hecho, ya que vamos a restringir d_P al ideal maximal

$$\mathfrak{m}_P = \{\alpha \in \mathcal{O}_P(V) \mid \alpha(P) = 0\},$$

donde la definición se reduce a

$$d_P(f/g) = \frac{d_Pf}{g(P)},$$

y en este caso las comprobaciones son mucho más sencillas. Ahora probamos:

Teorema 3.28 *Sea $V \subset A^n$ una variedad afín y $P \in V$. Entonces d_P induce un isomorfismo de espacios vectoriales $d_P : \mathfrak{m}_P/\mathfrak{m}_P^2 \longrightarrow T_PV^*$.*

Demostración: Fijemos un sistema de referencia en A^n respecto al que P tenga coordenadas nulas. Éste determina una estructura de espacio vectorial en A^n de modo que T_PV es un subespacio. Toda $\phi \in T_PV^*$ se extiende a una forma lineal $L \in (A^n)^*$, que no es más que una forma lineal $L(X) \in k[X_1, \ldots, X_n]$. Si llamamos $f = [L] \in k[V]$, es claro que $d_Pf = \phi$. Además $f(P) = f(0) = 0$, luego $f \in \mathfrak{m}_P$.

Con esto tenemos que d_P es suprayectiva. Sólo falta probar que su núcleo es $\mathfrak{m}_P^2$. Este ideal está generado por los productos $\alpha\beta$, con $\alpha, \beta \in \mathfrak{m}_P$. Claramente $d_P(\alpha\beta) = \alpha(P)d_P\beta + \beta(P)d_P\alpha = 0$, luego tenemos una inclusión. Supongamos ahora que $\alpha = g/h \in \mathfrak{m}_P$ cumple $d_P\alpha = 0$. Si $g = [G]$, entonces $d_0G \in I(T_PV)$, luego

$$d_0G = \alpha_1 d_PF_1 + \cdots + \alpha_m d_PF_m,$$

para ciertos $F_1, \ldots, F_m \in I(V)$ y $\alpha_1, \ldots, \alpha_m \in k$ (en principio los α_i podrían ser polinomios arbitrarios, pero como d_0G tiene grado 1, han de ser constantes).

Sea $G' = G - \alpha_1F_1 - \cdots - \alpha_mF_m$. Claramente, G' no tiene términos de grado 0 o 1, luego $G' \in (X_1, \ldots, X_n)^2$. Por otra parte, $G'|_V = G|_V = g$, luego $\alpha = [G']/h \in (x_1, \ldots, x_n)^2 = \mathfrak{m}_P^2$. ■

Puesto que T_PV puede identificarse canónicamente con su bidual, concluimos que la codiferencial

$$d_P^* : T_PV \longrightarrow (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$$

(es decir, la aplicación dual de la diferencial) determina un isomorfismo entre T_PV y el espacio dual de $\mathfrak{m}_P/\mathfrak{m}_P^2$. La importancia de este hecho radica en que $(\mathfrak{m}_P/\mathfrak{m}_P^2)^*$ está completamente determinado por el anillo $\mathcal{O}_P(V)$, y $\mathcal{O}_P(V)$ se conserva por isomorfismos, de donde podemos concluir que $\dim T_PV$ se conserva por isomorfismos. De todos modos podemos explicitar esto mucho más:

Si $\phi : V \longrightarrow W$ es una aplicación racional entre variedades afines, regular en $P \in V$, y $Q = \phi(P) \in W$, entonces ϕ induce un homomorfismo de anillos $\bar{\phi} : \mathcal{O}_Q(W) \longrightarrow \mathcal{O}_P(V)$, que claramente cumple $\bar{\phi}[\mathfrak{m}_Q] \subset \mathfrak{m}_P$, $\bar{\phi}[\mathfrak{m}_Q^2] \subset \mathfrak{m}_P^2$. Por consiguiente $\bar{\phi}$ induce una aplicación lineal $\bar{\phi} : \mathfrak{m}_Q/\mathfrak{m}_Q^2 \longrightarrow \mathfrak{m}_P/\mathfrak{m}_P^2$, la cual a su vez induce $\bar{\phi}^* : (\mathfrak{m}_P/\mathfrak{m}_P^2)^* \longrightarrow (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^*$. Componiendo con los isomorfismos d_P^* y d_Q^* obtenemos una aplicación lineal

$$d_P\phi : T_PV \longrightarrow T_QW,$$

a la que llamaremos *diferencial* de ϕ. Es fácil comprobar la relación

$$d_P(\phi \circ \psi) = d_P\phi \circ d_{\phi(P)}\psi,$$

así como que la diferencial de la identidad es la identidad. Ahora podemos ver explícitamente cómo un isomorfismo entre variedades induce isomorfismos entre sus espacios tangentes:

Teorema 3.29 *Sea $\phi : V \longrightarrow W$ una aplicación racional entre variedades afines que se restrinja a un isomorfismo entre un entorno de $P \in V$ y un entorno de $Q = \phi(P) \in W$. Entonces $d_P\phi : T_PV \longrightarrow T_PW$ es un isomorfismo de espacios vectoriales.*

Demostración: La hipótesis implica que ϕ es birracional, luego induce un isomorfismo de cuerpos $\bar{\phi} : k(W) \longrightarrow k(V)$ que se restringe a un isomorfismo de anillos $\bar{\phi} : \mathcal{O}_Q(W) \longrightarrow \mathcal{O}_P(V)$. Es claro entonces que la diferencial es también un isomorfismo. ■

El teorema 3.28 nos permite olvidarnos de la variedad tangente tal y como la hemos definido y trabajar en su lugar con el espacio $(\mathfrak{m}_P/\mathfrak{m}_P^2)^*$:

Definición 3.30 Sea V una variedad cuasiproyectiva y $P \in V$. Definimos el *espacio tangente* a V en P como el espacio vectorial $T_PV = (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$. El espacio $\mathfrak{m}_P/\mathfrak{m}_P^2$ se llama *espacio cotangente* de V en P.

Si $\phi : V \longrightarrow W$ es una aplicación racional regular en un punto $P \in V$, definimos la *diferencial* $d_P\phi : T_PV \longrightarrow T_{\phi(P)}W$ como la dual de la aplicación lineal $\bar{\phi} : \mathfrak{m}_{\phi(P)}/\mathfrak{m}_{\phi(P)}^2 \longrightarrow \mathfrak{m}_P/\mathfrak{m}_P^2$.

Tenemos así un espacio tangente abstracto que no depende de la forma en que V está sumergida en un espacio proyectivo. Cuando $V \subset A^n$, tenemos un isomorfismo canónico entre el espacio tangente abstracto y la variedad tangente $T_PV \subset A^n$. Aunque podríamos deducirlo de los hechos ya teníamos probados, es inmediato comprobar directamente que la diferencial de una composición es la composición de las diferenciales y la diferencial de un isomorfismo local es un isomorfismo.

Ejemplos *Si $c_Q : V \longrightarrow W$ es la función constante $c_Q(R) = Q$ y $P \in V$, entonces $d_Pc_Q = 0$.*

En efecto, para cada $f \in (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$ y cada clase $[\alpha] \in \mathfrak{m}_Q/\mathfrak{m}_Q^2$ tenemos que

$$d_Pc_Q([\alpha]) = \overline{c}_Q^*(f)([\alpha]) = (\overline{c}_Q \circ f)([\alpha]) = f([c_Q \circ \alpha]) = 0,$$

pues $c_Q \circ \alpha \in \mathfrak{m}_P/\mathfrak{m}_P^2$ es la función nula. ■

Sean V y W dos variedades cuasiproyectivas, sea $(P,Q) \in V \times W$, sean

$$p_1 : V \times W \longrightarrow V, \qquad p_2 : V \times W \longrightarrow W$$

las proyecciones y

$$i_Q^1 : V \longrightarrow V \times W, \qquad i_P^2 : W \longrightarrow V \times W$$

las aplicaciones dadas por $i_Q^1(R) = (R,Q)$, $i_P^2(R) = (P,R)$. Entonces,

$$d_Pi_Q^1 : T_PV \longrightarrow T_{(P,Q)}(V \times W), \qquad d_Qi_P^2 : T_QV \longrightarrow T_{(P,Q)}(V \times W)$$

son inyectivas y, si identificamos T_PV y T_QW con sus imágenes, se cumple que $T_{(P,Q)}(V \times W) = T_PV \oplus T_QW$ y las diferenciales $d_{(P,Q)}p_i$ son las proyecciones.

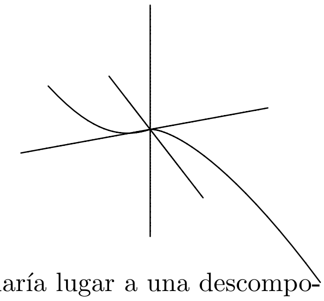
En efecto, se cumple que $i_Q^1 \circ p_1$ es la identidad, luego $d_Pi_Q^1 \circ d_{(P,Q)}p_1$ también es la identidad, lo que prueba que $d_Pi_Q^1$ es inyectiva. Por otro lado, $i_Q^1 \circ p_2$ es constante, luego $d_Pi_Q^1 \circ d_{(P,Q)}p_2 = 0$.

Si $v \in T_PV \cap T_QW$, entonces $v = d_Pi_Q^1(v')$, con $v' \in T_PV$, pero entonces $v' = d_{(P,Q)}p_1(v) = 0$, luego $v = 0$. Así pues, la suma de los dos espacios tangentes es directa.

Hemos visto que, en el caso en que V y W son variedades afines tenemos la relación $T_{(P,Q)}(V \times W) = T_PV \times T_QW$. De aquí se sigue que, en general, $\dim T_{(P,Q)}(V \times W) = \dim T_PV + \dim T_QW$. (Basta tomar entornos afines de P y Q en V y W y tener en cuenta que las dimensiones se conservan por isomorfismos.)

Por consiguiente la suma directa de los espacios tangentes coincide con $T_{(P,Q)}(V \times W)$. El hecho de que las $d_{(P,Q)}p_i$ son las proyecciones es ahora inmediato. ■

Ejercicio: En la situación del ejemplo anterior, pero suponiendo que V y W son variedades afines, demostrar que las diferenciales $d_{(P,Q)}p_i$ son las proyecciones de $T_{(P,Q)}(V \times W) = T_PV \times T_QW$ y que $d_Pi_Q^1$ y $d_Qi_P^2$ son la identidad en T_PV y T_QW.



Sea $\phi : A^1 \longrightarrow A^n$ la aplicación regular dada por

$$\phi(t) = (t^n, t^{n+1}, \ldots, t^{2n-1}).$$

Es fácil ver que su imagen V_n es un conjunto algebraico, definido por las ecuaciones

$$X_{i+1}^{n+i-1} = X_i^{n+1}, \quad X_1 X_{i+1} = X_2 X_i,$$

para $i = 1, \ldots, n-1$. Además V_n es irreducible, pues una descomposición en dos cerrados propios daría lugar a una descomposición de A^1. Claramente $V_n \subset A^n$ es una curva, pues $t = x_2/x_1$ es una base de trascendencia de $k(V_n)$. La figura muestra la curva V_3.

Sea $P = (0, \ldots, 0) \in V_n$. Vamos a probar que $T_P V_n = A^n$, lo cual implica que V_n no es isomorfa a ninguna curva contenida en A^m, para $m < n$. Hemos de ver que si $F \in I(V)$, entonces $d_P F = 0$.

Sea $d_P F = \sum\limits_i a_i X_i$, de modo que

$$F = \sum_i a_i X_i + G(X_1, \ldots, X_n),$$

donde $G \in (X_1, \ldots, X_n)^2$. Todo $t \in k$ es raíz del polinomio

$$\sum_i a_i T^{n-i+1} + G(T^n, \ldots, T^{2n-1}) \in k[T],$$

luego se trata del polinomio nulo. Ahora bien, esto sólo es posible si ambos sumandos son nulos, ya que el primero tiene grado $\leq 2n-1$ y el segundo $\geq 2n$.

■

Si V es una variedad afín, $P \in V$ y $f \in \mathfrak{m}_P$, entonces $d_P f \in T_P V^*$ y a través del isomorfismo del teorema 3.28 tenemos que $d_P f$ se identifica con $[f] \in \mathfrak{m}_P/\mathfrak{m}_P^2$.

Así, si V es una variedad cuasiproyectiva, $P \in V$ y $f \in \mathfrak{m}_P$, definimos $d_P f = [f]$. Más en general, si $f \in \mathcal{O}_P(V)$ podemos definir $d_P f = [f - f(P)]$. Se comprueba inmediatamente que

$$d_P(f+g) = d_P f + d_P g, \qquad d_P(fg) = g(P) d_P f + f(P) d_P g.$$

Obviamente, las diferenciales de las constantes son nulas, y esto permite probar a su vez que

$$d_P(1/f) = -\frac{d_P f}{f(P)^2}, \qquad d_P(f/g) = \frac{g(P) d_P f - f(P) d_P g}{g(P)^2}.$$

Ejercicio: Sea V una variedad cuasiproyectiva, $P \in V$ y $f \in \mathcal{O}_P(V)$. Entonces tenemos definida $d_P^1 f \in \mathfrak{m}_P/\mathfrak{m}_P^2$, pero, considerando a $f : V \longrightarrow A^1$ como función racional, también tenemos definida $d_P^2 f : (\mathfrak{m}_P/\mathfrak{m}_P^2)^* \longrightarrow (\mathfrak{m}_{f(P)}/\mathfrak{m}_{f(P)}^2)^*$. Probar que $(\mathfrak{m}_{f(P)}/\mathfrak{m}_{f(P)}^2)^*$ se identifica con k a través de $\phi \mapsto \phi([x - f(p)])$, con lo que $d_P^2 f$ se identifica con un elemento de $(\mathfrak{m}_P/\mathfrak{m}_P^2)^{**}$, el cual, a través de la identificación canónica entre un espacio y su bidual, se identifica con $d_P^1 f$.

Si $v \in T_PV$ y $f \in \mathcal{O}_P(V)$, podemos definir $v(f) = v(d_P f) = v[f - f(P)]$. De este modo podemos ver a v como aplicación $v : \mathcal{O}_P(V) \longrightarrow k$. Vectores tangentes distintos determinan aplicaciones distintas, pues si $[\alpha] \in \mathfrak{m}_P/\mathfrak{m}_P^2$ tenemos que $v([\alpha]) = v(\alpha)$. Además es inmediato que v cumple

$$v(af + bg) = av(f) + bv(g), \qquad v(fg) = g(P)v(f) + f(P)v(g),$$

para $a,b \in k$, f, $g \in \mathcal{O}_P(V)$.

Así pues, los vectores tangentes se pueden representar como *derivaciones* de $\mathcal{O}_P(V)$. Toda derivación —es decir, toda aplicación v que cumpla estas propiedades— está inducida por un único vector tangente, pues de la propiedad del producto implica que v se anula en $\mathfrak{m}_P^2$, luego induce una aplicación lineal en $\mathfrak{m}_P/\mathfrak{m}_P^2$.

Ejercicio: Probar que si $\phi : V \longrightarrow W$ es una aplicación racional en $P \in V$ y $v \in T_PV$, $f \in \mathcal{O}_{\phi(P)}(W)$, entonces $d_P\phi(v)(f) = v(\phi \circ f)$.

3.4 Puntos regulares

Vamos a ver que la dimensión de las variedades tangentes coincide "casi siempre" con la dimensión de la variedad.

Definición 3.31 Diremos que un punto P de una variedad V es *regular* si cumple que $\dim T_PV = \dim V$. En caso contrario diremos que es *singular.* Una variedad es *regular* si todos sus puntos son regulares.

Teorema 3.32 *Si V es una variedad, entonces $\dim T_PV \geq \dim V$ para todo $P \in V$. El conjunto de puntos donde se da la igualdad (es decir, el conjunto de los puntos regulares de V) es un abierto no vacío.*

Demostración: Consideremos primero el caso en que $V \subset A^{n+1}$ es una hipersuperficie, definida por la ecuación $F(X_1, \ldots, X_{n+1}) = 0$. Entonces la variedad tangente en un punto P de coordenadas $a \in k^n$ está determinada por la ecuación

$$\left.\frac{\partial F}{\partial X_1}\right|_a (X_1 - a_1) + \cdots + \left.\frac{\partial F}{\partial X_{n+1}}\right|_a (X_{n+1} - a_{n+1}) = 0.$$

Así pues, T_PV tendrá dimensión n excepto en los puntos que cumplan

$$\frac{\partial F}{\partial X_1}(P) = \cdots = \frac{\partial F}{\partial X_{n+1}}(P) = 0.$$

Esto significa que el conjunto de puntos singulares de V es cerrado. Sólo hay que probar que no es todo V, es decir, que no puede ocurrir que las derivadas parciales de F sean idénticamente nulas en V. Esto significaría que todas ellas serían divisibles entre F. Si el cuerpo k tiene característica 0, esto implica que F es constante, lo cual es absurdo, y si k tiene característica prima p, entonces $F = G(X_1^p, \ldots, X_{n+1}^p)$, para cierto polinomio G, pero como k es algebraicamente cerrado, los coeficientes de G son potencias p-ésimas, y entonces $F = H^p$, contradicción. Con esto hemos probado que las hipersuperficies cumplen el teorema.

Tomemos ahora una variedad cuasiproyectiva arbitraria V de dimensión n y sea $W \subset A^{n+1}$ una hipersuperficie birracionalmente equivalente (teorema 3.17). Esto significa que existen abiertos $V_1 \subset V$ y $W_1 \subset W$ junto con un isomorfismo $\phi : V_1 \longrightarrow W_1$. Por otra parte, existe un abierto $W_2 \subset W$ (que podemos tomar $W_2 \subset W_1$ formado por puntos regulares, es decir, tales que sus variedades tangentes tienen dimensión n. Los puntos de $V_2 = \phi^{-1}[W_2]$ cumplen lo mismo. Así pues, hemos probado que toda variedad tiene un abierto no vacío de puntos regulares. Vamos a ver que, de hecho, el conjunto de todos los puntos regulares es abierto.

Pasando a $\overline{V}$, podemos suponer que $V \subset \mathrm{P}^N$ es una variedad proyectiva. Sea $P \in V$ un punto cuya variedad tangente tenga dimensión mínima $\dim T_P V = d$. Podemos suponer que P cumple $X_{N+1} \neq 0$, con lo que $P \in V_* \subset A^N$.

Sea $I(V_*) = (F_1, \ldots, F_m)$ y sea $A(X)$ la matriz formada por las derivadas parciales de las funciones F_i en el punto X. Es claro que

$$\operatorname{codim} T_X V = \operatorname{rang} A(X),$$

luego $\operatorname{rang} A(P) = N - d$ es máximo. Existe una submatriz $d \times d$ en $A(X)$ cuyo determinante no se anula en P. Este determinante es un polinomio G que define una función $g = [G] \in k[V_*]$. En todos los puntos donde $g(x) \neq 0$, se tiene $\operatorname{rang} A(x) \geq N - d$, pero también se tiene la desigualdad contraria por la maximalidad. Por lo tanto, $U = \{Q \in V_* \mid g(Q) \neq 0\}$ es un abierto no vacío cuyos puntos cumplen $\dim T_Q V_* = d$. Por otra parte, V_* contiene un abierto de puntos regulares, la intersección de éste con U es no vacía y, por consiguiente, ha de ser $n = d$.

Hemos probado que $\dim V$ es la mínima dimensión posible para una variedad tangente a V. Ahora sabemos que el punto P que hemos tomado antes es cualquier punto regular de V, y hemos probado que existe un abierto U formado por puntos regulares tal que $P \subset U \subset V_* \subset V$, luego el conjunto de puntos regulares es abierto. ■

Ejercicio: Sea V la cúbica $Y^2 = X^3$ (ver la página 55). Probar que el único punto singular de V es $(0, 0)$. Probar que la aplicación $\phi : A^1 \longrightarrow V$ dada por $\phi(t) = (t^2, t^3)$ es biyectiva y regular, pero no un isomorfismo. Más concretamente, su inversa es regular en el abierto $U = V \setminus \{(0, 0)\}$, donde viene dada por $\phi^{-1}(x, y) = y/x$.

Ejemplo *Una cúbica con un punto singular es proyectivamente equivalente a* $Y^2 = X^3$ *o bien a* $X^3 + Y^3 = XY$. *(Suponiendo que la característica del cuerpo no sea* 3.*)*

En efecto, podemos tomar un sistema de referencia afín en el que el punto singular sea $(0,0)$. Es claro entonces que la ecuación de V es de la forma $F_3(X,Y) + F_2(X,Y) = 0$, donde F_i es una forma de grado i. La forma F_2 no puede ser nula (o la curva sería reducible) y se descompone en producto de dos formas lineales. Distingamos si la descomposición es de tipo $F_2(X,Y) = c(aX+bY)^2$ o bien $F_2(X,Y) = (aX+bY)(cX+dY)$, donde (a,b) y (c,d) son linealmente independientes.

En el primer caso, dividiendo entre c la ecuación y tras un cambio de variable $X' = X$, $Y' = aX + bY$ obtenemos una ecuación de la forma

$$Y^2 - aX^3 - bX^2Y - cXY^2 - dY^3 = 0.$$

Si fuera $a = 0$ la ecuación sería divisible entre Y, luego no sería irreducible. Así pues, $a \neq 0$ y el cambio $X' = \sqrt[3]{a}X$, $Y' = Y$ nos da una ecuación similar con $a = 1$. Haciendo $X = X' - (b/3)Y'$, $Y = Y'$ queda $b = 0$. La clausura proyectiva de la ecuación resultante es

$$Y^2Z - X^3 - cXY^2 - dY^3 = 0.$$

El cambio $X = X'$, $Y = Y'$, $Z = Z' + cX' + dY'$ nos da $c = d = 0$. Llegamos así a la curva $Y^2Z = X^3$ o, lo que es lo mismo, a $Y^2 = X^3$.

Consideramos ahora el caso en que F_2 tiene dos factores distintos. El cambio $X' = aX + bY$, $Y' = cX + dY$ nos da una ecuación

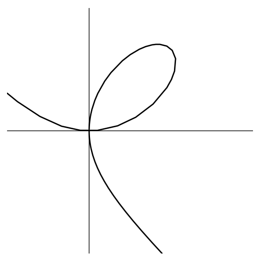
$$aX^3 + bX^2Y + cXY^2 + dY^3 - XY = 0.$$

Si fuera $a = 0$ o $d = 0$ la ecuación sería reducible, luego podemos hacer el cambio $X' = \sqrt[3]{a}X$, $Y' = \sqrt[3]{d}Y$ y obtenemos

$$X^3 + bX^2Y + cXY^2 + Y^3 - eXY = 0.$$

Homogeneizando, haciendo $Z = Z' + bX + cY$ y volviendo a deshomogeneizar queda

$$X^3 + Y^3 - eXY = 0.$$



Por último hacemos $X = eX'$, $Y = eY'$ y dividimos entre e^3, con lo que queda $X^3 + Y^3 = XY$. La figura muestra esta curva. Vemos que es la curva "alfa" en otra posición. De hecho, el argumento anterior muestra que ambas son proyectivamente equivalentes. En la página 141 veremos que las cúbicas $Y^2 = X^3$ y $X^3 + Y^3 = XY$ no son isomorfas, de modo que hay exactamente dos cúbicas singulares. Ahora es fácil hacer afirmaciones generales sobre cúbicas singulares. Por ejemplo, una cúbica singular tiene una única singularidad. ■

El ejemplo siguiente generaliza al ejemplo de la página 93 y al ejercicio anterior.

Ejemplo *Toda cúbica singular es birracionalmente equivalente a* P^1.

Sea V una cúbica singular. Como en el ejemplo anterior, podemos suponer que su ecuación es de la forma $F_3(X,Y)+F_2(X,Y)=0$, donde F_i es una forma de grado i. La forma F_2 no puede ser nula, pues entonces V sería reducible.

Para cada $t \in k$, calculamos la intersección de V con la recta $Y = tX$. Está formada por los puntos (X, tX) que cumplen $F_3(X,tX)+F_2(X,tX)=0$. Esto equivale a

$$X^3 f_3(t) + X^2 f_2(t) = 0,$$

donde f_3 y f_2 son polinomios no nulos de grados 3 y 2 respectivamente. Descartando la solución $X = 0$ (que corresponde al punto $(0,0)$) y los valores de t que anulan a f_3, tenemos que sólo hay otro punto de corte, dado por

$$\phi(t) = \left(-\frac{f_2(t)}{f_3(t)}, -\frac{tf_2(t)}{f_3(t)}\right).$$

Tenemos así $\phi : \mathrm{P}^1 \longrightarrow V$ racional. Más aún, es birracional, pues su inversa (definida sobre los puntos finitos de V donde no se anula x) es $\psi(x,y) = y/x$.

■

Vamos a estudiar con más detalle los puntos regulares de una variedad. En primer lugar definiremos y estudiaremos el análogo a un sistema de coordenadas (una carta) en geometría diferencial.

Definición 3.33 Sea V una variedad cuasiproyectiva de dimensión n y $P \in V$ un punto regular. Diremos que $x_1, \ldots, x_n \in \mathcal{O}_P(V)$ forman un *sistema de parámetros locales* en P si pertenecen al ideal $\mathfrak{m}_P$ y sus clases en $\mathfrak{m}_P/\mathfrak{m}_P^2$ (esto es, las diferenciales d_Px_i) forman una base de este espacio.

Vamos a caracterizar los sistemas de parámetros locales en un punto regular P de una variedad afín $V \subset A^n$. Tomemos un sistema de referencia en A^n de coordenadas $y_1, \ldots, y_N$. Sea a el vector de coordenadas de P. Tomemos funciones $x_1, \ldots, x_n \in k[V]$. En principio no exigimos que se anulen en P. Vamos a ver cuándo las funciones $x_i - x_i(P)$ forman un sistema de parámetros locales en P. Pongamos que $x_i = [F_i]$, con $F_i \in k[Y_1, \ldots, Y_N]$.

Dado el isomorfismo entre el espacio cotangente $\mathfrak{m}_P/\mathfrak{m}_P^2$ y el dual de la variedad tangente T_PV, podemos trabajar con éste último. Así, las funciones $x_i - a_i$ serán un sistema de parámetros locales en P si y sólo si las diferenciales $d_P(x_i - x_i(P)) = d_Px_i$ son linealmente independientes. Sabemos que

$$d_Px_i = \left.\frac{\partial F_i}{\partial Y_1}\right|_a dy_1 + \cdots + \left.\frac{\partial F_i}{\partial Y_N}\right|_a dy_N.$$

Como d_P es suprayectiva, es claro que las diferenciales d_Py_j son un sistema generador de T_PV^*, luego las diferenciales d_Px_i serán una base de T_PV^* si y sólo si la matriz de derivadas de los polinomios F_i en a tiene rango máximo igual a n.

Esto sucederá si y sólo si la matriz tiene un determinante $n \times n$ no nulo en a. Dicho determinante será un polinomio $G(Y_1, \ldots, Y_N)$, el cual determina un abierto U en V (que podemos tomar formado por puntos regulares), de modo que si $Q \in V$ entonces $x_1 - x_1(Q), \ldots, x_n - x_n(Q)$ son un sistema de parámetros locales alrededor de Q. Con esto casi hemos probado el teorema siguiente:

Teorema 3.34 *Sea P un punto regular de una variedad V y consideremos funciones $x_1, \ldots, x_n \in \mathcal{O}_P(V)$ tales que $x_i - x_i(P)$ formen un sistema de parámetros locales en P. Entonces P tiene un entorno U, formado por puntos regulares, de modo que $x_i \in k[U]$ y para todo $Q \in U$ las funciones $x_i - x_i(Q)$ forman un sistema local de parámetros en Q.*

Demostración: Tomamos un entorno afín U de P formado por puntos regulares donde todas las funciones x_i son regulares. Todos los razonamientos precedentes se aplican a una variedad afín isomorfa a U, y todas las conclusiones se conservan por isomorfismos. ■

Si $V \subset A^N$ es una variedad afín, entonces $x_1, \ldots, x_n \in \mathcal{O}_P(V)$ son un sistema de parámetros locales en un punto regular P si y sólo si $d_P x_1, \ldots, d_P x_n$ son una base de $T_P V^*$ o, equivalentemente, si el sistema $d_P x_1 = \cdots = d_P x_n = 0$ tiene únicamente la solución trivial (correspondiente a las coordenadas de P).

Elijamos, para cada i, una componente irreducible V_i que contenga a P de la variedad $\{Q \in V \mid x_i(Q) = 0\}$ (puede probarse que sólo hay una, pero no necesitaremos este hecho). Según 3.21 tenemos que $\dim V_i = n - 1$ (notemos que x_i no puede ser nula en V o si no $d_P x_i = 0$).

Es claro que $T_P V_i \subset T_P V$, así como que $d_P x_i|_{T_P V_i} = d_P(x_i|_{V_i}) = 0$. Así pues, si llamamos $L_i = \{Q \in T_P V \mid d_P x_i(Q) = 0\}$, tenemos que $T_P V_i \subset L_i$. Como $d_P x_i \neq 0$, es claro que $\dim L_i = n - 1$. Por otra parte, también tenemos que $\dim T_P V_i \geq \dim V_i = n - 1$, luego $\dim T_P V_i = n - 1$, lo que significa que P es un punto regular de cada V_i. Así mismo, $\bigcap\limits_i T_P V_i \subset \bigcap\limits_i L_i = \{P\}$, pues P es el único cero común de las funciones $d_P x_i$, luego $\bigcap\limits_i T_P V_i = \{P\}$.

Sea ahora V_0 una componente irreducible de $V_1 \cap \cdots \cap V_n$ que contenga a P. Así, $T_P V_0 \subset \bigcap\limits_i T_P V_i = \{P\}$, luego $\dim V_0 \leq \dim T_P V_0 = 0$. Por consiguiente,

$$\dim(V_1 \cap \cdots \cap V_n) = 0.$$

Según el teorema 3.21, en la sucesión

$$V_1, \quad V_1 \cap V_2, \quad V_1 \cap V_2 \cap V_3, \quad \ldots$$

la dimensión disminuye a lo sumo una unidad en cada paso. Como al cabo de n pasos alcanzamos la dimensión 0, concluimos que la dimensión disminuye exactamente en una unidad en cada paso. En particular:

Teorema 3.35 *Si V es una variedad cuasiproyectiva, $P \in V$ es un punto regular y $x_1, \ldots, x_n$ es un sistema de parámetros locales en P, entonces ninguna x_i es idénticamente nula sobre el conjunto de puntos de V donde se anulan las restantes.*

DEMOSTRACIÓN: Basta tomar un entorno afín U de P y aplicar los razonamientos precedentes a las restricciones $x_i|_U$. ■

Ahora demostraremos que un sistema de parámetros locales en P es un generador del ideal $\mathfrak{m}_P$. Para ello probamos primeramente:

Teorema 3.36 *Si V es una variedad y $P \in V$, entonces el anillo $\mathcal{O}_P(V)$ es noetheriano.*

DEMOSTRACIÓN:[2] Podemos suponer que V es una variedad afín. Si $\mathfrak{a}$ es un ideal de $\mathcal{O}_P(V)$, el conjunto $\bar{\mathfrak{a}} = \mathfrak{a} \cap k[V]$ es un ideal de $k[V]$. Como $k[V]$ es noetheriano (es un cociente de un anillo de polinomios) $\bar{\mathfrak{a}} = (f_1, \ldots, f_r)$, pero entonces también $\mathfrak{a} = (f_1, \ldots, f_r)$. En efecto, si $f/g \in \mathfrak{a}$, también $f \in \mathfrak{a}$, luego $f \in \bar{\mathfrak{a}}$ y así $f = h_1 f_1 + \cdots + h_r f_r$, con lo que $f/g = (h_1/g)f_1 + \cdots + (h_r/g)f_r$. ■

El resultado que buscamos es esencialmente una consecuencia del teorema de Nakayama:

Teorema 3.37 *Sea V una variedad y $P \in V$ un punto regular. Entonces todo sistema de parámetros locales en P es un generador del ideal $\mathfrak{m}_P$.*

DEMOSTRACIÓN: Aplicamos el teorema 1.22 tomando $\mathfrak{a} = M = \mathfrak{m}_P$. Los elementos de $1 + \mathfrak{m}_P$ son inversibles, porque son funciones que no se anulan en P, y por el teorema anterior $\mathfrak{m}_P$ es un ideal (o un $\mathcal{O}_P(V)$-módulo) finitamente generado. ■

Si V es una variedad de dimensión n, toda función racional en V puede expresarse como función algebraica de un sistema generador de $k(V)$, pero los sistemas generadores de $k(V)$ tienen, por lo general, más de n elementos. Ahora probaremos que toda función racional puede expresarse en un entorno de cada punto regular como función de un sistema de parámetros locales, pero la expresión ya no será algebraica sino analítica, como serie de potencias.

Consideremos una variedad V, un punto regular $P \in V$, un sistema de parámetros locales $x_1, \ldots, x_n$ en P y una función $\alpha \in \mathcal{O}_P(V)$. Sea $\alpha(P) = a_0$. Entonces $\alpha - a_0 \in \mathfrak{m}_P$, luego su clase módulo $\mathfrak{m}_P^2$ es combinación lineal de los parámetros $x_1, \ldots, x_n$, es decir, existen $a_1, \ldots, a_n \in k$ y $\alpha_1 \in \mathfrak{m}_P^2$ tales que

$$\alpha = a_0 + a_1 x_1 + \cdots + a_n x_n + \alpha_1.$$

Como $\alpha_1 \in \mathfrak{m}_P$, tenemos que $\alpha_1 = \sum_i \beta_i \gamma_i$, con β_i, $\gamma_i \in \mathfrak{m}_P$. Por lo tanto,

$$\beta_i = \sum_j b_{ij} x_j + \beta_i', \quad \gamma_i = \sum_j c_{ij} x_j + \gamma_i', \qquad \beta_i', \gamma_i' \in \mathfrak{m}_P^2.$$

[2]En realidad esto es consecuencia de un hecho general: Podemos suponer que V es afín, y entonces $\mathcal{O}_P(V)$ es la localización de $k[V]$ respecto al ideal maximal formado por las funciones que se anulan en P, y la localización de un anillo noetheriano es un anillo noetheriano.

Por lo tanto
$$\alpha_1 = \sum_{i,j} a_{ij} x_i x_j + \alpha_2, \qquad \alpha_2 \in \mathfrak{m}_P^3,$$
con lo que
$$\alpha = a_0 + \sum_i a_i x_i + \sum_{i,j} a_{ij} x_i x_j + \alpha_2.$$

De este modo vamos obteniendo una serie de potencias que satisface la definición siguiente:

Definición 3.38 Sea V una variedad cuasiproyectiva, sea $P \in V$ un punto regular, sea $x_1, \ldots, x_n$ un sistema de parámetros locales en P y $\alpha \in \mathcal{O}_P(V)$. Diremos que una serie $\sum F_m \in k[[X_1, \ldots, X_n]]$ es una *serie de Taylor* de α alrededor de P respecto al sistema de parámetros dado si para cada $r \geq 0$ se cumple que
$$\alpha - \sum_{m=0}^{r} F_m(x_1, \ldots, x_n) \in \mathfrak{m}_P^{r+1}.$$

Hemos probado que toda función regular en un punto regular admite una serie de Taylor. Más aún:

Teorema 3.39 *Si V es una variedad y $P \in V$ es un punto regular, entonces toda función $\alpha \in \mathcal{O}_P(V)$ admite un único desarrollo en serie de Taylor respecto a un sistema de parámetros locales dado.*

Demostración: Basta probar que la función nula sólo admite como desarrollo en serie de Taylor a la serie nula. Fijado un sistema de parámetros $x_1, \ldots, x_n$, supongamos que $\sum F_m$ es una serie de Taylor de la función nula. Entonces
$$\sum_{m=0}^{r} F_m(x_1, \ldots, x_n) \in \mathfrak{m}_P^{r+1}. \tag{3.6}$$

Basta probar que si F_m es una forma de grado m y $F_m(x_1, \ldots, x_n) \in \mathfrak{m}_P^{m+1}$ entonces $F_m = 0$. En efecto, entonces (3.6) para $r = 0$ nos da que $F_0 = 0$, a su vez, (3.6) para $r = 1$ nos da $F_1 = 0$, etc.

Supongamos que, por el contrario $F_m(X_1, \ldots, X_n) \neq 0$. Entonces existe $(a_1, \ldots, a_n) \in k^n$ tal que $F_m(a_1, \ldots, a_m) \neq 0$. Tomemos una matriz regular A tal que $(0, \ldots, 0, 1)A = (a_1, \ldots, a_m)$. Sea $F'_m(X') = F_m(X'A)$. Sean $u'_1, \ldots, u'_n \in \mathcal{O}_P(V)$ dados por $(u'_1, \ldots, u'_n) = (u_1, \ldots, u_n)A^{-1}$. Es claro que $u'_1, \ldots, u'_n$ forman también un sistema de parámetros locales en P y además $F'_m(u'_1, \ldots, u'_n) = F_m(u_1, \ldots, u_n) \in \mathfrak{m}_P^{m+1}$.

Por consiguiente podemos reemplazar los u_i por los u'_i y F_m por F'_m, con lo que además tenemos que $F_m(0, \ldots, 0, 1) \neq 0$, es decir, el coeficiente de X_n^m es no nulo. Digamos que
$$F_m = aX_n^m + G_1(X_1, \ldots, X_{n-1})X_n^{m-1} + \cdots + G_m(X_1, \ldots, X_{n-1}),$$
donde $a \neq 0$ y cada G_i es una forma de grado i. Como los parámetros locales generan el ideal $\mathfrak{m}_P$, una simple inducción muestra que todo elemento de $\mathfrak{m}_P^{m+1}$

puede expresarse como una forma de grado m en $x_1, \ldots, x_n$ con coeficientes en $\mathfrak{m}_P$. La hipótesis es entonces que

$$\begin{aligned} &a x_n^m + G_1(x_1, \ldots, x_{n-1}) x_n^{m-1} + \cdots + G_m(x_1, \ldots, x_{n-1}), \\ &= \alpha x_n^m + H_1(x_1, \ldots, x_{n-1}) x_n^{m-1} + \cdots + H_m(x_1, \ldots, x_{n-1}), \end{aligned}$$

donde $\alpha \in \mathfrak{m}_P$ y las H_i son formas de grado i con coeficientes en $\mathfrak{m}_P$. De aquí deducimos que $(a - \alpha) x_n^m \in (x_1, \ldots, x_{n-1})$. Como $a \neq 0$, se cumple que $a - \alpha \notin \mathfrak{m}_P$, luego $(a - \alpha)^{-1} \in \mathcal{O}_P(V)$ y llegamos a que $x_n^m \in (x_1, \ldots, x_{n-1})$. Esto contradice al teorema 3.35. ■

Teorema 3.40 *Si P es un punto regular de una variedad V y $x_1, \ldots, x_n$ es un sistema de parámetros locales en P, entonces la aplicación*

$$\tau : \mathcal{O}_P(V) \longrightarrow k[[X_1, \ldots, X_n]]$$

que asigna a cada función su serie de Taylor es un monomorfismo de anillos.

Demostración: Es claro que conserva la suma. Si

$$\tau(\alpha) = \sum_{m=0}^{\infty} F_m, \qquad \tau(\beta) = \sum_{m=0}^{\infty} G_m,$$

entonces

$$\alpha = \sum_{m=0}^{r} F_m(x_1, \ldots, x_n) + \alpha', \quad \beta = \sum_{m=0}^{r} G_m(x_1, \ldots, x_n) + \beta', \quad \alpha', \beta' \in \mathfrak{m}_P^{r+1},$$

$$\alpha\beta = \sum_{m=0}^{r} \sum_{i+j=m} F_i G_j + \sum_{m=r+1}^{2r} \sum_{i+j=m} F_i G_j + \beta' \sum_{m=0}^{r} F_m + \alpha' \sum_{m=0}^{r} G_m,$$

luego

$$\alpha\beta - \sum_{m=0}^{r} \sum_{i+j=m} F_i G_j \in \mathfrak{m}_P^{r+1}.$$

Esto prueba que $\tau(\alpha\beta) = \tau(\alpha)\tau(\beta)$, luego τ es un homomorfismo. Es claro que su núcleo es el ideal $M = \bigcap\limits_{r>0} \mathfrak{m}_P^r$. Según el teorema 1.24 tenemos que $M = 0$. ■

Si $\tau(\alpha) = \sum\limits_{i_1, \ldots, i_n}^{\infty} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$, escribiremos

$$\alpha = \sum_{i_1, \ldots, i_n}^{\infty} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

Hemos de observar que, en principio, una serie finita de este tipo tiene dos interpretaciones, pero es fácil ver que ambas coinciden.

De aquí deducimos una propiedad notable de los anillos locales $\mathcal{O}_P(V)$ de los puntos regulares: son dominios de factorización única. Necesitamos un resultado previo:

Teorema 3.41 *Sea A un anillo noetheriano contenido en un anillo noetheriano $\hat{A}$ con factorización única. Supongamos que A tiene un único ideal maximal $\mathfrak{m}$ y $\hat{A}$ tiene un único ideal maximal $\hat{\mathfrak{m}}$ de modo que:*

a) $\mathfrak{m}\hat{A} = \hat{\mathfrak{m}}$,

b) $(\mathfrak{m}^n \hat{A}) \cap A = \mathfrak{m}^n$ *para todo* $n > 0$,

c) para cada $\alpha \in \hat{A}$ *y cada* $n > 0$ *existe* $a_n \in A$ *tal que* $\alpha - a_n \in \mathfrak{m}^n \hat{A}$.

Entonces A es también un dominio de factorización única.

Demostración: Veamos que para todo ideal $\mathfrak{a} \subset A$ se cumple $(\mathfrak{a}\hat{A}) \cap A = \mathfrak{a}$. Como A es noetheriano tenemos que $\mathfrak{a} = (a_1, \ldots, a_n)$. Sea $x \in (\mathfrak{a}\hat{A}) \cap A$. Entones $x = \sum a_i \alpha_i$, con $\alpha_i \in \hat{A}$. Por c) existen elementos $a_i^{(n)} \in A$ tales que $\alpha_i = a_i^{(n)} + \xi_i^{(n)}$, con $\xi_i^{(n)} \in \mathfrak{m}^n \hat{A}$. Sustituyendo en la expresión de x llegamos a que $x = a + \xi$, donde $a \in \mathfrak{a}$ y $\xi \in \mathfrak{m}^n \hat{A}$. Por lo tanto $\xi = x - a \in A \cap \mathfrak{m}^n \hat{A} = \mathfrak{m}^n$. Concluimos que $x \in \mathfrak{a} + \mathfrak{m}^n$ para todo $n > 0$, luego $x \in \mathfrak{a}$ por 1.24.

Puesto que A es noetheriano, basta demostrar que todos sus elementos irreducibles son primos. En primer lugar demostramos que si a, $b \in A$, entonces $a \mid b$ en A si y sólo si $a \mid b$ en $\hat{A}$. En efecto, si $a \mid b$ en $\hat{A}$ hemos probado que $b \in A \cap (a)\hat{A} = (a)$, luego $a \mid b$ en A.

Supongamos ahora que a es irreducible en A y que $a \mid bc$, pero $a \nmid b$. Basta probar que $a \mid c$ (en $\hat{A}$). A su vez, para esto basta probar que a y b son primos entre sí en $\hat{A}$. En caso contrario, $a = \gamma\alpha$, $b = \gamma\beta$, con α, β, $\gamma \in \hat{A}$, de modo que γ no es unitario y α, β son primos entre sí. Entonces $a\beta - b\alpha = 0$.

Por hipótesis existen x_n, $y_n \in A$, u_n, $v_n \in \mathfrak{m}^n \hat{A}$ tales que $\alpha = x_n + u_n$, $\beta = y_n + v_n$. Entonces $ay_n - bx_n \in ((a, b)\mathfrak{m}^n \hat{A}) \cap A = (a, b)\mathfrak{m}^n$. Por consiguiente, $ay_n - bx_n = at_n + bs_n$, con s_n, $t_n \in \mathfrak{m}^n$. Reordenando, $a(y_n - t_n) = b(x_n + s_n)$, luego $\alpha(y_n - t_n) = \beta(x_n + s_n)$.

Como α y β son primos entre sí, tenemos que $x_n + s_n = \alpha\lambda$, con $\lambda \in \hat{A}$. Por el teorema 1.24 sabemos que la intersección de los ideales $\hat{m}^n$ es nula, luego existe un mínimo n suficientemente grande tal que $\alpha \notin \hat{\mathfrak{m}}^{n-1}$. Entonces $x_n + s_n \notin \mathfrak{m}^{n-1}$, luego $\lambda \notin \hat{\mathfrak{m}}$ (pues $\alpha \in \hat{\mathfrak{m}}^{n-2}$). Esto significa que λ es una unidad, luego $x_n + s_n \mid \alpha$ y, de aquí, $x_n + s_n \mid a$. Digamos que $a = (x_n + s_n)h$, con $h \in A$.

De la igualdad $a(y_n - t_n) = b(x_n + s_n)$ obtenemos que $b = (y_n + t_n)h$. Estamos suponiendo que a es irreducible en A y que no divide a b, luego h ha de ser una unidad en A. Concluimos que $(a) = (x_n + s_n) = (\alpha)$, luego γ es una unidad, y tenemos una contradicción. ■

Teorema 3.42 *Si P es un punto regular de una variedad V, entonces $\mathcal{O}_P(V)$ es un dominio de factorización única.*

Demostración: El teorema 3.40 nos permite considerar a $\mathcal{O}_P(V)$ como subanillo del anillo de series formales de potencias $\hat{\mathcal{O}}_P(V) = k[[X_1, \ldots, X_n]]$.

Sólo hemos de comprobar que se cumplen las hipótesis del teorema anterior. Ciertamente $\mathcal{O}_P(V)$ y $\hat{\mathcal{O}}_P(V)$ son ambos noetherianos y tienen un único ideal maximal $\mathfrak{m}_P$ y $\hat{\mathfrak{m}}_P$, respectivamente. Además $\hat{\mathcal{O}}_P(V)$ es un dominio de factorización única.

De la definición 3.38 se sigue que los elementos de $\mathfrak{m}_P$ tienen series de Taylor en $\hat{\mathfrak{m}}_P$. Esto prueba la inclusión $\mathfrak{m}_P\hat{\mathcal{O}}_P(V) \subset \hat{\mathfrak{m}}_P$. Además $\hat{\mathfrak{m}}_P = (X_1, \ldots, X_n)$ y las indeterminadas X_i son las series de Taylor de los parámetros x_i, luego están en $\mathfrak{m}_P$ y tenemos la igualdad. Más en general, de aquí se sigue que $\hat{\mathfrak{m}}_P^n = \mathfrak{m}_P^n\hat{\mathcal{O}}_P(V)$.

Un elemento $\alpha \in (\mathfrak{m}_P^n\hat{\mathcal{O}}_P(V)) \cap \mathcal{O}_P(V)$ es una función cuya serie de Taylor no tiene términos de grado menor que n, luego por la definición de la serie de Taylor se cumple que $\alpha \in \mathfrak{m}_P^r$.

Finalmente, a cada serie de $\hat{\mathcal{O}}_P(V)$ le podemos restar la serie finita formada por sus términos hasta grado $n-1$ (que es la serie de Taylor de una función de $\mathcal{O}_P(V)$) y así obtenemos una serie de $\hat{\mathfrak{m}}_P^n$. ■

De la prueba de los dos últimos teoremas podemos extraer una conclusión de interés en sí misma:

Teorema 3.43 *Sea P un punto regular de una variedad V y sea consideremos la aplicación $\tau : \mathcal{O}_P(V) \longrightarrow k[[X_1, \ldots, X_n]]$ que a cada función le asigna su serie de Taylor respecto a un sistema de parámetros prefijado. Entonces, para cada $r \geq 0$ se cumple que*

$$\mathfrak{m}_P^r = \{\alpha \in \mathcal{O}_P(V) \mid v(\tau(\alpha)) \geq r\}.$$

Demostración: En la prueba del teorema anterior hemos obtenido que $\hat{\mathfrak{m}}_P^r = \mathfrak{m}_P^r\hat{\mathcal{O}}_P(V)$, mientras que en la prueba de 3.41 hemos demostrado que $(\mathfrak{a}\hat{A}) \cap A = \mathfrak{a}$. Combinando ambos hechos concluimos que

$$\hat{\mathfrak{m}}_P^r \cap \mathcal{O}_P(V) = \mathfrak{m}_P^r.$$

Esto equivale a la relación del enunciado. ■

Como aplicación demostramos lo siguiente:

Teorema 3.44 *Sea $\phi : V \longrightarrow W$ una aplicación regular entre variedades, sea $P \in V$ y $Q = \phi(P) \in W$. Sean $t_1, \ldots, t_m$ y $x_1, \ldots, x_n$ sistemas de parámetros locales en P y Q respectivamente. Para cada $\alpha \in \mathcal{O}_Q(W)$, se cumple*

$$\tau(\overline{\phi}(\alpha)) = \tau(\alpha)(\tau(\overline{\phi}(x_1)), \ldots, \tau(\overline{\phi}(x_n))).$$

Demostración: Observemos en primer lugar que $\overline{\phi}(x_i) \in \mathfrak{m}_P(V)$, luego $v(\tau(\overline{\phi}(x_i))) \geq 1$. De aquí se sigue fácilmente que $\tau(\alpha)(\tau(\overline{\phi}(x_1)), \ldots, \tau(\overline{\phi}(x_n)))$ (entendido como el límite de las sumas parciales de $\tau(\alpha)$ evaluadas en las series $\tau(\overline{\phi}(x_i)))$ es convergente. En este sentido hay que entender el miembro derecho de la igualdad del enunciado.

Consideremos el diagrama siguiente:

$$\begin{tikzcd}
\mathcal{O}_Q(W) \arrow[r, "\overline{\phi}"] \arrow[d, "\tau"'] & \mathcal{O}_P(V) \arrow[d, "\tau"] \\
k[[X_1,\ldots,X_n]] \arrow[r, "\psi"'] & k[[T_1,\ldots,T_m]]
\end{tikzcd}$$

donde $\psi(F) = F(\tau(\overline{\phi}(x_1)),\ldots,\tau(\overline{\phi}(x_n)))$. Para probar el teorema basta demostrar que es conmutativo.

Como τ y $\overline{\phi}$ son k-homomorfismos de anillos, si $F(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$ tenemos que

$$\tau(\overline{\phi}(F(x_1,\ldots,x_n))) = F(\tau(\overline{\phi}(x_1)),\ldots,\tau(\overline{\phi}(x_n)))$$

$$= \psi(F(X_1,\ldots,X_n)) = \psi(\tau(F(t_1,\ldots,t_n))).$$

Así pues, el diagrama conmuta sobre $k[x_1,\ldots,x_n]$. Si identificamos $\mathcal{O}_Q(W)$ y $\mathcal{O}_P(V)$ con sus imágenes en los anillos de series de potencias tenemos que el anillo $k[x_1,\ldots,x_n]$ se corresponde con $k[X_1,\ldots,X_n]$, que es denso en $k[[X_1,\ldots,X_n]]$. Hemos demostrado que la aplicación correspondiente con $\overline{\phi}$ a través de la identificación coincide con $\psi|_{\mathcal{O}_Q(W)}$ sobre $k[X_1,\ldots,X_n]$. Si demostramos que ambas son continuas, entonces serán iguales.

Teniendo en cuenta que ambas conservan las sumas, basta probar que son continuas en 0, para lo cual a su vez basta ver que

$$v(\overline{\phi}(\alpha)) \geq v(\alpha), \qquad v(\psi(F)) \geq v(F).$$

La segunda desigualdad es obvia (teniendo en cuenta que $v(\tau(\overline{\phi}(x_i))) \geq 1$). La primera, escrita sin identificaciones, es $v(\tau(\overline{\phi}(\alpha))) \geq v(\tau(\alpha))$. Por el teorema anterior esto equivale a

$$\alpha \in \mathfrak{m}_Q^r \to \overline{\phi}(\alpha) \in \mathfrak{m}_P^r,$$

lo cual también es obvio. ■

Definición 3.45 Sea V una variedad, $P \in V$ un punto regular y $x_1,\ldots,x_n$ un sistema de parámetros locales en P. Entonces $d_Px_1,\ldots,d_Px_n$ es una base del espacio cotangente $T_PV^* = \mathfrak{m}_P/\mathfrak{m}_P^2$. Representaremos por

$$\left.\frac{\partial}{\partial x_1}\right|_P,\ldots,\left.\frac{\partial}{\partial x_n}\right|_P \in T_PV$$

a su base dual.

Si $f \in \mathcal{O}_P(V)$ y su serie de Taylor es

$$\tau(f) = f(P) + a_1X_1 + \cdots + a_nX_n + \cdots,$$

entonces $f - f(P) - a_1x_1 - \cdots - a_nx_n \in \mathfrak{m}_P^2$, luego

$$\left.\frac{\partial f}{\partial x_i}\right|_P = \left.\frac{\partial}{\partial x_1}\right|_P ([f - f(P)]) = \left.\frac{\partial}{\partial x_i}\right|_P [a_1x_1 + \cdots + a_nx_n]$$

$$= \left.\frac{\partial}{\partial x_i}\right|_P (a_1d_Px_1 + \cdots + a_nd_Px_n) = a_i.$$

Así pues, la derivada parcial respecto a x_i asigna a cada función f el coeficiente de X_i en su serie de Taylor o, equivalentemente, el término independiente de la derivada formal respecto de X_i de dicha serie.

Ejercicio: Sean V y W dos variedades, $x_1, \ldots, x_n$ un sistema de parámetros locales en un punto regular $P \in V$ y sea $y_1, \ldots, y_m$ un sistema de parámetros locales en un punto regular $Q \in W$. Consideremos la variedad producto $V \times W$, llamemos x_i a $p_1 \circ x_i$ e y_i a $p_2 \circ y_i$. Entonces $x_1, \ldots, x_n, y_1, \ldots, y_m$ forman un sistema de parámetros locales de $V \times W$ en (P, Q).

3.5 Inmersión de variedades

Como muestra de la forma en que la noción de dimensión puede usarse en razonamientos geométricos vamos a probar un resultado sobre inmersión de variedades regulares en espacios proyectivos. Necesitaremos varios hechos previos, todos ellos de interés en sí mismos.

Teorema 3.46 *Sea $\phi : V \longrightarrow W$ una aplicación regular y suprayectiva entre variedades V y W de dimensiones m y n respectivamente. Entonces $n \leq m$ y además:*

a) Para cada $P \in W$, las componentes irreducibles de la fibra $\phi^{-1}[P]$ tienen dimensión $\geq m - n$.

b) Existe un abierto $U \subset W$ no vacío tal que para todo $P \in U$ se cumple $\dim \phi^{-1}[P] = m - n$.

Demostración: Como ϕ permite identificar a $k(W)$ con un subcuerpo de $k(V)$, es claro que $n \leq m$.

Para probar a) empezamos aplicándole a $\overline{W}$ el razonamiento empleado al principio de la prueba de 3.18, con lo que obtenemos un conjunto algebraico finito $\overline{W}^n = \overline{W} \cap Z$, donde Z es el conjunto de ceros en $\overline{W}$ de un conjunto de n formas. Más aún, la construcción de estas formas permite exigir que no se anulen en P, con lo que $P \in W \cap Z$. Tomamos un entorno afín U de P tal que $W \cap Z \cap U = \{P\}$. Podemos sustituir W por U en W y V por $\phi^{-1}[U]$ sin alterar la fibra $\phi^{-1}[P]$. De este modo podemos suponer que $W \subset A^N$ es afín y que P es el conjunto de ceros en W de n funciones $f_1, \ldots, f_n \in k[W]$.

Entonces $\phi^{-1}[P]$ es el conjunto de puntos de V donde se anulan simultáneamente las funciones $\bar{\phi}(f_i) \in k[V]$, luego el teorema 3.23 implica que cada componente de $\phi^{-1}[P]$ tiene dimensión $\geq m - n$.

Para probar b) empezamos aplicando el teorema 3.12, que nos da un abierto afín U en W tal que $U' = \phi^{-1}[U]$ es afín. Equivalentemente, podemos suponer que V y W son variedades afines. A través de $\bar{\phi}$ podemos identificar a $k[W]$ con un subanillo de $k[V]$. Así mismo, $k(W) \subset k(V)$.

Sea $k[W] = k[w_1, \ldots, w_N]$, $k[V] = k[v_1, \ldots, v_M]$. El grado de trascendencia de $k(V)$ sobre $k(W)$ es $m - n$. Podemos suponer que $v_1, \ldots, v_{m-n}$ son algebraicamente independientes sobre $k(W)$. Los otros generadores cumplirán relaciones

$$F_i(v_i, v_1, \ldots, v_{m-n}, w_1, \ldots, w_M) = 0, \qquad i = m - n + 1, \ldots, N.$$

Consideramos a F_i como polinomio en $v_i, v_1, \ldots, v_{m-n}$ con coeficientes en $k[w_1, \ldots, w_M]$. Ha de haber al menos un coeficiente que no sea idénticamente nulo en W. Sea C_i el subconjunto algebraico de W donde se anula dicho coeficiente. Llamamos D a la unión de los C_i, que es un subconjunto algebraico propio de W. Su complementario U es un abierto no vacío.

Sea $P \in U$ y X una componente irreducible de $\phi^{-1}[P]$. Sea $\bar{v}_i$ la restricción de v_i a X. Así $k[X] = k[\bar{v}_1, \ldots, \bar{v}_M]$. Se cumple

$$F_i(\bar{v}_i, \bar{v}_1, \ldots, \bar{v}_{m-n}, w_1(P), \ldots, w_M(P)) = 0, \qquad i = m - n + 1, \ldots, N,$$

y los polinomios $F_i(X_i, X_1, \ldots, X_{m-n}, w_1(P), \ldots, w_M(P))$ no son idénticamente nulos, pues cada uno de ellos tiene al menos un monomio no nulo. Esto prueba que los $\bar{v}_i$ son algebraicamente dependientes de $\bar{v}_1, \ldots, \bar{v}_{m-n}$, luego se cumple $\dim X \leq m - n$. Por el apartado anterior tenemos la igualdad, de modo que para todo $P \in U$ se cumple que $\dim \phi^{-1}[P] = m - n$. ■

De aquí se sigue un criterio útil para probar que un conjunto algebraico es irreducible:

Teorema 3.47 *Sea $\phi : V \longrightarrow W$ una aplicación regular entre variedades proyectivas, sea $C \subset V$ cerrado tal que $W_0 = \phi[C]$ es irreducible y para cada $P \in W_0$, las fibras $\phi|_C^{-1}[P]$ son irreducibles y de la misma dimensión. Entonces C es irreducible.*

Demostración: Sea $C = C_1 \cup \cdots \cup C_r$ la descomposición de C en componentes irreducibles. Por el teorema 2.47, cada $\phi[C_i]$ es cerrado y, como W_0 es irreducible, existe un i tal que $W_0 = \phi[C_i]$. Llamemos n a la dimensión de las fibras de $\phi|_C$. Para cada i tal que $\phi[C_i] = W_0$, el teorema anterior nos da un abierto $U_i \subset W_0$ de modo que las fibras $\phi|_{C_i}^{-1}[P]$ con $P \in U_i$ tienen todas la misma dimensión n_i. Si $\phi[C_i] \neq W_0$ definimos $U_i = W_0 \setminus \phi[C_i]$. Tomemos $P \in U_1 \cap \cdots \cap U_r$. Como $\phi|_C^{-1}[P]$ es irreducible, ha de ser $\phi|_C^{-1}[P] \subset C_i$ para cierto i, digamos $i = 1$. En particular $P \in U_1 \cap \phi[C_1]$, luego $\phi[C_1] = W_0$.

Claramente $\phi|_C^{-1}[P] = \phi|_{C_1}^{-1}[P]$, luego $n = n_1$. Si $P \in W_0$ es arbitrario, tenemos que $\phi|_{C_1}^{-1}[P] \subset \phi|_C^{-1}[P]$. La primera fibra es no vacía y por el teorema anterior tiene dimensión $\geq n_1$, luego ha de ser $\phi|_C^{-1}[P] = \phi|_{C_1}^{-1}[P]$. Esto implica que $C = C_1$ es irreducible. ■

Como aplicación de este teorema introducimos la variedad tangente de una variedad proyectiva regular:

Definición 3.48 Si $V \subset \mathrm{P}^n$ es una variedad proyectiva regular, se define la *variedad tangente* de V como el conjunto

$$TV = \{(P, Q) \in V \times \mathrm{P}^n \mid Q \in T_P V\}.$$

Es claro que TV es un conjunto algebraico, definido por las ecuaciones (3.5). La proyección $\pi : V \times \mathrm{P}^n \longrightarrow V$ es regular y las fibras de $\pi|_{TV}$ son las variedades tangentes de V en cada punto. Ciertamente son irreducibles y, por hipótesis, todas tienen la misma dimensión $\dim V$. Por el teorema anterior concluimos que TV es una variedad proyectiva. El teorema 3.46 nos da además que

$$\dim TV = 2 \dim V.$$

Seguidamente damos una condición para que una aplicación regular sea un isomorfismo:

Teorema 3.49 *Sea $\phi : V \longrightarrow W$ una aplicación finita biyectiva entre variedades. Entonces ϕ es un isomorfismo si y sólo si para todo $P \in V$ la diferencial $d_P\phi : T_PV \longrightarrow T_{\phi(P)}W$ es inyectiva.*

DEMOSTRACIÓN: $\psi : W \longrightarrow V$ la aplicación inversa. Hemos de probar que es regular. Fijamos $Q \in W$. Sea $P = \psi(Q)$. Por definición de finitud, Q tiene un entorno afín U tal que $U' = \phi^{-1}[U]$ es afín y $\phi|_{U'} : U' \longrightarrow U$ es finita. Basta probar que $\psi|_U$ es regular en Q. Equivalentemente, podemos suponer que V y W son afines.

Recordemos que $d_P\phi$ es la aplicación dual de $\bar{\phi} : \mathfrak{m}_Q/\mathfrak{m}_Q^2 \longrightarrow \mathfrak{m}_P/\mathfrak{m}_P^2$. Por hipótesis $d_P\phi$ es inyectiva, luego $\bar{\phi}$ es suprayectiva. Así, si $\mathfrak{m}_Q = (\alpha_1, \ldots, \alpha_k)$, entonces $\bar{\phi}(\alpha_1) + \mathfrak{m}_P^2, \ldots, \bar{\phi}(\alpha_k) + \mathfrak{m}_P^2$ generan $\mathfrak{m}_P/\mathfrak{m}_P^2$. Por el teorema 1.22 resulta que $\mathfrak{m}_P = (\bar{\phi}(\alpha_1), \ldots, \bar{\phi}(\alpha_k))$. En otras palabras:

$$\mathfrak{m}_P = \bar{\phi}[\mathfrak{m}_Q]\mathcal{O}_P(V).$$

Veamos que $\mathcal{O}_P(V)$ es un $\mathcal{O}_Q(W)$-módulo finitamente generado. Por la finitud de ϕ y el teorema 1.13 tenemos que $k[V]$ es un $k[W]$-módulo finitamente generado, luego basta probar que todo elemento de $\mathcal{O}_P(V)$ puede expresarse en la forma $\alpha/\bar{\phi}(\beta)$, donde $\alpha \in k[V]$ y $\beta \notin \mathfrak{m}_Q$.

En principio, un elemento de $\mathcal{O}_P(V)$ es de la forma γ/δ, con γ, $\delta \in k[V]$, $\delta \notin \mathfrak{m}_P$. Basta encontrar $\beta \in k[W]$, $\beta \notin \mathfrak{m}_Q$ tal que $\bar{\phi}(\beta) = \delta\epsilon$, con $\epsilon \in k[V]$. De este modo, $\gamma/\delta = (\gamma\epsilon)/\bar{\phi}(\beta)$.

Sea $V_0 = \{R \in V \mid \delta(R) = 0\}$. Claramente V_0 es cerrado en V y por el teorema 3.6 tenemos que $\phi[V_0]$ es cerrado en W. Como ϕ es biyectiva $Q \notin \phi[V_0]$. Por lo tanto, existe una función $\eta \in k[W]$ que se anula en $\phi[V_0]$ pero $\eta(Q) \neq 0$. Entonces $\bar{\phi}(\eta)$ se anula en V_0 y $\bar{\phi}(\eta)(P) \neq 0$.

Digamos que $\bar{\phi}(\eta) = [F]$, $\delta = [G]$, de modo que

$$F \in I(V_0) = I(V(I(V), G)) = \operatorname{rad}(I(V), G),$$

luego $F^N \in (I(V), G)$ para cierto $N > 0$. Tomando clases $\bar{\phi}(\eta^N) \in (\delta)$. Así pues, llamando $\beta = \eta^N$ tenemos que $\bar{\phi}(\beta) = \delta\epsilon$ como queríamos.

Ahora podemos aplicar 1.22 a $\mathcal{O}_P(V)$ como $\mathcal{O}_Q(W)$-módulo. Tenemos que $\mathcal{O}_P(V)/\bar{\phi}(\mathfrak{m}_Q)\mathcal{O}_P(V) = \mathcal{O}_P(V)/\mathfrak{m}_P(V) \cong k$, luego el cociente está generado por la clase de la función constante 1. Concluimos que también $\mathcal{O}_P(V)$ está generado por la función 1 sobre $\mathcal{O}_Q(W)$, es decir, que $\mathcal{O}_P(V) = \bar{\phi}[\mathcal{O}_Q(W)]$.

Sea $k[V] = \langle \alpha_1, \ldots, \alpha_m \rangle_{k[W]}$. Como $\alpha_i \in \mathcal{O}_P(V)$, se cumple que $\alpha_i = \bar{\phi}(\beta_i)$, con $\beta_i \in \mathcal{O}_Q(W)$. Sea W_γ un abierto principal de W entorno de Q (para un $\gamma \in k[W]$) tal que todas las β_i sean regulares en W_γ. Así,

$$k[V_{\bar{\phi}(\gamma)}] = \big\langle \bar{\phi}(\beta_1), \ldots, \bar{\phi}(\beta_m) \big\rangle_{k[W_\gamma]} = \bar{\phi}[k[W_\gamma]].$$

Esto prueba que $\phi|_{V_{\bar{\phi}(\gamma)}} : V_{\bar{\phi}(\gamma)} \longrightarrow W_\gamma$ es un isomorfismo (pues induce un isomorfismo entre los anillos de funciones regulares). Como W_γ es un entorno de Q, esto implica que ψ es regular en Q. ■

Vamos a usar este teorema en el siguiente caso particular:

Teorema 3.50 *Sea $V \subset \mathrm{P}^N$ una variedad proyectiva regular y $P \in \mathrm{P}^N \setminus V$ un punto que no pertenezca a la variedad tangente de V en ningún punto y tal que cada recta que pasa por P corte a V a lo sumo en un punto. Entonces la proyección $\pi : V \longrightarrow \mathrm{P}^{N-1}$ de centro P es un isomorfismo en su imagen.*

Demostración: Podemos tomar un sistema de referencia en el que P tenga coordenadas $(1, \ldots, 1)$. Si identificamos P^{N-1} con el hiperplano $X_{N+1} = 0$, entonces la proyección π viene dada por $\pi(x) = (x_i - x_{N+1})$ (ver 3.7).

Por el teorema 2.47, el conjunto $W = \pi[V]$ es cerrado, y es irreducible porque una descomposición en cerrados daría lugar a otra de V. Vamos a ver que se cumplen las condiciones del teorema anterior. Sabemos que las proyecciones son aplicaciones finitas.

También se cumple que π es biyectiva. Notemos que cada $Q \in V$ está en la intersección con V de la recta que pasa por P y $\pi(Q)$. En efecto, si Q tiene coordenadas $(x_1, \ldots, x_{N+1})$, entonces la recta que pasa por P y Q está formada por los puntos de coordenadas

$$\lambda(1, \ldots, 1) + \mu(x_1, \ldots, x_{N+1}), \qquad \lambda, \mu \in k.$$

La intersección de esta recta con P^{N-1} es el punto determinado por la ecuación $\lambda + \mu x_{N+1} = 0$. De aquí se sigue que $\mu \neq 0$ y que el punto tiene coordenadas

$$(\mu(x_1 - x_{N+1}), \ldots, \mu(x_N - x_{N+1}), 0).$$

Ciertamente este punto es $\pi(Q)$. Si $\pi(Q) = \pi(Q')$, entonces la recta que pasa por P y este punto corta a V en Q y en Q'. Por hipótesis $Q = Q'$.

Finalmente veremos que la hipótesis sobre las variedades tangentes implica que la diferencial de π en cada punto Q es inyectiva. En primer lugar supondremos que Q satisface $x_{N+1} \neq 0$, con lo que podemos tomar un vector de coordenadas de la forma $Q = (b_1, \ldots, b_N, 1)$. Luego veremos que con esto no perdemos generalidad. Como $Q \in V$ y $P \notin V$, ha de ser $Q \neq P$, luego podemos suponer que $b_N \neq 1$.

Sea $V' = V \cap A^N$ y sea $\pi' : V' \longrightarrow A^{N-1}$ la restricción de π, dada por

$$\pi'(x_1, \ldots, x_N) = \left(\frac{x_1 - 1}{x_N - 1}, \ldots, \frac{x_{N-1} - 1}{x_N - 1} \right).$$

Ahora π' es una función racional definida en el abierto $x_N \neq 1$. Sea $R = \pi(Q)$. Supongamos que $d_Q\pi : (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^* \longrightarrow (\mathfrak{m}_R/\mathfrak{m}_R^2)^*$ no es inyectiva. Entonces existe $\alpha \in (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^*$ no nulo tal que $d_Q\pi(\alpha) = \bar{\pi} \circ \alpha = 0$.

Por otra parte, tenemos el isomorfismo $d_Q^* : (T_QV')^{**} \longrightarrow (\mathfrak{m}_Q/\mathfrak{m}_Q^2)^*$, de modo que existe $\beta \in T_Q(V')^{**}$ no nulo tal que $\alpha = d_Q^*(\beta)$. Por el isomorfismo canónico entre $T_Q(V')$ y su bidual, existe un $T \in T_QV'$, $T \neq Q$, tal que, para todo $\gamma \in T_Q(V')^*$, se cumple $\beta(\gamma) = \gamma(T)$.

Combinando todo esto, si $f \in \mathfrak{m}_R$, tenemos que $\bar{\pi}([f]) \in \mathfrak{m}_Q/\mathfrak{m}_Q^2$ y

$$0 = \alpha(\bar{\pi}([f])) = d_Q^*(\beta)(\bar{\pi}([f])) = \beta(d_Q(\bar{\pi}(f)) = d_Q(\bar{\pi}(f))(T).$$

Si $R = (d_1, \ldots, d_{N-1})$, aplicamos esto a las funciones $f_i(x) = x_i - d_i \in \mathfrak{m}_R$, de modo que $d_Q(\bar{\pi}(f_i))(T) = 0$. Vamos a calcular esta diferencial. En primer lugar,

$$\bar{\pi}(f_i) = \frac{x_i - 1}{x_N - 1} - \frac{b_i - 1}{b_N - 1} = \frac{(b_N - 1)(x_i - 1) - (b_i - 1)(x_N - 1)}{(b_N - 1)(x_N - 1)}.$$

Por lo tanto,

$$d_Q(\bar{\pi}(f_i)) = \frac{(b_n - 1)(x_i - b_i) - (b_i - 1)(x_N - b_N)}{(b_N - 1)^2}.$$

La igualdad $d_Q(\bar{\pi}(f_i))(x) = 0$ equivale a

$$(b_N - 1)(x_i - b_i) = (b_i - 1)(x_N - b_N).$$

Cuando $i = 1, \ldots, N-1$, estas ecuaciones determinan la recta que pasa por P y Q. Así pues, hemos probado que existe un punto $T \in T_QV'$, $T \neq Q$ que está en la recta que une P y Q o, equivalentemente, P está en la recta que pasa por dos puntos de T_QV', lo cual implica obviamente que $P \in T_QV' \subset T_QV$, contradicción.

Llamemos A_i^N al complementario del hiperplano H_i dado por $x_i = 0$ y sea $V_i = V \cap A_i^N$. Sea $\pi_i : V \longrightarrow H_i$ la proyección dada por

$$\pi_i(x) = (x_1 - x_i, \ldots, x_{N+1} - x_i).$$

El argumento anterior prueba en realidad que si $Q \in V_i$, entonces $d_Q\pi_i$ es inyectiva. Ahora bien, es fácil ver que $\pi = \pi_i \circ \pi|_{H_i}$, pues si L es la recta que une a P y Q, tenemos que $\pi(Q) = L \cap H_{N+1}$, $\pi_1(Q) = L \cap H_1$ y $\pi(\pi_1(Q))$ es el punto donde la recta que pasa por P y $\pi_1(Q)$ —o sea, L— corta a H_{N+1}, o sea, $\pi(Q)$.

Es fácil ver que $\pi|_{H_i} : H_i \longrightarrow H_{N+1}$ es un isomorfismo, de modo que podemos concluir que $d_Q\pi = d_Q\pi_1 \circ d_{\pi_1(Q)}\pi|_{H_1}$ es inyectiva. ■

Con esto podemos probar:

Teorema 3.51 *Toda variedad proyectiva regular de dimensión n es isomorfa a una subvariedad de* P^{2n+1}.

DEMOSTRACIÓN: Sea $V \subset \mathrm{P}^N$ una variedad proyectiva regular de dimensión n. El teorema quedará probado si, bajo la hipótesis de que $N > 2n+1$, encontramos un $P \in \mathrm{P}^N$ en las condiciones del teorema anterior. En efecto, si existe tal P, entonces V es isomorfa a su imagen por la proyección π, que es una subvariedad de P^{N-1}, y podemos repetir el argumento hasta sumergir V en P^{2n+1}.

Sea $C \subset \mathrm{P}^N \times V \times V$ el conjunto de todas las ternas de puntos colineales. La colinealidad de tres puntos equivale a que sus coordenadas homogéneas sean linealmente dependientes, lo cual equivale a que ciertos determinantes sean nulos, luego C es un conjunto algebraico. Consideremos la proyección $\pi : \mathrm{P}^N \times V \times V \longrightarrow V \times V$. Si $U = \{(Q_1, Q_2) \in V \times V \mid Q_1 \neq Q_2\}$, entonces, para todo $(Q_1, Q_2) \in U$, se cumple que $\pi|_C^{-1}[Q_1, Q_2] = L \times \{(Q_1, Q_2)\}$, donde L es la recta que pasa por Q_1 y Q_2. En particular $\pi|_C^{-1}[Q_1, Q_2]$ es irreducible de dimensión 1.

No podemos aplicar el teorema 3.47 porque esto tendría que ocurrir para todos los puntos de $V \times V$ y no sólo para los del abierto U. No obstante, si repasamos la prueba concluimos que en esta situación[3] existe una componente irreducible C_1 de C tal que $\pi[C_1] = V \times V$ y $\pi|_C^{-1}[U] \subset C_1$. Por el teorema 3.46 tenemos que $\dim C_1 \leq 2n+1$.

Consideramos la otra proyección $\pi' : \mathrm{P}^N \times V \times V \longrightarrow \mathrm{P}^N$. Por 2.47, se cumple que $\pi'[C_1]$ es cerrado. Por 3.46 sabemos además que $\dim \pi'[C_1] \leq 2n+1$, luego el abierto $U_1 = \mathrm{P}^N \setminus \pi'[C_1]$ no es vacío.

Ahora observamos que si $P \in U_1$, entonces $P \notin V$, o de lo contrario $(P, P, Q) \in U$, para cualquier $Q \in V$, $Q \neq P$, y tendríamos $P \in \pi'[U] \subset \pi'[C_1]$. Además una misma recta que pase por P no puede cortar a V en dos puntos distintos Q_1 y Q_2, pues entonces $(P, Q_1, Q_2) \in U$ y llegaríamos a la misma contradicción.

Consideremos ahora la proyección $\pi : V \times \mathrm{P}^N \longrightarrow \mathrm{P}^N$. Aplicando de nuevo el teorema 3.46 vemos que $\dim \pi[TV] \leq 2n$, luego $U_2 = \mathrm{P}^N \setminus \pi[TV]$ es un abierto no vacío. Si $P \in U_2$, entonces P no pertenece a ninguna variedad tangente de ningún punto de V. En resumen, un punto $P \in U_1 \cap U_2$ satisface las condiciones del teorema anterior. ■

3.6 Curvas algebraicas

Terminamos el capítulo con algunos resultados específicos para variedades de dimensión 1, es decir, para curvas. La mayoría de ellos sólo admiten generalizaciones parciales a dimensiones superiores.

[3]En el momento en que se toma $P \in U_1 \cap \cdots \cap U_r$ hay que exigir también $P \in U$.

Puntos regulares El teorema 3.42 afirma que si P es un punto regular de una variedad V entonces el anillo $\mathcal{O}_P(V)$ es un dominio de factorización única. En el caso de curvas podemos probar que es un dominio de ideales principales y, de hecho, esto resulta ser una caracterización de la regularidad. En primer lugar demostramos lo siguiente:

Teorema 3.52 *Un punto P de una curva V es regular si y sólo si el ideal maximal $\mathfrak{m}_P$ de $\mathcal{O}_P(V)$ es principal. En tal caso, los generadores de $\mathcal{O}_P(V)$ son los parámetros locales en P.*

DEMOSTRACIÓN: Una implicación es el teorema 3.37, en virtud del cual todo parámetro local genera $\mathfrak{m}_P$. Supongamos ahora que $\mathfrak{m}_P = (x)$ y veamos que $\mathfrak{m}_p/\mathfrak{m}_P^2 = \langle [x] \rangle_k$, con lo que $\dim \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$ y P será regular.

Todo $\alpha \in \mathfrak{m}_P$ es de la forma $\alpha = \beta x$, con $\beta \in \mathcal{O}_P(V)$. Sea $\beta(P) = a \in k$, de modo que $\beta - a \in \mathfrak{m}_P$, luego $\beta - a = \gamma x$, para cierto $\gamma \in \mathcal{O}_P(V)$. En definitiva tenemos que $\alpha = \beta x = ax + \gamma x^2$, luego $[\alpha] = a[x] \in \langle [x] \rangle_k$.

Falta probar que todo generador de $\mathcal{O}_P(V)$ es un parámetro local. Ahora bien, $x \in \mathcal{O}_P(V)$ es un parámetro local si y sólo si $x \in \mathfrak{m}_P$ y $x \notin \mathfrak{m}_P^2$. Es claro que si x cumple esto y ϵ es una unidad de $\mathcal{O}_P(V)$, entonces ϵx cumple lo mismo, luego todos los generadores de $\mathfrak{m}_P$ son parámetros locales en P. ■

Este teorema junto con 3.36 implica que si P es un punto regular de una curva, entonces el anillo $\mathcal{O}_P(V)$ es un dominio de ideales principales. Basta tener en cuenta el teorema siguiente:

Teorema 3.53 *Sea A un anillo noetheriano con un único ideal maximal $\mathfrak{m}$. Si $\mathfrak{m}$ es principal, entonces A es un dominio de ideales principales.*

DEMOSTRACIÓN: Sea $\mathfrak{m} = (\pi)$. Veamos que todo elemento no nulo de A es de la forma $\alpha = \epsilon\pi^n$, donde ϵ es una unidad y $n \geq 0$.

Si α es una unidad, es de esta forma con $n = 0$. En caso contrario $\alpha \in \mathfrak{m}$, pues $(\alpha) \neq 1$ y $\mathfrak{m}$ es el único ideal maximal. Así pues, $\alpha = \alpha_1\pi$, para cierto $\alpha_1 \in A$. Si α_1 tampoco es una unidad, entonces $\alpha_1 = \alpha_2\pi$, luego $\alpha = \alpha_2\pi^2$, para un cierto $\alpha_2 \in A$. Como A es noetheriano, la cadena de ideales

$$(\alpha) \subset (\alpha_1) \subset (\alpha_2) \subset \cdots$$

no puede prolongarse indefinidamente, luego hemos de llegar a una factorización $\alpha = \alpha_n\pi^n$ en la que α_n sea una unidad. La expresión es única, pues n está determinado por α como el único natural tal que $(\alpha) = \mathfrak{m}^n$. Definimos $v(\alpha) = n$, de modo que claramente $v(\alpha\beta) = v(\alpha) + v(\beta)$ (para α, $\beta \in A$ no nulos). El mismo argumento con que hemos probado el teorema 1.38 justifica que A es un dominio euclídeo con la norma v. En particular es un dominio de ideales principales. ■

Una propiedad notable de las curvas es la siguiente:

Teorema 3.54 *Si V es una curva, W es una variedad proyectiva y $\phi : V \longrightarrow W$ es una aplicación racional, entonces ϕ es regular en todos los puntos regulares de V.*

Demostración: Digamos que $W \subset \mathrm{P}^n$, sea $U \subset V$ el abierto donde ϕ es regular como aplicación en W y sea U' el abierto donde es regular como aplicación en P^n. En principio $U \subset U'$, pero es fácil ver que $\phi[U'] \subset \overline{\phi[U]} \subset W$, luego ϕ es regular como aplicación $\phi : U' \longrightarrow W$ (teorema 2.36). Así pues, $U = U'$, luego podemos suponer que $W = \mathrm{P}^n$.

Sea P un punto regular de V. Podemos suponer que $P \in U = \phi^{-1}[A^n]$ y basta probar que la restricción de ϕ a U es regular en P. Por 2.51, dicha restricción es de la forma $\phi(X) = (\alpha_1(X), \ldots, \alpha_n(X), 1)$, con $\alpha_1, \ldots, \alpha_n \in k(U)$. Teniendo en cuenta que $k(U)$ es el cuerpo de fracciones de $\mathcal{O}_P(U) = \mathcal{O}_P(V)$, podemos multiplicar por un factor adecuado para que

$$\phi(X) = (\alpha_1(X), \ldots, \alpha_{n+1}(X)),$$

donde $\alpha_1, \ldots, \alpha_{n+1} \in \mathcal{O}_P(V)$ no tienen ningún factor primo en común. En particular no se anulan todas en P, pues en tal caso tendrían como factor común a un parámetro local en P. Así pues, $\phi(P)$ está definido. ■

Teorema 3.55 *Si dos curvas proyectivas regulares son birracionalmente equivalentes, entonces son isomorfas.*

Demostración: Sea $\phi : V \longrightarrow W$ una aplicación birracional entre dos curvas proyectivas regulares. Por el teorema anterior tenemos que ϕ y ϕ^{-1} son regulares en V y W respectivamente, luego $\phi \circ \phi^{-1}$ es una aplicación regular que —al menos en un conjunto denso— coincide con la identidad. Por 2.44 tenemos que es la identidad. Igualmente al revés. ■

Ejemplo En el ejemplo de la página 63 hemos visto que la parábola (afín) $Y = X^2$ es isomorfa a la recta A^1. El isomorfismo es una aplicación birracional entre la parábola proyectiva y la recta P^1, luego ambas son isomorfas. En el ejemplo de la página 73 hemos visto que todas las cónicas son isomorfas, luego todas las cónicas son isomorfas a P^1. ■

Veamos otra caracterización útil de los puntos regulares:

Teorema 3.56 *Un punto P de una curva V es regular si y sólo si el anillo $\mathcal{O}_P(V)$ es íntegramente cerrado.*

Demostración: Ciertamente, si P es regular entonces $\mathcal{O}_P(V)$ es un dominio de factorización única y los dominios de factorización única son íntegramente cerrados (teorema 1.16).

Supongamos ahora que $\mathcal{O}_P(V)$ es íntegramente cerrado. Sustituyendo V por un entorno afín de P, podemos suponer que V es afín. Tomamos $f \in k[V]$ no nula tal que $f(P) = 0$. Por el teorema 3.21 sabemos que f se anula en un conjunto finito de puntos de V. Sustituyendo V por un entorno afín de P que no contenga a los demás puntos donde se anula f podemos suponer que f sólo se anula en P. Digamos que $f = [F]$. Si $\alpha \in \mathfrak{m}_P$, entonces $\alpha = [G]/[H]$, donde $G(P) = 0$, $H(P) \neq 0$. Por lo tanto,

$$G \in I(\{P\}) = I(V(I(V), F)) = \operatorname{Rad}(I(V), F),$$

luego existe un $m > 0$ tal que $G^m \in (I(V), F)$ y, por consiguiente, $[G]^m \in (f)$. A su vez, $\alpha^m \in (f)$. Si $\mathfrak{m}_P = (x_1, \ldots, x_r)$, podemos encontrar un mismo número natural $k > 0$ tal que $x_i^k \in (f)$. Tomando $m = kr$ concluimos que $\mathfrak{m}_P^m \subset (f)$ (pues un producto de m generadores ha de contener uno repetido k veces). Sea m el mínimo natural tal que $\mathfrak{m}_P^m \subset (f)$. Entonces existen $\alpha_1, \ldots, \alpha_{m-1} \in \mathfrak{m}_P$ tales que $\beta = \alpha_1 \cdots \alpha_{m-1} \notin (f)$ pero $\beta\mathfrak{m}_P \subset (f)$. Llamamos $\gamma = f/\beta$. Así, $\gamma^{-1} \notin \mathcal{O}_P(V)$ (o, de lo contrario, $\beta = \gamma^{-1}f \in (f)$), y además $\gamma^{-1}\mathfrak{m}_P \subset \mathcal{O}_P(V)$. Esto último implica que $\gamma^{-1}\mathfrak{m}_P$ es un ideal de $\mathcal{O}_P(V)$.

Por otra parte, $\gamma^{-1}\mathfrak{m}_p \not\subset \mathfrak{m}_P$, pues en caso contrario el teorema 1.10 implicaría que γ^{-1} es entero sobre $\mathcal{O}_P(V)$ y, como estamos suponiendo que $\mathcal{O}_P(V)$ es íntegramente cerrado, llegaríamos a que $\gamma^{-1} \in \mathcal{O}_P(V)$, contradicción.

Como $\mathfrak{m}_P$ es el único ideal maximal de $\mathcal{O}_P(V)$, ha de ser $\gamma^{-1}\mathfrak{m}_P = \mathcal{O}_P(V)$, lo cual equivale a que $\mathfrak{m}_P = (\gamma)$. ■

En el caso de curvas afines, este teorema tiene una versión global:

Teorema 3.57 *Una curva afín V es regular si y sólo si el anillo $k[V]$ es íntegramente cerrado.*

DEMOSTRACIÓN: Si V es regular, para probar que $k[V]$ es íntegramente cerrado tomamos $\alpha \in k(V)$ entero sobre $k[V]$ y vamos a ver que $\alpha \in k[V]$. Ahora bien, trivialmente α es entero sobre cada anillo $\mathcal{O}_P(V)$, con $P \in V$, y por hipótesis $\alpha \in \mathcal{O}_P(V)$. Así pues, α es regular sobre cada punto de V, es decir, $\alpha \in k[V]$.

Recíprocamente, supongamos que $k[V]$ es íntegramente cerrado, tomemos $P \in V$ y veamos que $\mathcal{O}_P(V)$ es íntegramente cerrado.[4] Dado $\alpha \in k(V)$ entero sobre $\mathcal{O}_P(V)$, tenemos que

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_0 = 0,$$

para ciertos $a_1, \ldots, a_n \in \mathcal{O}_P(V)$. Digamos que $a_i = u_i/v_i$ y sea $d = v_1 \cdots v_n$, de modo que $d \in \mathcal{O}_P(V)$, $d(P) \neq 0$. Multiplicando la igualdad anterior por d^n obtenemos que $\beta = d\alpha$ es entero sobre $k[V]$, luego por hipótesis $\beta \in k[V]$, luego $\alpha = \beta/d \in \mathcal{O}_P(V)$. ■

Regularización de una curva Ahora demostraremos que toda curva es birracionalmente equivalente a una curva regular, que además es única salvo isomorfismo si imponemos algunas restricciones, recogidas en la definición siguiente:

[4]Esto es un hecho general: toda localización de un dominio íntegro íntegramente cerrado es íntegramente cerrada.

Definición 3.58 Una *regularización* de una curva V es una curva regular V^r junto con una aplicación $r : V^r \longrightarrow V$ finita y birracional.

En primer lugar demostramos la existencia para curvas afines:

Teorema 3.59 *Toda curva afín tiene una regularización, que es también afín.*

Demostración: Sea V una curva afín y sea A la clausura entera de $k[V]$ en $k(V)$. Es claro que A es íntegramente cerrado. Vamos a probar que A es un $k[V]$-módulo finitamente generado. Por el teorema 1.32 podemos tomar una base de trascendencia x de $k(V)$ sobre k tal que la extensión $k(V)/k(x)$ sea finita separable. Más aún, si observamos detenidamente la prueba de 1.32 veremos que si partimos de un generador $k[V] = k[x_1, \ldots, x_n]$, entonces el x obtenido es combinación lineal de los x_i, con lo que podemos suponer que $x \in k[V]$. Tenemos que $k[x] \subset k[V] \subset A$, luego A es la clausura entera de $k[x]$ en $k(V)$. Por el teorema 1.19 concluimos que A es un $k[x]$-módulo finitamente generado, luego también un $k[V]$-módulo finitamente generado, como queríamos probar.

Combinando un generador de A sobre $k[V]$ con un generador de $k[V]$ sobre k obtenemos que $A = k[x_1, \ldots, x_n]$, para ciertos $x_1, \ldots, x_n \in A$. Es claro entonces que $A \cong k[X_1, \ldots, X_n]/I$, donde I es el núcleo del epimorfismo $X_i \mapsto x_i$. Como I es un ideal primo (porque A es un dominio íntegro), vemos que $V^r = V(I)$ es una variedad y $A \cong k[V^r]$. Más aún, V^r es una curva, pues el cuerpo de cocientes de A es $k(V)$, cuyo grado de trascendencia sobre k es 1. Además V^r es regular, pues A es íntegramente cerrado. La inclusión $k[V] \subset A = k[V^r]$ induce una aplicación finita $r : V^r \longrightarrow V$ y el teorema 2.54 nos da que es birracional. ■

De aquí pasamos al caso general:

Teorema 3.60 *Toda curva tiene una regularización.*

Demostración: Sea V una curva (cuasiproyectiva) y sea $V = \bigcup_{i=1}^{n} U_i$ un cubrimiento de V por abiertos afines.

Sea $r_i : U_i^r \longrightarrow U_i$ una regularización de U_i, que existe por el teorema anterior. Sea V_i la clausura proyectiva de U_i^r. Tomemos un abierto afín U_0 contenido en todos los abiertos U_i, que no contenga puntos singulares de V y tal que r_i se restrinja a un isomorfismo $r_i|_{U_0^i} : U_0^i \longrightarrow U_0$.

La composición $r_i \circ r_j^{-1}$ restringida a U_0^i se extiende a una aplicación birracional $\phi_{ij} : U_i^r \longrightarrow V_j$. El teorema 3.54 nos da que ϕ_{ij} es regular. Sea $W = \prod_i V_i$ y $\phi_i : U_i^r \longrightarrow W$ dada por

$$\phi_i(P) = (\phi_{i1}(P), \ldots, \phi_{in}(P)).$$

Definimos $V^r = \bigcup_i \phi_i[U_i^r]$. Vamos a probar que V^r es una curva (cuasiproyectiva).

Observemos que $X = \phi_i[U_i^0] = \{(r_1^{-1}(P), \ldots, r_n^{-1}(P)) \mid P \in U_0\}$ es una curva isomorfa a U_0 (independiente de i) tal que $X \subset \phi_i[U_i^r] \subset \overline{X}$. Para probar la última inclusión tomamos un punto $Q \in U_i^r$ y un abierto U en W tal que

$\phi_i(Q) \in U$, y hemos de probar que $U \cap X \neq \varnothing$. En efecto, $\phi_i^{-1}[U]$ es abierto en U_i^r (no vacío) al igual que U_i^0, luego $\phi_i^{-1}[U] \cap U_i^0 \neq \varnothing$ y, por lo tanto, $U \cap X \neq \varnothing$.

Por consiguiente, $X \subset V^r \subset \overline{X}$. Como $\overline{X} \setminus X$ es finito, lo mismo sucede con $\overline{X} \setminus V^r$, luego V^r es abierto en la curva proyectiva $\overline{X}$, luego V^r es una curva cuasiproyectiva. Notemos que, por el mismo motivo, cada $\phi_i[U_i^r]$ es abierto en $\overline{X}$ y, por consiguiente, en V^r.

Veamos ahora que V^r es regular. Para ello basta probar que cada $\phi_i[U_i^r]$ es regular, pues todo punto de V^r está contenido en uno de estos abiertos. A su vez basta ver que ϕ_i es un isomorfismo en su imagen. Ciertamente es regular, y su inversa es la proyección sobre V_i, pues $\phi_{ii} : U_i^r \longrightarrow V_i$ es la identidad en U_0^i, luego es la identidad en todo U_i^r.

Sea ahora $r_i' : \phi_i[U_i^r] \longrightarrow V$ la aplicación $r_i' = \phi_i^{-1} \circ r_i$. Según acabamos de comentar, ϕ_i^{-1} es simplemente la proyección i-ésima, luego r_i' es regular. Además todas las aplicaciones r_i' coinciden en X. Por el teorema 2.44, dos cualesquiera de ellas coinciden en su dominio común, luego entre todas inducen una aplicación regular $r : V^r \longrightarrow V$. De hecho es birracional, pues se restringe a un isomorfismo entre X y U_0. Por último, la finitud de las aplicaciones r_i implica claramente la finitud de cada r_i', y de aquí se sigue la finitud de r, pues r coincide con una r_i en un entorno de cada punto.

Así pues, $r : V^r \longrightarrow V$ es una regularización de V. ■

La unicidad de la regularización de una curva es consecuencia del teorema siguiente, más general:

Teorema 3.61 *Sea $r : V^r \longrightarrow V$ una regularización de una curva V y sea $\phi : W \longrightarrow V$ una aplicación regular densa definida sobre una curva regular W. Entonces existe una aplicación regular $\psi : W \longrightarrow V^r$ tal que $\psi \circ r = \phi$.*

Demostración: Supongamos primeramente que las tres curvas son afines. A través de ϕ podemos considerar $k[V] \subset k[W]$ y a través de r que $k[V] \subset k[V^r]$ y $k(V) = k(V^r)$. Así, todo $\alpha \in k[V^r]$ es entero sobre $k[V]$ y, en particular, sobre $k[W]$. Además $\alpha \in k(V) \subset k(W)$. Como W es regular, $k[W]$ es íntegramente cerrado, luego concluimos que $\alpha \in k[W]$. Así pues, $k[V] \subset k[V^r] \subset k[W]$. La segunda inclusión determina una aplicación ψ que cumple el teorema.

En el caso general, para cada $P \in W$ tomamos un entorno afín U de $\phi(P)$ tal que $U^r = r^{-1}[U]$ sea afín y la restricción de r sea finita (es claro entonces que U^r es una regularización de U). Tomemos un entorno afín U' de P tal que $U' \subset \phi^{-1}[U]$. Como los abiertos en las curvas son cofinitos, podemos cubrir W por un número finito de abiertos $U_1', \ldots, U_m'$ en estas condiciones. Por la parte ya probada, existen aplicaciones regulares $\psi_i : U_i \longrightarrow U_i^r$ que cumplen $\psi_i \circ r = \phi$. Basta probar que dos de ellas coinciden en su dominio común. Ahora bien, si $U_0 \subset V^r$ es un abierto donde r es un isomorfismo (tal que cada punto de $r[U_0]$ tiene una única antiimagen en V^r) y $U_0' = \phi^{-1}[r[U_0]]$, entonces dos aplicaciones ψ_i y ψ_j coinciden sobre los puntos del abierto $U_i' \cap U_j' \cap U_0'$. En efecto, si Q está en este conjunto, entonces

$$r(\psi_i(Q)) = r(\psi_j(Q)) = \phi(Q) \in r[U_0],$$

luego $\psi_i(Q) = \psi_j(Q) = r^{-1}(\phi(Q))$. Por lo tanto las aplicaciones ψ_i inducen una aplicación ψ que cumple el teorema. ■

Como consecuencia:

Teorema 3.62 *Si $r : V^r \longrightarrow V$ y $r' : V'^r \longrightarrow V$ son regularizaciones de una misma curva V, entonces existe un isomorfismo $\psi : V^r \longrightarrow V'^r$ tal que $\psi \circ r' = r$.*

DEMOSTRACIÓN: Aplicando el teorema anterior obtenemos una aplicación regular ψ que cumple el enunciado, pero también una aplicación $\psi' : V'^r \longrightarrow V^r$ regular que cumple $\psi' \circ r = r'$. Basta ver que son inversas, pero $\psi \circ \psi'$ coincide con la identidad en un abierto, luego es la identidad, y lo mismo vale para $\psi' \circ \psi$. ■

Es claro que la regularización de una curva puede obtenerse por restricción de la regularización de su clausura proyectiva, por lo que la existencia de la regularización de una curva proyectiva contiene el caso general. Respecto a ésta, podemos precisar un poco más:

Teorema 3.63 *La regularización de una curva proyectiva es proyectiva.*

DEMOSTRACIÓN: Sea V una curva proyectiva y $r : V^r \longrightarrow V$ su regularización. Si V^r no es proyectiva, llamamos W a su clausura proyectiva y tomamos $P \in W \setminus V^r$. Sea U un entorno afín de P en W. La regularización $r' : U^r \longrightarrow U$ se restringe a un isomorfismo entre un abierto de U^r y un abierto de V^r, luego $\phi = r' \circ r$ determina una aplicación birracional $\phi : U^r \longrightarrow V$. Como V es proyectiva, concluimos que ϕ es regular, es decir, está definida en todo U^r.

Por 3.61 existe una aplicación regular $\psi : U^r \longrightarrow V^r$ tal que $\psi \circ r = \phi$. Así ψ y r' coinciden sobre un abierto, luego $\psi = r'$, pero entonces

$$P \in U = r'[U^r] = \psi[U^r] \subset V^r,$$

contradicción. ■

En particular tenemos que toda curva proyectiva es birracionalmente equivalente a una curva proyectiva regular (única salvo isomorfismo). El teorema 3.51 muestra que la regularización puede tomarse contenida en P^3. El ejemplo de la página 314 muestra una curva proyectiva plana que no es birracionalmente equivalente a ninguna curva proyectiva plana regular.

Terminamos con una observación sobre la regularización $r : V^r \longrightarrow V$ de una curva V: los puntos regulares de V tienen una única antiimagen. En efecto, por el teorema 3.32 sabemos que el conjunto U de los puntos regulares de V es un abierto. Entonces, la restricción $r|_{r^{-1}[U]} : r^{-1}[U] \longrightarrow U$ es una regularización de U, pero la identidad en U es otra. Por la unicidad, $r|_{r^{-1}[U]}$ tiene que ser un isomorfismo, luego cada punto de U tiene una única antiimagen por r.

Por lo tanto, sólo una cantidad finita de puntos de V tiene más de una antiimagen por r (a lo sumo los puntos singulares). No obstante, un punto singular puede tener una sola antiimagen.

Ejemplo Consideremos la cúbica V dada por $Y^2 = X^3$ (ver la figura de la página 55 y el ejercicio de la página 119). Es claro que la aplicación $r : A^1 \longrightarrow V$ dada por $r(t) = (t^2, t^3)$ es biyectiva y regular y se restringe a un isomorfismo $A^1 \setminus \{0\} \longrightarrow V \setminus \{0, 0\}$, luego es birracional. También es finita, pues a través de r el anillo $k[V]$ se identifica con $k[t^2, t^3] \subset k[t]$, y la extensión es entera, pues t es raíz de $T^2 - t^2 \in k[V][T]$. Por lo tanto r es la regularización de V. De este modo, el punto $(0, 0)$ es un punto singular de V y tiene una única antiimagen por r. ■

Ejemplo *Las cúbicas singulares* $Y^2 = X^3$ *y* $X^3 + Y^3 = XY$ *no son isomorfas.* (Comparar con el ejemplo de la página 119.)

En lugar de $X^3 + Y^3 = XY$ podemos considerar la curva $Y^2 = X^2(X + 1)$, que es proyectivamente equivalente a la del enunciado y hemos trabajado más con ella. La aplicación construida en el ejemplo de la página 93 es claramente la regularización de la curva, y vemos que el punto singular tiene dos antiimágenes. Por el contrario, el ejemplo anterior muestra que la regularización de $Y^2 = X^3$ es biyectiva, luego el teorema 3.62 implica que las dos curvas no pueden ser isomorfas. ■

Capítulo IV

Variedades complejas

En este capítulo estudiaremos las variedades (cuasiproyectivas) complejas, es decir, las variedades sobre el cuerpo $k = \mathbb{C}$. Además del aparato algebraico que hemos introducido en los capítulos precedentes (anillos de funciones regulares, cuerpos de funciones racionales, etc.) ahora dispondremos de una estructura topológica y una estructura analítica. Veremos que muchos de los conceptos que hemos definido (como la dimensión, la regularidad de puntos y aplicaciones, etc.) pueden verse como caracterizaciones algebraicas de nociones geométricas análogas.

4.1 Las estructuras topológica y analítica

Según sabemos, fijado un sistema de referencia en P^n, los espacios A_i formados por los puntos de P^n que cumplen $X_i \neq 0$, para $i = 1, \ldots, n+1$, son un cubrimiento de P^n, y cada uno de ellos puede identificarse con $\mathbb{C}^n$ a través de la aplicación $p_i : A_i \longrightarrow \mathbb{C}^n$ que a cada P le asigna la n-tupla resultante de eliminar la i-ésima coordenada del único vector de coordenadas homogéneas de P que cumple $X_i = 1$.

Si consideramos dos índices distintos (por simplicidad tomaremos $i = 1$ y $j = n+1$), tenemos que

$$\begin{aligned} U_1 &= p_1[A_1 \cap A_{n+1}] = \{z \in \mathbb{C}^n \mid z_n \neq 0\}, \\ U_{n+1} &= p_{n+1}[A_1 \cap A_{n+1}] = \{z \in \mathbb{C}^n \mid z_1 \neq 0\}. \end{aligned}$$

La aplicación $\phi = p_1^{-1} \circ p_{n+1} : U_1 \longrightarrow U_{n+1}$ viene dada por

$$(z_1, \ldots, z_n) \mapsto (1, z_1, \ldots, z_n)$$

$$= \left(\frac{1}{z_n}, \frac{z_2}{z_n}, \ldots, \frac{z_{n-1}}{z_n}, 1\right) \mapsto \left(\frac{1}{z_n}, \frac{z_2}{z_n}, \ldots, \frac{z_{n-1}}{z_n}\right).$$

Es claro que esta aplicación es una transformación conforme entre U_1 y U_{n+1}.

Ahora es fácil ver que existe una única topología (de Hausdorff) en P^n para la cual los conjuntos A_i son abiertos y las aplicaciones p_i son homeomorfismos. Más aún, las aplicaciones p_i determinan una estructura analítica sobre P^n, lo que las convierte, de hecho, en transformaciones conformes entre cada A_i y $\mathbb{C}^n$.

Ahora veremos que la estructura analítica de P^n no depende de la elección del sistema de referencia con que la hemos construido. En definitiva, vamos a probar el teorema siguiente:

Teorema 4.1 *Existe una única estructura analítica sobre P^n (en particular, una única topología) tal que, para todo sistema de referencia, los espacios afines A_i son abiertos y las aplicaciones $p_i : A_i \longrightarrow \mathbb{C}^n$ son transformaciones conformes.*

DEMOSTRACIÓN: Basta probar que la topología y la estructura analítica que acabamos de construir no dependen del sistema de referencia. Esto nos da la existencia. La unicidad es clara. Consideramos otro sistema de referencia, el cual determina otros espacios A_i' con sus proyecciones correspondientes p_i'. Hemos de probar que los conjuntos A_i' son abiertos y que las aplicaciones p_i' son transformaciones conformes respecto de la estructura analítica determinada por los abiertos A_i y las aplicaciones p_i.

La relación entre las coordenadas homogéneas de un mismo punto respecto de cada sistema de referencia será de la forma $Z' = ZA$, donde A es una matriz regular. En particular,

$$A_i' = \{(z_1, \ldots, z_{n+1}) \mid a_{1i}z_1 + \cdots + a_{n+1\,i}\, z_{n+1} \neq 0\}.$$

Este conjunto será abierto si lo son todas las intersecciones $A_i' \cap A_j$, para lo cual basta que lo sean los conjuntos $p_j[A_i' \cap A_j]$. Por simplicidad tomamos $j = n+1$, con lo que

$$p_{n+1}[A_i' \cap A_{n+1}] = \{z \in \mathbb{C}^n \mid a_{1i}z_1 + \cdots + a_{ni}z_n + a_{n+1\,i} \neq 0\}.$$

Es obvio que este conjunto es abierto en $\mathbb{C}^n$. Veamos ahora que p_i' es holomorfa en un entorno de cada punto $z_0 \in A_i'$. Supongamos, por ejemplo, que $z_0 \in A_{n+1}$ y veamos que p_i' es holomorfa en $A_i' \cap A_{n+1}$.

Para ello observamos que si $z \in p_{n+1}[A_i' \cap A_{n+1}]$, entonces $(p_{n+1}^{-1} \circ p_i')(z)$ se calcula como sigue: primero pasamos a $p_{n+1}^{-1}(z)$, que es el punto cuyas coordenadas respecto al primer sistema de referencia son $(z_1, \ldots, z_n, 1)$, luego calculamos sus coordenadas respecto del segundo sistema de referencia, que son $(z_1, \ldots, z_n, 1)A$, luego dividimos entre la i-ésima, que es $a_{1i}z_1 + \cdots + a_{ni}z_n + a_{n+1\,i}$, y finalmente eliminamos el 1 que queda en la posición i. El resultado es una n-tupla de cocientes de polinomios de primer grado con denominador no nulo. Es claro que se trata de una función holomorfa, lo que prueba que p_i' es holomorfa. La holomorfía de la inversa se comprueba de forma similar. ■

En lo sucesivo consideraremos siempre a P^n como variedad analítica con la estructura dada por el teorema anterior. No obstante, hemos de distinguir entre la topología que acabamos de definir, a la que llamaremos *topología compleja* en P^n, y la topología de Zariski.

El teorema siguiente es un hecho técnico elemental que nos será útil en varias ocasiones:

Teorema 4.2 *La aplicación $p : \mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathrm{P}^n$ que a cada z le asigna el punto de P^n que tiene coordenadas z respecto a un sistema de referencia dado es holomorfa.*

DEMOSTRACIÓN: La restricción de p a $p^{-1}[A_{n+1}]$ seguida de p_{n+1} es

$$(z_1, \ldots, z_{n+1}) \mapsto \left(\frac{z_1}{z_{n+1}}, \ldots \frac{z_n}{z_{n+1}} \right),$$

que es holomorfa. Esto prueba que p es holomorfa en $p^{-1}[A_{n+1}]$ y es claro que lo mismo vale para todo $p^{-1}[A_i]$. Como estos abiertos cubren $\mathbb{C}^{n+1} \setminus \{0\}$, concluimos que p es holomorfa en todo su dominio. ■

Como primera aplicación observamos que la restricción de p a la esfera unidad de $\mathbb{C}^{n+1}$ es continua y suprayectiva, y la esfera es compacta. Por tanto:

Teorema 4.3 *Los espacios proyectivos son compactos.*

Ejercicio: Probar que P^1 (como variedad diferencial real) es difeomorfo a una esfera.

Ejercicio: Comprobar que todos los resultados que hemos probado aquí son ciertos para los espacios proyectivos reales cambiando la holomorfía por la diferenciabilidad.

Toda variedad cuasiproyectiva compleja V es un subconjunto de un espacio proyectivo P^n, luego, además de la topología de Zariski, podemos considerar en ella la topología inducida por la topología compleja de P^n. La llamaremos *topología compleja* en V. Observemos que la topología compleja en $A^n = \mathbb{C}^n$ es la topología usual.

Un polinomio es una función continua en A^n, luego el conjunto de sus ceros es cerrado. Por consiguiente, un conjunto algebraico afín es cerrado por ser una intersección de cerrados. Lo mismo es cierto para los conjuntos algebraicos proyectivos:

Teorema 4.4 *Todo subconjunto algebraico de P^n es compacto con la topología compleja.*

DEMOSTRACIÓN: Sea C un subconjunto algebraico de P^n y consideremos el cono $Cn(C) \subset \mathbb{C}^{n+1}$. Tenemos que $Cn(C)$ es un conjunto algebraico afín, luego es cerrado en $\mathbb{C}^{n+1}$, según las observaciones precedentes. También será cerrada la intersección C' del cono con la esfera unidad de $\mathbb{C}^{n+1}$. Más aún, como la esfera es compacta, C' también lo será. La aplicación $p : \mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathrm{P}^n$ dada por 4.2 es continua, y claramente $C = p[C']$, luego C es compacto. ■

Así pues, la topología de Zariski de P^n es menos fina que la topología compleja y, por consiguiente, lo mismo es válido sobre cualquier variedad cuasiproyectiva.

Las variedades algebraicas heredan, obviamente, la estructura topológica de P^n, pero no siempre heredan por completo su estructura analítica. Aquí interviene el concepto algebraico de regularidad:

Teorema 4.5 *Si $V \subset \mathrm{P}^n$ una variedad cuasiproyectiva de dimensión d, entonces el conjunto V_r de sus puntos regulares es una subvariedad analítica de P^n de dimensión d.*

DEMOSTRACIÓN: Según 1.74, basta probar que los puntos regulares de V son analíticos. Tomemos $P \in V_r$. Podemos suponer que cumple $z_{n+1} \neq 0$, de modo que $P \in V_r' = V_r \cap A^n$. Sea $I(V_r') = (F_1, \ldots, F_m)$, para ciertos polinomios $F_i \in \mathbb{C}[X_1, \ldots, X_n]$. En la prueba de 3.32 hemos visto que si $A(X)$ es la matriz formada por las derivadas de los polinomios F_i, entonces la regularidad de P equivale a que $\operatorname{rang} A(P) = n - d$. Además $r = n - d$ es el mayor rango que puede tener $A(X)$ en un punto cualquiera.

Consideremos una submatriz $r \times r$ cuyo determinante sea no nulo en P. El determinante es un polinomio en $X_1, \ldots, X_n$, luego el conjunto de puntos donde no se anula es un entorno de P, en el cual el rango de $A(X)$ es constante. Según el teorema 1.58, podemos expresar $A^n = \mathbb{C}^n = \mathbb{C}^d \times \mathbb{C}^r$, de modo que $P = (z_0, w_0)$, existen abiertos $z_0 \in U \subset \mathbb{C}^d$, $P \in U' \subset \mathbb{C}^n$ y una función holomorfa $g : U \longrightarrow \mathbb{C}^r$ de modo que

$$\tilde{U} = V_r' \cap U' = \{(z, g(z)) \mid z \in U\}.$$

La aplicación $f : U \longrightarrow \tilde{U}$ dada por $f(z) = (z, g(z))$ es un homeomorfismo (su inversa es una proyección), es holomorfa como aplicación en A^n (o en P^n) y su diferencial es inyectiva en todo punto (pues su matriz jacobiana tiene una submatriz igual a la identidad de orden d). Según 1.73, esto prueba que V_r es analítico en P. ■

En particular, las variedades cuasiproyectivas regulares en P^n son subvariedades analíticas de P^n. También vemos ahora que la noción algebraica de dimensión se corresponde debidamente con la noción geométrica.

Teorema 4.6 *Toda aplicación regular $\phi : V \longrightarrow W$ entre variedades cuasiproyectivas es continua y, si además V y W son regulares, entonces ϕ es holomorfa.*

DEMOSTRACIÓN: No perdemos generalidad si suponemos $W = \mathrm{P}^n$, pues si $W \subset \mathrm{P}^n$, entonces ϕ es continua u holomorfa como aplicación en W si y sólo si lo es como aplicación en P^n. Fijemos $P \in V$. Basta ver que ϕ es continua u holomorfa en un entorno de P. Según las observaciones tras el teorema 2.51, existe un entorno U de P en V para la topología de Zariski —luego también para la topología compleja— en el que ϕ viene dada por

$$\phi(Q) = (F_1(Q), \ldots, F_{n+1}(Q)),$$

donde $F_1, \ldots, F_{n+1}$ son formas del mismo grado que no se anulan simultáneamente en ningún punto. Más aún, podemos suponer que $U \subset A^m$. Así podemos tomar coordenadas afines y $\phi|_U$ se expresa como composición de las aplicaciones siguientes, todas continuas, y holomorfas en caso en que V y W sean regulares:

a) La aplicación que a cada Q le asigna su m-tupla de coordenadas afines. (Es la restricción a U de una función holomorfa en A^m.)

b) La aplicación polinómica $\mathbb{C}^m \longrightarrow \mathbb{C}^{n+1}$ definida por las formas (deshomogeneizadas) F_i.

c) La aplicación holomorfa $\mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathrm{P}^n$ dada por 4.2. ■

Ejercicio: Comprobar que la topología compleja en un producto $V \times W$ es el producto de las topologías complejas.

Si V es una variedad cuasiproyectiva regular, según 2.35, las funciones de $\mathbb{C}[V]$ pueden verse como funciones regulares $V \longrightarrow \mathbb{C}$, luego son holomorfas, es decir, tenemos que $\mathbb{C}[V] \subset \mathcal{H}(V)$. A su vez, esto implica que $\mathcal{O}_P(V) \subset \mathcal{H}_P(V)$.

Si $P \in V$, tenemos definidos dos espacios tangentes, el analítico y el algebraico. El primero está formado por las derivaciones de $\mathcal{H}_P(V)$, mientras que el segundo está formado por las derivaciones de $\mathcal{O}_P(V)$. Ahora bien, el teorema 1.75 aplicado a las coordenadas $x_1, \ldots, x_m$ de un entorno afín de P nos da que algunas de ellas se restringen a las funciones coordenadas de una carta de V alrededor de P, y son funciones de $\mathcal{O}_P(V)$, y un elemento del espacio tangente analítico está determinado por su acción sobre estas funciones. Por lo tanto, la restricción es un monomorfismo del espacio tangente analítico en el algebraico. Como ambos tienen la misma dimensión, de hecho es un isomorfismo.

Si $f \in \mathcal{O}_P(V)$ y $v \in T_PV$, la relación $d_Pf(v) = v(f)$ se cumple tanto para la diferencial algebraica como para la geométrica, luego ambas coinciden.

A su vez, 1.68 nos da ahora que unas funciones $x_1, \ldots, x_n \in \mathcal{O}_P(V)$ son las funciones coordenadas de una carta alrededor de P si y sólo si las funciones $x_i - x_i(P)$ son un sistema de parámetros locales en P.

Teorema 4.7 *Sea P un punto regular de una variedad V y sea $x_1, \ldots, x_n$ un sistema fundamental de parámetros alrededor de P. Si $\alpha \in \mathcal{O}_P(V)$, entonces su serie de Taylor*

$$\sum_{m=0}^{\infty} F_m \in \mathbb{C}[[X_1, \ldots, X_n]]$$

converge en un abierto $D \subset \mathbb{C}^n$ y, para todo punto Q en un cierto entorno de P en V, se cumple que $(x_1(Q), \ldots, x_n(Q)) \in D$ y

$$\alpha(Q) = \sum_{m=0}^{\infty} F_m(x_1(Q), \ldots, x_n(Q)).$$

Demostración: Sea G un entorno de P en V en el que α sea regular y tal que la aplicación $\phi : G \longrightarrow \mathbb{C}^n$ dada por $\phi(Q) = (x_1(Q), \ldots, x_n(Q))$ sea una carta de V alrededor de P. Entonces $\phi^{-1} \circ \alpha$ es una función holomorfa en un entorno de 0 en $\mathbb{C}^n$, luego admite un desarrollo en serie de Taylor

$$\alpha(\phi^{-1}(z_1, \ldots, z_n)) = \sum_{m=0}^{\infty} F_m(z_1, \ldots, z_n).$$

Sea U la antiimagen por ϕ del dominio de la serie de potencias, de modo que para todo $Q \in U$ se cumple

$$\alpha(Q) = \sum_{m=0}^{\infty} F_m(x_1(Q), \ldots, x_n(Q)).$$

Sólo hemos de probar que $\tau'(\alpha) = \sum\limits_{m=0}^{\infty} F_m(X_1, \ldots, X_n)$ es la serie de Taylor de α.

Tenemos definidos dos k-homomorfismos τ, $\tau' : \mathcal{O}_P(V) \longrightarrow k[[X_1, \ldots, X_n]]$, que asignan a cada función su serie de Taylor algebraica y analítica respectivamente. Obviamente $\tau(x_i) = X_i = \tau'(x_i)$, luego ambos coinciden sobre el anillo $k[x_1, \ldots, x_n]$.

Consideramos en $\mathcal{O}_P(V)$ la topología que resulta de identificarlo con su imagen por τ, respecto a la cual $k[x_1, \ldots, x_n]$ se corresponde con $k[X_1, \ldots, X_n]$ y es denso. Si probamos que τ' es continua respecto a esta topología, tendremos que $\tau = \tau'$, como queremos demostrar.

Como τ' conserva sumas basta ver que es continua en 0. Para ello a su vez basta probar que si $\alpha \in \mathfrak{m}_P^r$ entonces $v(\tau'(\alpha)) \geq r$. Ahora bien, esto es trivial, pues si $\alpha \in \mathfrak{m}_P$ entonces $\alpha(P) = 0$, luego $\tau'(\alpha)(0, \ldots, 0) = 0$, lo que se traduce en que $v(\tau'(\alpha)) \geq 1$, y ahora basta usar que τ' es un homomorfismo y las propiedades de las valoraciones. ■

Así pues, si llamamos $g : \tilde{U} \subset \mathbb{C}^n \longrightarrow \mathbb{C}$ a la función definida por la serie de Taylor y $x : U \longrightarrow \tilde{U}$ a la función $x(Q) = (x_1(Q), \ldots, x_n(Q))$, tenemos que x es una carta alrededor de P y, para todo $Q \in U$, se cumple $f(Q) = g(x(Q))$, luego g es la lectura de f en la carta x.

Teniendo esto en cuenta es inmediato que las derivadas parciales $\partial/\partial x_i|_P$ en el sentido algebraico coinciden con las analíticas. (En realidad ya sabíamos que esto es así porque ambas son la base dual de la base $d_P x_i$ de $T_P V^*$.)

Observemos ahora que $\mathbb{C}(V) \subset \mathcal{M}(V)$. En efecto, si $P \in V$, llamamos V_0 a la intersección de V con un espacio afín que contenga a P, de modo que V_0 es un entorno de P y cada $\alpha \in \mathbb{C}(V)$ se calcula (en los puntos de V_0 donde está definida) como cociente de dos funciones de $\mathbb{C}[V_0] \subset \mathcal{H}(V_0)$. Así pues, $\alpha|_{V_0} \in \mathcal{K}(V_0)$, luego $\alpha \in \mathcal{M}(V)$. A priori podría ocurrir que una función de $\mathbb{C}(V)$ estuviera definida en un punto como función meromorfa pero no como función racional. Vamos a ver que de hecho no es así:

Teorema 4.8 *Si V es una variedad cuasiproyectiva regular y $f \in \mathbb{C}(V)$ es holomorfa en un punto P, entonces f es regular en P.*

DEMOSTRACIÓN: Tenemos las inclusiones

$$\mathcal{O}_P(V) \subset \mathcal{H}_P(V) \subset \mathbb{C}[[X_1, \ldots, X_n]].$$

Pongamos que $f = u/v$, donde u, $v \in \mathcal{O}_P(V)$. Que f sea holomorfa en P significa que $v \mid u$ en $\mathcal{H}_P(V)$, luego también en $\mathbb{C}[[X_1, \ldots, X_n]]$. Ahora bien, en el teorema 3.42 hemos demostrado que $\mathcal{O}_P(V)$ y $\mathbb{C}[[X_1, \ldots, X_n]]$ cumplen las hipótesis del teorema 3.41, y en la prueba de éste hemos visto que si $v \mid u$ en $\mathbb{C}[[X_1, \ldots, X_n]]$, también $v \mid u$ en $\mathcal{O}_P(V)$, luego $f \in \mathcal{O}_P(V)$. ■

A veces es útil la siguiente caracterización interna de la topología compleja de una variedad:

Teorema 4.9 *Una base de una variedad cuasiproyectiva V para la topología compleja la forman los conjuntos*

$$U(\alpha_1, \ldots, \alpha_r; \epsilon) = \{P \in V \mid \alpha_i \in \mathcal{O}_P(V) \ y \ |\alpha_i(P)| < \epsilon\}, \quad \alpha_i \in \mathbb{C}(V), \ \epsilon > 0.$$

DEMOSTRACIÓN: Basta probarlo para la clausura proyectiva de V o, lo que es lo mismo, en el caso en que $V \subset \mathrm{P}^n$ es proyectiva. Si G es el conjunto de puntos de V donde todas las α_i son regulares, entonces G es abierto en V para la topología de Zariski, luego también para la compleja, el conjunto $U = U(\alpha_1, \ldots, \alpha_r; \epsilon)$ está contenido en G y todas las $\alpha_i|_G$ son continuas, luego U es abierto.

Consideremos ahora un abierto G en V y un punto $P \in G$. Tomemos un sistema de referencia proyectivo de P^n respecto al cual P tenga coordenadas homogéneas $(0, \ldots, 0, 1)$. Vamos a ver que existe un número real $\epsilon > 0$ tal que $P \in U(x_1, \ldots, x_n; \epsilon) \subset G$. En caso contrario existiría $P_m \in U(x_1, \ldots, x_n; 1/m)$ tal que $P_m \notin G$. La compacidad de V implica que $\{P_m\}$ tiene una subsucesión $\{P_{m_i}\}$ convergente a un punto $Q \in V \setminus G$. Como $|x_j(P_{m_i})| < 1/m_i$, concluimos que $x_j(Q) = 0$ para todo $j = 1, \ldots, n$, luego ha de ser $Q = P$, contradicción. ■

Sabemos que los abiertos de la topología de Zariski son densos. Pronto veremos que también son densos en la topología compleja, pero primero hemos de probar un caso particular:

Teorema 4.10 *El conjunto V_r de los puntos regulares de una variedad cuasiproyectiva V es denso en V (respecto a la topología compleja).*

DEMOSTRACIÓN: Es claro que el problema se reduce al caso de una variedad proyectiva y de aquí al de una variedad afín. Sea, pues, $V \subset A^n$ una variedad afín y supongamos que $W \subset V$ es un abierto no vacío que no contiene puntos regulares. Sea $I(V) = (F_1, \ldots, F_m)$ y sea $A(X)$ la matriz formada por las derivadas parciales de los polinomios F_i. Según hemos visto en la prueba de 3.32, ha de ser $\operatorname{rang} A(X) < \operatorname{codim} V$ para todo $X \in W$. Sea $P \in W$ un punto donde $\operatorname{rang} A(X) = r = n - d$ tome el valor máximo. Según lo dicho, $d > \dim V$.

Existe una submatriz de orden r en $A(X)$ con determinante no nulo en P y, por continuidad, en un entorno de P contenido en W. En dicho entorno, el rango de $A(X)$ no puede disminuir, ni tampoco aumentar por la maximalidad de r. A partir de aquí todo el razonamiento de 4.5 es válido igualmente, lo que nos da que V es analítica en P y, más aún, que existe un homeomorfismo $f : U \subset \mathbb{C}^d \longrightarrow \tilde{U} \subset V$ de la forma $f(z) = (z, g(z))$.

El abierto U contendrá un producto de abiertos $U_1 \times \cdots \times U_d$, de modo que en V podemos encontrar puntos $(x_1, \ldots, x_n)$ con coordenadas $x_i \in U_i$ determinadas arbitrariamente. Ahora bien, como $d > \dim V$, las funciones $x_1, \ldots, x_d \in \mathbb{C}[V]$ han de ser algebraicamente dependientes, luego existe un polinomio no nulo $F(X_1, \ldots, X_d) \in \mathbb{C}[X_1, \ldots, X_d]$ tal que $F(x_1, \ldots, x_d) = 0$. Esto nos lleva claramente a una contradicción: Fijados $(a_1, \ldots, a_{d-1}) \in U_1 \times \cdots \times U_{d-1}$, el polinomio $F(a_1, \ldots, a_{d-1}, X_d) \in \mathbb{C}[X_d]$ tiene infinitas raíces (todos los elementos de U_d), luego ha de ser nulo. Esto significa que los coeficientes de F (visto como polinomio en X_d) se anulan en todos los puntos de $U_1 \times \cdots \times U_{d-1}$. Repitiendo el argumento, los coeficientes de estos coeficientes (vistos como polinomios en X_{d-1}) se anulan en $U_1 \times \cdots \times U_{d-2}$, y así llegamos a que F es el polinomio nulo.

■

En la prueba anterior hemos visto que si una variedad $V \subset A^n$ es localmente la gráfica de una función $g : \tilde{U} \subset \mathbb{C}^d \longrightarrow \mathbb{C}^{n-d}$, entonces las coordenadas $x_1, \ldots, x_d$ son algebraicamente independientes en $\mathbb{C}(V)$.

Ahora podemos probar un principio notable. El teorema siguiente sería un mero caso particular de 1.60 si supiéramos que las variedades algebraicas son conexas (cosa que demostraremos más adelante):

Teorema 4.11 (Principio de prolongación analítica) *Si V es una variedad y $\alpha \in \mathbb{C}(V)$ se anula en un abierto no vacío U (para la topología compleja) entonces $\alpha = 0$.*

DEMOSTRACIÓN: Pasando a la clausura proyectiva, podemos suponer que V es una variedad proyectiva y cortando con un abierto afín podemos suponer que V es afín. Entonces $\alpha = [F]/[G]$. Cortando U con el conjunto de puntos donde G no se anula tenemos un abierto menor (al que seguimos llamando U) donde $f = [F]$ se anula. Basta probar que $f = 0$.

Por el teorema anterior, U contiene un punto regular P. Tomemos un sistema de referencia en el que P tenga coordenadas nulas. Según hemos visto en la prueba de 4.5 la variedad V es, en un entorno de P que podemos suponer contenido en U, la gráfica de una función $g : W^d \longrightarrow \mathbb{C}^{n-d}$, donde W es un entorno de 0 en $\mathbb{C}$ y $d = \dim V$. En particular, todos los puntos de la forma $(x, g(x))$, con $x \in W^d$, están en U, luego las funciones coordenadas $x_1, \ldots, x_d$ toman en U cualquier valor posible en W^d. Según la observación tras el teorema anterior, estas funciones son algebraicamente independientes en $\mathbb{C}(V)$, luego son una base de trascendencia.

La función f es algebraica sobre $\mathbb{C}(x_1, \ldots, x_d)$, luego es raíz de un polinomio irreducible (no necesariamente mónico) con coeficientes en $\mathbb{C}[x_1, \ldots, x_d]$, digamos

$$q_0(x_1, \ldots, x_d)f^m + \cdots + q_m(x_1, \ldots, x_d)f + q_m(x_1, \ldots x_d) = 0.$$

La irreducibilidad obliga a que $q_m \neq 0$ (al menos, supuesto $f \neq 0$). Si $(a_1, \ldots, a_d) \in W^d$, se cumple que $(a_1, \ldots, a_d, g(a_1, \ldots, a_d)) \in U$, luego por hipótesis

$$f(a_1, \ldots, a_d, g(a_1, \ldots, a_d)) = 0.$$

Por consiguiente $q_m(a_1, \ldots, a_d) = 0$. Si $q_m = [H]$, con $H \in \mathbb{C}[X_1, \ldots, X_d]$, tenemos que H se anula sobre todos los puntos de W^d. Es fácil ver entonces que $H = 0$ (por el argumento final del teorema anterior) y, por tanto, que $q_m = 0$, contradicción. ■

Como consecuencia podemos probar que una variedad proyectiva está determinada por cualquiera de sus fragmentos con interior no vacío:

Teorema 4.12 *Si V, $W \subset \mathrm{P}^n$ son dos variedades proyectivas y $U \subset \mathrm{P}^n$ es un abierto (para la topología compleja) tal que $U \cap V = U \cap W \neq \varnothing$, entonces $V = W$.*

DEMOSTRACIÓN: Es claro que basta probar el resultado análogo para variedades afines V, $W \subset A^n$. Hemos de probar que $I(V) = I(W)$. Para ello, basta probar que si $F \in \mathbb{C}[X_1, \ldots, X_n]$ se anula en $U \cap V$, entonces se anula en V. Equivalentemente, basta ver que si $f \in \mathbb{C}[V]$ se anula en $U \cap V$, entonces se anula en V, pero esto es el teorema anterior. ■

A su vez de aquí deducimos lo que habíamos anunciado:

Teorema 4.13 *Los abiertos no vacíos para la topología de Zariski de una variedad cuasiproyectiva son densos para la topología compleja.*

DEMOSTRACIÓN: Consideremos primero el caso de una variedad proyectiva $V \subset \mathrm{P}^n$. Un enunciado equivalente es que los cerrados propios de V (para la topología de Zariski) tienen interior vacío (para la topología compleja). Un cerrado en V es una unión finita de variedades proyectivas, luego basta ver que si $W \subsetneq V$ es una variedad, entonces W tiene interior vacío en V. En caso contrario existiría un abierto U en P^n tal que $\varnothing \neq U \cap V \subset W$, pero entonces $U \cap V = U \cap W$, en contradicción con el teorema anterior. El caso general se prueba ahora fácilmente. ■

Hemos visto que los puntos regulares de una variedad cuasiproyectiva son analíticos, y ahora vamos a demostrar el recíproco. De este modo, vemos que el concepto analítico de punto analítico es equivalente al concepto algebraico de punto regular.

Teorema 4.14 *Un punto de una variedad cuasiproyectiva es analítico si y sólo si es regular.*

DEMOSTRACIÓN: Sea V una variedad cuasiproyectiva y $P \in V$. Tanto el concepto de punto analítico como el de punto regular son locales, luego podemos sustituir V por su clausura proyectiva y ésta a su vez por su intersección con un abierto afín, de modo que no perdemos generalidad si suponemos que $V \subset \mathbb{C}^n$ es una variedad afín. El teorema 4.5 prueba que si P es un punto regular entonces es analítico. Supongamos ahora que P es analítico. Esto significa que tiene un entorno (conexo) W con estructura de subvariedad analítica de $\mathbb{C}^n$. Por el teorema 4.10, dicho entorno contiene puntos regulares de V. El teorema 4.5 nos da entonces que la dimensión de W como variedad analítica coincide con la dimensión de V como variedad algebraica. Llamemos d a esta dimensión.

La diferencial de la inclusión $W \longrightarrow \mathbb{C}^n$ nos permite identificar T_PW con un subespacio vectorial de $\mathbb{C}^n$ de dimensión d. Observemos que si $F : \mathbb{C}^n \longrightarrow \mathbb{C}$ es una función holomorfa tal que $F|_W = 0$, entonces $dF|_P|_{T_PW} = d(F|_W)_P = 0$. Esto se aplica en particular a todo polinomio $F \in I(V)$.

Fijemos un sistema generador $F_1, \ldots, F_m$ de $I(V)$, que determina una función holomorfa $F : \mathbb{C}^n \longrightarrow \mathbb{C}^m$. Sea $A(X)$ la matriz formada por las derivadas parciales de las funciones F_i, de modo que $A(P)$ es la matriz asociada a la diferencial $dF|_P : \mathbb{C}^n \longrightarrow \mathbb{C}^m$.

Acabamos de ver que T_PW está contenido en el núcleo de $dF|_P$, por lo que $\operatorname{rang} A(P) \leq r$. Esto lo sabíamos ya por la prueba del teorema 3.32, donde hemos visto, más aún, que la igualdad equivale a que el punto P sea regular en V. Supongamos que no lo es, lo que se traduce en que el núcleo N de $dF|_P$ contiene estrictamente a T_PW.

Tomemos una base de T_PW, extendámosla a una base de N y ésta a su vez a una base de $\mathbb{C}^n$. Esta base determina un sistema de referencia de $\mathbb{C}^n$ respecto del cual P tiene coordenadas nulas, $T_PW = \{(x, y) \in \mathbb{C}^d \times \mathbb{C}^r \mid y = 0\}$ y para todo $F \in I(V)$ se cumple que

$$\left.\frac{\partial F}{\partial X_i}\right|_P = 0, \quad i = 1, \ldots, d, \qquad \left.\frac{\partial F}{\partial Y_1}\right|_P = 0.$$

Las funciones coordenadas y_i en $\mathbb{C}^n$ cumplen $d(y_i|_W)_P = 0$. Por el teorema 1.75, tiene que haber d funciones coordenadas en $\mathbb{C}^n$ cuya restricción a W sean independientes en un entorno de P, luego no pueden ser otras más que $x_1, \ldots, x_d$.

Según la observación tras 1.75, restringiendo W podemos suponer que es la gráfica de una función holomorfa, es decir, que existe un entorno U' de 0 en $\mathbb{C}^d$, un entorno U de P en $\mathbb{C}^n$ y una función holomorfa $\phi : U' \longrightarrow \mathbb{C}^r$ de modo que

$$W = V \cap U = \{(x, y) \in U' \times \mathbb{C}^r \mid y = \phi(x)\}.$$

Vamos a ver que podemos reducir el problema al caso en que $n = d + 1$. Para ello suponemos que $d < n - 1$ y veamos que podríamos haber elegido el sistema de referencia de modo que se cumpliera una propiedad adicional: Sea L un subespacio vectorial de $\mathbb{C}^n$ de dimensión $n-1$ que contenga a N y vamos a escoger adecuadamente el último vector de la base que determina el sistema de referencia. Para ello tomamos un hiperplano L' paralelo a L. Sean $\overline{L}'$ y $\overline{V}$ las clausuras de L' y V en P^n. Consideramos la proyección $V \setminus \{P\} \longrightarrow \overline{L}'$, es decir, la aplicación que a cada punto $Q \in V \setminus \{P\}$ le hace corresponder la intersección con $\overline{L}'$ de la recta que pasa por P y Q. Se trata de una aplicación regular (es una aplicación del tipo definido en 3.7). Si llamamos $V' \subset \overline{L}'$ a la clausura de su imagen (en la topología de Zariski), tenemos una aplicación regular densa $V \setminus \{P\} \longrightarrow V'$, por lo que $\dim V' \leq d < \dim \overline{L}'$ (por ejemplo por los teoremas 3.11 y 3.46). Esto nos permite tomar como último vector de la base que determina el nuevo sistema de referencia de $\mathbb{C}^n$ un punto de $\overline{L}' \setminus V'$, y esto nos asegura que el único punto de la recta

$$x_1 = \cdots = x_d = y_1 = \cdots = y_{n-1} = 0$$

que está en la clausura proyectiva de V es P. Sea entonces Q el punto infinito de esta recta, y consideremos la proyección $\overline{V} \longrightarrow \mathrm{P}^{n-1}$ desde Q, donde P^{n-1} se identifica con la clausura proyectiva del hiperplano $y_n = 0$. Por 2.47 sabemos que la imagen de $\overline{V}$ es una variedad proyectiva $\overline{V}_0 \subset \mathrm{P}^{n-1}$. Llamemos V_0 a su intersección con el abierto afín $\mathbb{C}^{n-1}$. La proyección se restringe a la proyección $V \longrightarrow V_0$ que consiste en eliminar la coordenada y_n. Esta restricción no es necesariamente suprayectiva, pues en V_0 puede haber imágenes de puntos infinitos de V, pero la construcción garantiza que la única antiimagen de P es el propio P.

Observemos ahora que cada punto $(x, y) \in V_0 \cap U$ tiene una única antiimagen en W, a saber, $(x, \phi(x))$, y reduciendo los abiertos U y U' podemos suponer que dicha antiimagen es su única antiimagen en $\overline{V}$. En efecto, en caso contrario podríamos encontrar una sucesión de puntos $Q_n \in \overline{V} \setminus U$ con imágenes convergentes a P. Por compacidad podríamos extraer una subsucesión convergente a un punto $P' \in \overline{V} \setminus U$ cuya imagen debería ser P, lo cual es imposible.

En definitiva, $V_0 \subset \mathbb{C}^{n-1}$ es un conjunto algebraico que en un entorno de P es la gráfica de la función holomorfa ϕ' (resultante de eliminar la última coordenada de ϕ) y es claro que $I(V_0) \subset I(V)$, por lo que las derivadas parciales de los elementos de $I(V_0)$ respecto de $X_1, \ldots, X_d, Y_1$ son nulas en P. Más aún, es fácil ver que la variedad tangente $T_P V_0$ sigue siendo la dada por $y = 0$.

Repitiendo este proceso las veces necesarias, llegamos a una subvariedad de $\mathbb{C}^{d+1}$. En definitiva, podemos suponer que V es una hipersuperficie de $\mathbb{C}^{d+1}$, que por el teorema 3.16 será de la forma $V = V(F)$, para cierto polinomio F que podemos tomar irreducible, de modo que $I(V) = (F)$. Por una parte tenemos que

$$\left.\frac{\partial F}{\partial X_1}\right|_P = \cdots = \left.\frac{\partial F}{\partial X_d}\right|_P = \left.\frac{\partial F}{\partial Y}\right|_P = 0,$$

y por otra que existen abiertos $U \subset \mathbb{C}^{d+1}$, $U' \subset \mathbb{C}^d$ y una función holomorfa $\phi : U' \longrightarrow \mathbb{C}$ de manera que

$$W = \{(x, y) \in U \mid F(x, y) = 0\} = \{(x, y) \in U' \times \mathbb{C} \mid y = \phi(x)\}.$$

La condición sobre las derivadas equivale a que F no tiene términos de grado 1 (ni término independiente, pues $F(P) = 0$ y P tiene coordenadas nulas). Llamemos $s \geq 2$ al menor grado de un monomio no nulo de F y sea $F_s \neq 0$ la forma de grado s de F. Existe un punto $(a_1, \ldots, a_d, 1) \in \mathbb{C}^{d+1}$ tal que $F_s(a_1, \ldots, a_d, 1) \neq 0$. El polinomio

$$F^*(X'_1, \ldots, X'_d, Y) = F(X'_1 + a_1 Y, \ldots, X'_d + a_d Y, Y)$$

tiene únicamente monomios de grado $\geq s$, y $F_s^*(0,\ldots,0,1) \neq 0$, lo que significa que el coeficiente de Y^s en F_s^* es no nulo. Por otra parte, puesto que $dy|_P = 0$, resulta que las funciones $x_1', \ldots, x_d'$ son también independientes en P, luego la variedad $V(F^*)$ es también la gráfica de una función holomorfa $y = \phi(x')$ en un entorno de P. Equivalentemente, podemos suponer que el coeficiente de Y^s en F_s es no nulo, o incluso que es igual a 1.

Sea $D(X_1,\ldots,X_d)$ el discriminante[1] de F, visto como polinomio en Y. Como F es irreducible, sus raíces en la clausura algebraica de $\mathbb{C}(X_1,\ldots,X_d)$ son simples, luego el polinomio D es no nulo y, por 4.13, el conjunto de puntos de $\mathbb{C}^d$ donde no se anula es denso para la topología compleja. Si $Q \in \mathbb{C}^d$ es uno de estos puntos, tenemos que $F(Q,Y) \in \mathbb{C}[Y]$ es un polinomio no nulo y tiene todas sus raíces simples. Así pues, en todo entorno de $0 \in \mathbb{C}^d$ existen puntos Q tales que $F(Q,Y)$ sólo tiene raíces simples.

Ahora aplicamos el principio del argumento,[2] según el cual, si fijamos un disco $\Omega \subset \mathbb{C}$ de centro 0, la integral

$$N(Q) = \frac{1}{2\pi i}\int_{\partial\Omega} \frac{F'(Q,\zeta)}{F(Q,\zeta)}\,d\zeta$$

es igual al número de ceros del polinomio $F(Q,Y)$ (contados con su multiplicidad) contenidos en Ω (bajo el supuesto de que $F(Q,Y)$ no tenga ningún cero en la circunferencia sobre la que se calcula la integral).

Tomemos ahora un abierto $P \in U' \times \Omega \subset U$, donde U es el entorno de P en el que V es la gráfica de una función y Ω es un disco cuya frontera no contiene ningún cero del polinomio $F(0,Y)$. Entonces $N(0) \geq s \geq 2$, ya que

$$F(0,Y) = Y^s + \text{términos de grado superior}$$

tiene al menos un cero de orden s en $0 \in \Omega$.

Ahora bien, por compacidad, para todo Q en un entorno de $0 \in \mathbb{C}^d$, se cumple que $F(Q,Y)$ no se anula en $\partial\Omega$, luego está definido $N(Q)$. Además es una función continua de Q que sólo puede tomar valores enteros, luego es constante. Concluimos que $F(Q,Y)$ tiene al menos s ceros para todo punto Q en un entorno de 0, y podemos tomar puntos Q arbitrariamente cerca de 0 en los que $F(Q,Y)$ sólo tiene ceros simples, luego concluimos que existe un punto $Q \in U'$ para el que existen dos puntos distintos $y_1, y_2 \in \Omega$ tales que $F(Q,y_1) = F(Q,y_2) = 0$, luego (Q,y_1), $(Q,y_2) \in V \cap U$, lo que contradice que V sea en U la gráfica de una función. ■

4.2 El teorema de conexión

En esta sección demostraremos que las variedades algebraicas son conexas para la topología compleja. Para ello necesitamos algunos resultados previos.

[1] Ver el apéndice C de mi libro de *Álgebra*.

[2] Ver el teorema 8.8 de mi libro de *Funciones de variable compleja,* y la expresión para $I(\phi \circ f, 0)$ que aparece en la demostración.

Empezaremos estudiando más a fondo las aplicaciones finitas entre variedades algebraicas. Estos primeros resultados son válidos para variedades definidas sobre un cuerpo algebraicamente cerrado arbitrario.

Definición 4.15 Si $\phi : X \longrightarrow Y$ es una aplicación finita entre dos variedades algebraicas definidas sobre un cuerpo k, entonces ϕ induce un monomorfismo $k(Y) \longrightarrow k(X)$ que nos permite considerar a $k(X)$ como una extensión algebraica de $k(Y)$ (ver la prueba de 3.14). Puesto que $k(X)$ es finitamente generado sobre k, la extensión $k(X)/k(Y)$ es finita, luego podemos definir el *grado* de ϕ como $\operatorname{grad} \phi = |k(X) : k(Y)|$.

Teorema 4.16 *Si $\phi : X \longrightarrow Y$ es una aplicación finita de grado n entre variedades algebraicas e Y es regular, entonces cada punto de Y tiene a lo sumo n antiimágenes en X.*

Demostración: Tomemos un punto $y \in Y$. Sustituyendo Y por un entorno afín del punto y X por su antiimagen, podemos suponer que tanto X como Y son variedades afines. Así, $k[X]$ es una extensión entera de $k[Y]$ y $|k(X) : k(Y)| = n$. Por otra parte, la regularidad de Y implica que el anillo $k[Y]$ es íntegramente cerrado, pues esta implicación en el teorema 3.57 no requiere que Y sea una curva.

En estas condiciones, si $a \in k[X]$, tenemos que a es entero sobre $k[Y]$, luego los coeficientes del polinomio mínimo de a en $k(Y)$ son también enteros sobre $k[Y]$, y están en $k(Y)$, luego están en $k[Y]$.

Sean $x_1, \ldots, x_m \in X$ las antiimágenes de y. Podemos tomar un $a \in k[X]$ tal que las imágenes $a(x_i)$ sean distintas dos a dos. (Siempre es posible tomar un polinomio que tome valores distintos sobre un número finito de puntos prefijados.) Sea $F(T) \in k[Y][T]$ el polinomio mínimo de a, que cumple $\operatorname{grad} F \leq n$. Si llamamos $F(y)(T) \in k[T]$ al polinomio que resulta de evaluar en y los coeficientes de $F(T)$, vemos que todos los $a(x_i)$ son raíces de $F(y)(T)$, luego $m \leq \operatorname{grad} F(y)(T) = \operatorname{grad} F(T) \leq n$. ■

Definición 4.17 En las condiciones del teorema anterior, diremos que ϕ es *no ramificada* sobre el punto $y \in Y$ si y tiene exactamente n antiimágenes en X. Diremos que ϕ es *no ramificada* si lo es en todos los puntos de Y.

Teorema 4.18 *Si $\phi : X \longrightarrow Y$ es una aplicación finita entre variedades algebraicas e Y es regular, entonces el conjunto de puntos de Y donde ϕ es no ramificada es abierto, y es no vacío si $k(X)$ es una extensión separable de $k(Y)$.*

Demostración: Es claro que no perdemos generalidad si suponemos que X e Y son afines. Fijado un punto $y \in Y$, mantenemos la notación del teorema anterior. Si ϕ no se ramifica en y, entonces $\bar{F}$ tiene n raíces distintas en k, luego $\operatorname{grad} F(T) = \operatorname{grad} F(y)(T) = n$ y el discriminante $D(F(y)) = D(F)(y)$ es no nulo. Por consiguiente, tenemos además que $k(X) = k(Y)(a)$, es decir, que a es un elemento primitivo de la extensión $k(X)/k(Y)$.

En general, si $a \in k[X]$ es un elemento primitivo cualquiera de la extensión, F es su polinomio mínimo e $y \in Y$ es un punto que cumple $D(F)(y) \neq 0$, llamamos $U \subset Y$ al abierto afín formado por los puntos de Y donde $D(F)$ no se anula y vamos a probar que ϕ no se ramifica en U. Esto prueba también la segunda parte del teorema, pues, si la extensión $k(X)/k(Y)$ es separable, tiene un elemento primitivo a, que podemos tomar en $k[X]$, y F tiene raíces simples por la separabilidad, luego $D(F) \neq 0$, luego existe un punto $y \in Y$ donde $D(F)(y) \neq 0$, y esto implica la existencia de puntos no ramificados.

Sea $V = \phi^{-1}[U]$, que es un abierto afín de X porque ϕ es finita. Notemos que $F \in k[Y][T] \subset k[U][T]$, y $D(F) \in k[U]$ no se anula en ningún punto de U. Equivalentemente, podemos sustituir X por V e Y por U, y suponer que $D(F)$ no se anula en ningún punto de Y.

Sea $X' \subset Y \times A^1$ el conjunto algebraico afín formado por los pares (y, α) que cumplen $F(y)(\alpha) = 0$. Observemos que $k[X'] \cong k[Y][T]/(F)$ y F es irreducible en $k[Y]$, por lo que $k[X']$ es un dominio íntegro, luego X' es una variedad afín. Más aún, tenemos un isomorfismo natural $k[X'] \cong k[Y][a] \subset k[X]$. Los homomorfismos de k-álgebras

$$k[Y] \longrightarrow k[Y][T] \longrightarrow k[X'] \longrightarrow k[X]$$

se corresponden con aplicaciones regulares

$$X \longrightarrow X' \longrightarrow Y \times A^1 \longrightarrow Y,$$

cuya composición es ϕ. En definitiva, ϕ se descompone como una aplicación regular $X \longrightarrow X'$ seguida de la restricción $f : X' \longrightarrow Y$ de la proyección $Y \times A^1 \longrightarrow Y$. Observemos que f es no ramificada, pues, si $y \in Y$, el polinomio $F(y)(T)$ tiene n raíces distintas $\alpha_1, \ldots, \alpha_n \in k$, por lo que los puntos $(y, \alpha_i) \in X'$ son n antiimágenes de y.

Para terminar la demostración basta ver que X' es regular, pues entonces $k[X']$ será íntegramente cerrado (ver la prueba del teorema anterior), pero todo elemento de $k[X]$ es entero sobre $k[Y]$, luego sobre $k[Y][a]$, luego ha de estar en $k[Y][a]$. En definitiva, tendremos que $k[X] = k[Y][a] \cong k[X']$, luego la aplicación $X \longrightarrow X'$ es un isomorfismo, a través del cual ϕ se corresponde con f y, por consiguiente, es no ramificada.

Observemos que la dimensión de $Y \times A^1$ es una unidad más que la de Y, por lo que $\dim X' = \dim Y = d$. Tomemos un punto $x \in X'$ y sea $y = f(x) \in Y$. La aplicación f induce un homomorfismo $\mathfrak{m}_y/\mathfrak{m}_y^2 \longrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2$. Basta probar que es suprayectivo, pues entonces

$$d \leq \dim_k T_x X' = \dim_k \mathfrak{m}_x/\mathfrak{m}_x^2 \leq \dim_k \mathfrak{m}_y/\mathfrak{m}_y^2 = \dim_k T_y Y = d,$$

lo que implica que x es regular en X'.

Sea $u_1, \ldots, u_d \in \mathfrak{m}_y$ un sistema local de parámetros en y. Es claro que un sistema local de parámetros en x está formado por $u_1, \ldots, u_d, a$, por lo que sólo hemos de probar que $d_x a$ es combinación lineal de los $d_x u_i$. Ahora bien, si

$$F(T) = T^n + b_1 T^{n-1} + \cdots + b_n, \qquad b_i \in k[Y],$$

al calcular la diferencial de $F(a) = 0$ obtenemos que

$$F(y)'(a)d_x(a) + a^{n-1}(x)d_x b_1 + \cdots + d_x b_n = 0.$$

Por otra parte, como $x \in X'$, tenemos que $F(y)(a) = 0$, es decir, que a es una raíz de $F(y)(T)$. Como $D(F)(y) \neq 0$, se trata de una raíz simple, luego $F'(y)(a) \neq 0$, lo que nos permite despejar $d_x(a)$ como combinación lineal de las $d_x b_i$, que a su vez son combinaciones lineales de las $d_x u_i$. ■

A partir de aquí consideremos una variedad compleja X. Por el teorema de Noether 3.10, existe una aplicación finita $\phi : U \longrightarrow A^m$, para un cierto abierto afín U de X. Por el teorema anterior, sustituyendo U por un abierto menor, obtenemos una aplicación finita y no ramificada $\phi : U \longrightarrow V$, donde $V \subset A^m$ es un abierto afín. Restringiendo aún más U y V podemos suponer que ϕ es de la forma descrita en el teorema anterior, es decir, que $U \subset V \times A^1$ es regular y está definido por un polinomio irreducible $F \in \mathbb{C}[X_1, \ldots, X_m, T]$ (mónico en T) y que ϕ es la restricción de la proyección.

Veamos ahora que, respecto a la topología compleja, ϕ es un cubrimiento no ramificado, es decir, que cada punto $y \in V$ tiene un entorno V' tal que $\phi^{-1}[V']$ es unión de n abiertos disjuntos $U'_1, \ldots, U'_n$ tales que $\phi|_{U'_i} : U'_i \longrightarrow V'$ es un homeomorfismo.

En efecto, sean $x_1, \ldots, x_n \in U$ las antiimágenes de y. En la prueba del teorema anterior hemos visto que $d\phi_{x_i} : T_{x_i}U \longrightarrow T_yV$ es un isomorfismo (hemos visto que su dual es suprayectiva, y ambos espacios tienen la misma dimensión). Sabemos que la diferencial algebraica coincide con la diferencial analítica, luego el teorema de la función inversa nos da que ϕ se restringe a una transformación conforme entre un entorno U'_i de x_i y un entorno V'_i de y. Restringiendo estos entornos podemos suponer que los U'_i son disjuntos dos a dos y que todos los V'_i son un mismo abierto V'. De este modo, cada punto $y' \in V'$ tiene exactamente n antiimágenes en $U'_1 \cup \cdots \cup U'_n$, luego éstas son todas sus antiimágenes, y esta unión es todo $\phi^{-1}[V']$.

Vamos a usar la aplicación ϕ para demostrar que U es conexo, lo cual implica a su vez que la variedad original X es conexa, pues U es denso en X.

Observemos que V es conexo: Se trata de un abierto de A^m para la topología de Zariski. Dados dos puntos P, $Q \in V$, sea $L \subset A^m$ la recta que los contiene, que es homeomorfa a $\mathbb{C}$. Entonces, $L \cap V$ es un abierto no vacío en L para la topología de Zariski, luego es homeomorfo a $\mathbb{C}$ menos un número finito de puntos, luego es un conjunto conexo contenido en V que contiene a P y Q. Esto prueba que P y Q están en la misma componente conexa de V, luego V es conexo.

Supongamos que $U = M_1 \cup M_2$, donde los M_i son cerrados disjuntos no vacíos. El hecho de que ϕ sea un cubrimiento no ramificado implica claramente que es abierta y cerrada, por lo que $\phi[M_i]$ son abiertos y cerrados en V, que es conexo, luego $\phi[M_1] = \phi[M_2] = V$.

También es claro que la restricción $\phi_1 : M_1 \longrightarrow V$ es un cubrimiento no ramificado y el número de antiimágenes de cada punto es localmente constante, luego es constante. Llamémoslo r. Puesto que también $\phi[M_2] = V$, ha de ser $r < n$.

Sea $a \in \mathbb{C}[U]$ el elemento primitivo de la extensión $\mathbb{C}(U)/\mathbb{C}(V)$ según el teorema anterior. Fijemos un punto $v \in V$ y sea V_v un entorno en el que $\phi_1^{-1}[V_v] = U_1 \cup \cdots \cup U_r$ se descomponga como unión de abiertos disjuntos homeomorfos a V_v. Llamemos $\phi_i : U_i \longrightarrow V_v$ a las restricciones de ϕ_1, sean $a_i \in \mathcal{H}(U_i)$ las restricciones de a y sean $g_1, \ldots, g_r \in \mathcal{H}(V_v)$ los polinomios simétricos elementales en $\phi_i^{-1} \circ a_i$. Vamos a probar que existen polinomios $p_1, \ldots, p_r \in \mathbb{C}[A^m]$, independientes de v, cuyas restricciones a V_v coinciden con $g_1, \ldots, g_r$.

Esto significará que el polinomio $T^r - p_1 T^{r-1} + \cdots + (-1)^r p_r \in \mathbb{C}[V][T]$ se anula en cada $\phi_i^{-1} \circ a_i$, luego

$$P(T) = T^r - \bar{\phi}(p_1)T^{r-1} + \cdots + (-1)^r \bar{\phi}(p_r) \in \mathbb{C}[V][T]$$

se anula en cada a_i. (Aquí consideramos $\bar{\phi} : \mathbb{C}[V] \longrightarrow \mathbb{C}[U]$ como una inclusión, por lo que podemos escribir $\bar{\phi}(p_j) \in \mathbb{C}[V]$.) Esto implica a su vez que $P(T)$ se anula en la restricción de a a cada $\phi_1^{-1}[V_v]$, luego, en definitiva, $P(a|_{M_1}) = 0$.

Similarmente, podemos encontrar otro polinomio mónico $P' \in \mathbb{C}[V][T]$ de grado $r' < n$ tal que $P'(a|_{M_2}) = 0$. Entonces $P(a)P'(a) = 0$ en $\mathbb{C}[U]$, que es un dominio íntegro, por lo que llegamos a que a es raíz de un polinomio mónico de grado $< n$, lo cual es absurdo, ya que a es un elemento primitivo de $\mathbb{C}(U)/\mathbb{C}(V)$ y esta extensión tiene grado n.

Así pues, sólo nos falta probar la existencia de los polinomios p_i. Observemos en primer lugar que, para cada $w \in V_v$, la función $g_i(w)$ se calcula haciendo actuar un polinomio simétrico sobre las imágenes por a de las r antiimágenes de w en M_1, lo cual no depende de v, por lo que las funciones g_i están definidas realmente sobre todo V y son holomorfas en un entorno de cada punto, luego $g_i \in \mathcal{H}(V)$.

Sea $S = A^m \setminus V$, que es un conjunto algebraico afín, y tomemos $s \in S$. Sea $F \in \mathbb{C}[A^m][T]$ el polinomio mínimo de a. Para cada $v \in V$, tenemos que cada $a(\phi_i^{-1}(v))$ es raíz de $F(v)(T)$. Los coeficientes de $F(T)$ son polinomios en A^m, luego están acotados en un entorno compacto C de s, luego $\phi_i^{-1} \circ a$ está acotado[3] en $C \cap V$, luego g_i también lo está. El teorema 4.21 implica entonces que g_i se extiende a una función holomorfa $p_i \in \mathcal{H}(A^n)$. Sólo nos falta probar que p_i es un polinomio. Para ello usaremos el teorema 4.22.

Tomemos $z \in V$ y sea $|z| = \max |z_i|$. Tomemos un punto $x \in M_1$ tal que $\phi(x) = z$. Aplicando de nuevo la consecuencia del teorema de Rouché citada en la nota al pie, tenemos que $|a(x)| \leq 1 + \max |b_i(z)|$, donde $b_i \in \mathbb{C}[A^m]$ son los coeficientes de F. Los b_i son polinomios en m variables. Si N es el máximo de sus grados, para cada $\epsilon > 0$ existe una constante C_ϵ tal que $|a(x)| < C_\epsilon |z|^k$,

[3]En general, si M es una cota del módulo de los coeficientes de un polinomio mónico, el módulo de sus raíces está acotado por $1 + M$. Ver las observaciones tras el teorema de Rouché (8.11) en mi libro de *Funciones de variable compleja*.

para $|z| > \epsilon$. Puesto que $g_i(z)$ depende polinómicamente de los $a(x)$, donde x recorre las antiimágenes de z, tenemos una desigualdad similar $|g_i(z)| \leq C'_\epsilon |z|^{ik}$. En principio, esto vale para $z \in V$, pero como V es denso en A^m se cumple para todo $z \in A^m$ (tal que $|z| > \epsilon$). De acuerdo con 4.22, esto implica que g_i es un polinomio.

A falta de probar 4.21 y 4.22, llegamos al teorema que perseguíamos:

Teorema 4.19 *Toda variedad algebraica es conexa con respecto a la topología compleja.*

Como primera aplicación observamos lo siguiente:

Teorema 4.20 *Una variedad cuasiproyectiva es proyectiva si y sólo si es compacta (respecto a la topología compleja).*

DEMOSTRACIÓN: Si V es una variedad cuasiproyectiva, sabemos que V es abierta en su clausura proyectiva $\overline{V}$ (respecto a la topología de Zariski, luego también respecto a la topología compleja) y por ser compacta también es cerrada. Como $\overline{V}$ es conexa, ha de ser $V = \overline{V}$. ■

Veamos ahora los resultados pendientes:

Teorema 4.21 *Sea $S \subsetneq A^m$ un conjunto algebraico afín y $g \in \mathcal{H}(A^n \setminus S)$ una función acotada en un entorno de cada punto $s \in S$. Entonces S se extiende a una función holomorfa en todo A^m.*

DEMOSTRACIÓN: Fijado $s \in S$, basta encontrar un entorno U de s tal que g se extiende a una función holomorfa en U. El teorema 1.60 garantiza que todas las extensiones parciales son consistentes entre sí. Podemos sustituir S por un conjunto mayor, luego podemos suponer que está definido por un único polinomio $F(z_1, \ldots, z_m)$. Tras un cambio de coordenadas, podemos suponer que $s = 0$ y que la forma de mayor grado de F contiene el monomio z_m^k (igual que hicimos en la prueba de 1.39 con la forma de menor grado de la serie de potencias). Así,

$$F(z_1, \ldots, z_m) = z_m^k + H_1(z')z_m^{k-1} + \cdots + H_k(z'),$$

donde $z' = (z_1, \ldots, z_{m-1})$. Pongamos que el polinomio $F(0, z_m) \in \mathbb{C}[z_m]$ factoriza como

$$F(0, z_m) = z_m^t (z_m - \lambda_1) \cdots (z_m - \lambda_{k-t})$$

y tomemos un $\delta > 0$ y un $r > 0$ tal que los discos de centro $0, \lambda_1, \ldots, \lambda_{k-t}$ y radio δ no contengan ningún $w \in \mathbb{C}$ tal que $|w| = r$. Veamos ahora que existe un $\epsilon > 0$ tal que si $|z'| < \epsilon$ entonces las raíces de $F(z', z_m) \in \mathbb{C}[z_m]$ están en los discos indicados, luego ninguna cumple $|w| = r$.

En efecto, sea $M - 1$ una cota de $|H_i(z')|$ sobre el polidisco $|z'| \leq 1$, de modo que todo $w \in \mathbb{C}$ que cumpla $F(z', w) = 0$ para $|z'| \leq 1$ ha de cumplir $|w| \leq M$.

Si tomamos ϵ tal que cuando $|z'| < \epsilon$ entonces $|H_i(0) - H_i(z')| < \epsilon^k/kM^k$ para todo i, vemos que

$$|F(0,w)| = |F(0,w) - F(z',w)| \leq |H_1(0) - H_1(w)||w|^{k-1} + \cdots + |H_k(0) - H_k(z')|$$

$$\leq \frac{\epsilon^k}{kM^k} kM^k = \epsilon^k$$

y, si w distara de $0, \lambda_1, \ldots, \lambda_{k-t}$ más que ϵ, debería ser $|F(0,w)| > \epsilon^k$.

Así podemos definir, para $|z'| < \epsilon$, $|z_n| < r$,

$$G(z_1, \ldots, z_n) = \frac{1}{2\pi i} \int_{|w|=r} \frac{g(z',w)}{w - z_n}\, dw.$$

En efecto, si $|z'| < \epsilon$ y $|w| = r$ tenemos que $F(z',w) \neq 0$, por lo que $(z',w) \notin S$, luego $g(z',w)$ está definido. El mismo razonamiento que precede al teorema 1.48 prueba que la función G es holomorfa en el polidisco en que está definida. Sólo nos falta probar que es una prolongación analítica de g. Para ello fijamos un punto z' tal que $|z'| < \epsilon$ y observamos que $g(z', z_m)$, considerada como función de z_m, está definida en el disco $|z_m| < r$ salvo quizá en un número finito de puntos donde $F(z', z_m) = 0$. Ahora bien, por hipótesis g está acotada en un entorno de cada uno de estos puntos, luego son singularidades evitables de $g(z', z_m)$. La fórmula integral de Cauchy para funciones de una variable nos da entonces que $G(z', z_m) = g(z', z_m)$ para todo z_m tal que $|z_m| < r$ y donde g esté definida. Así pues, G es una prolongación analítica de g. ∎

Teorema 4.22 *Sea $f \in \mathcal{H}(\mathbb{C}^n)$ tal que existen $\epsilon > 0$ y $C > 0$ tales que, para todo $z \in \mathbb{C}^n$ con $|z| > \epsilon$, se cumple $|f(z)| < C|z|^k$. Entonces f es un polinomio de grado $\leq k$.*

Demostración: Supongamos, por reducción al absurdo, que la componente homogénea F_l de grado k de la serie de potencias de f alrededor de 0 es no nula, para un cierto $l > k$. Tomemos un punto $(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ tal que $F_l(\alpha_1, \ldots, \alpha_n) \neq 0$. Entonces la función $g(z) = f(\alpha_1 z, \ldots, \alpha_n z)$ es una función holomorfa en $\mathbb{C}$ que satisface una cota como la del enunciado y cuya serie de Taylor tiene no nulo el coeficiente de grado l. Si eliminamos los k primeros términos de dicha serie obtenemos una nueva función g_1 que sigue cumpliendo una acotación como la del enunciado. Más aún, como tiene un cero de orden $\geq k$, la función $g_1(z)/z^k$ está acotada en todo $\mathbb{C}$, luego ha de ser constante, pero entonces el coeficiente de Taylor de grado k de g_1 ha de ser nulo, y es el mismo que el de g, contradicción. ∎

4.3 Variedades proyectivas

En esta sección obtendremos algunos resultados que relacionan la estructura algebraica y la analítica de las variedades proyectivas regulares.

Teorema 4.23 *Si X es una variedad proyectiva regular, las funciones meromorfas en X coinciden con las funciones racionales, es decir,* $\mathcal{M}(X) = \mathbb{C}(X)$.

DEMOSTRACIÓN: Por el teorema 1.63 sabemos que $\mathcal{M}(X)$ es algebraico sobre $\mathbb{C}(X)$. Basta probar que $\mathcal{M}(X)$ es algebraicamente cerrado sobre $\mathbb{C}(X)$. Esto es cierto para cualquier variedad algebraica regular, no necesariamente proyectiva.

En efecto, tomemos una función $f \in \mathcal{M}(X)$ algebraica sobre $\mathbb{C}(X)$. Entonces f es raíz de un polinomio irreducible

$$F(T) = T^m + a_1 T^{m-1} + \cdots + a_m \in \mathbb{C}(X)[T].$$

Todo se reduce a demostrar que $m = 1$. Sea $U \subset X$ un abierto afín contenido en el complementario de la unión de los polos de las funciones racionales a_i, de modo que todas ellas son regulares en U y donde el discriminante $D(F) \in \mathbb{C}(X)$ no se anula. Basta probar que $f|_U \in \mathbb{C}(U)$, pues entonces $f|_U$ se extiende a una función $g \in \mathbb{C}(X)$, de modo que f y g son funciones meromorfas en X que coinciden en un abierto denso, luego son iguales. Equivalentemente, podemos sustituir X por U y suponer que $a_i \in \mathbb{C}[X]$ para todo i, así como que $D(F)$ no se anula en ningún punto de X.

Para cada punto $x \in X$, sabemos que $\mathcal{H}_x(X)$ es un dominio de factorización única, luego es íntegramente cerrado, y f se identifica con un cociente de elementos de $\mathcal{H}_x(X)$ entero sobre $\mathcal{H}_x(X)$, luego $f \in \mathcal{H}_x(X)$. Así pues, $f \in \mathcal{H}(X)$.

Sea $X' \subset X \times A^1$ el conjunto de los puntos (x, z) tales que $F(x, z) = 0$. Así X' es un conjunto algebraico afín tal que $\mathbb{C}[X'] = \mathbb{C}[X][T]/(F) \cong \mathbb{C}[X][f]$. Como F es irreducible, resulta que X' es una variedad afín.

Nos encontramos ahora en la misma situación que en la prueba de 4.18, por lo que podemos concluir como allí que X' es una variedad regular y que la restricción de la proyección $p : X' \longrightarrow X$ es una aplicación finita no ramificada de grado m. Por otra parte, podemos definir una aplicación regular $\phi : X \longrightarrow X'$ mediante $\phi(x) = (x, f(x))$, que cumple $\phi \circ p = 1$.

Ahora ya podemos llegar a una contradicción si suponemos que $m > 1$. Concretamente, vamos a probar que $\phi[X]$ y $X' \setminus \phi[X]$ son abiertos disjuntos no vacíos, lo que implica que X' no es conexo, en contra de lo que nos asegura el teorema 4.19.

En efecto, si $x \in X$, tras la prueba de 4.18 hemos visto que x tiene un entorno U para la topología compleja, que podemos tomar conexo, tal que $p^{-1}[U]$ se descompone en unión de m abiertos disjuntos U_i homeomorfos con U a través de p. Claramente, $\phi[U]$, al ser conexo, ha de estar contenido en uno de los U_i, luego ha de ser $\phi[U] = U_i$, para un cierto índice i. Por consiguiente U_i es un entorno de $\phi(x)$ en $\phi[X]$, mientras que los demás U_j son entornos de las otras antiimágenes de x por p en $X' \setminus \phi[X]$. Esto prueba que ambos conjuntos son abiertos y, desde luego, no vacíos. ■

Más en general:

Teorema 4.24 *Toda aplicación holomorfa $f : X \longrightarrow Y$ entre dos variedades proyectivas regulares es regular.*

Demostración: Tomemos un punto $x \in X$ y sea $y = f(x)$. Vamos a probar que f es regular en x. Pongamos que $Y \subset \mathrm{P}^n$ y elijamos un hiperplano infinito en P^n de modo que $y \in A^n$. Sean $z_1, \ldots, z_n \in \mathbb{C}[Y] \subset \mathcal{M}(Y)$ las funciones coordenadas de A^n. Es claro que $f \circ z_i \in \mathcal{M}(X) = \mathbb{C}(X)$ y, como cada $f \circ z_i$ es holomorfa en x, el teorema 4.8 implica que también es regular en x. Sea U un entorno afín de x tal que $f \circ z_i \in \mathbb{C}[U]$, para todo i. Esto implica que $U \subset f^{-1}[Y \cap A^n]$. Es claro que estas aplicaciones definen una aplicación regular $U \longrightarrow A^n$, que no es sino $f|_U$. Por consiguiente, f es regular en x. ■

En particular:

Teorema 4.25 *Dos variedades proyectivas regulares son isomorfas si y sólo si son conformemente equivalentes.*

El resultado más importante que relaciona las variedades analíticas y las algebraicas es el siguiente:

Teorema 4.26 *Toda subvariedad analítica compacta y conexa de una variedad proyectiva regular es una variedad proyectiva regular.*

Demostración: Sea V una subvariedad analítica compacta de una variedad proyectiva regular X. Como $X \subset \mathrm{P}^n$, para cierto n, tenemos que V es también una subvariedad analítica de P^n compacta y conexa. Elijamos un sistema de referencia en P^n de modo que la coordenada homogénea x_0 no sea idénticamente nula en V, es decir, que, si tomamos $V(X_0)$ como hiperplano infinito, entonces V contiene puntos finitos.

Sea Y la clausura de V respecto a la topología de Zariski. Ciertamente, Y es un conjunto algebraico proyectivo. Vamos a ver que es una variedad, para lo cual hemos de probar que $I(Y)$ es primo, es decir, que si P y Q son polinomios homogéneos tales que PQ se anula en Y, entonces uno de los factores se anula en Y. Si P no es idénticamente nulo en Y, el conjunto de los puntos de Y donde P no se anula es un abierto no vacío para la topología de Zariski, pero V es denso en Y para esta topología, luego P no se anula en algún punto de V, y el conjunto $U \subset V$ donde P no se anula es un abierto no vacío para la topología compleja.

Pongamos que $\operatorname{grad} Q = k$, de modo que $Q/X_0^k \in \mathcal{M}(V)$ se anula en U y, como V es conexo, el teorema 1.60 implica que se anula en todo V. Esto significa que Q se anula en todos los puntos de V salvo a lo sumo en los que cumplen $X_0 = 0$, pero considerando entonces las funciones Q/X_i^k concluimos que también se anula en estos puntos. En definitiva, Q se anula en un conjunto denso en Y (para la topología de Zariski), luego se anula en Y.

Una función racional de Y es de la forma P/Q, donde P y Q son polinomios homogéneos del mismo grado y Q no es idénticamente nulo en Y. Si Q se anulara en un abierto de V (para la topología compleja), razonando como antes con las funciones Q/X_i^k concluiríamos que se anula en todo V. Así pues, el cociente P/Q está definido en un conjunto denso en V (para la topología compleja). Esto significa que toda función de $\mathbb{C}(Y)$ se restringe a una función de $\mathcal{M}(V)$.

Razonando con P en lugar de Q concluimos que la restricción es única, por lo que podemos considerar $\mathbb{C}(Y) \subset \mathcal{M}(V)$.

Ahora bien, si $\dim V = m$ y $\dim Y = d$, tenemos ciertamente que $m \leq d$, pues el conjunto de puntos regulares de Y es abierto, luego existe un punto $v \in V$ regular en Y. Esto significa que v tiene un entorno $Y' \subset Y$ (para la topología compleja) que es una subvariedad analítica de P^n de dimensión d, y por otra parte v tiene un entorno $V' \subset V \cap Y'$ que es una subvariedad analítica de P^n de dimensión m. Entonces V' es también una subvariedad analítica de Y', lo que nos da la desigualdad entre las dimensiones.

Por otra parte, el teorema 1.63 nos da que el grado de trascendencia de $\mathcal{M}(V)$ es a lo sumo m, mientras que el de $\mathbb{C}(Y)$ es exactamente d. Así pues,

$$\dim V = \dim Y = d.$$

Sea Y_r el conjunto de los puntos regulares de Y, que es una variedad algebraica, y también una variedad analítica conexa (por el teorema 4.19). Como V es compacta, es cerrada en Y para la topología compleja, luego $V \cap Y_r$ es una subvariedad analítica cerrada en Y_r, pero una subvariedad de la misma dimensión ha de ser necesariamente abierta, luego por conexión $Y_r \subset V \subset Y$.

Finalmente, Y_r es denso en Y para la topología compleja, luego la compacidad de V implica que $Y = V$. El teorema 4.14 implica que Y es regular. ■

4.4 Superficies de Riemann

Estudiamos aquí con más detalle las variedades analíticas de dimensión 1:

Definición 4.27 Una *superficie de Riemann* es una variedad analítica conexa de dimensión (compleja) 1 (y por lo tanto de dimensión real 2).

En añadidura, cuando hablemos de superficies de Riemann sobrentenderemos que son compactas, pues es el único caso con el que vamos a tratar. Notemos que una superficie compacta puede cubrirse por un número finito de abiertos homeomorfos a discos de $\mathbb{R}^2$, luego tiene una base numerable de abiertos. Esto implica, entre otras cosas, que es metrizable.

El teorema 4.19 implica que las curvas proyectivas regulares son superficies de Riemann. El ejemplo más simple es la recta proyectiva P^1. Si fijamos un sistema de referencia podemos expresarla como $\mathbb{C}^\infty = \mathbb{C} \cup \{\infty\}$. Desde este punto de vista es más frecuente llamarla *esfera de Riemann.* Ciertamente es difeomorfa a una esfera (como variedad diferencial real).

Las propiedades básicas de las aplicaciones entre superficies de Riemann se deducen fácilmente de este teorema:

Teorema 4.28 *Sea $f : X \longrightarrow Y$ una función holomorfa no constante entre superficies de Riemann y sea $a \in X$. Entonces existen cartas $p : U \longrightarrow \mathbb{C}$ con $a \in U$ y $q : V \longrightarrow \mathbb{C}$ con $f(a) \in V$ de modo que $f[U] \subset V$, $p(a) = q(f(a)) = 0$ y para todo $z \in p[U]$ se cumple $(p^{-1} \circ f \circ q)(z) = z^k$, para cierto natural k.*

Demostración: Componiendo dos cartas con traslaciones oportunas, podemos exigir que $p(a) = q(f(a)) = 0$. Restringiendo p podemos hacer que $f[U] \subset V$. Llamemos $F = p^{-1} \circ f \circ q$. Se trata de una función holomorfa no constante en $p[U]$ tal que $F(0) = 0$, luego existe un k tal que $F(z) = z^k g(z)$, donde g es una función holomorfa en 0 tal que $g(0) \neq 0$. Restringiendo p de nuevo podemos exigir que g no se anule en $p[U]$.

Tomando una rama uniforme de la raíz k-ésima en un entorno de $g(0)$ (y restringiendo aún más p si es necesario) construimos una función holomorfa $h : p[U] \longrightarrow \mathbb{C}$ tal que $h(z)^k = g(z)$. Así pues, $F(z) = (z\,h(z))^k$.

La función $zh(z)$ tiene derivada no nula en 0, por lo que es inyectiva en un entorno de 0. Restringiendo p una vez más podemos suponer que es inyectiva en $p[U]$. Componiendo p con esta función obtenemos una nueva carta sobre U, digamos p_0, de modo que si $x \in U$ y $w = p(x)h(p(x)) \in p_0[U]$,

$$(p_0^{-1} \circ f \circ q)(w) = q(f(x)) = F(p(x)) = (p(x)h(p(x)))^k = w^k.$$

Así pues, las cartas p_0 y q cumplen lo pedido. ■

La función z^k (como toda función holomorfa no constante) es abierta, luego f es abierta en un entorno de cada punto, luego es abierta.

El número k dado por el teorema anterior puede caracterizarse con independencia de las cartas consideradas:

> *Para todo entorno U de a suficientemente pequeño existe un entorno V de $f(a)$ de modo que todo punto en V distinto de $f(a)$ tiene exactamente k antiimágenes en U.*

Esto se sigue claramente de que la función z^k tiene esta propiedad en 0. Por lo tanto, k está completamente determinado por f y a.

Definición 4.29 Sea $f : X \longrightarrow Y$ una aplicación holomorfa no constante entre superficies de Riemann y $a \in X$. El número natural k que cumple la propiedad anterior se llama *índice de ramificación* de f en a y lo representaremos por $e(f, a)$.

La función z^k no toma el valor 0 más que en 0, luego todo punto $a \in X$ tiene un entorno en el que $f(z) \neq f(a)$. Equivalentemente, para cada $c \in Y$, la fibra $f^{-1}[c]$ es discreta y, como X es compacto, es finita.

La función z^k tiene derivada no nula en todo punto distinto de 0, luego es localmente inyectiva salvo en $z = 0$. Esto hace que la función f sea localmente inyectiva en todo punto de U salvo a lo sumo en a. Así pues, el conjunto de puntos donde f no es localmente inyectiva es discreto en X. Por compacidad es finito.

Definición 4.30 Sea $f : X \longrightarrow Y$ una aplicación holomorfa no constante entre superficies de Riemann y sea $A \subset X$ el conjunto (finito) de puntos de X donde f no es localmente inyectiva. Los puntos de $B = f[A]$ se llaman *puntos de ramificación* de f, mientras que los puntos de $Y \setminus B$ se llaman *puntos de escisión* de f.

Observemos que f es localmente inyectiva alrededor de un punto $a \in X$ si y sólo si $e(f, a) = 1$. El teorema siguiente recoge los hechos que acabamos de probar junto con algunos más.

Teorema 4.31 *Sea $f : X \longrightarrow Y$ una aplicación holomorfa no constante entre superficies de Riemann. Entonces:*

a) f es abierta, cerrada y suprayectiva.

b) Para cada $y \in Y$, el conjunto $f^{-1}[y]$ es finito.

c) Para cada $y \in Y$ y cada abierto V que contenga a $f^{-1}[y]$, existe un entorno abierto U de y tal que $f^{-1}[U] \subset V$.

d) Para cada punto de escisión $y \in Y$ existe un entorno abierto U de y tal que

$$f^{-1}[U] = \bigcup_{i=1}^{n} V_i,$$

donde los conjuntos V_i son abiertos disjuntos en X y todas las aplicaciones $f|_{V_i} : V_i \longrightarrow U$ son transformaciones conformes.

Demostración: a) Ya hemos visto que f es abierta y por compacidad es cerrada. Por consiguiente, $f[X]$ es abierto y cerrado en Y, luego por conexión $f[X] = Y$.

b) Ya está probado.

c) El conjunto $X \setminus V$ es cerrado en X, luego $B = f[X \setminus V]$ es cerrado en Y y no contiene a y, luego $U = Y \setminus B$ es un entorno abierto de y que cumple lo pedido.

d) Sea $f^{-1}[y] = \{x_1, \ldots, x_n\}$, donde $x_i \neq x_j$ para $i \neq j$. Como y es un punto de escisión, cada x_i tiene un entorno abierto W_i tal que $f|_{W_i}$ es inyectiva. Podemos tomar los W_i disjuntos dos a dos. Entonces $W = W_1 \cup \cdots \cup W_n$ es un abierto que contiene a $f^{-1}[y]$, luego por el apartado anterior existe un entorno abierto U de y tal que $f^{-1}[U] \subset W$. Podemos suponer que $U \subset f[W_i]$ para todo i. Sea $V_i = W_i \cap f^{-1}[U]$. Es claro que los conjuntos V_i cumplen lo pedido.

■

Finalmente probamos que el número de antiimágenes de los puntos de escisión es constante:

Teorema 4.32 *Sea $f : X \longrightarrow Y$ una aplicación holomorfa no constante entre superficies de Riemann. Entonces existe un número natural n tal que cada punto de escisión $b \in Y$ tiene exactamente n antiimágenes por f. Además, si $f^{-1}[b] = \{a_1, \ldots, a_n\}$, existe un entorno abierto U de b en Y y entornos abiertos disjuntos V_i en X de cada a_i de modo que $f^{-1}[U] = V_1 \cup \cdots \cup V_n$ y las restricciones $f|_{V_i} : V_i \longrightarrow U$ son conformes.*

Demostración: El conjunto B de los puntos de escisión para f en Y es conexo (pues si a una superficie conexa le quitamos un conjunto finito de puntos no perdemos la conexión). Si llamamos $p(y)$ al número de antiimágenes de y, el último apartado del teorema anterior prueba que p es localmente constante en B, y por conexión necesariamente p es constante en B. El resto del teorema es consecuencia inmediata del citado teorema. ■

Definición 4.33 Llamaremos *grado* de una aplicación holomorfa no constante $f : X \longrightarrow Y$ entre superficies de Riemann al número de antiimágenes de cualquiera de los puntos de escisión de Y. Lo representaremos por $n(f)$.

Puede probarse que toda aplicación regular no constante entre curvas proyectivas regulares es finita, y es claro entonces que el grado que acabamos de definir coincide con el definido en 4.15. El teorema siguiente nos da más información sobre los puntos de ramificación:

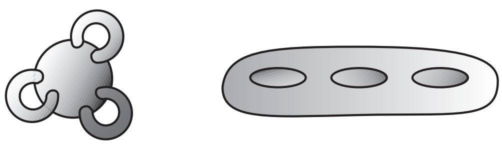
Teorema 4.34 *Sea $f : X \longrightarrow Y$ una aplicación holomorfa no constante entre superficies de Riemann. Para cada punto $y \in Y$ se cumple*

$$n(f) = \sum_{x \in f^{-1}[y]} e(f, x).$$

Demostración: Por las propias definiciones el resultado es cierto si y es un punto de escisión. Tomemos ahora un punto de ramificación $b \in Y$ y supongamos que tiene s antiimágenes distintas $a_1, \ldots, a_s$. Sea $n_j = e(f, a_j)$.

Por la definición del grado de f en un punto, existen entornos abiertos V_j de cada a_j disjuntos dos a dos y entornos U_j de b tales que cada $y \in U_j \setminus \{b\}$ tiene exactamente n_j antiimágenes en V_j. Por el teorema 4.31 existe un entorno abierto U de b tal que $U \subset U_1 \cap \cdots \cap U_s$ y $f^{-1}[U] \subset V_1 \cup \cdots \cup V_s = V$. Entonces todo punto de escisión $y \in U$ tiene exactamente $n = n_1 + \cdots + n_s$ antiimágenes, luego $n = n(f)$. ■

Las superficies de Riemann son superficies compactas, conexas y orientables (toda variedad analítica es orientable como variedad real). La estructura topológica de estas superficies es conocida:[4] toda superficie compacta conexa y orientable es homeomorfa a una esfera con g asas o, equivalentemente, con g agujeros, o a g toros pegados. El número g se llama *género* de la superficie, entendiendo que la esfera es la superficie de género $g = 0$. Dos superficies compactas, conexas y orientables son homeomorfas si y sólo si tienen el mismo género. La figura muestra dos superficies de género 3.



[4]Todos los resultados que enunciamos a continuación están demostrados en mi libro de *Topología algebraica.*

Una caracterización más operativa del género de una superficie viene dada en términos de triangulaciones. Recordemos que un *triángulo* T en una superficie S es un homeomorfismo en la imagen $T : \Delta \longrightarrow S$, donde Δ es un triángulo usual, por ejemplo

$$\Delta = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0,\ y \geq 0,\ x + y \leq 1\}.$$

Las *aristas* y los *vértices* de T son las imágenes por T de las aristas y vértices de Δ en el sentido obvio. Una *triangulación* de S es un conjunto finito de triángulos en S cuyas imágenes cubran S y de modo que dos cualesquiera de ellas sean disjuntas o bien tengan en común una arista o un vértice. Las imágenes de los triángulos se llaman *caras* de la triangulación. Puede probarse que toda superficie compacta S admite una triangulación, así como que $\chi_S = V - A + C$, donde V, A y C son respectivamente el número de vértices, aristas y caras de una triangulación dada, no depende de la triangulación con que se calcula, sino que es un invariante conocido como *característica de Euler* de S. Además si S es conexa y orientable de género g, entonces $\chi_S = 2 - 2g$.

Así, por ejemplo, la característica de Euler de la esfera es 2, mientras que la del toro es 0. Todos estos hechos se prueban con relativa facilidad salvo la existencia de triangulaciones. No obstante, nosotros vamos a construir explícitamente una triangulación en una superficie de Riemann dada, con la cual obtendremos una expresión para el género que nos permitirá no volver a hablar de triangulaciones.

Sea, pues, X una superficie de Riemann y sea $f : X \longrightarrow \mathbb{C}^\infty$ una función holomorfa no constante. Sea $n = n(f)$. Partamos de una triangulación de la esfera $\mathbb{C}^\infty$ (es fácil construir una explícitamente). Es claro que podemos subdividir los triángulos que la forman hasta que los puntos de ramificación de f formen parte de los vértices, así como que cada triángulo tenga a lo sumo un vértice ramificado.

Para cada punto de ramificación $b \in \mathbb{C}^\infty$ con antiimágenes $a_1, \ldots, a_m \in X$, tomamos un entorno abierto V_b y entornos U_i de cada a_i de modo que las lecturas de f respecto de cartas adecuadas en cada U_i y en V_b sean de la forma z^{k_i}, donde $k_i = e(z, a_i)$. Por 4.31 podemos tomar $f^{-1}[V_b] \subset U_1 \cup \cdots \cup U_m$. Es claro que subdividiendo la triangulación podemos exigir que cada triángulo con un vértice igual a b esté contenido en V_b.

La unión de los triángulos cuyos vértices son puntos de escisión es un conjunto compacto, que puede ser cubierto con un número finito de abiertos U en las condiciones de 4.32 (abiertos tales que $f^{-1}[U] = V_1 \cup \cdots \cup V_n$ y las restricciones $f|_{V_i} \longrightarrow U$ son transformaciones conformes). Refinando la triangulación podemos exigir que todo triángulo cuyos vértices sean puntos de escisión esté contenido en uno de estos abiertos.[5]

[5]Aquí usamos el teorema de Lebesgue, en virtud del cual existe un $\epsilon > 0$ tal que todo conjunto de diámetro menor que ϵ está contenido en un abierto del cubrimiento, así como que todo triángulo puede subdividirse en triángulos de diámetro arbitrariamente pequeño. Las subdivisiones se hacen uniendo los vértices con un punto interior, de modo que se conservan las aristas exteriores.

Llamemos V, A y C al número de vértices, aristas y caras de la triangulación de la esfera así obtenida. Sabemos que $V - A + C = 2$.

La antiimagen por f de un triángulo cuyos vértices sean puntos de escisión es la unión de n triángulos disjuntos en X. Por otra parte, si un triángulo T tiene un vértice ramificado b, analizando el comportamiento de la función z^{k_i} vemos que (con la notación anterior) $f|_{U_i}^{-1}[T]$ es la unión de k_i triángulos con a_i como único punto en común. Por el teorema 4.34 concluimos que $f^{-1}[T]$ es unión de m triángulos en X "arracimados" en m grupos de k_i triángulos unidos por un vértice.

Es claro que los triángulos así obtenidos forman una triangulación de X, digamos con V' vértices, A' aristas y C' caras. Según hemos visto, $C' = nC$ y, claramente, $A' = nA$ (las aristas están formadas por puntos de escisión, salvo quizá un vértice, luego cada una se escinde en n aristas).

Sea r el número de puntos de ramificación de f y, para cada uno de ellos $b \in \mathbb{C}^\infty$, sea m_b el número de antiimágenes. Así,

$$V' = n(V - r) + \sum_b m_b,$$

donde b recorre los puntos de ramificación. Equivalentemente:

$$\begin{aligned} V' &= nV - nr + \sum_b m_b = nV + \sum_b (m_b - n) \\ &= nV + \sum_b \sum_{a \in f^{-1}[b]} (1 - e(f, a)) \\ &= nV + \sum_a (1 - e(f, a)), \end{aligned}$$

donde en la última suma a recorre los puntos de V tales que $f(a)$ es un punto de ramificación o, equivalentemente, los puntos con $e(f, a) > 1$ (pues sus imágenes son puntos de ramificación y los sumandos con $e(f, a) = 1$ son nulos). La característica de Euler de la superficie X resulta ser

$$\chi_X = V' - A' + C' = nV + \sum_a (1 - e(f, a)) - nA + nC = 2n + \sum_a (1 - e(f, a)).$$

En definitiva, hemos probado lo siguiente:

Teorema 4.35 (Fórmula de Hurwitz) *Sea X una superficie de Riemann y $f : X \longrightarrow \mathbb{C}^\infty$ una función holomorfa no constante. Entonces el género g de X viene determinado por la relación*

$$2 - 2g = 2n(f) + \sum_a (1 - e(f, a)),$$

donde a recorre los puntos de X para los que $e(f, a) > 1$.

Conviene observar ahora que las funciones holomorfas $f : X \longrightarrow \mathbb{C}^\infty$ no son sino las funciones meromorfas en X:

Teorema 4.36 *Si X es una superficie de Riemann, podemos identificar las funciones meromorfas en X con las funciones holomorfas $f : X \longrightarrow \mathbb{C}^\infty$ distintas de la función constante ∞.*

Demostración: Sea $f \in \mathcal{M}(X)$ y $x \in X$. Entonces f se expresa en un entorno U de x (que podemos tomar difeomorfo a un abierto de $\mathbb{C}$) como cociente de dos funciones holomorfas en U. Ahora bien, los cocientes de funciones holomorfas en un abierto de $\mathbb{C}$ definen funciones meromorfas en el sentido usual de la teoría de funciones de (una) variable compleja, esto es, funciones holomorfas en U salvo en un número finito de puntos, donde tienen polos. Recordemos ahora que una función meromorfa $U' \longrightarrow \mathbb{C}$, donde U' es un abierto de $\mathbb{C}$, se extiende[6] a una función holomorfa $U' \longrightarrow \mathbb{C}^\infty$. Lo mismo vale, obviamente, para $f|_U$ y, por consiguiente, para f.

Recíprocamente, si $f : X \longrightarrow \mathbb{C}^\infty$ es una función holomorfa distinta de la constante ∞, entonces ∞ tiene un número finito de antiimágenes. Si U es un abierto de X difeomorfo a un abierto en $\mathbb{C}$, entonces $f|_U$ se corresponde con una función meromorfa en el sentido de la teoría de funciones de una variable compleja (es holomorfa salvo en un número finito de singularidades donde tiene límite ∞, luego son polos), luego $f|_U$ se corresponde con un cociente de funciones holomorfas y, por consiguiente, $f|_U$ es a su vez un cociente de funciones holomorfas en U. Esto prueba que f es meromorfa en el sentido de 1.61. ■

Así, si X es una superficie de Riemann, $\mathcal{M}(X)$ está formado por las funciones $f : X \longrightarrow \mathbb{C}$ cuyas lecturas en las cartas de X son meromorfas en el sentido usual de la teoría de funciones de una variable compleja. Llamaremos *polos* de f a los puntos de X donde f no está definida o, equivalentemente, donde toma el valor ∞ (que son un número finito).

Conviene destacar que la existencia de funciones meromorfas no constantes en una superficie de Riemann no es trivial en absoluto, aunque lo cierto es que siempre existen tales funciones.[7] En el caso en que X es una curva proyectiva regular, la existencia de funciones meromorfas no constantes es inmediata, ya que $\mathcal{M}(X) = \mathbb{C}(X)$.

Ejemplo Consideremos la cúbica V dada por $Y^2 = X(X-1)(X-2)$.

Ciertamente es irreducible, como se sigue del criterio de Eisenstein aplicado al primo X. Es fácil ver que todos sus puntos son regulares, incluso su único punto infinito, que es $(0,1,0)$. Consideremos $f = x \in \mathbb{C}(V)$, obviamente regular en todos los puntos finitos de V. En coordenadas homogéneas es $f(X,Y,Z) = (X,Z)$. Esta expresión no nos permite calcular $f(0,1,0)$ (lo cual se debe a que,

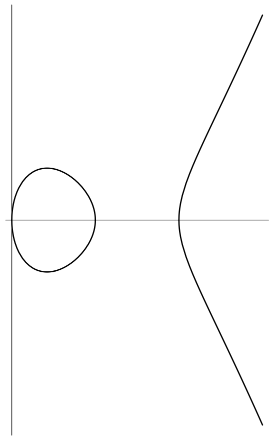
[6] Si $z_0 \in U$ es un polo de $f = g/h$, donde g y h son holomorfas en U', el orden de g en z_0 es menor que el de h, por lo que, dividiendo ambas fracciones entre una potencia de $z - z_0$, podemos suponer que $g(z_0) \neq 0$. Entonces, definiendo $f(z_0) = \infty$ y tomando $1/z$ como carta de $\mathbb{C}^\infty$ alrededor de ∞, la lectura de f en dicha carta es h/g, que es holomorfa en un entorno de z_0.

[7] Ver el teorema 14.32 de mi libro de *Funciones de variable compleja.*

en principio, sólo es válida para $Z \neq 0$), pero la relación $y^2z = x(x-z)(x-2z)$ nos da que

$$\frac{x}{z} = \frac{y^2}{(x-z)(x-2z)},$$

luego una expresión alternativa para f es $f(X,Y,Z) = (Y^2, (X-Z)(X-2Z))$, con la que obtenemos $f(0,1,0) = (1,0) = \infty$. Así pues, f tiene un único polo en el punto infinito $(0,1,0)$.



Cada $x \in \mathbb{C}$ tiene tantas antiimágenes por f como soluciones tiene la ecuación $Y^2 = x(x-1)(x-2)$. Vemos que hay dos soluciones excepto para $x = 0, 1, 2$, luego concluimos que el grado de f es $n(f) = 2$. Los puntos de ramificación de f son 0, 1, 2, ∞, pues cada uno de ellos tiene una única antiimagen en V que, por consiguiente, tendrá índice de ramificación 2 (recordemos que la suma de los índices ha de ser 2). Según el teorema anterior, el género g de V verifica

$$2 - 2g = 4 + (1-2) + (1-2) + (1-2) + (1-2) = 0,$$

luego $g = 1$. Esto significa que V es homeomorfa a un toro. Al completar la rama derecha de V con el punto infinito obtenemos dos (curvas reales homeomorfas a dos) circunferencias, que constituyen el corte del toro con el plano real. ■

Si V es una curva proyectiva, no necesariamente regular, podemos definir el *género* de V como el de su regularización, y si V es cuasiproyectiva definimos su género como el de su clausura proyectiva.

Puesto que una curva proyectiva se obtiene de su regularización identificando un número finito de puntos a un número finito de puntos, tenemos la estructura topológica general de cualquier curva proyectiva: es una esfera con g asas en la que un número finito de puntos ha sido identificado a un número finito de puntos. De momento no estamos en condiciones de estudiar las sutilezas derivadas de la existencia de puntos singulares en una curva.

Los resultados del capítulo anterior muestran ahora que las rectas y las cónicas son topológicamente esferas (pues son isomorfas a P^1), mientras que una cúbica singular es bien una esfera o bien una esfera con dos puntos pegados (ver las páginas 119 y 141).

Ejercicio: Comprobar la fórmula de Hurwitz sobre la circunferencia $X^2 + Y^2 = 1$ y la aplicación x.

4.5 El teorema de Lefschetz

Puede probarse que toda variedad diferencial real es difeomorfa a una subvariedad de $\mathbb{R}^n$, para un n suficientemente grande. Sin embargo, no se cumple un teorema análogo para variedades complejas. Existen toros complejos que no son conformemente equivalentes a ninguna subvariedad de $\mathbb{C}^n$, o incluso de P^n. En virtud del teorema 4.26, esto implica que no toda variedad analítica compacta es conformemente equivalente a una variedad algebraica.

No vamos a dar ejemplos de estos hechos, pero, por ejemplo, sucede que hay toros complejos T en los que las únicas funciones meromorfas son las constantes o, en otros términos, tales que $\mathcal{M}(T) = \mathbb{C}$. En cambio, si T es proyectivo, es decir, si es conformemente equivalente a una variedad proyectiva, sabemos que $\mathcal{M}(T)$ ha de tener grado de trascendencia sobre $\mathbb{C}$ igual $\dim T$. En general, saber que una variedad analítica compacta es proyectiva proporciona mucha información sobre ella.

El propósito de esta sección es demostrar un teorema de inmersión de Lefschetz que proporciona una condición suficiente para que un toro complejo sea proyectivo. Ello nos lleva a estudiar las llamadas funciones zeta:

Definición 4.37 Sea V un espacio vectorial complejo de dimensión g y R un retículo en V. Una *función zeta* en V con respecto a R es una función $F \in \mathcal{H}(V)$ no nula tal que existen funciones $L : V \times R \longrightarrow \mathbb{C}$ y $J : R \longrightarrow \mathbb{C}$ de modo que L es $\mathbb{C}$-lineal en su primera variable y, para todo $z \in V$ y todo $r \in R$, se cumple que

$$F(z + r) = F(z)e^{2\pi i(L(z,r)+J(r))}.$$

Una función zeta es *trivial* si no se anula en ningún punto.

Una definición tan técnica como ésta requiere una explicación:

En el estudio de una variedad analítica compacta X tiene interés investigar los subconjuntos de X que son localmente ceros de funciones holomorfas. Aunque no nos va a hacer falta en ningún momento, esto se precisa mediante el concepto de divisor de Cartier: Un *divisor (entero) de Cartier* D en una variedad X está determinado por una familia de pares (U_i, f_i), donde los conjuntos U_i forman un cubrimiento abierto de X y las funciones $f_i \in \mathcal{H}(U_i)$ cumplen que los cocientes $f_i/f_j \in \mathcal{H}(U_i \cap U_j)$ no se anulan en ningún punto. El *soporte* de D es el conjunto $Z \subset X$ formado por los puntos en los que se anulan las funciones f_i. Es en este sentido en el que podemos decir que los soportes de los divisores de Cartier son localmente ceros de funciones holomorfas.

En general, las funciones f_i que definen a Z no pueden "pegarse" para formar una única función $f \in \mathcal{H}(X)$, pues dicha f habría de ser constante, luego estaríamos en uno de los casos triviales $Z = \varnothing$ o bien $Z = X$. Sin embargo, si $X = V/R$ es un toro complejo, puede probarse que las funciones f_i pueden manipularse adecuadamente (sin modificar el soporte Z) de modo que sus composiciones con la proyección $p : V \longrightarrow V/R$ sí pueden pegarse para formar una función zeta en V.

Observemos que si F es una función zeta en V respecto de R, el toro V/R puede cubrirse por abiertos U_i donde p tiene inversa, y que los pares $(U_i, p|_{U_i}^{-1} \circ F)$ forman un divisor de Cartier de V/R. Lo que hemos afirmado es que todo divisor de Cartier del toro puede obtenerse de este modo a partir de una función zeta.

No vamos a demostrar este hecho porque no lo vamos a necesitar, pero conviene recordar que, esencialmente, una función zeta está definiendo un "conjunto de ceros" en V/R. Por ejemplo, esto explica el interés de las funciones zeta triviales: son las asociadas al conjunto vacío.

Veamos ahora que es fácil determinar explícitamente las funciones zeta triviales.

Si F es una función zeta trivial, entonces[8] $F(z) = e^{2\pi i f(z)}$, para una función $f \in \mathcal{H}(V)$. Sean L y J según la definición de función zeta. Fijado un $r \in R$, tenemos que

$$f(z+r) - f(z) = L(z,r) + J(r) + k_r,$$

para un cierto $k_r \in \mathbb{Z}$ que es una función continua de z, luego es constante. (Recordemos que $L(z,r)$, para un r fijo, es una función lineal, luego continua.) El miembro derecho, para un r fijo, es una función lineal, luego todas las derivadas parciales de orden 2 del miembro derecho son nulas. Equivalentemente,

$$\left.\frac{\partial^2 f}{\partial z_i \partial z_j}\right|_z = \left.\frac{\partial^2 f}{\partial z_i \partial z_j}\right|_{z+r},$$

para todo $z \in V$ y todo $r \in R$. Por consiguiente, estas derivadas segundas inducen funciones holomorfas $V/R \longrightarrow \mathbb{C}$, luego son constantes por 1.60. Concluimos que f es un polinomio de grado ≤ 2, luego podemos descomponerlo como $f(z) = q(z) + \lambda(z) + c$, donde $q(z)$ es una forma cuadrática, $\lambda(z)$ es una forma lineal y $c \in \mathbb{C}$. Con esto tenemos probada la mayor parte del teorema siguiente:

Teorema 4.38 *Si R es un retículo en V, las funciones zeta triviales en V respecto de R son las funciones de la forma $F(z) = e^{2\pi i(q(z)+\lambda(z)+c)}$, donde $q(z)$ es una forma cuadrática, $\lambda(z)$ es una forma lineal y $c \in \mathbb{C}$.*

DEMOSTRACIÓN: Sólo falta probar que cualquier función de la forma descrita en el enunciado es realmente una función zeta. Observemos en primer lugar que $q(z) = b(z,z)$, donde $b : V \times V \longrightarrow \mathbb{C}$ es una forma bilineal simétrica. Evaluando $b(z_1+z_2, z_1+z_2)$ vemos que

$$q(z_1+z_2) - q(z_1) - q(z_2) = 2b(z_1,z_2),$$

[8] Es claro que F tiene un logaritmo holomorfo en un entorno de cada punto, y dos logaritmos holomorfos definidos en un mismo abierto conexo se diferencian en un múltiplo de $2\pi i$. Si F no tuviera un logaritmo holomorfo definido en todo V, podríamos tomar el supremo $r > 0$ de todos los radios tales que F admite un logaritmo holomorfo en la bola abierta $B(0,r) \subset V$. La frontera de dicha bola podría cubrirse por un número finito de bolas abiertas con centro en $\partial B(0,r)$ y en las que F admite un logaritmo holomorfo. Si B es una de estas bolas, $B \cap B(0,r)$ es convexo, luego conexo, luego el logaritmo en B puede tomarse de modo que extienda al definido en $B(0,r)$. Si B' es otra de las bolas y $B \cap B' \neq \varnothing$, entonces $B(0,r) \cap B \cap B'$ es un abierto convexo no vacío en el que las dos prolongaciones coinciden, luego ambas coinciden en $B \cap B'$. De este modo tenemos un logaritmo de F definido sobre un abierto que contiene a la bola cerrada de radio r, luego también a una bola abierta de radio mayor, en contradicción con la elección de r.

por lo que la función $e^{2\pi i q(z)}$ cumple la definición de función zeta con las funciones

$$L(z,r) = 2b(z,r), \qquad J(r) = q(r).$$

Por otra parte, la función $e^{2\pi i\lambda(z)}$ cumple la definición de función zeta con $L = 0$ y $J = \lambda$. La constante e^c es trivialmente una función zeta y la función del enunciado es el producto de las tres. ■

La construcción de funciones zeta no triviales es un problema más delicado del que nos ocuparemos más adelante.

Las funciones L y J que aparecen en la definición de las funciones zeta satisfacen ciertas relaciones. En primer lugar, si tomamos r, $s \in R$ y calculamos $F(z+r+s)/F(z)$ de las dos formas obvias, obtenemos:

$$L(z,r+s) + J(r+s) \equiv L(z,s) + L(z+s,r) + J(r) + J(s) \text{ (mód } \mathbb{Z}). \tag{4.1}$$

Haciendo $z = 0$ queda

$$J(r+s) - J(r) - J(s) \equiv L(r,s) \text{ (mód } \mathbb{Z}). \tag{4.2}$$

Como el miembro izquierdo es simétrico en r y s, deducimos a su vez que

$$L(r,s) \equiv L(s,r) \text{ (mód } \mathbb{Z}). \tag{4.3}$$

Sustituyendo (4.2) en (4.1) obtenemos

$$L(z,r+s) \equiv L(z,s) + L(z+s,r) - L(r,s) \text{ (mód } \mathbb{Z}).$$

Usando (4.3) y la linealidad de L en la primera componente resulta

$$L(z,r+s) \equiv L(z,r) + L(z,s) \text{ (mód } \mathbb{Z}).$$

Fijados r y s, la diferencia entre ambos miembros es un entero que depende linealmente de z, luego ha de ser nulo. Así pues:

$$L(z,r+s) = L(z,r) + L(z,s).$$

Esto nos permite extender L a una función $L : V \times V \longrightarrow \mathbb{C}$ que es $\mathbb{C}$-lineal en la primera variable y $\mathbb{R}$-lineal en la segunda. Definimos ahora

$$K(r) = J(r) - \frac{1}{2}\, L(r,r).$$

De (4.2) se sigue que

$$K(r+s) \equiv K(r) + K(s) \text{ (mód } \mathbb{Z}).$$

Llamemos $K' : V \longrightarrow \mathbb{C}$ a la aplicación $\mathbb{R}$-lineal que coincide con K en una base de R. Entonces $K'(r) \equiv K(r)$ (mód $\mathbb{Z}$). Ahora bien, la función

$$J'(r) = J(r) + K'(r) - K(r)$$

cumple también la definición de función zeta para F, luego cambiando J por J' podemos suponer que K es $\mathbb{R}$-lineal. En definitiva, hemos probado el teorema siguiente:

Teorema 4.39 *Sea F una función zeta en V respecto a un retículo R y sean L y J las funciones que cumplen la definición de función zeta. Entonces L se extiende a una función $L : V \times V \longrightarrow \mathbb{C}$ que es $\mathbb{C}$-lineal en la primera variable y $\mathbb{R}$-lineal en la segunda, y la función J puede elegirse de modo que la función $K(r) = J(r) - \frac{1}{2}L(r,r)$ es $\mathbb{Z}$-lineal y se extiende a una función $\mathbb{R}$-lineal $K : V \longrightarrow \mathbb{C}$.*

En términos de K y L, la relación que define las funciones zeta equivale a

$$F(z+r) = F(z)\exp(2\pi i(L(z,r) + \frac{1}{2}L(r,r) + K(r))). \tag{4.4}$$

Si estamos dispuestos a modificar la función F de forma no esencial, todavía podemos decir más. Para ello definimos la equivalencia de funciones zeta. Notemos que el producto de dos funciones zeta en V respecto al mismo retículo R es también una función zeta, así como que la inversa de una función zeta trivial es también una función zeta trivial, luego las funciones zeta triviales forman un grupo.

Definición 4.40 Diremos que dos funciones zeta en V respecto a un retículo R son *equivalentes* si su cociente es una función zeta trivial.

La idea subyacente es que dos funciones zeta son equivalentes si determinan el mismo conjunto de ceros en el toro V/R. Como las funciones zeta triviales forman un grupo, es obvio que la equivalencia de funciones zeta es en efecto una relación de equivalencia. Vamos a asociar algunos invariantes a cada clase de equivalencia. En primer lugar, la aplicación $E : V \times V \longrightarrow \mathbb{R}$ dada por

$$E(z,w) = L(z,w) - L(w,z) \tag{4.5}$$

es una forma $\mathbb{R}$-bilineal alternada. Por (4.3) vemos que E toma valores enteros en $R \times R$, y la bilinealidad implica entonces que toma valores reales en $V \times V$.

A su vez, la forma $S : V \times V \longrightarrow \mathbb{R}$ dada por

$$S(z,w) = E(iz,w)$$

es $\mathbb{R}$-bilineal simétrica.

En efecto, $S(z,w) = L(iz,w) - L(w,iz)$, $S(w,z) = L(iw,z) - L(z,iw)$. Por lo tanto,

$$S(z,w) - S(w,z) = i(E(z,w) - E(iz,iw)).$$

Como un miembro es real y el otro imaginario puro, ambos miembros son nulos y S es simétrica. Además obtenemos que $E(z,w) = E(iz,iw)$.

Finalmente definimos $H : V \times V \longrightarrow \mathbb{C}$ mediante

$$H(z,w) = E(iz,w) + iE(z,w). \tag{4.6}$$

Así H es una forma hermitiana, es decir, para cada $\lambda \in \mathbb{C}$, se cumple

$$H(\lambda z,w) = \lambda H(z,w), \quad H(z,\lambda w) = \bar{\lambda}H(z,w), \quad H(z,w) = \overline{H(w,z)}.$$

En efecto:

$$\begin{aligned}\overline{H(w,z)} &= E(iw,z) - iE(w,z) = -E(z,iw) + iE(z,w) \\ &= E(iiz,iw) + iE(z,w) = E(iz,w) + i(z,w) = H(z,w).\end{aligned}$$

Se comprueba inmediatamente que $H(iz,w) = iH(z,w)$, de donde se sigue la $\mathbb{C}$-linealidad en la primera variable, mientras que la semilinealidad en la segunda se sigue de ésta y de la tercera propiedad.

La forma E y, por consiguiente, también las formas S y H, no se alteran al pasar de una función zeta a otra equivalente. En efecto, si dos funciones zeta F y F' cumplen la definición con funciones L y L', entonces FF' cumple la definición con $L + L'$. Si $F'(z) = e^{2\pi i(q(z)+\lambda(z)+c)}$ es una función zeta trivial, en la prueba del teorema 4.38 hemos visto que cumple la definición de función zeta con $L'(z,w) = 2b(z,w)$, donde b es la forma bilineal simétrica que cumple $q(z) = b(z,z)$. Esto hace que FF' cumple la definición de función zeta con $L + 2b$, y la simetría de b implica que la forma E para FF' es la misma que la asociada a F. ■

Vemos también que, para una función zeta trivial, partiendo de $L = 2b$, obtenemos $E = S = H = 0$.

Diremos que una función zeta está *normalizada* si la función K toma valores reales y

$$L(z,w) = -\frac{i}{2}\,H(z,w). \tag{4.7}$$

El interés de esta definición radica en el teorema siguiente:

Teorema 4.41 *Toda función zeta es equivalente a una función zeta normalizada.*

Demostración: Una función zeta trivial es de la forma $e^{2\pi i(q(z)+\lambda(z)+c)}$, donde $q(z) = b(z,z)$, para una cierta forma bilineal simétrica $b : V \times V \longrightarrow \mathbb{C}$. Al multiplicar una función zeta por esta función trivial, a la función L se le suma la forma $2b(z,r)$. Vamos a probar que

$$2b(z,w) = -L(z,w) - \frac{i}{2}\,H(z,w)$$

es simétrica, con lo que será una forma $\mathbb{C}$-bilineal (ya que es $\mathbb{C}$-lineal en la primera variable). Así, al multiplicar la función zeta correspondiente a L por la función zeta trivial definida por esta b, obtenemos una función zeta cuya función L cumple la segunda condición de la definición de normalización. En definitiva, hemos de probar que

$$\frac{i}{2}\,(H(z,w) - H(w,z)) = L(w,z) - L(z,w),$$

y ciertamente

$$\begin{aligned}\frac{i}{2}\,(H(z,w) - H(w,z)) &= \frac{i}{2}\,(H(z,w) - \overline{H(z,w)}) = -E(z,w) \\ &= E(w,z) = L(w,z) - L(z,w).\end{aligned}$$

Por otra parte, al multiplicar por la función zeta trivial, a la función J (y, por consiguiente, a K) se le suma la forma lineal $\lambda(z)$. Hemos de probar que existe una forma lineal $\lambda(z)$ que hace que $K(z)+\lambda(z)$ tome valores reales.

Como K es $\mathbb{R}$-lineal, también lo es $\operatorname{Im} K : V \longrightarrow \mathbb{R}$. Por consiguiente, si $z=(a_1+ib_1,\ldots,a_g+ib_g)$, entonces $\operatorname{Im} K(z) = c_1a_1+d_1b_1+\cdots+c_ga_g+d_gb_g$, para ciertos c_i, $d_i \in \mathbb{R}$. Sea $\alpha_i = d_i + ic_i$ y $\lambda(z) = -\alpha_1 z_1 - \cdots - \alpha_g z_g$. Es claro que $\operatorname{Im} K(z) + \operatorname{Im}\lambda(z) = 0$. ■

Para una función zeta normalizada, la relación (4.4) se expresa en la forma:

$$F(z+r) = F(z)\exp(2\pi i(-\frac{i}{2}\,H(z,r) - \frac{i}{4}\,H(r,r) + K(r))). \tag{4.8}$$

Observemos que si partimos de esta ecuación entendiendo que $L=-(i/2)H$ (y suponiendo que H es una forma hermitiana), la forma E dada por (4.5) es $E=\operatorname{Im} H$, y la forma H dada por (4.6) es la forma H dada.

Más aún, la ecuación (4.8) determina completamente la forma H. En efecto, si una función F cumple (4.8) con dos formas H y H' (y dos funciones K, K'), las exponenciales correspondientes han de coincidir, al igual que los logaritmos de sus módulos, que son

$$\pi E(iz,r) + \frac{\pi}{2}E(ir,r) = \pi E'(iz,r) + \frac{\pi}{2}E'(ir,r).$$

Equivalentemente, $E(i(2z+r),r) = E'(i(2z+r),r)$. Como esto vale para todo $z\in V$, de hecho $E(z,r)=E'(z,r)$. Como podemos tomar una $\mathbb{R}$-base de V contenida en R, esto implica que $E=E'$, luego $H=H'$. ■

Teorema 4.42 *La forma hermitiana H asociada a una función zeta es semidefinida positiva, es decir, $H(z,z)\geq 0$.*

Demostración: Sea F una función zeta. No perdemos generalidad si suponemos que está normalizada. Sea $f(z) = F(z)\exp(-\frac{\pi}{2}\,H(z,z))$. Así, para todo $r\in R$,

$$\begin{aligned} f(z+r) &= F(z+r)\exp(-\frac{\pi}{2}H(z+r,z+r)) \\ &= F(z)\exp(2\pi i(-\frac{i}{4}\,H(z,r) + K(r) + \frac{i}{4}H(z,z) + \frac{i}{4}H(r,z))) \\ &= f(z)\exp(2\pi i(\frac{1}{2}\operatorname{Im} H(z,r) + K(r))) = f(z)\exp(2\pi i(\frac{1}{2}E(z,r) + K(r))). \end{aligned}$$

Como E y K toman valores reales, resulta que $|f(z+r)| = |f(z)|$. Por consiguiente, $|f|$ induce una función continua en el toro compacto V/R, luego está acotada. Si C es una cota, tenemos que

$$F(z) \leq Ce^{\frac{\pi}{2}H(z,z)}.$$

Si $H(z_0,z_0)<0$, entonces la función $\mathbb{C}\longrightarrow\mathbb{C}$ dada por $\lambda\mapsto F(\lambda z_0)$ es entera y tiende a 0 en ∞, luego tiene que ser idénticamente nula. En particular

$F(z_0) = 0$. Hemos probado que si $H(z_0, z_0) < 0$ entonces $F(z_0) = 0$. Como $H(z, z)$ ha de ser negativa en un entorno de z_0, resulta que F se anula en un abierto, luego es idénticamente nula, en contradicción con la definición de función zeta. ■

Nos ocupamos ahora del problema de la existencia de funciones zeta para las que H es, más precisamente, definida positiva, es decir, que cumple $H(z, z) > 0$ siempre que $z \neq 0$. Notemos que esto es equivalente a que $E(iz, z) > 0$ y, por lo tanto, a que E satisfaga la definición siguiente:

Definición 4.43 Sea V un espacio vectorial complejo de dimensión g y R un retículo en V. Una *forma de Riemann* en V respecto a R es una forma bilineal alternada $E : V \times V \longrightarrow \mathbb{R}$ que toma valores enteros en $R \times R$ y tal que la forma bilineal $S(z, w) = E(iz, w)$ es simétrica y definida positiva.

Diremos que una función zeta en un espacio V respecto a un retículo R es *no degenerada* si su forma H asociada es definida positiva o, equivalentemente, si su forma E asociada es una forma de Riemann.

Necesitamos un poco de álgebra lineal:

Teorema 4.44 (Frobenius) *Si $E : R \times R \longrightarrow \mathbb{Z}$ es una forma bilineal alternada definida positiva en un $\mathbb{Z}$-módulo libre R de rango finito, entonces $R = \langle e_1, v_1 \rangle \perp \cdots \perp \langle e_g, v_g \rangle$, donde $E(e_j, v_j) = d_j$ es un número natural no nulo y $d_1 \mid d_2 \mid \cdots \mid d_g$.*

Demostración: La notación $A \perp B$ indica suma directa ortogonal, es decir, una suma directa tal que $E(a, b) = 0$ para todo $a \in A$ y todo $b \in B$. Notemos que la imagen de E en $\mathbb{Z}$ es un ideal no nulo. Sea $d_1 > 0$ su generador, de modo que d_1 divide a cualquier entero en la imagen de E. Pongamos que $E(e_1, v_1) = d_1$. Sea $R_1 = \langle e_1, v_1 \rangle$ y sea

$$R_1^\perp = \{r \in R \mid E(e_1, r) = E(v_1, r) = 0\}.$$

Es claro que $R_1 \cap R_1^\perp = 0$. Veamos que $R = R_1 + R_1^\perp$. Para ello tomamos un $r \in R$ y consideramos los elementos de la forma $r - me_1 - nv_1$, para ciertos m, $n \in \mathbb{Z}$. Vemos que

$$E(r - me_1 - nv_1, e_1) = E(r, e_1) + nd_1.$$

Sabemos que $d_1 \mid E(r, e_1)$, luego podemos tomar n de modo que la expresión anterior sea nula. Eligiendo m de modo similar obtenemos $r - me_1 - nv_1 \in R_1^\perp$, luego $r \in R_1 + R_1^\perp$. Así pues, $R = R_1 \perp R_1^\perp$, y la restricción de E a $R_1^\perp \times R_1^\perp$ satisface las hipótesis del teorema. Ahora basta razonar inductivamente sobre el rango de R. ■

La descomposición dada por el teorema anterior se llama una *descomposición de Frobenius* de R respecto de E, y una base $e_1, v_1, \ldots, e_g, v_g$ en las condiciones del teorema anterior se llama una *base de Frobenius* de R respecto de E.

En las condiciones de la definición 4.43, una base de R como $\mathbb{Z}$-módulo es también una base de V como $\mathbb{R}$-espacio vectorial. Si M y M' son las matrices de la forma E respecto a dos de estas bases, entonces $M' = AMA^t$, donde A es la matriz de cambio de base, que tiene determinante ± 1, por lo que $\det M = \det M'$. A este determinante lo llamaremos *determinante* de E, y lo representaremos por $\det E$. En particular, si calculamos el determinante de E mediante una base de Frobenius de R, vemos que $\det E = d_1^2 \cdots d_g^2$. Así pues, $\det E$ es un cuadrado perfecto.

Notemos también que si $e_1, v_1, \ldots, e_g, v_g$ es una base de Frobenius de R, entonces $e_1, \ldots, e_g$ es una $\mathbb{C}$-base de V. En efecto, basta ver que son linealmente independientes sobre $\mathbb{C}$. Si $\lambda_1 e_1 + \cdots + \lambda_g e_g = 0$, para ciertos $\lambda_i = a_i + ib_i \in \mathbb{C}$, tomamos $z = a_1 e_1 + \cdots a_g e_g$, $w = b_1 e_1 + \cdots + b_g e_g$, de modo que $z + iw = 0$. Entonces,

$$S(w, w) = E(iw, w) = E(-z, w) = 0,$$

pues $E(e_i, e_j) = 0$ para todo i, j. Como S es definida positiva, ha de ser $w = 0$, luego también $z = 0$, de donde concluimos que todos los λ_i son nulos. ■

Finalmente estamos en condiciones de probar la existencia de funciones zeta no triviales:

Partamos de dos funciones $L : V \times R \longrightarrow \mathbb{C}$ y $K : V \longrightarrow \mathbb{R}$ tales que L sea $\mathbb{C}$-lineal en la primera variable y $\mathbb{R}$-lineal en la segunda, mientras que K es $\mathbb{R}$-lineal. Supongamos que la función E dada por (4.5) es una forma de Riemann en V respecto a R. Llamaremos $\Theta_R(L, K)$ al conjunto formado por la función nula en V más todas las funciones zeta en V respecto a R que cumplen (4.4) con estas L y K. Es claro que se trata de un espacio vectorial sobre $\mathbb{C}$.

Teorema 4.45 *En las condiciones anteriores:* $\dim \Theta_R(L, K) = \sqrt{\det E}$.

Demostración: Fijamos una base de Frobenius de R respecto de E y sea $W = \langle e_1, \ldots, e_g \rangle_{\mathbb{R}}$. Como E es nula sobre W, vemos que L es simétrica en W. Como $e_1, \ldots, e_g$ es una $\mathbb{C}$-base de V, podemos tomar una forma bilineal simétrica $B : V \times V \longrightarrow \mathbb{C}$ que coincida con L sobre W. Tomemos también la forma lineal $\lambda : V \longrightarrow \mathbb{C}$ dada por $\lambda(e_i) = K(e_i)$.

Si G es la función zeta trivial determinada por $-B$ y por $-\lambda$, tenemos que la multiplicación por G determina un isomorfismo de espacios vectoriales

$$\Theta_R(L, K) \longrightarrow \Theta_R(L - B, K - \lambda),$$

y la función $L - B$ da lugar a la misma forma E. Así pues, no perdemos generalidad si suponemos que L es nula en $W \times W$ y que K es nula en W.

Como L es $\mathbb{C}$-lineal en su primera componente y $e_1, \ldots, e_g$ es una $\mathbb{C}$-base de V, vemos que $L(z, e_j) = 0$ para todo $z \in V$. Así pues, (4.4) implica que toda $F \in \Theta_R(L, K)$ cumple $F(z + e_j) = F(z)$.

Por otra parte, si $d_j = E(e_j, v_j)$ y $c_j = \frac{1}{2} L(v_j, v_j) + K(v_j)$, para cada $z = z_1 e_1 + \cdots + z_g e_g$ tenemos que

$$L(z, v_j) = \sum_k z_k L(e_k, v_j) = \sum_k z_k (E(e_k, v_j) + L(v_j, e_k)) = z_j d_j,$$

luego

$$F(z + v_j) = F(z)\exp(2\pi i(z_j d_j + c_j)).$$

En definitiva, tenemos que $\Theta_R(L, K)$ es el espacio formado por la función nula en V y las funciones $F \in \mathcal{H}(V)$ que satisfacen las relaciones:

$$F(z + e_j) = F(z), \qquad F(z + v_j) = F(z)e^{2\pi i(z_j d_j + c_j)}, \tag{4.9}$$

donde $c_j \in \mathbb{C}$ y los $d_j = E(e_j, v_j)$. Hemos de probar que la dimensión de este espacio es $d_1 \cdots d_g$.

No perdemos generalidad si suponemos que $V = \mathbb{C}^g$ y que $e_1, \ldots, e_g$ es la base canónica. Así, toda función $F \in \Theta_R(L, K)$ no nula tiene periodo 1 en cada variable. Si $w \in \mathbb{C}^g$ no tiene ninguna coordenada nula y $w_i = e^{2\pi i z_i}$, entonces z_i está determinado módulo $\mathbb{Z}$, pero $f(w_1, \ldots, w_g) = F(z_1, \ldots, z_g)$ es independiente de la elección de los logaritmos z_i. Puesto que podemos definir logaritmos holomorfos en sendos entornos de los w_i, es claro que la función f así definida es holomorfa y, para cada $z \in \mathbb{C}^g$, se cumple que

$$F(z) = f(e^{2\pi i z_1}, \ldots, e^{2\pi i z_g}).$$

El teorema 1.55 nos da un desarrollo en serie de Laurent para la función f convergente en todo $\mathbb{C}^n$ menos donde alguna variable se anula. Equivalentemente, tenemos un desarrollo de F en serie de Fourier:

$$F(z) = \sum_{m \in \mathbb{Z}^g} a_m e^{2\pi i\, mz},$$

donde $mz = m_1 z_1 + \cdots + m_g z_g$. En estos términos, la segunda condición de (4.9) se traduce en que

$$\sum_{m \in \mathbb{Z}^g} a_m e^{2\pi i m v_j} e^{2\pi i\, mz} = \sum_{m \in \mathbb{Z}^g} a_m e^{2\pi i c_j} e^{2\pi i((m + d_j e_j)z)}.$$

La unicidad de los desarrollos en serie de Laurent se traduce en la unicidad de los coeficientes de Fourier, por lo que concluimos que

$$a_m = a_{m - d_j e_j} e^{2\pi i(c_j - m v_j)}. \tag{4.10}$$

De aquí se sigue que los coeficientes a_m están completamente determinados por los correspondientes a los multiíndices m tales que $0 \leq m_j < d_j$. Sólo falta probar que cualquier elección de estos coeficientes da lugar a una serie de Fourier convergente en todo $\mathbb{C}^g$. Eso demostrará que la dimensión de $\Theta_R(L, K)$ es $d_1 \cdots d_g$, como queremos probar.

Por linealidad podemos fijar un multiíndice m_0 tal que $0 \leq m_{0j} < d_j$ y considerar la serie dada por los coeficientes a_m que cumplen (4.10) con $a_{m_0} = 1$ y $a_m = 0$ para todos los demás multiíndices m que cumplen $0 \leq m_j < d_j$. Esto hace que $a_m \neq 0$ si y sólo si $m_j \equiv m_{0j}$ (mód d_j) para todo j. Para estos multiíndices podemos hacer $a_m = e^{2\pi i g(m)}$, de modo que (4.10) equivale a

$$g(m - d_j e_j) - g(m) = m v_j - c_j. \tag{4.11}$$

En realidad no deberíamos haber escrito una igualdad, sino una congruencia módulo $\mathbb{Z}$, pero si encontramos una función $g : \mathbb{Z}^g \longrightarrow \mathbb{C}$ que cumpla (4.11) y $g(m_0) = 0$, entonces los coeficientes

$$a_m = \begin{cases} e^{2\pi i g(m)} & \text{si } m_j \equiv m_{0j} \text{ (mód } d_j) \text{ para todo } j, \\ 0 & \text{en otro caso,} \end{cases}$$

son los únicos que cumplen (4.10) con $a_{m_0} = 1$ y $a_m = 0$ para todo $m \neq m_0$ tal que $0 \leq m_j < d_j$.

Notemos que la existencia de g es trivial, lo que necesitamos es determinarla de forma explícita (no recursiva) para estudiar la convergencia de la serie de Laurent definida por los coeficientes a_m.

Para ello consideramos la forma bilineal $T : V \times V \longrightarrow \mathbb{C}$ determinada por que $T(e_i, e_j)$ es la coordenada i-ésima de v_j/d_j (en la base canónica $e_1, \ldots, e_g$). Así,

$$v_j = d_j \sum_i T(e_i, e_j) e_i$$

y, recordando que, según hemos visto, $L(z, e_j) = 0$ para todo $z \in V$, resulta que

$$\begin{aligned} L(v_j, v_k) &= d_j \sum_i T(e_i, e_j) T(e_i, e_j) L(e_i, v_k) \\ &= d_j \sum_i T(e_i, e_j) T(e_i, e_j) E(e_i, v_k) = d_j T(e_k, e_j) d_k. \end{aligned} \tag{4.12}$$

Por otra parte, como $E(v_j, v_k) = 0$, resulta que $L(v_j, v_k) = L(v_k, v_j)$, y esto implica a su vez que $T(e_i, e_j) = T(e_j, e_i)$ o, lo que es lo mismo, que la forma bilineal T es simétrica.

Teniendo esto en cuenta, es fácil probar que la función

$$g(m) = -\frac{1}{2} T(m, m) - \frac{1}{2} m v_j + \sum_j \frac{m_j c_j}{d_j} + c,$$

donde $c \in \mathbb{C}$ es la constante que hace que $g(m_0) = 0$, cumple la relación (4.11). Así pues,

$$g(m) = -\frac{1}{2} T(m, m) - \frac{\lambda(m)}{2\pi} + c,$$

donde $\lambda : \mathbb{C}^g \longrightarrow \mathbb{C}$ es una aplicación lineal. Por consiguiente,

$$|e^{2\pi i g(m)}| = |e^{2\pi i c}| e^{\pi \operatorname{Im} T(m,m) + \operatorname{Im} \lambda(m)}.$$

Teniendo en cuenta que a_m puede ser nulo, para un m arbitrario tenemos la desigualdad

$$|a_m| \leq C e^{\pi \operatorname{Im} T(m,m) + \lambda'(m)},$$

donde $\lambda' : \mathbb{R}^g \longrightarrow \mathbb{R}$ es una aplicación lineal. Veamos ahora que $\operatorname{Im} T(v, v) < 0$ para todo $z \in \mathbb{R}^g$ no nulo. En efecto, consideremos $w = \sum (z_j/d_j) v_j \in V$. Usando (4.12) vemos que

$$T(z, z) = \sum_{j,k} z_j z_k T(e_j, e_k) = \sum_{j,k} \frac{z_j z_k}{d_j d_k} L(v_j, v_k) = L(w, w).$$

Descompongamos $w = x + iy$, donde x, y tienen coordenadas reales. No puede ser $y = 0$, pues en tal caso $w \in \langle e_1, \ldots, e_g\rangle_{\mathbb{R}} \cap \langle v_1, \ldots, v_g\rangle_{\mathbb{R}} = 0$. Además,

$$L(w, w) = L(x, w) + iL(y, w),$$

y $L(x, w), L(y, w) \in \mathbb{R}$, ya que $L(e_i, v_j) = E(e_i, v_j) \in \mathbb{Z}$. Por consiguiente, lo que hemos de probar es que $L(y, w) < 0$, lo cual se debe a que

$$0 < E(iy, y) = E(x + iy, y) = E(w, y) = L(w, y) - L(y, w) = -L(y, w).$$

En resumen, tenemos que $|a_m| \leq Ce^{q(m)+cm}$, donde $q : \mathbb{R}^g \longrightarrow \mathbb{R}$ es una forma cuadrática definida negativa y $c \in \mathbb{R}^g$.

Hemos de probar que la serie de Laurent con coeficientes a_m converge en todos los puntos de $\mathbb{C}^g$ de coordenadas no nulas. Esto equivale a probar que, para cada vector de signos ϵ, la serie de potencias con coeficientes $a'_m = a_{\epsilon_1 m_1,\ldots,\epsilon_g m_g}$ (para $m_i \geq 0$) converge en $\mathbb{C}^g$. Es claro que los coeficientes a'_m cumplen una cota análoga a la que hemos obtenido para los a_m (cambiando $q(m)$ por $q'(m) = q(\epsilon_1 m_1, \ldots, \epsilon_g m_g)$, que es también una forma cuadrática definida negativa). Equivalentemente, hemos de probar que la serie

$$\sum_{m\in\mathbb{N}^g} a_m z_1^{m_1} \cdots z_g^{m_g}$$

converge en $\mathbb{C}^g$, sabiendo que $|a_m| \leq Ce^{q(m)+cm}$ con q definida negativa y $c \in \mathbb{R}^g$. A su vez, para esto basta probar que la serie converge absolutamente en $z = (e^r, \ldots, e^r)$, para todo $r > 0$, es decir, hemos de probar la convergencia de

$$\sum_{m\in\mathbb{N}^g} |a_m| e^{rm_1+\cdots+rm_g} \leq C \sum_{m\in\mathbb{N}^g} e^{q(m)+c'm},$$

donde $c'_i = c + r$. Si $c'' = (1, \ldots, 1)$, observamos que la función

$$f(x) = -\frac{(c' + c'')x}{q(x)}$$

es continua en la esfera unidad de $\mathbb{R}^g$, luego está acotada por un $M > 0$. Así, para todo x tal que $\|x\| > M$, se cumple que

$$|f(x)| = \frac{|f(x/\|x\|)|}{\|x\|} < 1.$$

Por consiguiente, para todo multiíndice $m \in \mathbb{N}^g$ salvo a lo sumo un número finito de ellos, tenemos que $q(m) + c'm < -c''m$, luego la serie está mayorada por

$$C \sum_{m\in\mathbb{N}^g} e^{-m_1-\cdots-m_g} = C\left(\sum_{m=0}^{\infty} e^{-m}\right)^g = \frac{C}{(1 - e^{-1})^g}.$$

■

En el teorema anterior hemos partido de dos funciones L y K. Ahora bien, si partimos de una forma de Riemann E y definimos H mediante (4.6) y L

mediante (4.7), entonces la forma E definida por L mediante (4.5) es la E de la que hemos partido. Por consiguiente, la construcción de funciones zeta que acabamos de realizar requiere únicamente la existencia de una forma de Riemann en V respecto de R (como función K sirve cualquiera).

En particular, la existencia de funciones zeta no degeneradas en un espacio V respecto de un retículo R es equivalente a la existencia de una forma de Riemann en V respecto de R.

Supongamos ahora que tenemos dos retículos $R \subset R' \subset V$ y unas funciones L y K tales que la forma E correspondiente a L sea una forma de Riemann respecto de R' (lo que equivale a que sea una forma de Riemann respecto de R y que tome valores enteros sobre R'). Es claro entonces que $\Theta_{R'}(L,K) \subset \Theta_R(L,K)$.

Podemos tomar[9] una base $v_1,\ldots,v_{2g}$ de R' tal que $k_1v_1,\ldots,k_{2g}v_{2g}$ sea una base de R, para ciertos $k_i \in \mathbb{Z}$. Claramente $|R':R| = k_1\cdots k_{2g}$. Calculando el determinante de E con estas bases es claro que $\det_R E = |R':R|^2 \det_{R'} E$, luego el teorema anterior nos da que

$$\dim \Theta_R(L,K) = |R':R| \dim \Theta_{R'}(L,K).$$

En particular vemos que si $R \subsetneq R'$, entonces $\Theta_{R'}(L,K) \subsetneq \Theta_R(L,K)$.

Notemos ahora que, fijados V, R, L y K de modo que la forma E asociada a L sea una forma de Riemann respecto de R, sólo puede haber un número finito de retículos R' por encima de R tales que E sea una forma de Riemann respecto de R'. En efecto, si fijamos una base de Frobenius $e_1,v_1,\ldots,e_g,v_g$ de R respecto de E, cada $r' \in R'$ se expresa como

$$r' = a_1e_1 + b_1v_1 \cdots + a_ge_g + b_gv_g,$$

con $a_i, b_i \in \mathbb{R}$. Entonces $E(r',e_j) = -b_jd_j$ y $E(r',v_j) = a_jd_j$ son enteros, luego las coordenadas a_j, b_j de r' son números racionales de la forma $u_j/d_j, v_j/d_j$. Si llamamos $d = d_1\cdots d_g$, vemos que $R \subset R' \subset \frac{1}{d}R$ y, como $|\frac{1}{d}R : R|$ es finito, sólo hay un número finito de retículos intermedios.

Más aún, fijado un retículo R', recordemos que si sustituimos K por otra función K' tal que $K'|_R \equiv K|_R$ (mód $\mathbb{Z}$), el espacio $\Theta_R(L,K)$ no varía, pero esto nos permite considerar distintos espacios $\Theta_{R'}(L,K')$. Vamos a ver, no obstante, que sólo hay un número finito de posibilidades. En efecto, K' está determinada por los valores que toma sobre una base de R'. Si r' es un miembro de dicha base, hemos visto antes que $dr' \in R$, luego $K'(dr') = K(dr') + u$, para un cierto $u \in \mathbb{Z}$. Equivalentemente,

$$K'(r') = \frac{K(dr')}{d} + \frac{u}{d},$$

donde sólo podemos elegir el entero u, pero si sustituimos u por su resto módulo d (para cada vector de la base) obtenemos una nueva función K'' que cumple $K''|_{R'} \equiv K'|_{R'}$ (mód $\mathbb{Z}$), luego sólo hay un número finito de funciones K' que definan espacios $\Theta_{R'}(L,K')$ distintos. En conclusión:

[9] Ver el teorema 7.30 de mi libro de *Álgebra*.

Teorema 4.46 *Sea V un espacio vectorial complejo, sea R un retículo en V, sea $L : V \times V \longrightarrow \mathbb{C}$ una función $\mathbb{C}$-lineal en la primera variable y $\mathbb{R}$-lineal en la segunda, sea $K : V \longrightarrow \mathbb{R}$ una función $\mathbb{R}$-lineal y supongamos que la forma E asociada a L sea una forma de Riemann respecto de R. Entonces existen funciones en $\Theta_R(L, K)$ que no pertenecen a ningún espacio $\Theta_{R'}(L, K')$ para ningún retículo $R \subsetneq R' \subset V$ y ninguna K' tal que $K'|_R \equiv K|_R$ (mód $\mathbb{Z}$).*

DEMOSTRACIÓN: Acabamos de probar que hay un número finito de espacios $\Theta_{R'}(L, K')$ y que todos ellos están estrictamente contenidos en $\Theta_R(L, K)$. Un espacio vectorial no puede expresarse como unión de un número finito de subespacios propios. (Por ejemplo, porque un espacio vectorial complejo es una variedad algebraica irreducible.) ■

Necesitamos discutir ahora las traslaciones de funciones zeta:

Definición 4.47 Si F es una función zeta en un espacio V respecto a un retículo R y $a \in V$, definimos la *traslación* F_a como la función dada por $F_a(z) = F(z-a)$.

Se trata de una función zeta, pues

$$F_a(z + r) = F(z - a + r) = F(z - a) + \exp(2\pi i(L(z - a, r) + \frac{1}{2}L(r, r) + K(r)))$$

$$= F_a(z) \exp(2\pi i(L(z, r) + \frac{1}{2}L(r, r) - L_a(r) + K(r))),$$

donde $L_a(r) = L(a, r)$, de modo que F_a cumple la definición de función zeta con la misma función L que F y con $J'(r) = \frac{1}{2}L(r, r) - L_a(r) + K(r)$.

Si F está normalizada, la traslación F_a no lo está necesariamente, sino que cumple

$$F_a(z + r) = F_a(z) \exp(2\pi i(-\frac{i}{2} H(z, r) - \frac{i}{4} H(r, r) + K(r) + \frac{i}{2}H_a(r))).$$

Estaría normalizada si la función $(i/2)H_a$ tomara únicamente valores reales. Por consiguiente, para normalizar F_a basta multiplicarla por la función zeta trivial $\exp(2\pi i(-\frac{i}{2}H(z, a)))$. Esto suma al exponente el término $2\pi i(-\frac{i}{2}\overline{H_a(r)})$ y la nueva función K pasa a ser $K - E_a$.

Necesitamos estudiar el conjunto de los puntos $a \in V$ tales que F y F_a son equivalentes, es decir, tales que F_a/F es una función zeta trivial:

Teorema 4.48 *Sea F una función zeta no degenerada en un espacio V respecto a un retículo R. Sea E su forma de Riemann asociada. Si $a \in V$ cumple que F_a es equivalente a F, entonces $E_a(w) = E(a, w)$ toma valores enteros en R. Además, el conjunto de los $[a] \in V/R$ tales que E_a cumple esto es un subgrupo finito de orden* $\det E$.

Demostración: Supongamos que $F_a(z) = F(z)g(z)$, para una cierta función zeta trivial $g(z) = e^{2\pi i(q(z)+\lambda(z)+c)}$. Entonces

$$\frac{F_a(z+r)}{F(z+r)} = \frac{F_a(z)}{F(z)} e^{2\pi i L(-a,r)}$$

y, por otra parte, esto es igual a

$$g(z+r) = g(z)e^{2\pi i(2b(z,r)+b(r,r)+\lambda(r))},$$

donde b es la forma bilineal simétrica asociada a la forma cuadrática q. Por lo tanto:

$$e^{2\pi i L(-a,r)} = e^{2\pi i(2b(z,r)+b(r,r)+\lambda(r))}.$$

Haciendo $z = 0$ queda $e^{2\pi i L(-a,r)} = e^{2\pi i(b(r,r)+\lambda(r))}$, luego $e^{2\pi i 2b(z,r)} = 1$. Esto implica que $2b(z,r) \in \mathbb{Z}$ para todo z, lo cual es imposible salvo si $b = 0$.

Nos queda entonces que $e^{2\pi i L(-a,r)} = e^{2\pi i(\lambda(r))}$, luego

$$\lambda(r) = L(-a,r) + m(r) = L(r,-a) + E(-a,r) + m(r)$$

para una cierta función $m : R \longrightarrow \mathbb{Z}$. Despejándola en la igualdad anterior vemos que se extiende a una aplicación $\mathbb{R}$-lineal $m : V \longrightarrow \mathbb{R}$. (El hecho de que sea lineal y tome valores enteros sobre R implica que la extensión toma valores en $\mathbb{R}$.) Tenemos, pues, que

$$\lambda(z) - L(z,-a) = E(-a,z) + m(z),$$

pero el miembro izquierdo es $\mathbb{C}$-lineal en z y el miembro derecho toma valores en $\mathbb{R}$. Esto sólo puede ser si ambos miembros son nulos. Por lo tanto llegamos a que $\lambda(z) = L(z,-a)$ y $E(a,z) = m(z)$. En particular E_a toma valores enteros sobre R.

Consideremos ahora una base de Frobenius $e_1, v_1, \ldots, e_g, v_g$ de R respecto de E. Dado un $a \in V$ lo expresamos como

$$a = a_1e_1 + b_1v_1 \cdots + a_ge_g + b_gv_g,$$

con $a_i, b_i \in \mathbb{R}$. Entonces $E(a, e_j) = -b_jd_j$ y $E(a, v_j) = a_jd_j$ son enteros si y sólo si las coordenadas a_j, b_j de a son números racionales de la forma $u_j/d_j, v_j/d_j$. Es claro entonces que, módulo R, hay únicamente $\det R = d_1^2 \cdots d_g^2$ puntos a posibles. ■

Definición 4.49 Si F es una función zeta normalizada no degenerada en un espacio V respecto de un retículo R, llamaremos $\mathcal{L}(F)$ al espacio vectorial de las funciones zeta que cumplen (4.8) con las mismas H y K.

Hemos visto que (4.8) determina la forma H, y esto a su vez implica que $e^{2\pi i K(r)}$ está unívocamente determinada, por lo que cambiar K por otra función con la que F cumpla también (4.8) no altera a $\mathcal{L}(F)$. También sabemos que $\mathcal{L}(F) = \Theta_R(H, K)$ es un espacio vectorial de dimensión finita.

Finalmente estamos en condiciones de estudiar la inmersión de un toro complejo $T = V/R$ en un espacio proyectivo. Sea $p : V \longrightarrow T$ la proyección canónica y, para cada función zeta F en V respecto a R, consideremos su conjunto de ceros

$$Z_F = \{[z] \in T \mid F(z) = 0\}.$$

Ya hemos comentado que la definición de función zeta hace que la condición $F(z) = 0$ sólo dependa de la clase de z en T. Es claro que $Z_F \subsetneq T$ es cerrado, así como que $Z_{FG} = Z_F \cup Z_G$. En particular T no puede cubrirse por un número finito de conjuntos Z_F.

Supongamos que F es una función zeta no degenerada en V respecto de R y sea $F_0, \ldots, F_m$ una base del espacio $\mathcal{L}(F)$. Sea $U = T \setminus \bigcap\limits_i Z_{F_i}$. Podemos definir una aplicación $f : U \longrightarrow \mathrm{P}^m$ mediante

$$f([z]) = (F_0(z), \ldots, F_m(z)).$$

La clave está en que si sumamos a z un elemento de R todas las funciones $F_i(z)$ se multiplican por el mismo factor no nulo, luego definen el mismo punto de P^m. Observemos que $[z] \in U$ si y sólo si existe una $G \in \mathcal{L}(F)$ tal que $G(z) \neq 0$.

Observemos que la aplicación f es holomorfa en U. En efecto, dado $[z_0] \in U$, existe un i tal que $F_i(z) \neq 0$. Pongamos, por ejemplo que $F_0(z_0) \neq 0$. Esto significa que $f([z_0]) \in A^m$, y la lectura de f en una carta de T formada por una inversa local de p y la carta de P^m formada por las coordenadas afines en A^m es

$$z \mapsto \left(\frac{F_1(z)}{F_0(z)}, \ldots, \frac{F_m(z)}{F_0(z)} \right). \tag{4.13}$$

Las funciones F_i/F_0 son holomorfas en un entorno de z_0, luego f es holomorfa en z_0. Vamos a ver que, eligiendo adecuadamente la función F de partida, podemos demostrar que f cumple las propiedades siguientes:

a) f está definida en todo T.

b) f es inyectiva.

c) Para cada $P \in T$, la diferencial $df_P : T_P T \longrightarrow T_P\, \mathrm{P}^m$ es inyectiva.

Admitiendo esto, como T es compacto resulta que f es un homeomorfismo en su imagen $T' = f[T]$, y f dota a $T' \subset \mathrm{P}^m$ de una estructura de variedad analítica conformemente equivalente a T. La inclusión $i : T' \longrightarrow \mathrm{P}^m$ es holomorfa, pues se descompone como $f^{-1} : T' \longrightarrow T$ (que es una transformación conforme) seguida de $f : T \longrightarrow \mathrm{P}^m$, que es holomorfa, y del mismo modo concluimos que, para cada punto $P' = f(P) \in T'$, la diferencial $di_{P'} : T_{P'}T' \longrightarrow T_{P'}\, \mathrm{P}^m$ es inyectiva. En resumen, llegamos a que T' es una subvariedad de P^m y, por lo tanto, a que T es conformemente equivalente a una subvariedad de P^m.

Según hemos indicado, para que se cumplan las propiedades a), b) y c) es necesario elegir F adecuadamente. En realidad basta sustituir F por F^3. Observemos que si F es una función zeta no degenerada, asociada a una forma de Riemann E, entonces F^3 es también una función zeta no degenerada asociada a la forma $3E$. En lo sucesivo suponemos, pues, que $F_0, \ldots, F_m$ es una base de $\mathcal{L}(F^3)$.

Empezamos probando que $U = T$. Para ello vemos que si a, $b \in V$, entonces $F_a F_b F_{-a-b} \in \mathcal{L}(F^3)$. En efecto, si F cumple (4.4) con unas funciones L y K, entonces los tres factores cumplen la definición de función zeta con exponentes

$$L(z,r) + \frac{1}{2}L(r,r) + K(r) - L_a(r),$$

$$L(z,r) + \frac{1}{2}L(r,r) + K(r) - L_b(r),$$

$$L(z,r) + \frac{1}{2}L(r,r) + K(r) + L_{a+b}(r),$$

respectivamente, luego el producto de los tres cumple (4.4) con las funciones $3L$ y $3K$, que son las correspondientes a la función F^3. Así pues, para probar que $U = T$ basta ver que para todo $z \in V$ existen a, $b \in V$ tales que $F_a(z)F_b(z)F_{-a-b}(z) \neq 0$.

Notemos que si G es una función zeta, también lo es la función dada por $G^-(z) = G(-z)$. Teniendo esto en cuenta, basta elegir $a \in V$ que no anule a $(F^-)_z$, con lo que $F_a(z) \neq 0$, y luego elegimos otro $b \in V$ que no anule a $(F^-)_b((F^-)_{z+a})^-$, con lo que $F_b(z)F_{-a-b}(z) \neq 0$.

Veamos ahora que f es inyectiva. Para ello suponemos que z, $w \in V$ cumplen que $f([z]) = f([w])$. Entonces existe un $\gamma \in \mathbb{C}$ no nulo tal que $F_i(z) = \gamma F_i(w)$, luego de hecho $G(z) = \gamma G(w)$ para todo $G \in \mathcal{L}(F^3)$. Si $G \in \mathcal{L}(F)$ y a, $b \in V$, entonces $G_a G_b G_{-a-b} \in \mathcal{L}(F^3)$, luego

$$G(z-a)G(z-b)G(z+a+b) = \gamma G(w-a)G(w-b)G(w+a+b).$$

Razonando como en la prueba de a), para cualquier $b_0 \in V$ podemos encontrar un $a \in V$ tal que

$$G(z-a)G(z+a+b_0)G(w-a)G(z+a+b_0) \neq 0.$$

Esta desigualdad sigue cumpliéndose para todo b en un entorno de b_0. En dicho entorno, definimos

$$g_0(b) = \frac{\gamma G(w-a)G(w+a+b)}{G(z-a)G(z+a+b)},$$

de modo que g_0 es una función holomorfa en un entorno de b_0 que no se anula en ningún punto (de dicho entorno) y tal que

$$G(z-b) = G(w-b)g_0(b).$$

Esta relación implica que dos de estas funciones g_0 (para distintos b_0) han de coincidir en su dominio común, luego se extienden a una misma función $g \in \mathcal{H}(V)$ sin ceros tal que

$$G(z-b) = G(w-b)g(b)$$

para todo $b \in V$. Si llamamos $v = z - w$ y cambiamos b por $w - b$, esto equivale a

$$G(b+v) = G(b)h(b), \tag{4.14}$$

donde $h(b) = g(w-b)$ es también una función holomorfa en V sin ceros. Notemos que para cada $r \in R$ se cumple

$$h(b+r) = \frac{G(b+v+r)}{G(b+r)} = h(b)e^{2\pi i L(v,r)}, \tag{4.15}$$

luego h es una función zeta trivial. Puesto que $G_{-v} = Gh$, el teorema 4.48 nos da que E_v toma valores enteros en R. Más aún, en la prueba hemos visto que $h(b) = e^{2\pi i(\lambda(b)+c)}$, donde $\lambda(b) = L(b,v)$, así como que, fijada una base de Frobenius de R respecto de E, el vector v tiene coordenadas racionales. Si $s \in \mathbb{N}$ es un múltiplo de los denominadores de dichas coordenadas, tenemos que $R' = R + \mathbb{Z}v \subset \frac{1}{s}R$ y, como $\frac{1}{s}R$ es obviamente un retículo en V, vemos que R' también lo es.

Recordemos que $v = z - w$ y, por lo tanto, lo que queremos demostrar es que $v \in R$. Si no es así, tenemos una inclusión estricta $R \subsetneq R'$. La ecuación (4.14) es ahora

$$G(b+v) = G(b)e^{2\pi i(L(b,v)+c)},$$

lo que implica, más en general, que

$$G(b+r+kv) = G(b)e^{2\pi i(L(b,r+kv)+J(r)+kc)},$$

para todo $k \in \mathbb{Z}$, donde $J : R \longrightarrow \mathbb{C}$ es la función con la que G cumple la definición de función zeta. Por consiguiente, si para cada $r' \in R' \setminus R$ elegimos una representación $r' = r + kv$, con $r \in R$ y $k \in \mathbb{Z}$, y definimos $J'(r') = J(r) + kc$ (y definimos $J'(r) = J(r)$ para $r \in R$), tenemos que G es una función zeta respecto de R' con las funciones L y J'. El teorema 4.39 nos permite modificar J' módulo $\mathbb{Z}$ de modo que la función $K'(r') = J'(r') - \frac{1}{2}L(r',r')$ se extienda a una función $\mathbb{R}$-lineal $K' : V \longrightarrow \mathbb{R}$. Entonces $K'|_R \equiv K|_R$ (mód $\mathbb{Z}$).

Así hemos probado que toda función $G \in \mathcal{L}(F) = \Theta_R(L,K)$ pertenece también a un espacio $\Theta_{R'}(L,K')$, para una cierta función K' congruente con K módulo $\mathbb{Z}$ sobre R. Esto contradice al teorema 4.46, luego ha de ser $v \in R$ y, por consiguiente, f es inyectiva.

Nos falta probar que, para cada $P \in T$, la diferencial df_P es inyectiva. Sea $P = [w]$ y supongamos, sin pérdida de generalidad, que $F_0(w) \neq 0$. Entonces df_P se corresponde, a través de los isomorfismos determinados por las diferenciales de cartas de T y P^m, con la diferencial de su lectura en tales cartas. Si elegimos las cartas adecuadamente, dicha lectura es (4.13).

Hemos de ver que, para todo $v \in T_wV$ no nulo, se cumple $d(F_i/F_0)_w(v) \neq 0$ para algún $i = 1, \ldots, m$. Ahora bien, basta encontrar una función $G \in \mathcal{L}(F^3)$ tal que $d(G/F_0)_w(v) \neq 0$, ya que dicha G se expresará como combinación lineal de las F_i (con algún coeficiente no nulo correspondiente a un índice $i > 0$, pues de lo contrario G/F_0 sería constante y tendría diferencial nula) y $d(G/F_0)_w$ será también combinación lineal de las $d(F_i/F_0)_w$, luego una de éstas no se anulará en v.

Más en general, vamos a probar que si $H \in \mathcal{L}(F^3)$ cumple que $H(w) \neq 0$ y $v \in T_wV$ no nulo, entonces existe otra $G \in \mathcal{L}(F^3)$ tal que $d(G/H)_w(v) \neq 0$. A través de un sistema de coordenadas, podemos identificar V y T_wV con $\mathbb{C}^g$. Eligiéndolo adecuadamente, podemos suponer que $v = (1, 0 \ldots, 0)$.

Supongamos, por reducción al absurdo, que $d(G/H)_w(v) = 0$ para toda $G \in \mathcal{L}(F^3)$. Tenemos que

$$d(G/H)_w = \frac{H(w)dG_w - G(w)dH_w}{H(w)^2},$$

luego, para todo G que cumpla además $G(w) \neq 0$, tenemos que

$$\frac{dG_w(v)}{G(w)} = \frac{dH_w(v)}{H(w)}.$$

Llamemos $\alpha \in \mathbb{C}$ a este valor independiente de G. Como $v = (1, 0, \ldots, 0)$, vemos que

$$\frac{dG_w(v)}{G(w)} = \frac{1}{G(w)} \left.\frac{\partial G}{\partial z_1}\right|_w = \alpha. \tag{4.16}$$

Tomemos a, $b \in \mathbb{C}^g$ y consideremos

$$G(z) = F(z-a)F(z-b)F(z+a+b),$$

que, como ya sabemos, cumple $G \in \mathcal{L}(F)$. Además, podemos elegir a y b tales que $G(w) \neq 0$. Más aún, si consideramos a $G(w)$ como una función holomorfa de (a, b), es claro que existe un abierto $U \times V \subset \mathbb{C}^g \times \mathbb{C}^g$ donde $G(w) \neq 0$. Si llamamos

$$u(z) = \frac{1}{F(z)} \frac{\partial F}{\partial z_1},$$

al calcular (4.16) obtenemos la relación

$$u(w-a) + u(w-b) + u(w+a+b) = \alpha.$$

Considerando el miembro izquierdo como función (constante) de a en U, sus derivadas parciales deben ser nulas, es decir,

$$-\left.\frac{\partial u}{\partial z_j}\right|_{w-a} + \left.\frac{\partial u}{\partial z_j}\right|_{w+a+b} = 0$$

o, equivalentemente,

$$\left.\frac{\partial u}{\partial z_j}\right|_{w-a} = \left.\frac{\partial u}{\partial z_j}\right|_{w+a+b}.$$

Ahora bien, esto vale para todo $b \in V$, lo que significa que el miembro derecho es constante cuando $a \in U$. Equivalentemente, las derivadas de u son constantes en un cierto abierto. En dicho abierto,

$$u(z) = \frac{1}{F(z)} \frac{\partial F}{\partial z_1} = \alpha_1 z_1 + \cdots + \alpha_g z_g + \beta,$$

para ciertos α_i, $\beta \in \mathbb{C}$. Sea

$$q(z) = \frac{1}{2}\alpha_1 z_1^2 + \alpha_2 z_1 z_2 + \cdots + \alpha_g z_1 z_g + \beta z_1$$

y sea $F^*(z) = F(z)e^{-q(z)}$. La exponencial es una función zeta trivial, luego F^* es una función zeta no degenerada. Notemos que

$$\frac{\partial F^*}{\partial z_1} = \frac{\partial F}{\partial z_1} e^{-q(z)} - F(z)e^{-q(z)} \frac{\partial q}{\partial z_1}$$

$$= e^{-q(z)} F(z) \left(u(z) - \alpha_1 z_1 - \cdots - \alpha_g z_g - \beta\right) = 0$$

en un cierto abierto, luego en todo $\mathbb{C}^g$.

Esto quiere decir que F^* no depende de la variable z_1, pero entonces resulta que $F^*_{(\lambda,0,\ldots,0)} = F^*$ para todo $\lambda \in \mathbb{C}$, lo que contradice al teorema 4.48.

Con esto hemos demostrado el teorema siguiente:

Teorema 4.50 (Lefschetz) *Si $T = V/R$ es un toro complejo tal que existe una forma de Riemann en V respecto del retículo R, entonces T es conformemente equivalente a una subvariedad analítica de un espacio proyectivo complejo.*

Puede probarse que la existencia de la forma de Riemann no sólo es suficiente, sino también necesaria, pero no vamos a entrar en ello.

Capítulo V

Cuerpos métricos

En los capítulos siguientes veremos que en el estudio de las curvas algebraicas pueden usarse fructíferamente las técnicas de la teoría algebraica de números. En este capítulo desarrollaremos los preliminares necesarios.

5.1 Valores absolutos

Definición 5.1 Un *valor absoluto* en un cuerpo K es una aplicación

$$|\ \ | : K \longrightarrow [0, +\infty[$$

que cumpla las propiedades siguientes:

a) $|\alpha| = 0$ si y sólo si $\alpha = 0$,

b) $|\alpha + \beta| \leq |\alpha| + |\beta|$,

c) $|\alpha\beta| = |\alpha||\beta|$.

Es obvio que el valor absoluto usual en $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es un valor absoluto en el sentido de la definición anterior. En general, la restricción de un valor absoluto a un subcuerpo es un valor absoluto en dicho subcuerpo. Por otro lado todo cuerpo K admite al menos un valor absoluto: el llamado *valor absoluto trivial,* dado por

$$|\alpha|_0 = \begin{cases} 0 & \text{si } \alpha = 0 \\ 1 & \text{si } \alpha \neq 0 \end{cases}$$

Las propiedades a) y c) de la definición de valor absoluto afirman que todo valor absoluto en un cuerpo K es un homomorfismo entre el grupo multiplicativo K^* de K y el grupo $]0, +\infty[$. En particular esto implica que $|1| = 1$ y $|\alpha^{-1}| = |\alpha|^{-1}$. Por lo tanto, $|-1|^2 = |(-1)^2| = 1$, luego $|-1| = 1$. Más en general, $|-\alpha| = |\alpha|$. El mismo argumento empleado en $\mathbb{R}$ con el valor absoluto usual prueba en general que $|\alpha \pm \beta| \geq \big||\alpha| - |\beta|\big|$.

Todo valor absoluto en un cuerpo induce en éste una distancia —en el sentido topológico— dada por $d(\alpha,\beta) = |\alpha-\beta|$. Un *cuerpo métrico* es un par $(K,\mathcal{T})$, donde K es un cuerpo y $\mathcal{T}$ es una topología en K determinada por un valor absoluto.

Los mismos argumentos que se emplean en el caso de los números reales y complejos sirven para demostrar que la suma y el producto son aplicaciones continuas en un cuerpo métrico, así como cualquiera de sus valores absolutos, los polinomios, la función $1/x$ (salvo en 0), etc.

Equivalencia Notemos que no hemos definido un cuerpo métrico como un par formado por un cuerpo y un valor absoluto, sino que sólo hemos fijado la topología. La razón es que —como veremos a continuación— cuando dos valores absolutos inducen la misma topología ambos son muy similares, hasta el punto de que es irrelevante considerar uno u otro.

Dado un cuerpo métrico K, llamaremos *valores absolutos* de K a los valores absolutos que inducen la topología de K. Diremos que dos valores absolutos en un mismo cuerpo K son *equivalentes* si inducen la misma topología en K.

Teorema 5.2 *Sean* $|\ \ |_1$ *y* $|\ \ |_2$ *dos valores absolutos en un mismo cuerpo* K. *Las afirmaciones siguientes son equivalentes:*

a) $|\ \ |_1$ *y* $|\ \ |_2$ *son equivalentes.*

b) Para todo $\alpha \in K$, *se cumple* $|\alpha|_1 < 1$ *si y sólo si* $|\alpha|_2 < 1$.

c) Para todo $\alpha, \beta \in K$, *se cumple* $|\alpha|_1 < |\beta|_1$ *si y sólo si* $|\alpha|_2 < |\beta|_2$.

d) Existe un número real $\rho > 0$ *tal que para todo* $\alpha \in K$, $|\alpha|_1 = |\alpha|_2^\rho$.

Demostración: b) $\Rightarrow$ c), c) $\Rightarrow$ a) y d) $\Rightarrow$ b) son evidentes.

a) $\Rightarrow$ b), pues $|\alpha| < 1$ equivale a que $\lim\limits_n \alpha^n = 0$.

Sólo falta demostrar d) a partir de las propiedades anteriores. Es fácil ver que el valor absoluto trivial no es equivalente a ningún otro (por ejemplo por la propiedad b), luego podemos descartarlo. Si $|\ \ |_1$ no es trivial existe un $\alpha \in K$ no nulo tal que $|\alpha|_1 < 1$ (existe un elemento no nulo que cumple $|\alpha|_1 \neq 1$ y si es necesario tomamos su inverso).

Sea β cualquier elemento no nulo de K. Un par de números enteros (m,n) cumple $|\alpha^m|_1 < |\beta^n|_1$ si y sólo si cumple $|\alpha^m|_2 < |\beta^n|_2$. Pero $|\alpha^m|_1 < |\beta^n|_1$ equivale a $|\alpha|_1^m < |\beta|_1^n$, y a su vez a que

$$\frac{\log|\alpha|_1}{\log|\beta|_1} < \frac{n}{m}.$$

Como lo mismo vale para $|\ \ |_2$ concluimos que todo número racional r cumple

$$r > \frac{\log|\alpha|_1}{\log|\beta|_1} \quad \text{si y sólo si} \quad r > \frac{\log|\alpha|_2}{\log|\beta|_2},$$

La densidad de $\mathbb{Q}$ en $\mathbb{R}$ implica que los cocientes de logaritmos son iguales, luego para todo β no nulo de K se cumple

$$\frac{\log|\alpha|_1}{\log|\beta|_1} = \frac{\log|\alpha|_2}{\log|\beta|_2} = \rho,$$

donde ρ es una constante positiva, ya que $|\alpha|_1 < 1$ implica que $|\alpha|_2 < 1$. De aquí se sigue que $|\beta|_2 = |\beta|_1^\rho$ para todo β de K. ■

Isometrías e isomorfismos topológicos Sean k y K dos cuerpos dotados de sendos valores absolutos $|\ \ |_k$ y $|\ \ |_K$. Una *isometría* de k en K respecto a los valores absolutos dados es un monomorfismo de cuerpos $\phi : k \longrightarrow K$ tal que $\big|\phi(\alpha)\big|_K = |\alpha|_k$, para todo $\alpha \in k$.

Un *isomorfismo topológico* $\phi : k \longrightarrow K$ entre dos cuerpos métricos es una aplicación que es a la vez isomorfismo y homeomorfismo. Dejamos al lector la prueba (elemental) del teorema siguiente:

Teorema 5.3 *Sea $\phi : k \longrightarrow K$ un isomorfismo topológico entre dos cuerpos métricos. Para cada valor absoluto de k existe un único valor absoluto de K de modo que ϕ es una isometría entre ambos. Esta correspondencia define una biyección entre los valores absolutos de k y los de K.*

Compleciones De acuerdo con la topología general, una sucesión (α_n) en un cuerpo métrico es *de Cauchy* si para todo número real $\epsilon > 0$ existe un número natural r tal que si $m, n \geq r$ entonces $|\alpha_m - \alpha_n| < \epsilon$. Notemos que por el apartado d) del teorema 5.2 esta propiedad no depende del valor absoluto considerado.

Es fácil ver que toda sucesión convergente es de Cauchy. Un cuerpo métrico K es *completo* si todas sus sucesiones de Cauchy son convergentes.

Teorema 5.4 *Si k es un cuerpo métrico, existe un cuerpo métrico completo K tal que k es denso en K. Además K es único salvo isomorfismo topológico, es decir, si K y K' son cuerpos métricos completos que contienen a k como conjunto denso, entonces existe un isomorfismo topológico de K en K' que deja fijos a los elementos de k.*

DEMOSTRACIÓN: La prueba es formalmente idéntica a la conocida construcción de $\mathbb{R}$ mediante sucesiones de Cauchy. Por ello nos limitaremos a esbozarla. Sea A el conjunto de todas las sucesiones de Cauchy de k. Claramente A es un anillo con la suma y el producto definidos término a término. El conjunto I formado por las sucesiones convergentes a 0 es un ideal de A (se comprueba que las sucesiones de Cauchy están acotadas y de aquí que el producto de una sucesión de Cauchy por una convergente a 0 converge a 0).

Sea K el anillo cociente A/I. Se cumple que K es un cuerpo, pues si $[x_n] \in K$ no es nulo, entonces la sucesión (x_n) no converge a 0. Más aún, no tiene a 0 como punto de acumulación, pues una sucesión de Cauchy converge a cualquiera de sus puntos de acumulación. En particular, (x_n) es finalmente no nula, y modificando sus primeros términos podemos tomar otra equivalente (congruente módulo I) de modo que todos sus términos sean no nulos. Entonces $[1/x_n]$ es la inversa de $[x_n]$ (se comprueba fácilmente que la sucesión $(1/x_n)$ es de Cauchy).

Si $[x_n] \in K$, se comprueba que la sucesión $|x_n|$ es una sucesión de Cauchy en $\mathbb{R}$, luego converge a un número $\big|[x_n]\big|$ que depende exclusivamente de la clase de equivalencia y no del representante. Es inmediato comprobar que esto define un valor absoluto en K.

La aplicación que a cada $x \in k$ le asigna la clase $\big[(x)\big] \in K$ (la clase de la sucesión constantemente igual a x) es claramente un monomorfismo de cuerpos. Si identificamos a k con su imagen, es claro que k es un subcuerpo de K y que el valor absoluto que hemos definido en K extiende al dado en k.

Ahora, si $[x_n] \in K$, la sucesión (x_n), considerada como sucesión en K, converge precisamente a $[x_n]$. En efecto, dado $\epsilon > 0$, existe un natural r tal que si $m, n \geq r$ entonces $|x_n - x_m| < \epsilon$, luego $\lim\limits_n |x_n - x_m| \leq \epsilon$, luego por la definición del valor absoluto de K tenemos que $\big|[(x_n - x_m)_n]\big| \leq \epsilon$, o sea, $\big|[x_n] - x_m\big| \leq \epsilon$, para todo $m \geq r$, luego la sucesión (x_m) converge a $[x_n]$.

Esto implica que k es denso en K. Además K es completo, pues dada una sucesión de Cauchy (y_n) en K, para cada n existe un elemento $x_n \in k$ tal que $|y_n - x_n| < 1/n$, de donde se sigue fácilmente que la sucesión (x_n) es de Cauchy en k, luego converge a un $x \in K$. Es inmediato que x es un punto de acumulación de (y_n), luego (y_n) es convergente.

Falta probar la unicidad. Si K y K' son dos cuerpos completos que contienen a k como conjunto denso, entonces cada $x \in K$ es el límite de una sucesión (x_n) en k, que será de Cauchy en K', luego convergerá a un elemento $\phi(x) \in K'$ independiente de la sucesión elegida.

Esto define una aplicación $\phi : K \longrightarrow K'$ y se comprueba sin dificultad que se trata de una isometría que fija a los elementos de k. ■

El cuerpo métrico K construido en el teorema anterior se llama *compleción* del cuerpo k. Hemos probado que cada valor absoluto se k se extiende a su compleción (de forma única por densidad).

El teorema de aproximación En los próximos capítulos trabajaremos simultáneamente con varios valores absolutos en un mismo cuerpo. El teorema siguiente será de gran utilidad.

Teorema 5.5 (Artin-Whaples) *Sea K un cuerpo y sean $|\ \ |_1, \ldots, |\ \ |_n$ valores absolutos en K no triviales y no equivalentes dos a dos. Sean $x_1, \ldots, x_n \in K$ y $\epsilon > 0$. Entonces existe un $x \in K$ tal que $|x - x_i|_i < \epsilon$ para $i = 1, \ldots, n$.*

Demostración: Notemos en primer lugar que si dos valores absolutos no triviales cumplen que cuando $|\alpha|_1 \leq 1$ también $|\alpha|_2 \leq 1$, entonces ambos son equivalentes.

En efecto, existe un cierto $c \in K$ tal que $0 < |c|_2 < 1$. De este modo $|\alpha|_1 < 1$ implica que $|\alpha^n|_1 \leq |c|_1$ para n suficientemente grande, luego $|\alpha^n/c|_1 \leq 1$, luego $|\alpha^n/c|_2 \leq 1$, luego $|\alpha^n|_2 \leq |c|_2 < 1$, y por lo tanto $|\alpha|_2 < 1$. Recíprocamente, $|\alpha|_1 \geq 1$ implica que $|1/\alpha|_1 \leq 1$, luego $|1/\alpha|_2 \leq 1$ y $|\alpha|_2 \geq 1$.

Así pues, $|\alpha|_1 < 1$ si y sólo si $|\alpha|_2 < 1$, y esto implica que son equivalentes.

Ahora las hipótesis del teorema nos dan que existen $\alpha, \beta \in K$ tales que

$$|\alpha|_1 < 1, \quad |\alpha|_2 \geq 1, \quad |\beta|_1 \geq 1, \quad |\beta|_2 < 1.$$

Llamando $y = \beta/\alpha$ resulta que $|y|_1 > 1$, $|y|_2 < 1$.

Veamos por inducción sobre n que existe un cierto $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n$. Lo tenemos probado para $n = 2$. Supongamos que existe un $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n-1$. Tomemos también un $z \in K$ que cumpla $|z|_1 > 1$, $|z|_n < 1$.

Si se cumple $|y|_n \leq 1$ entonces $y^m z$ cumple lo pedido cuando m es suficientemente grande. Si $|y|_n > 1$ consideramos la sucesión $u_m = y^m/(1 + y^m)$, que claramente tiende a 1 respecto a los valores absolutos $|\ |_1$ y $|\ |_n$ y tiende a 0 respecto a los restantes. Cuando m es suficientemente grande $u^m z$ cumple lo pedido.

Sea, pues, $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n$. Usamos de nuevo que la sucesión $y^m/(1+y^m)$ tiende a 1 respecto al primer valor absoluto y tiende a 0 respecto a los demás. Multiplicándola por x_1 y tomando un término suficientemente lejano obtenemos un elemento $y_1 \in K$ tal que $|x_1 - y_1|_1 < \epsilon/n$ y $|y_1|_i < \epsilon/n$ para $i = 2, \ldots, n$.

Del mismo modo podemos obtener elementos y_i tales que $|x_i - y_i|_i < \epsilon/n$, $|y_i|_j < \epsilon/n$ para $j \neq i$. El teorema se cumple con $x = y_1 + \cdots + y_n$. ■

Valores absolutos no arquimedianos Todos los valores absolutos con los que vamos a trabajar cumplirán una versión fuerte de la desigualdad triangular:

Definición 5.6 Un valor absoluto es *no arquimediano* si para todo $\alpha, \beta \in K$, se cumple $|\alpha + \beta| \leq \max\bigl\{|\alpha|, |\beta|\bigr\}$.

De hecho, si $|\alpha| \neq |\beta|$ y el valor absoluto es no arquimediano, entonces se tiene la igualdad $|\alpha + \beta| = \max\{|\alpha|, |\beta|\}$. En efecto, si $|\alpha| < |\beta|$, entonces

$$|\beta| = |\alpha + \beta - \alpha| \leq \max\{|\alpha + \beta|, |\alpha|\} = |\alpha + \beta|,$$

pues si el máximo fuera $|\alpha|$ tendríamos $|\beta| < |\alpha|$, contradicción. La desigualdad contraria se sigue directamente de la desigualdad triangular no arquimediana, luego $|\alpha + \beta| = |\beta| = \max\{|\alpha|, |\beta|\}$. ■

La propiedad no arquimediana tiene una caracterización muy simple:

Teorema 5.7 *Un valor absoluto en un cuerpo K es no arquimediano si y sólo si para todo natural n se cumple $|n| \leq 1$.*

Demostración: Si el valor absoluto es no arquimediano se comprueba que $|n| \leq 1$ por inducción sobre n. Recíprocamente, para todo natural n se cumple

$$\begin{aligned} |\alpha+\beta|^n &= \Big|\sum_{k=0}^{n}\binom{n}{k}\alpha^k\beta^{n-k}\Big| \leq \sum_{k=0}^{n}|\alpha|^k|\beta|^{n-k} \\ &\leq (n+1)\,\text{máx}\big\{|\alpha|,|\beta|\big\}^n. \end{aligned}$$

Tomando raíces n-simas queda $|a+b| \leq \sqrt[n]{n+1}\,\text{máx}\big\{|\alpha|,|\beta|\big\}$, y tomando el límite en n obtenemos la desigualdad triangular no arquimediana. ■

Es claro que dos valores absolutos equivalentes son ambos arquimedianos o ambos no arquimedianos, luego podemos definir un cuerpo métrico *arquimediano* como un cuerpo métrico cuya topología esté inducida por valores absolutos no arquimedianos. Del teorema anterior se sigue que la compleción de un cuerpo no arquimediano es no arquimediana.

Las sucesiones de Cauchy tienen una caracterización sencilla en los cuerpos no arquimedianos:

Teorema 5.8 *Una sucesión (α_n) en un cuerpo métrico no arquimediano es de Cauchy si y sólo si $\lim\limits_n(\alpha_n - \alpha_{n-1}) = 0$.*

Demostración: Supongamos que la sucesión cumple esta propiedad y sea $\epsilon > 0$. Por definición de límite existe un $r > 0$ tal que si $n \geq r$ entonces $|\alpha_n - \alpha_{n-1}| < \epsilon$. Si tomamos $r \leq m \leq n$, entonces

$$|\alpha_n - \alpha_m| = \big|(\alpha_n - \alpha_{n-1}) + \cdots + (\alpha_{m+1} - \alpha_m)\big| \leq \max_{m<i\leq n}|\alpha_i - \alpha_{i-1}| < \epsilon,$$

luego la sucesión es de Cauchy. El recíproco es claro. ■

Como consecuencia inmediata:

Teorema 5.9 *En un cuerpo métrico completo no arquimediano, la serie $\sum\limits_{n=0}^{\infty} x_n$ es convergente si y sólo si $\lim\limits_n x_n = 0$.*

Esto hace que las series convergentes en cuerpos completos no arquimedianos sean (trivialmente) absolutamente convergentes, por lo que todos los resultados válidos para series absolutamente convergentes de números complejos valen para series convergentes en cuerpos no arquimedianos (así, las series pueden reordenarse y se pueden asociar sus sumandos sin alterar la convergencia o el valor de la suma).

5.2 Valoraciones

En realidad, la noción de valor absoluto que acabamos de estudiar será para nosotros un concepto auxiliar. El concepto central será el de valoración, que introducimos seguidamente:

Definición 5.10 Una *valoración* en un cuerpo K es una aplicación suprayectiva $v : K^* = K \setminus \{0\} \longrightarrow \mathbb{Z}$ tal que:

a) $v(\alpha\beta) = v(\alpha) + v(\beta)$ para todo α, $\beta \in K^*$,

b) $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$, para todo α, $\beta \in K^*$, $\alpha \neq -\beta$.

En la práctica conviene extender las valoraciones mediante $v(0) = +\infty$, y así las propiedades a) y b) se cumplen para todo α, $\beta \in K$, con el convenio de que una suma que contenga a $+\infty$ vale $+\infty$ y que $+\infty$ es mayor que cualquier entero.

Ejemplo Sea D un dominio de ideales principales, sea K su cuerpo de cocientes y sea $\mathfrak{p} = (\pi)$ un ideal primo en D. Para cada $\alpha \in D \setminus \{0\}$ definimos $v_\mathfrak{p}(\alpha)$ como la multiplicidad de π en la descomposición en factores primos de α (es claro que ésta no varía si cambiamos π por un primo asociado, luego sólo depende de $\mathfrak{p}$). Se comprueba inmediatamente que $v_\mathfrak{p} : D \longrightarrow \mathbb{N}$ es suprayectiva y cumple las propiedades a) y b) de la definición de valoración. Ahora extendemos $v_\mathfrak{p}$ a K^* mediante $v_\mathfrak{p}(\alpha/\beta) = v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(\beta)$. Es claro que la extensión está bien definida y es una valoración en K. ■

El teorema 5.12 muestra que toda valoración en un cuerpo K puede obtenerse de este modo a partir del anillo D adecuado. Veamos algunas consecuencias elementales de la definición de valoración:

Teorema 5.11 *Sea v una valoración en un cuerpo K. Entonces:*

a) $v(1) = v(-1) = 0$.

b) Para todo $\alpha \in K$, se cumple $v(\alpha) = v(-\alpha)$.

c) Si $\alpha \in K$, $\beta \in K^*$, entonces $v(\alpha/\beta) = v(\alpha) - v(\beta)$.

d) Si α, $\beta \in K$ cumplen $v(\alpha) \neq v(\beta)$, entonces $v(\alpha + \beta) = \min\{v(\alpha), v(\beta)\}$.

Demostración: a) $v(1) = v(1 \cdot 1) = v(1) + v(1)$, luego $v(1) = 0$. Similarmente, $0 = v(1) = v(-1) + v(-1) = 2v(-1)$, luego $v(-1) = 0$.

b) es consecuencia inmediata de a).

c) Claramente $0 = v(1) = v(\beta\beta^{-1}) = v(\beta) + v(\beta^{-1})$, luego $v(\beta^{-1}) = -v(\beta)$ y por consiguiente $v(\alpha/\beta) = v(\alpha) + v(\beta^{-1}) = v(\alpha) - v(\beta)$.

d) Podemos suponer $v(\alpha) < v(\beta)$. Entonces

$$v(\alpha) = v(\alpha + \beta - \beta) \geq \min\{v(\alpha + \beta), v(\beta)\} = v(\alpha + \beta),$$

pues si el mínimo fuera $v(\beta)$ tendríamos $v(\alpha) \geq v(\beta)$. La desigualdad contraria se sigue de la definición de valoración. ■

Cuerpos métricos discretos Probablemente el lector habrá notado una cierta analogía entre las propiedades de las valoraciones y las de los valores absolutos. En efecto, sucede que hay una estrecha relación entre ambos:

Si v es una valoración en un cuerpo K y $0 < \rho < 1$ es un número real, podemos definir $|\alpha| = \rho^{v(\alpha)}$, para cada $\alpha \in K$, (entendiendo que $\rho^{+\infty} = 0$). Es inmediato comprobar que $|\ \ |$ es un valor absoluto no arquimediano en K.

Si consideramos dos bases ρ_1 y ρ_2 y llamamos $\rho = \log \rho_1 / \log \rho_2 > 0$, entonces $\rho_1 = \rho_2^{\rho}$ y, por consiguiente, $|\alpha|_1 = |\alpha|_2^{\rho}$. Así pues, al variar ρ recorremos una clase de valores absolutos equivalentes en K, por lo que la valoración v induce una única estructura de cuerpo métrico no arquimediano en K.

Un *cuerpo métrico discreto* es un par (K, v) formado por un cuerpo K y una valoración v en K.

Según lo dicho, todo cuerpo métrico discreto es, en particular, un cuerpo métrico no arquimediano.

Notemos que una valoración puede ser recuperada a partir de uno cualquiera de los valores absolutos que induce mediante la relación

$$v(\alpha) = \log |\alpha| / \log \rho.$$

No necesitamos conocer ρ a priori, pues ρ se recupera como el menor valor absoluto positivo de un elemento de K.

Teniendo en cuenta que un valor absoluto es continuo respecto a la topología que induce, la relación anterior muestra que una valoración también es continua respecto de su propia topología.

Sea k un cuerpo métrico discreto y K su compleción. Dado $\alpha \in K^*$, existe una sucesión $\{\alpha_n\}$ en k convergente a α. Por la continuidad del valor absoluto $\big\{|\alpha_n|\big\}$ converge a $|\alpha| \neq 0$. Por la continuidad del logaritmo concluimos que $\big(v(\alpha_n)\big)$ ha de converger a $\log |\alpha| / \log \rho$, pero se trata de una sucesión de números enteros, luego el límite ha de ser entero. Así pues, si definimos $v(\alpha) = \log |\alpha| / \log \rho$ tenemos una aplicación $v : K^* \longrightarrow \mathbb{Z}$ que extiende a la valoración de k. Es fácil ver que se trata de una valoración en K que induce los valores absolutos de éste. Esto prueba que la compleción de un cuerpo métrico discreto es discreta.

La aritmética de los cuerpos discretos Sea K un cuerpo métrico discreto y v su valoración. Definimos

$$\begin{aligned}
\mathfrak{O} &= \{\alpha \in K \mid v(\alpha) \geq 0\} = \big\{\alpha \in K \bigm| |\alpha| \leq 1\big\}, \\
U &= \{\alpha \in K \mid v(\alpha) = 0\} = \big\{\alpha \in K \bigm| |\alpha| = 1\big\}, \\
\mathfrak{p} &= \{\alpha \in K \mid v(\alpha) \geq 1\} = \{\alpha \in K \mid |\alpha| < 1\}.
\end{aligned}$$

Es inmediato comprobar que $\mathfrak{O}$ es un anillo, U su grupo de unidades y $\mathfrak{p}$ es el único ideal maximal de $\mathfrak{O}$. Diremos que $\mathfrak{O}$ es el *anillo de enteros* de K y que U es el *grupo de unidades* de K.

La continuidad de v muestra que $\mathfrak{O}$, U y $\mathfrak{p}$ son abiertos y cerrados en K.

Fijemos un elemento $\pi \in K$ tal que $v(\pi) = 1$. Para todo $\alpha \in K$ no nulo, si $v(\alpha) = n$, entonces $\epsilon = \alpha/\pi^n$ cumple $v(\epsilon) = 1$, luego $\alpha = \epsilon\pi^n$ y $\epsilon \in U$. Esta descomposición es única, pues necesariamente $n = v(\alpha)$.

En particular vemos que $\mathfrak{p} = (\pi)$, con lo que π es primo, y la descomposición que acabamos de obtener (cuando α es entero) es —de hecho— una descomposición de α en factores primos. Más aún, ahora es claro que $\mathfrak{O}$ es un dominio euclídeo, tomando como norma euclídea la propia valoración v. Efectivamente, se cumple que $v(\alpha) \leq v(\alpha\beta)$, para α y β no nulos, y dados $\Delta, \delta \in \mathfrak{O}$ con $\delta \neq 0$, la división euclídea es simplemente $\Delta = \delta \cdot 0 + \Delta$ si $v(\Delta) < v(\delta)$ o bien $\Delta = \frac{\Delta}{\delta}\,\delta + 0$ en caso contrario. El teorema siguiente es ahora inmediato:

Teorema 5.12 *Sea K un cuerpo métrico discreto. Entonces su anillo de enteros $\mathfrak{O}$ es un dominio de ideales principales con un único ideal primo $\mathfrak{p}$. Sus únicos ideales no nulos son los ideales*

$$\mathfrak{p}^n = \{\alpha \in \mathfrak{O} \mid v(\alpha) \geq n\}.$$

Si $\alpha \in \mathfrak{O}$, se cumple $v(\alpha) = n$ si y sólo si $(\alpha) = \mathfrak{p}^n$. En particular $\pi \in \mathfrak{O}$ es primo si y sólo si $v(\pi) = 1$. Fijado un primo π, todo elemento no nulo de K se expresa de forma única como $\alpha = \epsilon\pi^n$, donde $\epsilon \in U$ y, necesariamente, $n = v(\alpha)$. En particular K es el cuerpo de cocientes de $\mathfrak{O}$.

Observemos además que v es la valoración derivada de $\mathfrak{p}$ según 5.2.

Ejercicio: Demostrar que un dominio íntegro D es el anillo de enteros de una valoración en su cuerpo de cocientes si y sólo si cumple las condiciones del teorema 3.53.

Definición 5.13 Si K es un cuerpo métrico discreto, llamaremos *cuerpo de restos* de K al cociente $\overline{K} = \mathfrak{O}/\mathfrak{p}$ de su anillo de enteros sobre su único ideal primo.

Puesto que $\mathfrak{p}$ es —de hecho— un ideal maximal, tenemos que el cuerpo de restos es efectivamente un cuerpo.

Teorema 5.14 *Sea k un cuerpo métrico discreto y K su compleción. Sea $\mathfrak{o}$ el anillo de enteros de k y $\mathfrak{O}$ el de K. Sea $\mathfrak{p}$ el ideal primo de k y $\mathfrak{p}^*$ el de K. Entonces $\mathfrak{O}$ es la clausura de $\mathfrak{o}$, $\mathfrak{p}^*$ es la clausura de $\mathfrak{p}$, $\mathfrak{o} = \mathfrak{O} \cap k$, $\mathfrak{p} = \mathfrak{p}^* \cap \mathfrak{o}$ y para todo α, $\beta \in \mathfrak{o}$ se cumple*

$$\alpha \equiv \beta \ (\text{mód } \mathfrak{p}) \quad \textit{si y sólo si} \quad \alpha \equiv \beta \ (\text{mód } \mathfrak{p}^*).$$

Además, la inclusión $\mathfrak{o} \longrightarrow \mathfrak{O}$ induce un isomorfismo $\overline{k} \cong \overline{K}$.

Demostración: Sabemos que la valoración de K extiende a la de k y es continua. Es claro que $\mathfrak{o} \subset \mathfrak{O}$ y que $\mathfrak{O}$ es abierto y cerrado en K, luego $\overline{\mathfrak{o}} \subset \mathfrak{O}$.

Para probar la inclusión opuesta tomamos $\alpha \in \mathfrak{O}$. Podemos suponer $\alpha \neq 0$. Existe una sucesión $\{a_n\} \subset k$ convergente a α. Entonces $v(\alpha_n)$ converge a

$v(\alpha)$, pero como son números enteros la sucesión ha de ser finalmente igual a $v(\alpha)$, luego, eliminando los primeros términos, podemos suponer que $\{a_n\} \subset \mathfrak{o}$ (puesto que $v(a_n) = v(\alpha) \geq 0$), luego $\alpha \in \overline{\mathfrak{o}}$.

La relación $\mathfrak{o} = \mathfrak{O} \cap k$ es inmediata a partir de las definiciones. Las propiedades correspondientes para $\mathfrak{p}$ y $\mathfrak{p}^*$ se prueban análogamente. La relación entre las congruencias es inmediata. Para probar la última afirmación sólo hay que comprobar que todo elemento $\alpha \in \mathfrak{O}$ es congruente módulo $\mathfrak{p}^*$ con un elemento $a \in \mathfrak{o}$. Ahora bien, esto equivale a pedir que $|\alpha - a| < 1$, con lo que a existe por la densidad de $\mathfrak{o}$ en $\mathfrak{O}$. ■

En vista del teorema anterior escribiremos $\mathfrak{p}$ indistintamente para el ideal primo de $\mathfrak{o}$ o el de $\mathfrak{O}$. Tampoco distinguiremos los cuerpos de restos.

Teorema 5.15 *Sea K un cuerpo métrico discreto completo. Sea $\mathfrak{p} = (\pi)$ su ideal primo y sea F un conjunto de representantes de las clases módulo $\mathfrak{p}$ tal que $0 \in F$. Entonces todo $\alpha \in K^*$ se expresa de forma única como*

$$\alpha = \sum_{n=k}^{\infty} x_n \, \pi^n, \tag{5.1}$$

donde $x_n \in F$, $k \in \mathbb{Z}$ y $x_k \neq 0$. Además $k = v(\alpha)$.

Demostración: Sea $k = v(\alpha)$ y sea $\alpha_0 = \pi^{-k}\alpha$. Entonces $v(\alpha_0) = 0$, luego α_0 es una unidad del anillo de enteros $\mathfrak{O}$ de K. Por lo tanto, su clase módulo $\mathfrak{p}$ es no nula, luego existe $x_k \in F$, $x_k \neq 0$ tal que $\alpha_0 = x_k + \pi\alpha_1$, con $\alpha_1 \in \mathfrak{O}$. Existe $x_{k+1} \in F$ tal que $\alpha_1 \equiv x_{k+1}$ (mód $\mathfrak{p}$), luego $\alpha_0 = x_k + x_{k+1}\pi + \alpha_2\pi^2$, con $\alpha_2 \in \mathfrak{O}$. Repitiendo el proceso obtenemos sucesiones $\{\alpha_n\}_{n=0}^{\infty}$ y $\{x_n\}_{n=k}^{\infty}$ de modo que

$$\alpha_0 = \sum_{n=k}^{k+r} x_n \pi^{n-k} + \alpha_{r+1}\pi^{r+1}.$$

La sucesión $\{\alpha_{r+1}\pi^{r+1}\}$ tiende a 0, luego

$$\alpha_0 = \sum_{n=k}^{\infty} x_n \pi^{n-k}.$$

Multiplicando por π^k tenemos la expresión buscada para α. Observemos que si en (5.1) multiplicamos ambos miembros por π^{-k} obtenemos una serie todos cuyos términos son enteros, luego el límite también (el anillo de enteros de K es cerrado). De hecho, el resto módulo $\mathfrak{p}$ de dicho límite es $x_k \neq 0$. Por lo tanto $v(\pi^{-k}\alpha) = 0$ y $v(\alpha) = k$.

Si un mismo α admite dos desarrollos de tipo (5.1), ambos tendrán el mismo $k = v(\alpha)$:

$$x_k\pi^k + x_{k+1}\pi^{k+1} + x_{k+2}\pi^{k+2} + \cdots = y_k\pi^k + y_{k+1}\pi^{k+1} + y_{k+2}\pi^{k+2} + \cdots$$

Multiplicamos por π^{-k} y obtenemos una igualdad de enteros:

$$x_k + x_{k+1}\pi + x_{k+2}\pi^2 + \cdots = y_k + y_{k+1}\pi + y_{k+2}\pi^2 + \cdots$$

Claramente entonces $x_k \equiv y_k$ (mód π), y como ambos están en F, necesariamente $x_k = y_k$. Restando y dividiendo entre π queda

$$x_{k+1} + x_{k+2}\pi + \cdots = y_{k+1} + y_{k+2}\pi + \cdots$$

Del mismo modo concluimos que $x_{k+1} = y_{k+1}$, e inductivamente llegamos a que todos los coeficientes coinciden. ■

5.3 Cuerpos de series formales de potencias

El ejemplo principal de cuerpos métricos completos con los que vamos a trabajar es el de los cuerpos de series formales de potencias. En 1.35 hemos definido los anillos de series de potencias de varias indeterminadas sobre un cuerpo k. Para el caso de una indeterminada, los elementos de $k[[x]]$ son simplemente las sucesiones $\{a_n\}_{n=0}^{\infty}$ en k, si bien las representamos en la forma

$$\sum_{n=0}^{\infty} a_n x^n \qquad a_n \in k.$$

Las operaciones en $k[[x]]$ son

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n, \\ \Big(\sum_{n=0}^{\infty} a_n x^n\Big)\Big(\sum_{n=0}^{\infty} b_n x^n\Big) &= \sum_{n=0}^{\infty} \Big(\sum_{i=0}^{n} a_i b_{n-i}\Big) x^n. \end{aligned} \tag{5.2}$$

El anillo $k[[x]]$ es un dominio íntegro, por lo que podemos definir el cuerpo de las *series formales de potencias* sobre k como el cuerpo de cocientes de $k[[x]]$, y lo representaremos por $k((x))$.

Podemos identificar los polinomios con coeficientes en k con las series cuyos coeficientes son finalmente nulos, de modo que $k[x]$ es un subanillo de $k[[x]]$ y, similarmente, el cuerpo de funciones racionales $k(x)$ es un subcuerpo de $k((x))$.

Según el teorema 1.36, las unidades de $k[[x]]$ son las series con término independiente no nulo. Si

$$\alpha = \sum_{n=0}^{\infty} a_n x^n$$

es una serie no nula, podemos considerar el menor natural r tal que $a_r \neq 0$, con lo que

$$\alpha = \Big(\sum_{n=0}^{\infty} a_{n+r} x^n\Big) x^r,$$

y la serie de la izquierda es una unidad de $k[[x]]$. En definitiva, todo elemento no nulo de $k[[x]]$ es de la forma ϵx^r, donde ϵ es una unidad y $r \geq 0$, luego todo elemento no nulo de $k((x))$ es de esta misma forma pero con $r \in \mathbb{Z}$.

En otros términos, todo elemento $\alpha \in k((x))$ con $\alpha \neq 0$ es de la forma

$$\alpha = \sum_{n=r}^{\infty} a_n x^n, \qquad r \in \mathbb{Z},$$

con el convenio de que si r es negativo esta expresión ha de entenderse como

$$\alpha = \sum_{n=r}^{-1} a_n x^n + \sum_{n=0}^{\infty} a_n x^n.$$

El primer sumando se llama *parte singular* de α, mientras que el segundo es la *parte regular.* Es fácil ver que las fórmulas (5.2) son válidas también para series de esta forma, con parte singular. Los coeficientes a_n están unívocamente determinados por α, pues si

$$\alpha = \sum_{n=r}^{\infty} a_n x^n = \sum_{n=r'}^{\infty} b_n x^n,$$

con $r \leq r'$, entonces

$$x^{-r}\alpha = \sum_{n=0}^{\infty} a_{n+r} x^n = \sum_{n=r'-r}^{\infty} b_{n+r} x^n,$$

donde ambos términos pertenecen a $k[[x]]$, luego sus coeficientes son iguales. Así pues, $a_n = 0$ para $n < r'$ y $a_n = b_n$ para $n \geq r'$.

En particular $\alpha = 0$ es la única serie con todos sus coeficientes nulos. Todo $\alpha \neq 0$ admite una única expresión de la forma

$$\alpha = \sum_{n=r}^{\infty} a_n x^n, \quad \text{con } r \in \mathbb{Z}, \quad a_r \neq 0. \tag{5.3}$$

Definimos el *orden* de α como $v(\alpha) = r$. Es decir, $v(\alpha)$ es el menor índice cuyo coeficiente en el desarrollo de α es no nulo. Convenimos que $v(0) = +\infty$.

Si $v(\alpha) = n > 0$ diremos que α tiene un *cero* de orden n, si $v(\alpha) = -n < 0$ diremos que tiene un *polo* de orden n.

Cuando no queramos especificar el orden de una serie usaremos la notación

$$\alpha = \sum_{-\infty \ll n} a_n x^n,$$

dejando así constancia de que el número de coeficientes negativos no nulos ha de ser finito.

Es fácil comprobar que v es una valoración en $k((x))$, cuyo anillo de enteros es $k[[x]]$. Las series de $k[[x]]$ se llaman también series *enteras.* Esta observación nos da la estructura algebraica de $k[[x]]$: se trata de un dominio de ideales principales con un único primo, concretamente el ideal generado por x.

En lo sucesivo consideraremos siempre a $k((x))$ como cuerpo métrico con la topología inducida por la valoración v. Es claro que si α es de la forma (5.3), entonces

$$v\left(\alpha - \sum_{n=r}^{s} a_n x^n\right) \geq s,$$

por lo que
$$\alpha = \lim_s \sum_{n=r}^{s} a_n x^n,$$
es decir: una serie formal es el límite de sus sumas parciales en el sentido topológico usual. En particular vemos que $k(x)$ es denso en $k((x))$.

Teorema 5.16 *El cuerpo métrico $k((x))$ es completo.*

Demostración: Tomamos una sucesión de Cauchy $\{s_r\}_{r=0}^{\infty}$ en $k((x))$. Para cada $n \in \mathbb{Z}$ existe un r_n tal que si $r \geq r_n$ entonces $v(s_r - s_{r_n}) \geq n$, y en particular todas las series s_r para $r \geq r_n$ tienen el mismo coeficiente n-simo, digamos a_n. Vamos a probar que la sucesión converge a
$$s = \sum_{-\infty \ll n} a_n x^n,$$
pero para que esto tenga sentido hemos de justificar que $a_n = 0$ para índices suficientemente pequeños. Ahora bien, sabemos que $v(s_r - s_{r_0}) \geq 0$ para $r \geq r_0$, luego $v(s_r) \geq \min\{0, v(s_{r_0})\} = p$ para todo $r \geq r_0$. Esto implica que $a_n = 0$ para $n \leq p$.

Todas las series s_r con $r \geq r_n$ tienen los mismos coeficientes de índice $m \geq n$, luego estos coeficientes son los a_m. En otros términos, $v(s - s_r) \geq n$, para todo $r \geq r_n$. Esto prueba que $\{s_r\}$ converge a s. ■

Convergencia Todo lo dicho hasta aquí vale para series sobre un cuerpo arbitrario k. En el caso concreto en que el cuerpo de constantes es $k = \mathbb{C}$ se plantea la cuestión adicional de si una serie dada converge o no en un punto. Cada serie entera de potencias en $\mathbb{C}$ tiene un *radio de convergencia* r, de modo que la serie converge en el disco abierto $D(0, r)$ y diverge en el complementario de su clausura. Pueden darse los casos extremos $r = 0$ (y entonces la serie sólo converge en 0) y $r = \infty$ (y entonces la serie converge en todo el plano $\mathbb{C}$).

Es claro que si la serie tiene parte singular esto sólo hace que deje estar definida en 0, pero su convergencia en los puntos restantes no se altera. En tal caso convendremos que en 0 toma el valor ∞, con lo que sigue definiendo una función en todo su disco de convergencia.

También es conocido que la función definida por una serie convergente es holomorfa, en particular continua, y de hecho la continuidad no se pierde en a aunque tenga un polo, considerando en $\mathbb{C}^\infty$ la topología usual. Además, la suma (resp. el producto) de dos series convergentes —en el sentido formal de $\mathbb{C}((x))$— converge a la suma (resp. al producto) de las funciones definidas por los sumandos en la intersección de los discos de convergencia. En particular, la suma y el producto de series con radio de convergencia no nulo tiene radio de convergencia no nulo.

Otro hecho importante es que si una serie de potencias converge a una función idénticamente nula en un entorno de 0, entonces es la serie nula. Como consecuencia, la inversa de una serie con radio de convergencia no nulo $S \neq 0$

tiene radio de convergencia no nulo y converge en un entorno de 0 a la inversa de la función definida por S. En efecto, si la serie S determina la función f, existe un entorno reducido de 0 en el cual f no se anula. Por lo tanto $1/f$ tiene a lo sumo un polo en 0, luego admite un desarrollo en serie de Laurent T. La serie $T \in \mathbb{C}((x))$ tiene radio de convergencia no nulo, luego lo mismo vale para la serie $ST-1$, que converge a la función nula, luego $ST = 1$ y así $T = S^{-1}$. Por consiguiente las que tienen radio de convergencia no nulo forman un subcuerpo de $\mathbb{C}((x))$. ■

Si K es un cuerpo métrico, k es un subcuerpo de K y $\pi \in K$, diremos que $K = k((\pi))$ si todo elemento de K se expresa de forma única como serie de potencias de π con coeficientes en k y la aplicación

$$\sum_{-\infty \ll n} a_n x^n \mapsto \sum_{-\infty \ll n} a_n \pi^n$$

es un isomorfismo topológico.

El teorema 5.15 casi viene a decir que todos los cuerpos métricos discretos completos son de la forma $k((\pi))$, pero esto no es exacto. Si $K = k((x))$ es un cuerpo de series de potencias y $\mathfrak{p}$ es el ideal primo de $k[[x]]$, es claro que toda serie de $k[[x]]$ es congruente módulo $\mathfrak{p}$ con su término independiente, así como que dos constantes no son congruentes módulo $\mathfrak{p}$. Esto se traduce en que la aplicación natural $k \longrightarrow \overline{K}$ dada por $a \mapsto [a]$ es un isomorfismo de cuerpos.

Así pues, una condición necesaria para que un cuerpo métrico discreto completo sea topológicamente isomorfo a un cuerpo de series de potencias es que su anillo de enteros contenga un subcuerpo isomorfo a su cuerpo de restos. A continuación probamos que la condición es suficiente:

Teorema 5.17 *Sea K un cuerpo métrico discreto completo que posea un subcuerpo k contenido en su anillo de enteros de modo que la aplicación natural en el cuerpo de restos $k \longrightarrow \overline{K}$ sea un isomorfismo. Entonces $K = k((\pi))$, donde π es cualquier primo de su anillo de enteros.*

Demostración: Sea $\mathfrak{O}$ el anillo de enteros de K y sea π un primo en $\mathfrak{O}$. El teorema 5.15 aplicado con $F = k$ nos da que todo $\alpha \in \mathfrak{O}$ se expresa de forma única como

$$\alpha = \sum_{n=0}^{\infty} a_n \pi^n,$$

con $a_n \in k$. Por consiguiente la sustitución de x por π es una biyección entre $k[[x]]$ y $\mathfrak{O}$. Es inmediato comprobar que se trata de un isomorfismo de anillos, que se extiende a su vez a un isomorfismo de cuerpos entre $k((x))$ y K (que, de hecho, sigue siendo la sustitución de x por π).

Finalmente, es fácil ver que la valoración de K (que es la inducida por π) asigna a cada serie el menor entero n cuyo coeficiente n-simo es no nulo, de donde se sigue que la sustitución por π transforma v_x en v_π, luego es un isomorfismo topológico. Por lo tanto, $K = k((\pi))$. ■

5.4 El lema de Hensel

Demostramos ahora un resultado nada trivial sobre cuerpos métricos completos, del cual deduciremos los resultados que necesitamos sobre valoraciones.

En primer lugar observamos que si K es un cuerpo métrico no arquimediano (no necesariamente discreto), podemos definir su *anillo de enteros* como

$$E = \{\alpha \in K \mid |\alpha| \leq 1\}.$$

Claramente se trata de un anillo y K es su cuerpo de cocientes. Las unidades de E son los elementos de K con valor absoluto 1. También es claro que E tiene un único ideal maximal, a saber,

$$\mathfrak{p} = \{\alpha \in K \mid |\alpha| < 1\}.$$

(Es único porque está formado por los elementos no unitarios de E.) También tenemos definido el *cuerpo de restos* $\overline{K} = E/\mathfrak{p}$.

Teorema 5.18 *Sea K un cuerpo métrico no arquimediano. Entonces cualquier valor absoluto de K se extiende a un valor absoluto no arquimediano sobre el cuerpo de funciones racionales $K(x)$ de manera que para cada polinomio $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ se cumple $|f(x)| = \max\limits_{0 \leq i \leq n} \{|a_i|\}$.*

Demostración: Consideremos la aplicación definida sobre el anillo de polinomios $K[x]$ como indica el enunciado y vamos a probar que verifica los axiomas de un valor absoluto no arquimediano.

El único que no es inmediato es que esta aplicación conserva los productos. Si tenemos dos polinomios f y g con coeficientes $\{a_i\}$ y $\{b_j\}$ entonces un coeficiente de su producto es de la forma $\sum\limits_{i=0}^{k} a_i b_{k-i}$, y ciertamente

$$\Bigl|\sum_{i=0}^{k} a_i b_{k-i}\Bigr| \leq \max_i |a_i b_{k-i}| \leq \max_i |a_i| \max_j |b_j|,$$

de donde $|f(x)g(x)| \leq |f(x)|\,|g(x)|$. Hemos de probar la igualdad.

Llamemos $f_1(x)$ a la suma de los monomios $a_i x^i$ tales que $|a_i| = |f(x)|$ y $f_2(x)$ a la suma de los monomios restantes. Así $f(x) = f_1(x) + f_2(x)$. Descomponemos igualmente $g(x) = g_1(x) + g_2(x)$. Notemos que $|f_2(x)| < |f_1(x)|$ y $|g_2(x)| < |g_1(x)|$. Así

$$f(x)g(x) = f_1(x)g_1(x) + f_1(x)g_2(x) + f_2(x)g_1(x) + f_2(x)g_2(x).$$

Es fácil ver que el valor absoluto de los tres últimos factores es estrictamente menor que el del primero, luego por la desigualdad triangular no arquimediana (que ya hemos dicho que se cumple) concluimos que $|f(x)g(x)| = |f_1(x)g_1(x)|$.

Por la desigualdad ya probada $|f_1(x)g_1(x)| \leq |f_1(x)|\,|g_1(x)|$ y, considerando el coeficiente director, vemos que de hecho se tiene la igualdad. Así pues $|f(x)g(x)| = |f_1(x)|\,|g_1(x)| = |f(x)||g(x)|$.

Esta propiedad justifica que $|f(x)/g(x)| = |f(x)|/|g(x)|$ no depende del representante elegido para la fracción algebraica y claramente es un valor absoluto en $K(x)$ (conviene probar la desigualdad triangular usual, y el hecho de que la restricción a K sea el valor absoluto no arquimediano de partida implica que la extensión es no arquimediana). ■

Observemos que los distintos valores absolutos de K inducen valores absolutos equivalentes en $K(x)$, por lo que, en definitiva, cada cuerpo métrico no arquimediano K induce una única estructura de cuerpo métrico no arquimediano en $K(x)$. Veamos ahora un resultado técnico previo al lema de Hensel.

Teorema 5.19 *Sea K un cuerpo métrico no arquimediano, sean dos polinomios $g(x)$, $g_0(x) \in K[x]$ de modo que $g_0(x)$ es mónico y $|g_0(x)| \leq 1$. Consideremos la división euclídea*

$$g(x) = g_0(x)c(x) + r(x), \qquad \operatorname{grad} r(x) < \operatorname{grad} g_0(x), \qquad c(x), r(x) \in K[x].$$

Entonces $|r(x)| \leq |g(x)|$.

Demostración: Sean

$$g(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad g_0(x) = x^m + \cdots + b_1 x + b_0.$$

Entonces

$$|g_0(x) a_n x^{n-m}| = |g_0(x)|\,|a_n| \leq |a_n| \leq |g(x)|,$$

luego $|g(x) - g_0(x) a_n x^{n-m}| \leq |g(x)|$. Continuando el proceso de la división llegamos a que $|r(x)| \leq |g(x)|$. ■

Si K es un cuerpo métrico no arquimediano, E es su anillo de enteros y

$$\mathfrak{p} = \{f(x) \in E[x] \mid |f(x)| < 1\},$$

es claro que $\mathfrak{p}$ es un ideal primo de $E[x]$ y que el cociente $E[x]/\mathfrak{p}$ es isomorfo de forma natural al anillo de polinomios $\overline{K}[x]$. Representaremos por $\bar{f}(x)$ la clase de $f(x)$ en el cociente.

Teorema 5.20 (Lema de Hensel) *Sea K un cuerpo métrico completo no arquimediano y sea E su anillo de enteros. Supongamos que un polinomio de $E[x]$ factoriza módulo $\mathfrak{p}$ como $\bar{f}(x) = \bar{g}_0(x)\bar{h}_0(x)$, donde $g_0(x)$ es mónico y $\bar{g}_0(x)$ y $\bar{h}_0(x)$ son primos entre sí. Entonces existen polinomios $g(x)$, $h(x) \in E[x]$ tales que $f(x) = g(x)h(x)$, $g(x)$ es mónico, tiene el mismo grado que $g_0(x)$ y $\bar{g}(x) = \bar{g}_0(x)$, $\bar{h}(x) = \bar{h}_0(x)$.*

Demostración: Por hipótesis existe un polinomio $p(x) \in E[x]$ tal que

$$f(x) = g_0(x)h_0(x) + p(x) \qquad \text{y} \qquad |p(x)| < 1. \tag{5.4}$$

El hecho de que $\bar{g}_0(x)$ y $\bar{h}_0(x)$ sean primos entre sí se traduce en que existen polinomios $a(x)$, $b(x)$, $c(x) \in E[x]$ de modo que

$$a(x)g_0(x) + b(x)h_0(x) = 1 + c(x) \qquad \text{y} \qquad |c(x)| < 1. \tag{5.5}$$

Multiplicamos por $p(x)$:

$$a(x)p(x)g_0(x) + b(x)p(x)h_0(x) = p(x) + c(x)p(x). \tag{5.6}$$

Dividimos $b(x)p(x)$ y $c(x)p(x)$ entre $g_0(x)$:

$$\begin{aligned} b(x)p(x) &= g_0(x)q(x) + u_1(x), \qquad \operatorname{grad} u_1(x) < \operatorname{grad} g_0(x), & (5.7)\\ c(x)p(x) &= g_0(x)q_1(x) + r(x), \qquad \operatorname{grad} r(x) < \operatorname{grad} g_0(x). & (5.8)\end{aligned}$$

El teorema anterior nos da

$$\begin{aligned} |u_1(x)| &\leq |b(x)p(x)| = |b(x)|\,|p(x)| \leq |p(x)| < 1, & (5.9)\\ |r(x)| &\leq |c(x)p(x)| = |c(x)||p(x)| \leq |p(x)| < 1. & (5.10)\end{aligned}$$

Sustituyendo (5.7) y (5.8) en (5.6) obtenemos:

$$\big(a(x)p(x) + q(x)h_0(x) - q_1(x)\big)g_0(x) + u_1(x)h_0(x) = p(x) + r(x).$$

Llamamos $v_1(x)$ a la expresión entre paréntesis, y así queda

$$v_1(x)g_0(x) + u_1(x)h_0(x) = p(x) + r(x). \tag{5.11}$$

La desigualdad triangular junto con (5.9), (5.10) y (5.11) nos da que

$$|v_1(x)g_0(x)| \leq \text{máx}\{|u_1(x)h_0(x)|, |p(x)|, |r(x)|\} = |p(x)|$$

y, como $|g_0(x)| = 1$, concluimos que

$$|v_1(x)| \leq |p(x)| < 1. \tag{5.12}$$

Definimos

$$\begin{aligned} g_1(x) &= g_0(x) + u_1(x), & (5.13)\\ h_1(x) &= h_0(x) + v_1(x). & (5.14)\end{aligned}$$

Así $g_1(x)$ es mónico y del mismo grado que $g_0(x)$. Por (5.9) y (5.12) resulta

$$|g_1(x)| = |g_0(x)| = 1, \quad |h_1(x)| \leq 1, \quad \bar{g}_1(x) = \bar{g}_0(x), \quad \bar{h}_1(x) = \bar{h}_0(x).$$

Sea

$$p_1(x) = f(x) - g_1(x)h_1(x). \tag{5.15}$$

Usando (5.4) y (5.11) tenemos

$$\begin{aligned} p_1(x) &= f(x) - g_0(x)h_0(x) - g_0(x)v_1(x) - u_1(x)h_0(x) - u_1(x)v_1(x)\\ &= p(x) - p(x) - r(x) - u_1(x)v_1(x) = -r(x) - u_1(x)v_1(x), \end{aligned}$$

luego por (5.9), (5.10) y (5.12)

$$\begin{aligned} |p_1(x)| &\leq \text{máx}\big\{|r(x)|, |u_1(x)v_1(x)|\big\} \leq \text{máx}\big\{|c(x)|\,|p(x)|, |p(x)|\,|p(x)|\big\}\\ &\leq \text{máx}\big\{|c(x)|, |p(x)|\big\}|p(x)| = k|p(x)|, & (5.16)\end{aligned}$$

donde $k = \max\{|c(x)|, |p(x)|\} < 1$. Más aún, (5.5), (5.13) y (5.14) implican

$$\begin{aligned} a(x)g_1(x) + b(x)h_1(x) &= a(x)g_0(x) + a(x)u_1(x) + b(x)h_0(x) + b(x)v_1(x) \\ &= 1 + c(x) + a(x)u_1(x) + b(x)v_1(x) = 1 + c_1(x), \end{aligned}$$

con $c_1(x) = c(x) + a(x)u_1(x) + b(x)v_1(x)$ y, en virtud de (5.9), (5.12) y (5.16),

$$|c_1(x)| < 1, \quad \max\{|c_1(x)|, |p_1(x)|\} \leq \max\{|c(x)|, |p(x)|\} = k.$$

Por otro lado,

$$\begin{aligned} &\operatorname{grad}(g_1(x)h_1(x)) = \operatorname{grad}(g_0(x)h_1(x)) \\ &\quad\leq \quad [(5.14)]\max\{\operatorname{grad}(g_0(x)h_0(x)), \operatorname{grad}(g_0(x)v_1(x))\} \\ &\quad\leq \quad [(5.4),(5.11)]\max\{\operatorname{grad} f(x), \operatorname{grad} p(x), \operatorname{grad}(u_1(x)h_0(x)), \operatorname{grad} r(x)\} \\ &\quad\leq \quad [(5.4),(5.7),(5.8)]\max\{\operatorname{grad} f(x), \operatorname{grad} p(x)\} = m. \end{aligned}$$

En resumen, tenemos dos polinomios $g_1(x)$, $h_1(x)$ que cumplen las hipótesis del teorema en lugar de $g_0(x)$ y $h_0(x)$ y además

$$|p_1(x)| \leq k|p(x)|, \qquad \operatorname{grad}(g_1(x)h_1(x)) \leq m.$$

Podemos repetir el proceso indefinidamente, y así obtenemos polinomios $g_n(x)$, $h_n(x)$, $p_n(x)$, $u_n(x)$, $v_n(x)$ tales que

$$\begin{aligned} g_n(x) &= g_0(x) + \sum_{i=1}^n u_i(x), \quad |u_i(x)| \leq |p_{i-1}(x)| \leq k^i, \\ h_n(x) &= h_0(x) + \sum_{i=1}^n v_i(x), \quad |v_i(x)| \leq |p_{i-1}(x)| \leq k^i, \\ f(x) &= g_n(x)h_n(x) + p_n(x), \quad |p_n(x)| \leq k^{n+1}. \end{aligned}$$

Además los polinomios $g_n(x)$ son mónicos, todos del mismo grado y

$$\operatorname{grad} h_n(x) \leq m - \operatorname{grad} g_0(x).$$

Definimos

$$g(x) = g_0(x) + \sum_{i=1}^\infty u_i(x), \qquad h(x) = h_0(x) + \sum_{i=1}^\infty v_i(x).$$

Notemos que la convergencia de las series no se sigue simplemente de que las sucesiones $|u_i(x)|$ y $|v_i(x)|$ tiendan a 0, pues $K(x)$ no es completo, pero el grado de los sumandos está acotado y, al intercambiar formalmente las series con las sumas de cada polinomio, obtenemos un polinomio cuyos coeficientes son series convergentes (pues K sí que es completo) y es fácil ver que tales polinomios son realmente las sumas de las series.

Por otro lado es claro que la sucesión $p_n(x)$ tiende a 0, luego $f(x) = g(x)h(x)$. Claramente

$$|g(x) - g_0(x)| \leq \max_i\{|u_i(x)|\} < 1, \qquad |h(x) - h_0(x)| \leq \max_i\{|v_i(x)|\} < 1$$

y además $g(x)$ es mónico y tiene el mismo grado que $g_0(x)$. ■

Veamos dos casos particulares:

Teorema 5.21 *Sea K un cuerpo completo no arquimediano y*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

un polinomio con coeficientes enteros (en K), $a_n \neq 0$. Si $|a_n| < 1$ y $|a_i| = 1$ para un $i \neq 0$ entonces f es reducible.

Demostración: Sea $0 < i < n$ el mayor índice tal que $|a_i| = 1$. Definimos

$$g_0(x) = \frac{1}{a_i}(a_i x^i + \cdots + a_1 x + a_0), \qquad h_0(x) = a_i.$$

Claramente ambos polinomios tienen coeficientes enteros, son primos entre sí, $g_0(x)$ es mónico y

$$|f(x) - g_0(x)h_0(x)| = |a_n x_n + \cdots + a_{i+1}x^{i+1}| < 1.$$

También es obvio que $\bar{g}_0(x)$ y $\bar{h}_0(x)$ son primos entre sí. El lema de Hensel implica que f se descompone en producto de dos polinomios, uno de grado i y otro de grado $n - i$, luego es reducible. ■

Teorema 5.22 *Sea K un cuerpo completo no arquimediano y $f(x)$ un polinomio mónico irreducible en $K[x]$. Si el término independiente de $f(x)$ es entero, entonces los coeficientes restantes también lo son.*

Demostración: Sea c el coeficiente de $f(x)$ con mayor valor absoluto. Hemos de probar que $|c| \leq 1$. En caso contrario $f(x)/c$ tiene todos sus coeficientes enteros y uno de ellos igual a 1. Su coeficiente director es $1/c$, y se cumple $|1/c| < 1$, luego por el teorema anterior $f(x)$ sería reducible, en contra de lo supuesto. ■

5.5 Extensión de valores absolutos

Nos ocupamos ahora del problema de extender el valor absoluto de un cuerpo completo a una extensión finita. En primer lugar probaremos que si k es un cuerpo métrico completo, entonces cada valor absoluto de k admite una única extensión a cualquier extensión finita de k. Empezaremos ocupándonos de la unicidad, para lo cual necesitamos la noción de norma:

Definición 5.23 Sea K un cuerpo métrico y V un espacio vectorial sobre K. Una *norma* en V (para un valor absoluto prefijado en K) es una aplicación $\|\ \| : V \longrightarrow \mathbb{R}$ que cumpla las propiedades siguientes:

a) $\|v\| \geq 0$ para todo $v \in V$ y $\|v\| = 0$ si y sólo si $v = 0$,

b) $\|v + w\| \leq \|v\| + \|w\|$ para todo v, $w \in V$,

c) $\|\alpha v\| = |\alpha|\|v\|$ para todo $\alpha \in K$ y todo $v \in V$.

Claramente V es un espacio métrico con la distancia dada por $\|v - w\|$. Se comprueba sin dificultad que la suma y el producto en V son funciones continuas.

Dos normas $\| \ \|_1$ y $\| \ \|_2$ en un mismo espacio V son *equivalentes* si existen números reales $0 < m < M$ tales que

$$\|v\|_1 \leq m\|v\|_2 \qquad \text{y} \qquad \|v\|_2 \leq M\|v\|_1$$

para todo $v \in V$. Es obvio que dos normas equivalentes inducen la misma topología en V.

Teorema 5.24 *Sea K un cuerpo métrico en el que hemos prefijado un valor absoluto. Entonces la aplicación en K^n definida mediante*

$$\|x\| = \operatorname{máx}\{|x_i| \bigm| i = 1, \ldots, n\}$$

es una norma. Si K es completo entonces K^n es completo con esta norma.

Demostración: La comprobación de que en efecto es una norma es rutinaria. Observemos que $\| \ \|$ induce en K^n la topología producto (las bolas abiertas para la norma son productos de bolas abiertas en K del mismo radio). Es fácil ver que si una sucesión es de Cauchy en K^n, entonces sus coordenadas son de Cauchy en K, luego si K es completo convergen, y la sucesión dada también. ■

Teorema 5.25 *Sea K un cuerpo métrico completo y sea V un K-espacio vectorial de dimensión finita. Entonces todas las normas sobre V (para un valor absoluto prefijado) son equivalentes y V es completo con cualquiera de ellas.*

Demostración: Supongamos primero que $V = K^n$. Sea $\| \ \|^*$ cualquier norma en K^n y sea $\| \ \|$ la norma definida en el teorema anterior. Basta ver que ambas son equivalentes. Sea $e_1, \ldots, e_n$ la base canónica de K^n. Entonces para todo $x \in K^n$ se cumple

$$\|x\|^* = \|x_1e_1 + \cdots + x_ne_n\|^* \leq |x_1|\|e_1\|^* + \cdots + |x_n|\|e_n\|^* \leq M\|x\|,$$

donde $M = \|e_1\|^* + \cdots + \|e_n\|^*$.

Ahora hemos de probar la relación opuesta. Basta ver que existen constantes N_i de modo que si $x \in K^n$, entonces $|x_i| \leq N_i\|x\|^*$, pues en tal caso $N = \operatorname{máx} N_i$ cumple $\|x\| \leq N\|x\|^*$. Lo probaremos por inducción sobre n.

Si $n = 1$ basta tomar $N_1 = 1/\|1\|^*$. Supuesto cierto para $n-1$, identificamos K^{n-1} con los elementos de K^n cuya última coordenada es nula. Las restricciones a K^{n-1} de las dos normas consideradas son normas en K^{n-1}. Por hipótesis de inducción son equivalentes y K^{n-1} es completo para la restricción de la norma $\| \ \|^*$, luego es cerrado en K^n para la topología inducida esta norma.

Supongamos, por reducción al absurdo, que para todo natural m existe un $w_m \in \mathbb{K}^n$ de manera que $|(w_m)_n| > m\|w_m\|^*$. Podemos suponer que $(w_m)_n = 1$ (basta dividir w_m entre $(w_m)_n$ si es preciso), y entonces la desigualdad se reduce a $\|w_m\|^* < 1/m$. Por otra parte esta condición adicional implica también que $w_m - e_n \in K^{n-1}$.

De este modo tenemos que $\{w_m\}$ tiende a 0 y que $w_m - e_n$ tiende a $-e_n$ pero, como K^{n-1} es cerrado, esto implica que $e_n \in K^{n-1}$, lo cual es absurdo. Por lo tanto existe un m tal que $|w_n| \leq m\|w\|^*$ para todo $w \in K^n$. El mismo razonamiento se aplica a cualquier otro índice.

Si V es un espacio vectorial cualquiera de dimensión n sobre K, cada norma en V induce una en K^n a través de un isomorfismo de espacios vectoriales. Del hecho de que las normas inducidas sean equivalentes se sigue obviamente que las normas de partida también lo sean. Igualmente se concluye que V es completo con cualquiera de ellas. ■

Con esto es fácil probar que un valor absoluto admite a lo sumo una extensión a una extensión finita, pero podemos probar algo más preciso:

Teorema 5.26 *Sea k un cuerpo métrico completo y K/k una extensión finita de grado n. Si un valor absoluto de k se extiende a K, entonces la extensión viene dada necesariamente por $|\alpha| = \sqrt[n]{|\operatorname{N}(\alpha)|}$, para todo $\alpha \in K$, donde $\operatorname{N} : K \longrightarrow k$ es la norma de K/k. Además K es completo con este valor absoluto.*

Demostración: Sea $\{\alpha_1, \ldots, \alpha_n\}$ una k-base de K. Si $\alpha \in K$ se expresa como

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n, \qquad \text{con } x_1, \ldots, x_n \in k,$$

teniendo en cuenta el teorema 5.24, es claro que la aplicación

$$\|\alpha\| = \max_{1 \leq i \leq n} |x_i|$$

es una norma en K, que por 5.25 será equivalente al valor absoluto de K (pues éste también es una norma). En particular el valor absoluto de K es completo.

Tomemos un $\alpha \in K$ tal que $|\alpha| < 1$. Entonces la sucesión $\{\alpha^m\}$ tiende a 0 (para el valor absoluto y, por lo tanto, para la norma). Sea

$$\alpha^m = x_{m1}\alpha_1 + \cdots + x_{mn}\alpha_n, \qquad \text{con } x_{mj} \in k.$$

La convergencia en norma implica que las sucesiones $\{x_{mj}\}_m$ tienden a 0 (respecto al valor absoluto de k).

Notemos que $N(x_{m1}\alpha_1 + \cdots + x_{mn}\alpha_n)$ se calcula como producto de n polinomios homogéneos lineales en las variables $x_1, \ldots, x_n$. No es difícil ver que sus coeficientes están en k, luego concluimos[1] que $\{N(\alpha^m)\}$ converge a 0 en k.

Como $\operatorname{N}(\alpha^m) = \operatorname{N}(\alpha)^m$, concluimos que $|\operatorname{N}(\alpha)| < 1$. Tomando inversos deducimos que si $|\alpha| > 1$ entonces $|\operatorname{N}(\alpha)| > 1$. Por lo tanto $|\alpha| = 1$ si y sólo si $|\operatorname{N}(\alpha)| = 1$.

Ahora, si $\alpha \in K$ es no nulo, tenemos $\operatorname{N}(\alpha^n/\operatorname{N}(\alpha)) = 1$, luego $|\alpha^n/\operatorname{N}(\alpha)| = 1$ y así $|\alpha|^n = \operatorname{N}(\alpha)$. Como $|\alpha| > 0$ podemos tomar raíces n-simas. ■

[1]Alternativamente, los coeficientes están en una extensión finita de k, las sucesiones $\{x_{mj}\}_m$ tienden a 0 respecto a la norma en dicha extensión, luego la sucesión $\{N(\alpha^m)\}$ converge a 0 en dicha extensión y, al estar en k, converge a 0 en k.

Para completar este teorema sólo falta probar que $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$ es realmente un valor absoluto en K.

Teorema 5.27 *Sea k un cuerpo métrico completo no arquimediano. Sea K/k una extensión finita de grado n. Entonces cada valor absoluto de k se extiende de forma única a un valor absoluto de K, que viene dado por $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$. La extensión es completa.*

Demostración: Es obvio que la aplicación $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$ extiende al valor absoluto de k, así como que satisface los axiomas de valor absoluto salvo quizá la desigualdad triangular. La completitud la garantiza el teorema anterior.

Hemos de probar que si $|\alpha| \leq |\beta|$ entonces $|\alpha+\beta| \leq |\beta|$ o, equivalentemente, que $|\alpha/\beta+1| \leq 1$, para todo α, $\beta \in K$, $\beta \neq 0$. Alternativamente, basta ver que si $|\alpha| \leq 1$ entonces $|\alpha+1| \leq 1$. En nuestro caso concreto esto equivale a que si $|\,\mathrm{N}(\alpha)| \leq 1$ entonces $|\,\mathrm{N}(\alpha+1)| \leq 1$. Como $\mathrm{N}_{K/k}(\alpha) = (\mathrm{N}_{k(\alpha)/k}(\alpha))^{|K:k(\alpha)|}$, podemos suponer que $K = k(\alpha)$.

Sea $f(x)$ el polinomio mínimo de α en $k[x]$. Su término independiente es, salvo el signo, $\mathrm{N}_{K/k}(\alpha)$, luego es entero en k. El teorema 5.22 implica que todos sus coeficientes son enteros. El polinomio mínimo de $\alpha+1$ es $f(x-1)$, que también tiene sus coeficientes enteros, en particular su término independiente, luego $|\,\mathrm{N}(\alpha+1)| \leq 1$. ■

Notemos que dos valores absolutos de k se diferencian en un exponente, luego lo mismo les sucede a sus extensiones. Así pues, la estructura métrica que obtenemos en K no depende del valor absoluto de k del que partamos, luego K se convierte en un cuerpo métrico completo cuyos valores absolutos están en biyección con los de k.

Teorema 5.28 *Si k es un cuerpo métrico discreto completo y K es una extensión finita de k, entonces K es también discreto. Además, si v^* es la valoración de K y v es la valoración de k, existe un número natural e tal que $v^*(\alpha) = ev(\alpha)$, para todo $\alpha \in k^*$.*

Demostración: Si un valor absoluto de k es $|\alpha| = \rho^{v(\alpha)}$, con $0 < \rho < 1$, entonces la imagen de k^* por el valor absoluto es el subgrupo cíclico de $\mathbb{R}^*$ generado por ρ. La imagen de K^* por la norma es un subgrupo de k^*, y la imagen de éste por el valor absoluto de k es un subgrupo de $\langle\rho\rangle$, luego será de la forma $\langle\rho^f\rangle$, para un cierto natural no nulo f. Las raíces n-simas de los elementos de este grupo forman el grupo $\langle\rho^{f/n}\rangle$. Así pues, para cada $\alpha \in K^*$ existe un único entero $v^*(\alpha)$ tal que $|\alpha| = \rho^{(f/n)v^*(\alpha)}$. Equivalentemente,

$$v^*(\alpha) = \frac{n\log|\alpha|}{f\log\rho}.$$

Es fácil ver que v^* es una valoración en K que induce su valor absoluto. También es claro que si $\alpha \in k^*$ entonces $v^*(\alpha) = ev(\alpha)$, donde $e = n/f$. Tomando un $\alpha \in k^*$ tal que $v(\alpha) = 1$ concluimos que e es un número natural. ■

Definición 5.29 Sea K/k una extensión finita de cuerpos métricos completos discretos. El número e que cumple el teorema anterior se llama *índice de ramificación* de la extensión, y lo representaremos por $e(K/k)$.

Es claro que si tenemos una cadena de extensiones $k \subset K \subset L$, entonces

$$e(L/k) = e(L/K)e(K/k).$$

En estas circunstancias, si $\mathfrak{o}$, $\mathfrak{O}$ son los anillos de enteros de k y K y $\mathfrak{p}$, $\mathfrak{P}$ son sus respectivos ideales primos, es claro que $\mathfrak{o} \subset \mathfrak{O}$ y $\mathfrak{p} \subset \mathfrak{P}$. Por lo tanto, la inclusión $\mathfrak{o} \longrightarrow \mathfrak{O}$ induce un monomorfismo de cuerpos $\overline{k} \longrightarrow \overline{K}$. En lo sucesivo consideraremos a $\overline{K}$ como una extensión de $\overline{k}$ a través de este monomorfismo.

Teorema 5.30 *Sea K/k una extensión finita de cuerpos métricos discretos completos, la extensión $\overline{K}/\overline{k}$ es finita.*

DEMOSTRACIÓN: Sean $\mathfrak{o}$, $\mathfrak{O}$, $\mathfrak{p}$ y $\mathfrak{P}$ como en el párrafo previo al teorema. Sea $\mathfrak{P} = (\pi)$ y sea $\bigl\{[\omega_1], \ldots, [\omega_f]\bigr\}$ un conjunto $\overline{k}$-linealmente independiente en $\overline{K}$. Veamos que los elementos

$$\omega_i\pi^j, \qquad \text{para } i = 1, \ldots, f,\ j = 0, \ldots, e-1$$

son k-linealmente independientes en K. Consideremos una combinación lineal

$$\sum_{i,j} c_{ij}\,\omega_i\,\pi^j, \qquad \text{con } c_{ij} \in k.$$

Fijado j, supongamos que algún coeficiente c_{ij} es no nulo. Reordenándolos podemos suponer que $c_{1j} \neq 0$ es el coeficiente con mayor valor absoluto. Entonces

$$\Bigl|\sum_i c_{ij}\,\omega_i\Bigr| = |c_{1j}|\,\left|\omega_1 + \frac{c_{2j}}{c_{1j}}\,\omega_2 + \cdots + \frac{c_{fj}}{c_{1j}}\,\omega_f\right|.$$

Todos los coeficientes de la última combinación lineal son enteros, luego podemos tomar clases módulo $\mathfrak{P}$. Como el coeficiente de $[\omega_1]$ es 1, concluimos que toda la combinación lineal es no nula, es decir, que no está en $\mathfrak{P}$ (pero sí en $\mathfrak{O}$), luego es una unidad y tiene valor absoluto 1. En definitiva (y teniendo en cuenta la reordenación que hemos hecho)

$$\Bigl|\sum_i c_{ij}\,\omega_i\Bigr| = \max_i |c_{ij}|.$$

Obviamente, si todos los coeficientes fueran nulos esta igualdad se sigue cumpliendo. Por lo tanto

$$\Bigl|\sum_i c_{ij}\,\omega_i\,\pi^j\Bigr| = |\pi|^j\,\max_i |c_{ij}|.$$

La imagen de K^* por el valor absoluto es el subgrupo $G_K = \langle|\pi|\rangle$ de $\mathbb{R}^*$, mientras que la imagen de k^* es el subgrupo $G_k = \langle|\pi|^e\rangle$. Claramente, las potencias $|\pi|^j$, para $j = 0, \ldots, e-1$, son representantes de las e clases del cociente G_K/G_k, luego los miembros derechos de la igualdad anterior son representantes de esas mismas clases. En particular son distintos dos a dos, luego la desigualdad triangular no arquimediana para su suma es de hecho una igualdad:

$$\Big|\sum_{i,j} c_{ij}\,\omega_i\,\pi^j\Big| = \max_j \Big|\sum_i c_{ij}\,\omega_i\,\pi^j\Big| = \max_{i,j} |c_{ij}|\,|\pi|^j. \tag{5.17}$$

Ahora es claro que los elementos $\omega_i\,\pi^j$ son linealmente independientes (en particular distintos dos a dos), pues si el miembro izquierdo es nulo el miembro derecho muestra que todos los c_{ij} son nulos.

Con esto hemos probado que el grado de $\overline{K}/\overline{k}$ está acotado por n/e, donde $n = |K : k|$. ■

Definición 5.31 Sea K/k una extensión finita de cuerpos métricos completos discretos. Llamaremos *grado de inercia* de la extensión al grado de la extensión de cuerpos de restos:

$$f(K/k) = |\overline{K} : \overline{k}|.$$

Es inmediato que si $k \subset K \subset L$ es una cadena de cuerpos, se cumple

$$f(L/k) = f(L/K)f(K/k).$$

Teorema 5.32 *Sea K/k una extensión de grado n de cuerpos métricos discretos completos. Entonces $n = e(K/k)f(K/k)$.*

DEMOSTRACIÓN: Sea $\mathfrak{O}$ el anillo de enteros de K, sea $\mathfrak{P} = (\pi)$ su ideal primo y sea $[\omega_1], \ldots, [\omega_f]$ una $\overline{k}$-base de $\overline{K}$. Basta probar que los elementos $\omega_i\,\pi^j$, para $i = 1, \ldots, f$, $j = 0, \ldots, e-1$, son una k-base de K. En la prueba del teorema 5.30 hemos visto que son linealmente independientes.

Sea $\mathfrak{o}$ el anillo de enteros de k y $\mathfrak{p} = (\rho)$ su ideal primo. Si v^* es la valoración de K y v la de k, tenemos que $v^*(\rho) = ev(\rho) = e$. Para cada entero m sea $m = ke + r$, con $0 \leq r < e$. Definimos $\pi_m = \rho^k\pi^r$. De este modo $v^*(\pi_m) = m$, luego $\pi_m = \epsilon_m\pi^m$, donde ϵ_m es una unidad de $\mathfrak{O}$.

Sea A un conjunto de representantes de las clases de $\overline{K}$ formado por combinaciones lineales de $\omega_1, \ldots, \omega_f$ con coeficientes en $\mathfrak{o}$. Es claro que $A_m = \epsilon_m A$ también es un conjunto de representantes de las clases de $\overline{K}$.

Es claro que la prueba de 5.15 puede modificarse levemente para probar que todo $\alpha \in K^*$ admite una expresión

$$\alpha = \sum_{m=s}^{+\infty} y_m\pi^m, \qquad \text{con } y_m \in A_m, \quad s \in \mathbb{Z}.$$

Así, $y_m = x_m\epsilon_m$, con $x_m \in A$, luego

$$\alpha = \sum_{m=s}^{+\infty} x_m\pi_m.$$

Equivalentemente,

$$\alpha = \sum_{k=k_0}^{+\infty} \sum_{r=0}^{e-1} \Big(\sum_{i=1}^{f} a_{kri}\, \omega_i \Big) \rho^k \pi^r = \sum_{r=0}^{e-1} \sum_{i=1}^{f} \Big(\sum_{k=k_0}^{+\infty} a_{kri}\, \rho^k \Big) \omega_i\, \pi^r.$$

(Aquí usamos la asociatividad infinita de las series en cuerpos no arquimedianos.)

Las series del miembro derecho están en k porque k es cerrado en K (es completo). Así pues, α es combinación k-lineal de los elementos $\omega_i \pi^r$, luego éstos forman una base. Más aún, vamos a ver que los enteros de K son exactamente los elementos con coordenadas enteras en esta base. Obviamente los elementos con coordenadas enteras son enteros. Supongamos ahora que

$$\alpha = \sum_{i,j} c_{ij}\, \omega_i\, \pi^j, \qquad |\alpha| \leq 1.$$

La igualdad (5.17) prueba que $|c_{ij}\pi^j| \leq 1$, luego

$$|c_{ij}| \leq |\pi|^{-j} < |\pi|^{-e} = |\rho|^{-1}.$$

Equivalentemente, $v(c_{ij}) > -v(\rho) = -1$, luego $v(c_{ij}) \geq 0$ y así cada c_{ij} es entero. ■

Veamos ahora que el grado de inercia y el índice de ramificación se pueden separar en dos extensiones sucesivas:

Teorema 5.33 *Sea K/k una extensión finita de cuerpos métricos discretos completos tal que el cuerpo de restos $\overline{k}$ sea perfecto, sea $e = e(K/k)$. Entonces existe un cuerpo intermedio $k \subset L \subset K$ tal que*

$$|K : L| = e(K/L) = e(K/k) \quad y \quad |L : k| = f(L/k) = f(K/k).$$

DEMOSTRACIÓN: Supongamos primeramente que la extensión K/k es separable. Entonces el número de cuerpos intermedios es finito, luego podemos tomar uno L tal que $e(L/k) = 1$ y ningún cuerpo mayor cumpla lo mismo. Entonces $e(K/L) = e$, y basta probar que $f(K/L) = 1$. En caso contrario, $\overline{K}$ es una extensión separable de grado $d > 1$ de $\overline{L}$, luego $\overline{K} = \overline{L}(\alpha)$. El polinomio mínimo de α sobre $\overline{L}$ será la imagen de un polinomio $p(x) \in \mathfrak{O}_L[x]$ mónico de grado d, necesariamente irreducible en $\mathfrak{O}_L[x]$ (luego también en $L[x]$).

Por la separabilidad, en $\overline{K}[x]$ tenemos que $\overline{p}(x) = (x-\alpha)\overline{g}(x)$ con $x - \alpha$ y $\overline{g}(x)$ primos entre sí. Por el lema de Hensel 5.20, el polinomio $p(x)$ tiene una raíz $a \in \mathfrak{O}_K$ tal que $\alpha = [a]$. El cuerpo $L' = L(a)$ tiene grado d sobre L y además $\overline{L}' = \overline{L}(\alpha) = \overline{K}$, luego $f(L'/L) = d$ y así $e(L'/L) = 1$, luego también $e(L'/k) = 1$, en contradicción con la elección de L.

En el caso general consideramos la clausura separable K_s de k en K. Basta probar que $f(K/K_s) = 1$, pero si $[a] \in \overline{K}$, con $a \in \mathfrak{O}$ y p es la característica de k, entonces $a^{p^r} \in K_s$ para cierto $r \geq 0$, luego $[a]^{p^r} \in \overline{K}_s$. Esto implica que la extensión $\overline{K}/\overline{K}_s$ es puramente inseparable, pero tiene que ser separable, ya que $\overline{k}$ es perfecto, luego $\overline{K} = \overline{K}_s$. ■

Este teorema permite reducir el estudio de una extensión de cuerpos métricos discretos completos (en las condiciones indicadas) al estudio de una extensión *no ramificada* (es decir, con índice de ramificación igual a 1) seguida de una extensión *totalmente ramificada* (con grado de inercia igual a 1). Veamos un resultado más sobre este último tipo de extensiones.

Recordemos que un *polinomio de Eisenstein* para un primo π en un dominio de factorización única es un polinomio mónico cuyos coeficientes sean todos divisibles entre π excepto el coeficiente director y cuyo término independiente no sea divisible entre π^2. El criterio de irreducibilidad de Eisenstein afirma que los polinomios de Eisenstein son siempre irreducibles.

Teorema 5.34 *Sea k un cuerpo métrico discreto completo y K una extensión de k de grado n totalmente ramificada, es decir, tal que $e(K/k) = n$ y sea π un primo en K. Entonces $K = k(\pi)$ y el polinomio mínimo de π es un polinomio de Eisenstein.*

DEMOSTRACIÓN: En la prueba de 5.32 se ve que $1, \pi, \ldots, \pi^{n-1}$ son linealmente independientes sobre k, luego $K = k(\pi)$. Consideremos extensión finita de K que contenga a todos los k-conjugados de π. Fijado un valor absoluto, todos los conjugados cumplen $|\alpha| < 1$, pues los k-automorfismos son isometrías. Los coeficientes distintos del director del polinomio mínimo de π se obtienen de sumas de productos de los conjugados de π, y como el valor absoluto es no arquimediano resulta que todos tienen valor absoluto menor que 1. Esto significa que todos son divisibles entre el primo $\mathfrak{p}$ de k. El término independiente es, concretamente, el producto de todos los conjugados de π, luego su valor absoluto es $|\pi|^n$. Como $v_K|_k = nv_k$, es claro que dicho término independiente no es divisible entre $\mathfrak{p}^2$. ■

Para terminar probamos que los enteros de una extensión finita son enteros en el sentido algebraico:

Teorema 5.35 *Si K/k es una extensión finita de cuerpos métricos discretos completos, entonces el anillo $\mathfrak{O}$ de los enteros de K es la clausura entera en K del anillo $\mathfrak{o}$ de los enteros de k.*

DEMOSTRACIÓN: Si $\alpha \in \mathfrak{O}$, tomamos una extensión finita de K que contenga todos los conjugados de α sobre k. Fijado un valor absoluto, todos ellos cumplirán $|\beta| \leq 1$ (pues la unicidad de la extensión del valor absoluto de k hace que los k-automorfismos sean isometrías). Como los coeficientes del polinomio mínimo de α dependen polinómicamente de los conjugados de α (con coeficientes enteros), la desigualdad triangular no arquimediana implica que todos ellos tienen valor absoluto ≤ 1, luego α es entero sobre $\mathfrak{o}$.

Recíprocamente, si $\alpha \in K$ es entero sobre $\mathfrak{o}$, en particular es entero sobre $\mathfrak{O}$, pero $\mathfrak{O}$ es íntegramente cerrado, por ser un dominio de factorización única, luego $\alpha \in \mathfrak{O}$. ■

Capítulo VI

Funciones algebraicas I

Una curva proyectiva regular V sobre un cuerpo de constantes k_0 está completamente determinada por su cuerpo de funciones racionales $K = k_0(V)$. Vamos a ver que es posible aplicar a K técnicas procedentes de la teoría algebraica de números. Estas técnicas no sólo nos proporcionarán mucha información sobre las curvas proyectivas y sus cuerpos asociados, sino que son aplicables en un contexto más general en el que no es necesario suponer que el cuerpo k_0 es algebraicamente cerrado. Entramos así en lo que se conoce como la teoría de las funciones algebraicas.

La idea básica es que los puntos de una curva algebraica se corresponden de forma natural con unos objetos definibles algebraicamente a partir de su cuerpo de funciones racionales. Estos objetos reciben el nombre de divisores primos, y tienen sentido en cuerpos más generales. A partir del concepto local de divisor primo es posible definir una noción global de divisor, sobre el cual descansa una potente teoría aritmética, que a su vez es el contexto idóneo para formular y demostrar una serie de resultados profundos sobre cuerpos de funciones algebraicas, en particular sobre curvas algebraicas y superficies de Riemann.

6.1 Cuerpos de funciones algebraicas

Los cuerpos de funciones racionales de curvas algebraicas tienen una caracterización obvia independiente de la geometría algebraica. En el contexto en el que vamos a trabajar es costumbre referirse a ellos como cuerpos de funciones algebraicas.

Definición 6.1 Un *cuerpo de funciones algebraicas* (de una variable) sobre un cuerpo de constantes k_0 es una extensión K finitamente generada y con grado de trascendencia 1 sobre k_0.

Observemos que toda extensión K/k de cuerpos de funciones algebraicas (sobre un mismo cuerpo de constantes k_0) es necesariamente finita. En efecto, como ambos cuerpos tienen grado de trascendencia 1 sobre k_0 es algebraica y, como K es finitamente generado sobre k_0, también lo es sobre k, y una extensión algebraica finitamente generada es finita.

Si K es un cuerpo de funciones algebraicas, el teorema 1.32 nos da que existe $x \in K$ tal que la extensión $K/k_0(x)$ es separable. Como toda extensión finita separable tiene un elemento primitivo α. Así, $K = k_0(x, \alpha)$. El caso más simple se da cuando $K = k_0(x)$ (donde x es trascendente sobre k_0). Entonces diremos que K es un *cuerpo de fracciones algebraicas* sobre k_0.

La relación con la geometría algebraica es la siguiente:

Teorema 6.2 *Si k_0 es un cuerpo algebraicamente cerrado, entonces una extensión K de k_0 es un cuerpo de funciones algebraicas si y sólo si es k_0-isomorfo al cuerpo de funciones racionales de una curva cuasiproyectiva sobre k_0.*

DEMOSTRACIÓN: Ciertamente, si K es k_0-isomorfo a un cuerpo de funciones racionales $k_0(V)$, entonces K es finitamente generado sobre k_0 y tiene grado de trascendencia 1. Recíprocamente, sea $x \in K$ una base de trascendencia de K sobre k_0. Entonces la extensión $K/k_0(x)$ es algebraica y finitamente generada. Digamos que $K = k_0(x, \alpha_1, \ldots, \alpha_n)$. Sea $\phi : k_0[X_0, \ldots, X_n] \longrightarrow K$ el homomorfismo de anillos dado por $\phi(X_0) = x$, $\phi(X_i) = \alpha_i$, para $i = 1, \ldots, n$. Su imagen es un dominio íntegro, luego su núcleo I es un ideal primo, de modo que $V = V(I) \subset A^{n+1}(k_0)$ es una variedad afín. Además $k_0[V] \cong \mathrm{Im}\phi$, luego $k_0(V) \cong K$. De aquí se sigue además que $k_0[V]$ tiene grado de trascendencia 1, luego V es una curva. ■

Observemos que la curva del teorema anterior puede tomarse de hecho proyectiva y regular, pues si V es una curva cuasiproyectiva, entonces $k_0(V)$ es k_0-isomorfo al cuerpo de funciones racionales de la regularización de la clausura proyectiva de V.

Notemos también que si $\phi : V \longrightarrow W$ es una aplicación regular no constante entre curvas proyectivas regulares sobre un cuerpo k_0, entonces ϕ es, de hecho, suprayectiva (pues por el teorema 2.47 sabemos que la imagen es cerrada, luego es todo W o bien un conjunto finito de puntos, pero en tal caso ha de ser un punto o, de lo contrario, las antiimágenes de cada punto contradirían la irreducibilidad de V).

Sabemos que ϕ induce un k_0-monomorfismo $\overline{\phi} : k_0(W) \longrightarrow k_0(V)$. Esto nos permite considerar a $k_0(V)$ como una extensión (finita) de $k_0(W)$. Recíprocamente, todo k_0-monomorfismo entre los cuerpos $k_0(W)$ y $k_0(V)$ está inducido por una aplicación regular no constante ϕ (en principio racional densa, según el teorema 2.52, pero es regular por 3.54).

En definitiva, al igual que cada curva proyectiva regular se corresponde con un cuerpo de funciones algebraicas, tenemos que cada aplicación regular no constante entre curvas proyectivas regulares se corresponde con una extensión de cuerpos de funciones algebraicas.

Definición 6.3 Si $\phi : V \longrightarrow W$ es una aplicación regular no constante entre curvas proyectivas regulares sobre un cuerpo k_0, llamaremos *grado* de ϕ a

$$\operatorname{grad} \phi = |k_0(V) : \overline{\phi}[k_0(W)]|.$$

Igualmente, diremos que ϕ es separable, inseparable, etc. según lo sea la extensión de cuerpos $k_0(V)/\overline{\phi}[k_0(W)]$.

Conviene fijarse en un caso particular: si $\alpha \in k_0(V)$ no es constante, entonces $\alpha : V \longrightarrow \mathrm{P}^1$. Tenemos que $k_0(\mathrm{P}^1) = k_0(x)$, donde x es simplemente la identidad en P^1, luego la imagen de $k_0(\mathrm{P}^1)$ en $k_0(V)$ inducida por α es simplemente $k_0(\overline{\alpha}(x)) = k_0(\alpha)$.

6.2 Divisores primos

A lo largo de esta sección veremos cómo una curva proyectiva regular puede ser recuperada a partir de su cuerpo de funciones racionales. Los puntos de la curva se recuperan a partir de las valoraciones en el cuerpo. Para ver cómo es esto posible recordamos que si P es un punto regular de una curva cuasiproyectiva V, entonces el anillo $\mathcal{O}_P(V)$ es noetheriano y tiene un único ideal maximal $\mathfrak{m}_P$, formado por las funciones que se anulan en P. El teorema 3.53 nos da entonces que $\mathcal{O}_P(V)$ es un dominio de ideales principales, luego sus únicos ideales no nulos son los ideales $\mathfrak{m}_P^r$, para $r \geq 0$.

Definición 6.4 Sea V una curva cuasiproyectiva sobre un cuerpo de constantes k_0 y sea P un punto regular de V. Para cada función $\alpha \in \mathcal{O}_P(V)$ no nula definimos $v_P(\alpha)$ como el número natural r tal que $(\alpha) = \mathfrak{m}_P^r$. Equivalentemente $v_P(\alpha) = r$ si y sólo si $\alpha = \epsilon t^r$, donde t es un parámetro local de V en P (un generador de $\mathfrak{m}_P$) y ϵ es una unidad de $\mathcal{O}_P(V)$.

Es claro que $v_P(\alpha\beta) = v_P(\alpha) + v_P(\beta)$. Como $K = k_0(V)$ es el cuerpo de cocientes de $\mathcal{O}_P(V)$, tenemos que todo $\gamma \in K$ no nulo se expresa como $\gamma = \alpha/\beta$, con α, $\beta \in \mathcal{O}_P(V)$, y es claro que podemos definir $v_P(\gamma) = v_P(\alpha) - v_P(\beta)$ sin que importe la representación de γ como fracción. Así mismo es claro que $v_P : K^* \longrightarrow \mathbb{Z}$ es una valoración en K cuyo anillo de enteros es $\mathcal{O}_P(V)$.

Si $\alpha \in K$ y $v_P(\alpha) = r \geq 0$, entonces α es regular en P y se dice que tiene un *cero* de orden r en P (de modo que si α tiene un cero de orden 0 es que es regular en P pero no se anula). En cambio, si $v_P(\alpha) = -r < 0$, entonces α es singular en P y se dice que tiene un *polo* de orden r en P.

Si $k_0 = \mathbb{C}$ estas nociones coinciden con las usuales en la teoría de funciones de variable compleja.[1] La función t es una carta alrededor de P y la lectura

[1]Es fácil ver que si $f : U \longrightarrow \mathbb{C}$ es una función meromorfa en un entorno de un punto P de una superficie de Riemann V y z es una carta alrededor de P, entonces el orden en $z(P)$ de la lectura $z^{-1} \circ f$ es independiente de la carta, por lo que podemos llamarlo *orden* de f en P, y así podemos hablar del orden de un cero o de un polo de una función meromorfa sobre una superficie de Riemann.

de $\alpha = \epsilon t^r$ es la función $f(z) = \epsilon(t^{-1}(z))z^r$, donde el primer factor no se anula en 0, por lo que f tiene orden r en 0. Así pues, $v_P(\alpha)$ es el orden de α en P como función meromorfa.

En un cuerpo de funciones algebraicas, estos hechos nos llevan a la noción general de divisor primo:

Definición 6.5 Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0. Llamaremos *divisores primos* de K a las valoraciones en K que se anulan sobre k_0^*. Llamaremos Σ_K al conjunto de todos los divisores primos de K.

Si V es una curva cuasiproyectiva y $K = k_0(V)$, definimos $\Sigma_V = \Sigma_K$. A los divisores primos de K los llamaremos también *divisores primos*[2] de V.

Si $P \in V$ es un punto regular, la valoración v_P se anula sobre las funciones constantes de k_0^*, luego es un divisor primo de V. Así, si V es regular tenemos una aplicación $V \longrightarrow \Sigma_K$ dada por $P \mapsto v_P$. Enseguida veremos que se trata de una biyección.

Los divisores primos de un cuerpo de funciones algebraicas van a desempeñar un triple papel: a veces nos convendrá verlos como las valoraciones que son, a veces convendrá pensar en ellos como "puntos abstractos" y a veces los trataremos como "números primos abstractos" de una teoría aritmética que desarrollaremos después. Pensando en los dos últimos puntos de vista, los representaremos mediante letras góticas $\mathfrak{p}$, $\mathfrak{q}$, etc. Cuando queramos ver un primo $\mathfrak{p}$ como valoración escribiremos $v_\mathfrak{p}$ y hablaremos de "la valoración asociada a $\mathfrak{p}$", si bien —desde un punto de vista conjuntista— tenemos la identidad $\mathfrak{p} = v_\mathfrak{p}$. Representaremos por $\mathfrak{o}_\mathfrak{p}$ al anillo de enteros de $\mathfrak{p}$ y también llamaremos $\mathfrak{p}$ a su único ideal maximal.

Así, si P es un punto regular de una curva cuasiproyectiva y $\mathfrak{p}$ es su divisor primo asociado, se cumple (por definición) que $v_\mathfrak{p} = v_P$ y $\mathfrak{o}_\mathfrak{p} = \mathcal{O}_P$. Como ideales, $\mathfrak{p} = \mathfrak{m}_P$. Para incluir los puntos singulares en esta correspondencia hemos de debilitarla un poco:

Definición 6.6 Sea V una curva proyectiva sobre un cuerpo de constantes k_0 y $K = k_0(V)$. Diremos que un divisor primo $\mathfrak{p}$ de K *está situado sobre* un punto $P \in V$ si $\mathcal{O}_P \subset \mathfrak{o}_\mathfrak{p}$ y $\mathfrak{m}_P \subset \mathfrak{p}$.

Teorema 6.7 *Si V es una curva proyectiva sobre un cuerpo de constantes k_0 y $K = k_0(V)$, entonces cada divisor $\mathfrak{p}$ de K está situado sobre un único punto $P \in V$. La correspondencia $\mathfrak{p} \mapsto P$ es una aplicación $\Sigma_K \longrightarrow V$ para la cual cada punto regular $P \in V$ tiene una única antiimagen $\mathfrak{p}$, la dada por $v_\mathfrak{p} = v_P$. En particular, si V es regular tenemos una biyección entre Σ_K y V.*

Demostración: Podemos suponer que $V \subset \mathrm{P}^n$ no está contenida en ningún hiperplano, pues un hiperplano de P^n es isomorfo a P^{n-1}, luego podemos ir rebajando n hasta que esto ocurra. En particular, ninguna de las $n+1$ funciones

[2] En geometría algebraica es más frecuente referirse a ellos como "lugares" de V.

coordenadas x_i es idénticamente nula en V y, en consecuencia, los cocientes x_i/x_j son funciones no nulas de K. Sea $N = \max\limits_{i,j} v_{\mathfrak{p}}(x_i/x_j)$.

Reordenando las coordenadas podemos suponer que $N = v_{\mathfrak{p}}(x_1/x_{n+1})$, con lo que, para todo i,

$$v_{\mathfrak{p}}(x_i/x_{n+1}) = v_{\mathfrak{p}}\big((x_1/x_{n+1})(x_i/x_1)\big) = N - v_{\mathfrak{p}}(x_1/x_j) \geq 0.$$

Sea $V_* = V \cap A^n$. Acabamos de probar que las n coordenadas afines x_i están en $\mathfrak{o}_{\mathfrak{p}}$, luego $k_0[V_*] = k_0[x_1, \ldots, x_n] \subset \mathfrak{o}_{\mathfrak{p}}$.

Si $\mathfrak{p}$ es el ideal maximal de $\mathfrak{o}_{\mathfrak{p}}$, entonces $I = \mathfrak{p} \cap k_0[V_*]$ es un ideal primo de $k_0[V_*]$, que será de la forma $J/I(V_*)$, para un ideal primo J de $k_0[X_1, \ldots, X_n]$. Sea $W = V(J) \subset V_*$. Si fuera $W = V_*$ entonces sería $J = I(V_*)$ y por lo tanto $I = 0$. Esto significa que todos los elementos de $k_0[V_*]$ serían unidades de $\mathfrak{o}_{\mathfrak{p}}$, pero entonces todos los elementos de K serían unidades, lo cual es absurdo.

Como W es una subvariedad (cerrada) de V_*, ha de ser un punto $W = \{P\}$. Si $\alpha \in \mathcal{O}_P$, entonces $\alpha = \beta/\gamma$, donde β, $\gamma \in k_0[V_*]$ y $\gamma(P) \neq 0$. Así tenemos que β, $\gamma \in \mathfrak{o}_{\mathfrak{p}}$ y $\gamma \notin I$, luego $\gamma \notin \mathfrak{p}$, luego $\alpha = \beta/\gamma \in \mathfrak{o}_{\mathfrak{p}}$.

Si además $\alpha \in \mathfrak{m}_P$, entonces $\beta(P) = 0$, luego $\beta \in I \subset \mathfrak{p}$ y (como γ es una unidad de $\mathfrak{o}_{\mathfrak{p}}$) $\alpha \in \mathfrak{p}$.

Supongamos ahora que $\mathcal{O}_P \subset \mathfrak{o}_{\mathfrak{p}}$, $\mathcal{O}_Q \subset \mathfrak{o}_{\mathfrak{p}}$, $\mathfrak{m}_P \subset \mathfrak{p}$ y $\mathfrak{m}_Q \subset \mathfrak{p}$. Tomando un sistema de referencia adecuado, podemos suponer que $x_1(P) = 0$, $x_1(Q) \neq 0$, $x_{n+1}(P) \neq 0$, $x_{n+1}(Q) \neq 0$, es decir, que la función coordenada afín x_1 sea regular en ambos puntos y no se anule en Q. Así, $x_1 \in \mathfrak{m}_P$, $1/x_1 \in \mathcal{O}_Q$, luego $x_1 \in \mathfrak{p}$, $1/x_1 \in \mathfrak{o}_{\mathfrak{p}}$, lo cual es absurdo.

Si $P \in V$ es regular y $\mathfrak{p}$ es el divisor primo dado por $v_{\mathfrak{p}} = v_P$, es claro que $\mathfrak{p}$ es una antiimagen de P. Si hubiera otra $\mathfrak{q}$, tendríamos que $\mathfrak{o}_{\mathfrak{p}} = \mathcal{O}_P \subset \mathfrak{o}_{\mathfrak{q}}$ y $\mathfrak{p} = \mathfrak{m}_P \subset \mathfrak{q}$, pero esto es imposible (salvo si $\mathfrak{p} = \mathfrak{q}$), por ejemplo por 5.5. ■

El teorema siguiente prueba que la aplicación $\Sigma_K \longrightarrow V$ que acabamos de describir es suprayectiva, es decir, todo punto de V está situado bajo un primo.

Teorema 6.8 *Sea V una curva proyectiva sobre un cuerpo k_0 y $r : V_r \longrightarrow V$ su regularización. Entonces el diagrama siguiente es conmutativo:*

$$\begin{tikzcd} \Sigma_{V_r} \arrow[r, "r^*"] \arrow[d] & \Sigma_V \arrow[d] \\ V_r \arrow[r, "r"'] & V \end{tikzcd}$$

donde r^* es la biyección inducida por el isomorfismo $\bar{r} : k_0(V) \longrightarrow k_0(V_r)$, es decir, la biyección que cumple $v_{r^*(\mathfrak{p})}(\alpha) = v_{\mathfrak{p}}(\bar{r}(\alpha))$, para todo $\alpha \in k_0(V)$ y todo $\mathfrak{p} \in \Sigma_{V_r}$. En particular la aplicación $\Sigma_V \longrightarrow V$ es suprayectiva.

Demostración: Tomamos $\mathfrak{p} \in \Sigma_{V_r}$, su imagen $P \in V_r$ y $Q = r(P) \in V$. Hemos de probar que Q es también la imagen de $r^*(\mathfrak{p})$, es decir, que $\mathcal{O}_Q \subset \mathfrak{o}_{r^*(\mathfrak{p})}$ y $\mathfrak{m}_Q \subset r^*(\mathfrak{p})$.

Para probarlo tomamos $\alpha \in \mathcal{O}_Q$. El teorema 2.52 nos da que $\bar{r}(\alpha) \in \mathcal{O}_P = \mathfrak{o}_\mathfrak{p}$, luego $0 \leq v_\mathfrak{p}(\bar{r}(\alpha)) = v_{r^*(\mathfrak{p})}(\alpha)$, luego $\alpha \in \mathfrak{o}_{r^*(\mathfrak{p})}$.

Si $\alpha \in \mathfrak{m}_Q$ sabemos además que $\alpha(Q) = 0$ y $\bar{r}(\alpha)(P) = \alpha(r(P)) = \alpha(Q) = 0$, luego $\bar{r}(\alpha) \in \mathfrak{m}_P$. La conclusión es análoga.

Teniendo en cuenta que las flechas horizontal superior y vertical izquierda son biyecciones, y que la horizontal inferior es suprayectiva, es claro que la vertical derecha es también suprayectiva, como afirmábamos. ■

Si pensamos en Σ_V como una "reconstrucción abstracta" de V_r, entonces la aplicación $\Sigma_V \longrightarrow V$ es el equivalente abstracto de r.

Veamos ahora que las aplicaciones regulares entre curvas proyectivas regulares inducen aplicaciones entre los conjuntos de divisores primos. En principio sabemos que determinan una extensión finita entre sus cuerpos de funciones, así que vamos a estudiar dichas extensiones. Empezamos con un hecho elemental:

Teorema 6.9 *Si K/k es una extensión algebraica, la única extensión a K del valor absoluto trivial de k es el valor absoluto trivial.*

DEMOSTRACIÓN: En caso contrario existe $\alpha \in K$ con $|\alpha| > 1$. Entonces

$$\alpha^n = c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0, \quad \text{con } c_i \in k.$$

Pero de aquí se sigue que $|\alpha|^n = |\alpha|^{n-1}$, lo cual es imposible. ■

Así, si K/k es una extensión de cuerpos de funciones algebraicas y $\mathfrak{P}$ es un divisor primo de K, la valoración $v_\mathfrak{P}$ no puede ser idénticamente nula en k^*, pues entonces cualquier valor absoluto de $v_\mathfrak{P}$ en K se restringiría al valor absoluto trivial en k, en contra del teorema anterior. Como $v_\mathfrak{P} : K^* \longrightarrow \mathbb{Z}$ es un homomorfismo de grupos, ha de ser $v_\mathfrak{P}[k^*] = e\mathbb{Z}$, para cierto $e \geq 1$. Es claro entonces que $v = (1/e)v_\mathfrak{P}|_k$ es una valoración en k que se anula en k_0^*, luego se corresponde con un divisor primo $\mathfrak{p}$ de k. En resumen:

Teorema 6.10 *Si K/k es una extensión de cuerpos de funciones algebraicas, para cada divisor primo $\mathfrak{P}$ de K existe un único divisor primo $\mathfrak{p}$ de k tal que $v_\mathfrak{P}|_k = ev_\mathfrak{p}$, para cierto natural $e = e(\mathfrak{P}/\mathfrak{p})$.*

Definición 6.11 En la situación del teorema anterior, diremos que el primo $\mathfrak{P}$ *divide* a $\mathfrak{p}$, y lo representaremos por $\mathfrak{P} \mid \mathfrak{p}$. El número $e(\mathfrak{P}/\mathfrak{p})$ (o $e_\mathfrak{P}$) se llama *índice de ramificación* de $\mathfrak{p}$ en $\mathfrak{P}$. Si $e(\mathfrak{P}/\mathfrak{p}) > 1$ diremos que $\mathfrak{p}$ se *ramifica* en $\mathfrak{P}$. En este caso diremos también que $\mathfrak{p}$ es un primo de k *ramificado* en K o que $\mathfrak{P}$ es un primo de K *ramificado* sobre k. Se comprueba inmediatamente que $\mathfrak{P} \mid \mathfrak{p}$ si y sólo si la restricción a k biyecta los valores absolutos de $\mathfrak{P}$ con los de $\mathfrak{p}$.

Vemos así que una inclusión $k \subset K$ de cuerpos de funciones algebraicas (o, más en general, un k_0-monomorfismo entre ellos) da lugar a una aplicación $\Sigma_K \longrightarrow \Sigma_k$. Si k_0 es algebraicamente cerrado esta aplicación tiene una interpretación geométrica.

Teorema 6.12 *Sea $\phi : V \longrightarrow W$ una aplicación regular suprayectiva entre dos curvas proyectivas y sea $\overline{\phi} : k_0(W) \longrightarrow k_0(V)$ el k_0-monomorfismo que induce. Éste nos permite considerar a $k_0(V)$ como extensión de $k_0(W)$, lo que nos da una aplicación $\phi : \Sigma_V \longrightarrow \Sigma_W$. Entonces el diagrama natural conmuta:*

$$\begin{tikzcd} \Sigma_V \arrow[r, "\phi"] \arrow[d] & \Sigma_W \arrow[d] \\ V \arrow[r, "\phi"] & W \end{tikzcd}$$

DEMOSTRACIÓN: Sea $\mathfrak{P} \in \Sigma_V$ y $\mathfrak{p}$ el primo de W que divide a $\mathfrak{P}$. Sea $P \in V$ el punto situado bajo $\mathfrak{P}$. Hemos de probar que $\phi(P)$ está situado bajo $\mathfrak{p}$. En efecto, si $f \in \mathcal{O}_{\phi(P)}(W)$, tenemos que $v_\mathfrak{p}(f) = e(\mathfrak{P}/\mathfrak{p})^{-1} v_\mathfrak{P}(\overline{\phi}(f)) \geq 0$, pues $\overline{\phi}(f) \in \mathcal{O}_P(V) \subset \mathfrak{O}_\mathfrak{P}$. Esto prueba que $\mathcal{O}_{\phi(P)}(W) \subset \mathfrak{o}_\mathfrak{p}$, y el mismo razonamiento nos da que $\mathfrak{m}_{\phi(P)} \subset \mathfrak{p}$, luego $\mathfrak{p}$ está sobre $\phi(P)$. ■

A partir de aquí ya podemos identificar sin ambigüedades los puntos de una curva proyectiva regular con sus divisores primos asociados. Así, por ejemplo, si V y W son curvas proyectivas regulares, el teorema anterior afirma que (los divisores primos de) los puntos de V que dividen a (el divisor primo de) un punto $P \in W$ son (los asociados a) las antiimágenes de P.

En particular, dada una aplicación $\phi : V \longrightarrow W$ entre curvas proyectivas regulares, podemos hablar del índice de ramificación $e(\phi, P)$ para cada punto $P \in V$.

Volviendo al caso general, es claro que si tenemos una cadena de extensiones $k \subset K \subset L$ con primos correspondientes $\mathfrak{Q} \mid \mathfrak{P} \mid \mathfrak{p}$, se tiene la relación multiplicativa:

$$e(\mathfrak{Q}/\mathfrak{p}) = e(\mathfrak{Q}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p}).$$

Si $\mathfrak{p}$ es un divisor primo de un cuerpo de funciones algebraicas k, llamaremos $k_\mathfrak{p}$ a la compleción correspondiente, llamaremos $\mathfrak{o}_\mathfrak{p}$ indistintamente al anillo de enteros de k o de $k_\mathfrak{p}$, llamaremos $\mathfrak{p}$ indistintamente al ideal primo de cualquiera de los dos anillos y $\overline{k}_\mathfrak{p}$ a cualquiera de los dos cuerpos de restos. Según 5.14, ambos son isomorfos a través de la aplicación inducida por la inclusión entre los anillos de enteros.

Si K/k es una extensión de cuerpos de funciones algebraicas, la clausura de k en $K_\mathfrak{P}$ es una compleción de k respecto de $\mathfrak{p}$, luego es topológicamente isomorfa a $k_\mathfrak{p}$. De hecho, podemos tomarla como $k_\mathfrak{p}$ y así $k_\mathfrak{p} \subset K_\mathfrak{P}$. Más aún, $Kk_\mathfrak{p}$ es una extensión finita de $k_\mathfrak{p}$, luego es un cuerpo métrico completo (por el teorema 5.27), luego es cerrado en $K_\mathfrak{P}$ y contiene a K, luego $K_\mathfrak{P} = Kk_\mathfrak{p}$.

La relación $v_\mathfrak{P}|_k = ev_\mathfrak{p}$, que en principio se cumple sobre k, se cumple de hecho sobre $k_\mathfrak{p}$ por la densidad de k y la continuidad de las valoraciones. Esto significa que el índice de ramificación $e(\mathfrak{P}/\mathfrak{p})$ es el mismo que el de $K_\mathfrak{P}/k_\mathfrak{p}$.

Por otra parte, el hecho de que los valores absolutos de $\mathfrak{P}$ se restrinjan a los de $\mathfrak{p}$ se traduce en que $\mathfrak{o}_\mathfrak{p} \subset \mathfrak{O}_\mathfrak{P}$ (vistos como anillos en K y k) y $\mathfrak{p} \subset \mathfrak{P}$

(vistos como ideales en dichos anillos). Por consiguiente, la inclusión induce un monomorfismo $\overline{k}_{\mathfrak{p}} \longrightarrow \overline{K}_{\mathfrak{P}}$ entre los cuerpos de restos correspondientes. Más aún, tenemos el diagrama conmutativo

$$\begin{tikzcd} \overline{K}_{\mathfrak{P}} \arrow[r] & \overline{K}_{\mathfrak{P}} \\ \overline{k}_{\mathfrak{p}} \arrow[u] \arrow[r] & \overline{k}_{\mathfrak{p}} \arrow[u] \end{tikzcd}$$

donde los cuerpos de la izquierda son los de K y k, mientras que los de la derecha son los de $K_{\mathfrak{P}}$ y $k_{\mathfrak{p}}$. Por lo tanto, el cuerpo de restos de K es una extensión finita del cuerpo de restos de k, del mismo grado que la correspondiente extensión entre los cuerpos de restos de las compleciones.

Definición 6.13 Sea K/k una extensión de cuerpos de funciones algebraicas, sea $\mathfrak{p}$ un divisor primo en k y $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K. Llamaremos *grado de inercia* de $\mathfrak{p}$ en $\mathfrak{P}$ al grado

$$f_{\mathfrak{P}} = f(\mathfrak{P}/\mathfrak{p}) = |\overline{K}_{\mathfrak{P}} : \overline{k}_{\mathfrak{p}}|,$$

que coincide con el grado de inercia de la extensión local $K_{\mathfrak{P}}/k_{\mathfrak{p}}$.

Al igual que sucede con el índice de ramificación, si $k \subset K \subset L$ es una cadena de extensiones con primos $\mathfrak{Q} \mid \mathfrak{P} \mid \mathfrak{p}$, es claro que se cumple la relación:

$$f(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p}).$$

Si definimos el *grado local* de $\mathfrak{p}$ en $\mathfrak{P}$ como

$$n_{\mathfrak{P}} = n(\mathfrak{P}/\mathfrak{p}) = |K_{\mathfrak{P}} : k_{\mathfrak{p}}|,$$

entonces el teorema 5.32 nos da la relación

$$n(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}).$$

Pronto demostraremos que si k_0 es algebraicamente cerrado todos los grados de inercia valen 1, por lo que el grado de inercia no tiene interpretación geométrica. Para ello necesitamos algunos resultados generales. Notemos que —de momento— ni siquiera tenemos garantizado que un cuerpo de funciones algebraicas arbitrario tenga divisores primos. El teorema siguiente muestra que los cuerpos de fracciones algebraicas tienen divisores primos:

Teorema 6.14 *Sea $k = k_0(x)$, donde x es trascendente sobre k_0. Entonces los divisores primos de k son los asociados a los ideales primos de $k_0[x]$ según el ejemplo de la página* 197 *y el primo infinito ∞ dado por*[3] $v_\infty(f) = -\operatorname{grad} f$. *Todos ellos son distintos dos a dos.*

[3]Definimos el grado de una fracción algebraica $f = p(x)/q(x)$ como la diferencia de los grados $\operatorname{grad} p - \operatorname{grad} q$.

DEMOSTRACIÓN: Sea $\mathfrak{p}$ un divisor primo de k y supongamos que $v_{\mathfrak{p}}(x) \geq 0$. Entonces $v_{\mathfrak{p}}(p(x)) \geq 0$ para todo $p(x) \in k_0[x]$. Si todos los polinomios tuvieran valor nulo, de hecho $v_{\mathfrak{p}}$ sería idénticamente nula, luego ha de existir un polinomio $p(x)$ tal que $v_{\mathfrak{p}}(p(x)) > 0$. Descomponiéndolo en primos, podemos suponer que $p(x)$ es primo. Entonces $p(x)$ es el único primo (salvo asociados) con valor positivo, pues si $q(x)$ es otro primo, entonces existen polinomios $a(x)$ y $b(x)$ tales que $a(x)p(x) + b(x)q(x) = 1$. Si $v_{\mathfrak{p}}(q(x)) > 0$, el miembro izquierdo tiene valor positivo, pero el derecho no, contradicción.

Ahora es claro que $v_{\mathfrak{p}}$ coincide con la valoración inducida por el ideal $(p(x))$ y como ideales distintos inducen valoraciones distintas, podemos identificar cada ideal con su divisor correspondiente $\mathfrak{p} = (p(x))$.

Supongamos ahora que $v_{\mathfrak{p}}(x) < 0$. Entonces el valor de un monomio es $v_{\mathfrak{p}}(ax^n) = nv_{\mathfrak{p}}(x)$ y, en una suma de monomios, el monomio de mayor grado tiene menor valor. Por consiguiente $v_{\mathfrak{p}}(p(x)) = \operatorname{grad} p(x) v_{\mathfrak{p}}(x)$ para todo polinomio $p(x) \in k_0[x]$, y de aquí se sigue que la igualdad vale también para todo $p(x) \in k$. Como $v_{\mathfrak{p}}$ ha de ser suprayectiva, necesariamente $v_{\mathfrak{p}}(x) = -1$, con lo que $\mathfrak{p} = \infty$. (En realidad, para completar la prueba hay que comprobar que v_∞ es una valoración, lo cual es inmediato.)

Ciertamente v_∞ es distinta de todas las valoraciones asociadas a ideales primos, pues es la única que toma un valor negativo sobre x. ■

Es fácil ver que un polinomio $p(z) \in \mathbb{C}[z]$ tiene un polo en ∞ de orden igual a su grado, luego la valoración v_∞ en $\mathbb{C}(z)$ asigna a cada polinomio (y, por consiguiente, a cada fracción algebraica) su orden en el punto ∞ en el sentido de la teoría de funciones de variable compleja.

Si k_0 es un cuerpo algebraicamente cerrado, el teorema anterior muestra explícitamente la biyección del teorema 6.7: podemos pensar en $k_0(x)$ como el cuerpo de funciones racionales de $\mathrm{P}^1(k_0) = k_0 \cup \{\infty\}$. Los ideales primos de $k_0[x]$ son los de la forma $(x - a)$, con $a \in k_0$, y es claro que el divisor primo asociado a $(x - a)$ es el único primo situado sobre a, mientras que el primo ∞ es el único primo situado sobre el punto ∞.

Volviendo al caso general, podemos clasificar los divisores primos de un cuerpo $k_0(x)$ en divisores primos finitos (identificables con los ideales primos de $k_0[x]$) y el primo infinito. No obstante, hemos de tener presente que esta clasificación es relativa a la base de trascendencia x. Por ejemplo, si $y = 1/x$, entonces $k = k_0(x) = k_0(y)$, y si $\mathfrak{p}$ es el primo infinito para x, se cumple que $v_{\mathfrak{p}}(y) = -v_{\mathfrak{p}}(x) = 1$, luego $v_{\mathfrak{p}}$ es la valoración asociada al ideal (y) de $k_0[y]$. Vemos, pues, que un mismo divisor primo $\mathfrak{p}$ puede ser finito para una base e infinito para otra. Esto hace que en muchas ocasiones no perdamos generalidad si trabajamos únicamente con primos finitos. El teorema siguiente es un ejemplo:

Teorema 6.15 *Sea $k = k_0(x)$ un cuerpo de fracciones algebraicas y $\mathfrak{p}$ un divisor primo de k. Entonces cuerpo de restos $\overline{k}_{\mathfrak{p}}$ es una extensión finita de k_0. Si $\mathfrak{p}$ es un primo finito asociado al ideal primo $\mathfrak{p} = (p(x))$ de $k_0[x]$, entonces $|\overline{k}_{\mathfrak{p}} : k_0| = \operatorname{grad} p$. Si $\mathfrak{p}$ es el primo infinito, entonces $|\overline{k}_{\mathfrak{p}} : k_0| = 1$.*

Demostración: Supongamos primero que $\mathfrak{p} = (p(x))$ es finito. Un elemento arbitrario de $\mathfrak{o}_\mathfrak{p}$ es una fracción $f(x)/g(x)$ tal que $p(x) \nmid g(x)$. Existen polinomios $u(x)$ y $v(x)$ tales que $u(x)p(x) + v(x)g(x) = 1$, luego

$$f(x) = f(x)u(x)p(x) + f(x)v(x)g(x).$$

Por consiguiente

$$f(x)v(x) - \frac{f(x)}{g(x)} = \frac{f(x)v(x)g(x) - f(x)}{g(x)} = -\frac{f(x)u(x)}{g(x)}p(x) \in \mathfrak{p}.$$

(Aquí $\mathfrak{p}$ es el ideal de $\mathfrak{o}_\mathfrak{p}$.) Esto prueba que la clase de f/g en $\overline{k}_\mathfrak{p}$ es la misma que la del polinomio $f(x)v(x)$, luego el monomorfismo de cuerpos $k_0[x]/\mathfrak{p} \longrightarrow \overline{k}_\mathfrak{p}$ es un isomorfismo.

La inclusión $k_0 \longrightarrow \overline{k}_\mathfrak{p}$ factoriza como $k_0 \longrightarrow k_0[x]/\mathfrak{p} \longrightarrow \overline{k}_\mathfrak{p}$ y es bien conocido que el cuerpo intermedio es una extensión finita de k_0 cuyo grado es $\operatorname{grad} p(x)$.

Si $\mathfrak{p}$ es el primo infinito, llamando $y = 1/x$ tenemos que $\mathfrak{p}$ es el primo asociado al ideal (y) de $k_0[y]$. Como el polinomio y tiene grado 1, la parte ya probada nos da que $|\overline{k}_\mathfrak{p} : k_0| = 1$. ■

Los divisores primos de un cuerpo de funciones algebraicas arbitrario K los estudiaremos a partir del hecho de que K es una extensión de un cuerpo de fracciones algebraicas $k = k_0(x)$. Por lo pronto, sabemos que si $\mathfrak{P}$ es un divisor primo de K y $\mathfrak{p}$ es el divisor primo de k que cumple $\mathfrak{P} \mid \mathfrak{p}$, la extensión $\overline{K}_\mathfrak{P}/\overline{k}_\mathfrak{p}$ es finita (de grado $f(\mathfrak{P}/\mathfrak{p})$ y la extensión $\overline{k}_\mathfrak{p}/k_0$ es finita por el teorema anterior. Esto justifica la definición siguiente:

Definición 6.16 Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 y $\mathfrak{P}$ un divisor primo de K. Llamaremos *grado* de $\mathfrak{P}$ a

$$\operatorname{grad} \mathfrak{P} = |\overline{K}_\mathfrak{P} : k_0|.$$

El teorema anterior afirma que si $\mathfrak{p} = (p(x))$ es un divisor finito de un cuerpo de fracciones algebraicas $k = k_0(x)$, entonces $\operatorname{grad} \mathfrak{p} = \operatorname{grad} p(x)$, mientras que $\operatorname{grad} \infty = 1$.

Si K/k es una extensión de cuerpos de funciones algebraicas, $\mathfrak{P}$ es un divisor primo en K y $\mathfrak{p}$ es el primo de k al cual divide, es claro que se cumple la relación

$$\operatorname{grad} \mathfrak{P} = f(\mathfrak{P}/\mathfrak{p}) \operatorname{grad} \mathfrak{p}. \tag{6.1}$$

Ahora es evidente que si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes algebraicamente cerrado, entonces todos los divisores primos tienen grado 1 y los grados de inercia en todas las extensiones son 1.

Ahora probaremos que todo primo de k es divisible entre un primo de K, así como que el número de divisores es finito.

Sea k un cuerpo de funciones algebraicas y $\mathfrak{p}$ un divisor primo en k. Por simplificar fijaremos un valor absoluto $|\ |_\mathfrak{p}$ asociado a $\mathfrak{p}$ en k (aunque es fácil ver que la elección es irrelevante en todo lo que sigue). Llamaremos igual a su extensión a la compleción $k_{\mathfrak{p}}$. Sea $\mathbb{K}_{\mathfrak{p}}$ una clausura algebraica de $k_{\mathfrak{p}}$. El teorema 5.27 nos da que el valor absoluto de $k_{\mathfrak{p}}$ se extiende de forma única a cada extensión finita de $k_{\mathfrak{p}}$, luego se extiende a todo $\mathbb{K}_{\mathfrak{p}}$. Seguiremos llamando $|\;|_{\mathfrak{p}}$ a la extensión. Así $\mathbb{K}_{\mathfrak{p}}$ es un cuerpo métrico.[4] No es cierto que sea discreto o completo, pero cada subcuerpo de grado finito sobre $k_{\mathfrak{p}}$ sí lo es (por 5.28).

Teorema 6.17 *Sea K/k una extensión de cuerpos de funciones algebraicas y $\mathfrak{p}$ un divisor primo de k. Entonces:*

a) Para cada k-monomorfismo $\sigma : K \longrightarrow \mathbb{K}_{\mathfrak{p}}$ existe un primo $\mathfrak{P}$ en K divisor de $\mathfrak{p}$ tal que $|\alpha|_{\mathfrak{P}} = |\sigma(\alpha)|_{\mathfrak{p}}$ para todo $\alpha \in K$.

b) Para cada primo $\mathfrak{P}$ de K que divide a $\mathfrak{p}$, los k-monomorfismos que inducen el primo $\mathfrak{P}$ según el apartado a) son exactamente las restricciones a K de los $k_{\mathfrak{p}}$-monomorfismos $\sigma : K_{\mathfrak{P}} \longrightarrow \mathbb{K}_{\mathfrak{p}}$. Además, monomorfismos distintos tienen restricciones distintas.

Demostración: Notemos que $\sigma[K]$ es una extensión finita de k, luego $L = k_{\mathfrak{p}}\sigma[K]$ es una extensión finita de $k_{\mathfrak{p}}$. Por consiguiente, L es un cuerpo métrico discreto y completo. En particular L es cerrado, luego contiene a la clausura de $\sigma[K]$, la cual contiene a su vez a la clausura de k, que es $k_{\mathfrak{p}}$. Esto prueba que $\sigma[K]$ es denso en L. Sea v la valoración de L. La continuidad de v hace que $\sigma[K]$ contenga elementos de valor 1, luego $v|_{\sigma[K]}$ es una valoración en $\sigma[K]$ (que se anula sobre k_0^*). Sea $\mathfrak{P}$ el divisor de K que convierte a σ en un isomorfismo topológico. La unicidad de la compleción implica que σ se extiende a una isometría $\sigma : K_{\mathfrak{P}} \longrightarrow \mathbb{K}_{\mathfrak{p}}$. Esto significa que un valor absoluto de $\mathfrak{P}$ es el dado por

$$|\alpha|_{\mathfrak{P}} = |\sigma(\alpha)|_{\mathfrak{p}}, \qquad \text{para todo } \alpha \in K_{\mathfrak{P}}.$$

En particular $\mathfrak{P}$ cumple a), y también hemos visto que σ se extiende a una isometría en $K_{\mathfrak{P}}$. Por otra parte, si $\mathfrak{P}$ es un divisor primo de $\mathfrak{p}$ en K, el teorema 5.27 implica que cada $k_{\mathfrak{p}}$-monomorfismo $\sigma : K_{\mathfrak{P}} \longrightarrow \mathbb{K}_{\mathfrak{p}}$ es una isometría, pues el valor absoluto en $K_{\mathfrak{P}}$ dado por $|\alpha| = |\sigma(\alpha)|_{\mathfrak{p}}$ extiende al valor absoluto de $k_{\mathfrak{p}}$, luego ha de ser el valor absoluto de $K_{\mathfrak{P}}$.

Sólo falta probar la última afirmación de b), pero es claro que la densidad de K en $K_{\mathfrak{P}}$ implica que las restricciones a K de dos $k_{\mathfrak{p}}$-monomorfismos distintos han de ser dos k-monomorfismos distintos. ■

Como el número de k-monomorfismos $\sigma : K \longrightarrow \mathbb{K}_{\mathfrak{p}}$ es finito (es el grado de separabilidad de K/k) concluimos que cada divisor primo de k tiene un número finito de divisores en K.

Con esto hemos probado que si $k \subset K$ entonces la aplicación $\Sigma_K \longrightarrow \Sigma_k$ es suprayectiva y cada punto de Σ_k tiene una cantidad finita de antiimágenes.

[4] Es fácil ver que si partimos de otro valor absoluto asociado a $\mathfrak{p}$, la extensión es equivalente, por lo que la estructura métrica de $\mathbb{K}_{\mathfrak{p}}$ sólo depende de $\mathfrak{p}$ y no del valor absoluto de partida.

Ahora es inmediato que todo cuerpo de funciones algebraicas K tiene divisores primos, pues K es una extensión de un cuerpo $k = k_0(x)$ de funciones racionales, y ya hemos visto que estos cuerpos tienen divisores primos.

El teorema anterior nos da información mucho más precisa que la mera finitud de los divisores de un primo en una extensión:

Teorema 6.18 *Sea K/k una extensión separable de grado n de cuerpos de funciones algebraicas y $\mathfrak{p}$ un primo en k. Entonces $\mathfrak{p}$ es divisible por un número finito de primos $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ en K, de modo que*

$$n = n(\mathfrak{P}_1/\mathfrak{p}) + \cdots + n(\mathfrak{P}_r/\mathfrak{p}).$$

Equivalentemente, si $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ y $f_i = f(\mathfrak{P}_i/\mathfrak{p})$, se cumple la relación

$$n = e_1 f_1 + \cdots + e_r f_r.$$

DEMOSTRACIÓN: Si la extensión K/k es separable, también lo son todas las extensiones $K_{\mathfrak{P}_i}/k_{\mathfrak{p}}$, pues $K_{\mathfrak{P}_i} = Kk_{\mathfrak{p}}$. Por lo tanto, el número de $k_{\mathfrak{p}}$-monomorfismos $\sigma : K_{\mathfrak{P}_i} \longrightarrow \mathbb{K}_{\mathfrak{p}}$ es exactamente $n_i = n(\mathfrak{P}_i/\mathfrak{p})$, los cuales se restringen a otros tantos k-monomorfismos $\sigma : K \longrightarrow \mathbb{K}_{\mathfrak{p}}$. Puesto que cada uno de estos monomorfismos se extiende a una única compleción $K_{\mathfrak{P}_i}$, resulta que las $n_1 + \cdots + n_r$ restricciones son todos los k-monomorfismos de K, luego son n en total. ■

Si k_0 es algebraicamente cerrado todos los f_i valen 1, con lo que la relación se reduce a $e_1 + \cdots + e_r = n$.

El teorema siguiente puede verse como una generalización del principio de prolongación analítica (afirma que una función algebraica no nula tiene un número finito de ceros y polos):

Teorema 6.19 *Si K es un cuerpo de funciones algebraicas y $x \in K^*$, entonces existe a lo sumo una cantidad finita de divisores primos $\mathfrak{P}$ en K tales que $v_{\mathfrak{P}}(x) \neq 0$.*

DEMOSTRACIÓN: Si x es algebraico sobre el cuerpo de constantes k_0, entonces $v_{\mathfrak{P}}(x) = 0$ para todo divisor primo $\mathfrak{P}$ (por el teorema 6.9). Si es trascendente, consideramos el cuerpo $k = k_0(x)$. Obviamente K/k es una extensión de cuerpos de funciones algebraicas. Si hay infinitos primos en K cuyas valoraciones no se anulan en x, los primos de k a los que dividen son infinitos también, y sus valoraciones no se anulan en x. Ahora bien, k es un cuerpo de funciones racionales y sólo hay dos primos cuyas valoraciones no se anulan en x, a saber, el primo infinito y el primo finito asociado al ideal (x) de $k_0[x]$. ■

Con esto estamos en condiciones de probar que los elementos de un cuerpo de funciones algebraicas K sobre un cuerpo de constantes algebraicamente cerrado pueden verse como funciones definidas sobre Σ_K. En efecto:

Definición 6.20 Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes algebraicamente cerrado k_0 y sea $\alpha \in K$. Para cada $\mathfrak{P} \in \Sigma_K$, definimos $\alpha(\mathfrak{P}) \in k_0 \cup \{\infty\}$ como sigue:

a) Si $v_{\mathfrak{P}}(\alpha) \geq 0$, tenemos que $\alpha \in \mathfrak{O}_{\mathfrak{P}}$ y $\mathfrak{O}_{\mathfrak{P}}/\mathfrak{P} = \overline{K}_{\mathfrak{P}} \cong k_0$, luego podemos tomar como $\alpha(\mathfrak{P}) \in k_0$ el único elemento que cumple

$$\alpha \equiv \alpha(\mathfrak{P}) \ (\text{mód } \mathfrak{P}).$$

b) Si $v_{\mathfrak{P}}(\alpha) < 0$ definimos $\alpha(\mathfrak{P}) = \infty$ (y entonces diremos que α tiene un *polo* en $\mathfrak{P}$).

Así tenemos definida una función $\alpha : \Sigma_K \longrightarrow k_0 \cup \{\infty\}$ que podemos identificar con α, pues si $\alpha, \beta \in K$ determinan la misma función, entonces para todos los divisores primos $\mathfrak{P}$ de K tales que $v_{\mathfrak{P}}(\alpha) \geq 0$ y $v_{\mathfrak{P}}(\beta) \geq 0$ (todos salvo una cantidad finita) se cumple $\alpha \equiv \beta$ (mód $\mathfrak{P}$), luego $v_{\mathfrak{P}}(\alpha - \beta) > 0$, luego $\alpha - \beta$ tiene infinitos ceros, lo cual sólo puede ocurrir si $\alpha = \beta$.

Más aún, si $\mathfrak{P}$ no es un polo de ninguna de las dos funciones α, $\beta \in K$, entonces

$$(\alpha + \beta)(\mathfrak{P}) = \alpha(\mathfrak{P}) + \beta(\mathfrak{P}), \qquad (\alpha\beta)(\mathfrak{P}) = \alpha(\mathfrak{P})\beta(\mathfrak{P}).$$

En resumen, si el cuerpo de constantes k_0 es algebraicamente cerrado, los elementos de un cuerpo de funciones algebraicas K pueden verse como funciones sobre Σ_K con valores en $k_0 \cup \{\infty\}$ y las operaciones de K se corresponden con las definidas puntualmente.

Nota Si V es una curva proyectiva, entonces cada $\alpha \in k_0(V)$ puede verse como función sobre V o como función sobre Σ_V. Ambas funciones se corresponden a través de la biyección natural entre ambos conjuntos. En efecto, si un primo $\mathfrak{P}$ de V está situado sobre un punto $P \in V$ y $\alpha \in \mathcal{O}_P(V)$, se cumple que $\alpha - \alpha(P) \in \mathfrak{m}_P \subset \mathfrak{P}$, luego $\alpha(\mathfrak{P}) = \alpha(P)$. Si V es regular, esto nos dice que al identificar V con Σ_V cada función $\alpha \in k_0(V)$ se identifica consigo misma. ■

En general, si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 no algebraicamente cerrado, no podemos considerar a los elementos de K como funciones sobre Σ_K. De hecho, los elementos de K no son funciones en ningún sentido. No obstante, nada nos impide llamarlos "funciones", e incluso podemos decir que una función $\alpha \in K$ tiene un *cero* de orden n en un primo $\mathfrak{P}$ cuando $v_{\mathfrak{P}}(\alpha) = n$, o que tiene un *polo* de orden n si $v_{\mathfrak{P}}(\alpha) = -n$, o que α es *regular* o *singular* en $\mathfrak{P}$, según si $v_{\mathfrak{P}}(\alpha) \geq 0$ o $v_{\mathfrak{P}}(\alpha) < 0$, etc.

Disponemos así de un lenguaje geométrico aplicable a un contexto algebraico abstracto. Los resultados geométricos que conocemos continúan siendo ciertos en este contexto general en la medida en que tienen sentido. Por ejemplo, resulta natural conjeturar que las funciones sin ceros ni polos son exactamente las constantes, lo cual es cierto con un matiz:

Definición 6.21 Si K es un cuerpo de funciones algebraicas sobre un cuerpo k_0, llamaremos *cuerpo exacto de constantes* de K a la clausura algebraica k_1 de k_0 en K.

Es claro que K es también un cuerpo de funciones algebraicas sobre k_1, y el teorema 6.9 nos da que los divisores primos de K son los mismos respecto a cualquiera de los dos cuerpos. Si $\mathfrak{P}$ es un divisor primo, entonces $\overline{K}_{\mathfrak{P}}$ ha de ser una extensión finita tanto de k_0 como de k_1, luego la extensión k_1/k_0 es finita. Estos hechos hacen que en muchas ocasiones no perdamos generalidad si suponemos $k_1 = k_0$. No obstante, hay que tener en cuenta es que el grado de un divisor depende del cuerpo de constantes. La relación es:

$$\operatorname{grad}_{k_0} \mathfrak{P} = |k_1 : k_0| \operatorname{grad}_{k_1} \mathfrak{P}.$$

Ahora ya podemos determinar las funciones sin ceros ni polos:

Teorema 6.22 *Si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0, entonces las funciones de K sin ceros ni polos son exactamente las de k_1^*. Si α, $\beta \in K$ cumplen $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{P}}(\beta)$ para todo $\mathfrak{P} \in \Sigma_K$, entonces $\alpha = c\beta$, con $c \in k_1^*$.*

DEMOSTRACIÓN: Si $v_{\mathfrak{P}}(x) = 0$ para todo $\mathfrak{P} \in \Sigma_K$, entonces x es algebraico sobre k_0, pues si fuera trascendente podríamos considerar $k = k_0(x)$ y el primo $\mathfrak{p} = (x)$, que cumple $v_{\mathfrak{p}}(x) = 1$. Si $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K se cumple $v_{\mathfrak{P}}(x) \neq 0$, contradicción. Así pues, $x \in k_1$. El recíproco es obvio, por el teorema 6.9.

Para la segunda parte, es claro que si una de las dos funciones es nula la otra también lo es. En caso contrario α/β es una función sin ceros ni polos, luego es una constante de k_1. ■

6.3 Funciones algebraicas complejas

En esta sección estudiamos con más detalle el caso de los cuerpos de funciones algebraicas sobre $k_0 = \mathbb{C}$. Sabemos que podemos identificarlos con los cuerpos de funciones racionales de las curvas proyectivas regulares, las cuales son superficies de Riemann. Vamos a ver que los conjuntos de divisores primos también admiten una estructura natural de superficie de Riemann. En efecto:

Teorema 6.23 *Si K es un cuerpo de funciones algebraicas complejas, entonces Σ_K admite una única estructura de superficie de Riemann respecto a la cual $\mathcal{M}(\Sigma_K) = K$.*

DEMOSTRACIÓN: Veamos primero la existencia. Supongamos primero que $K = \mathbb{C}(V)$, donde V es una curva proyectiva regular. (Por claridad, aquí distinguiremos entre V y Σ_V.) La biyección natural $f : \Sigma_V \longrightarrow V$ permite transportar la estructura analítica de V al conjunto Σ_V, con lo que se convierte en una superficie de Riemann y f pasa a ser una transformación conforme.

Además las funciones meromorfas de Σ_V pasan a ser las composiciones de f con las funciones meromorfas de V, que son las funciones de $\mathbb{C}(V)$. Ahora bien, la nota de la página 229 nos dice que dichas composiciones son precisamente las funciones de $\mathbb{C}(V)$ vistas como funciones sobre Σ_V. Así, $\mathcal{M}(\Sigma_V) = \mathbb{C}(V)$.

Si K es un cuerpo arbitrario, el teorema 6.2 (y la observación posterior) nos dan una curva proyectiva regular V y un $\mathbb{C}$-isomorfismo $\overline{\phi} : \mathbb{C}(V) \longrightarrow K$. Es claro que $\overline{\phi}$ induce una biyección natural $\phi : \Sigma_K \longrightarrow \Sigma_V$, de modo que, para todo $\alpha \in \mathbb{C}(V)$ y todo $\mathfrak{P} \in \Sigma_K$, se cumple $\overline{\phi}(\alpha)(\mathfrak{P}) = \alpha(\phi(\mathfrak{P}))$.

Esta biyección nos permite a su vez transportar la estructura analítica que hemos definido en Σ_V al conjunto Σ_K, y con ello ϕ se convierte en una transformación conforme. Las funciones meromorfas de Σ_K son precisamente las composiciones con ϕ de las funciones de $\mathbb{C}(V)$, pero estas composiciones son precisamente las funciones de K. Así pues, $\mathcal{M}(\Sigma_K) = K$.

Veamos ahora la unicidad. Supongamos que tenemos dos estructuras de superficie de Riemann sobre Σ_K y veamos que son la misma. Basta ver que la identidad $I : \Sigma_K \longrightarrow \Sigma_K$ es una transformación conforme entre ambas estructuras. Sea $z \in K$ cualquier función no constante. Sea E el conjunto de los puntos de Σ_K que son puntos de ramificación (según la definición 4.30) para z respecto de una de las dos estructuras. Entonces z se restringe a una carta en un entorno de cada punto de $\Sigma_K \setminus E$ (para ambas estructuras), de donde se sigue que la identidad $I : \Sigma_K \setminus E \longrightarrow \Sigma_K \setminus E$ es una transformación conforme de una estructura en la otra.

Veamos ahora que I también es continua en los puntos de E. Dado $\mathfrak{P} \in E$, sea $\alpha \in K$ tal que $\alpha(\mathfrak{P}) = 0$ y sean $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}_n$ los divisores primos donde se anula α. Por 5.5 existe $\beta \in K$ tal que $\beta(\mathfrak{P}) = 0$ y $\beta(\mathfrak{P}_i) \neq 0$ para $i = 2, \ldots, n$. De este modo, $\mathfrak{P}$ es el único punto de Σ_K donde $\alpha(\mathfrak{P}) = \beta(\mathfrak{P}) = 0$.

Sea $\{x_n\} \subset \Sigma_K$ una sucesión que converja a $\mathfrak{P}$ respecto de una de las topologías. Por compacidad, tomando una subsucesión si es preciso, podemos suponer que $\{x_n\}$ converge a un punto $\mathfrak{Q}$ respecto de la otra topología, pero como α y β son continuas para ambas, tenemos que $\alpha(x_n)$ y $\beta(x_n)$ convergen a 0 y $\alpha(\mathfrak{Q}) = \beta(\mathfrak{Q}) = 0$, luego $\mathfrak{P} = \mathfrak{Q}$. Esto prueba que la identidad es continua, luego por compacidad es un homeomorfismo. En otras palabras, ambas estructuras inducen la misma topología.

Veamos, por último, que I es holomorfa en todo $\mathfrak{P} \in E$. Tomamos cartas X e Y alrededor de $\mathfrak{P}$ para ambas estructuras tales que $X(\mathfrak{P}) = Y(\mathfrak{P}) = 0$ cuyos dominios no contengan otros puntos de E. Entonces $f = X^{-1} \circ Y$ es un homeomorfismo de un entorno de 0 en un entorno de 0 y como I es holomorfa en $\Sigma_K \setminus E$, tenemos que f es holomorfa salvo a lo sumo en 0. Es claro entonces que 0 es una singularidad evitable, luego, de hecho, f es holomorfa en 0 y la identidad I es holomorfa en $\mathfrak{P}$. ■

Así pues, podemos hablar de la *superficie de Riemann* Σ_K de un cuerpo de funciones algebraicas K sobre $\mathbb{C}$. De la prueba del teorema anterior se sigue que si V es una curva proyectiva regular, entonces la identificación $\Sigma_V \longrightarrow V$ es una transformación conforme, lo cual significa que la identificación entre V y Σ_V no da lugar a ninguna ambigüedad en lo referente a las estructuras analíticas.

Es claro que un $\mathbb{C}$-isomorfismo entre dos cuerpos de funciones algebraicas induce una biyección entre sus superficies de Riemann que permite traspasar la estructura analítica de una a la otra. Por la unicidad concluimos que dicha biyección ha de ser una transformación conforme. Por consiguiente:

Teorema 6.24 *Dos cuerpos de funciones algebraicas complejas son isomorfos si y sólo si sus superficies de Riemann son conformemente equivalentes.*

De aquí se sigue que si V es una curva proyectiva, no necesariamente regular, la superficie de Riemann de Σ_V es conformemente equivalente a la regularización de V (pues$\mathbb{C}(V)$ es $\mathbb{C}$-isomorfo a $\mathbb{C}(V_r)$). La aplicación $\Sigma_V \longrightarrow V$ es holomorfa por el teorema 6.8.

Vamos a dar una descripción explícita de la estructura analítica de Σ_K. Teniendo en cuenta que todo cuerpo K de funciones algebraicas puede verse como el cuerpo de funciones racionales de una curva proyectiva regular V, el teorema 4.9 se traduce inmediatamente a una descripción de la topología de Σ_K:

Teorema 6.25 *Si K es un cuerpo de funciones algebraicas complejas, una base de Σ_K la forman los conjuntos*

$$U(\alpha_1,\ldots,\alpha_r;\epsilon) = \{\mathfrak{P} \in \Sigma_K \mid \alpha_i \in \mathfrak{O}_{\mathfrak{P}} \text{ y } |\alpha_i(\mathfrak{P})| < \epsilon\}, \quad \alpha_i \in K,\ \epsilon > 0.$$

También podemos describir explícitamente la estructura analítica:

Teorema 6.26 *Si K es un cuerpo de funciones algebraicas complejas, $\mathfrak{P} \in \Sigma_K$ y $\alpha \in K$ cumple $v_{\mathfrak{P}}(\alpha) = 1$, entonces α se restringe a una transformación conforme de un entorno de $\mathfrak{P}$ en un entorno de 0.*

Demostración: No perdemos generalidad si suponemos que $K = \mathbb{C}(V)$, donde V es una curva proyectiva regular. Sea P el primo de V situado bajo $\mathfrak{P}$. Basta probar que α se restringe a una carta en un entorno de P, pero la condición $v_{\mathfrak{P}}(\alpha) = 1$ equivale a que $(\alpha) = \mathfrak{m}_P$, es decir, a que α es un parámetro local en P, luego, en efecto, determina una carta. ■

Más en general:

Teorema 6.27 *Sea K/k una extensión de cuerpos de funciones algebraicas complejas. Entonces la aplicación natural $\phi : \Sigma_K \longrightarrow \Sigma_k$ es holomorfa de grado $|K : k|$ (en el sentido de 4.33) y para cada $\mathfrak{P} \in \Sigma_K$, el índice de ramificación $e_{\mathfrak{P}}$ coincide con el índice de ramificación $e(\phi, \mathfrak{P})$ en el sentido de 4.29.*

Demostración: No perdemos generalidad si suponemos que K y k son los cuerpos de funciones racionales de dos curvas proyectivas regulares V y W, y entonces la inclusión $k \subset K$ se traduce en la existencia de una aplicación regular suprayectiva $\phi : V \longrightarrow W$, que en virtud de 6.12 podemos identificar con la aplicación del enunciado.

Sea $P \in V$ y sean $w \in K$, $z \in k$ tales que $v_P(w) = v_{\phi(P)}(z) = 1$. Por el teorema anterior w y z determinan cartas alrededor de P y $\phi(P)$ respectivamente.

Si llamamos $e = e_P$ (en el sentido algebraico), entonces $v_P(z) = ev_{\phi(P)}(z) = e$, luego $z = \epsilon w^e$, para cierta $\epsilon \in K$ que cumple $v_P(\epsilon) = 0$ (es decir, $\epsilon(P) \neq 0, \infty$). La lectura de ϕ en las cartas w y z es la función holomorfa $t \mapsto \epsilon(w^{-1}(t))t^e$, que tiene un cero de orden e en 0. La prueba del teorema 4.28 muestra que e es el índice de ramificación en el sentido analítico. Ahora basta tener en cuenta los teoremas 6.18 y 4.34 para concluir que el grado de ϕ es $|K : k|$. ■

Teniendo en cuenta el teorema 6.12, el grado de una aplicación regular no constante $\phi : V \longrightarrow W$ entre curvas proyectivas regulares (en el sentido analítico) coincide con el grado de ϕ definido algebraicamente al comienzo del tema (como el grado $|\mathbb{C}(V) : \mathbb{C}(W)|$). Ahora es inmediata la versión siguiente del teorema 4.35:

Teorema 6.28 (Fórmula de Hurwitz) *Sea K un cuerpo de funciones algebraicas, sea $z \in K$ una función no constante y $k = \mathbb{C}(z)$. Entonces el género g de Σ_K viene determinado por la relación*

$$2 - 2g = 2|K : k| + \sum_{\mathfrak{P}} (1 - e_{\mathfrak{P}}),$$

donde $\mathfrak{P}$ recorre los divisores primos de K ramificados sobre k.

Notemos que esta fórmula presupone que el número de primos ramificados es finito, cosa que sabemos por la teoría sobre superficies de Riemann, pero que no tenemos probado para extensiones sobre cuerpos de constantes arbitrarios (de hecho, veremos que dicha finitud sólo es cierta para extensiones separables).

Con esta fórmula podemos calcular el género de una curva proyectiva no necesariamente regular (definido como el género de su regularización).

Ejemplo Consideremos ahora la curva “alfa” $V = V(Y^2 - X^2(X + 1))$ y su cuerpo de funciones racionales, $K = \mathbb{C}(x, y)$. Vamos a estudiar la aplicación $x : V \longrightarrow \mathbb{C}^\infty$. Su grado es $|K : \mathbb{C}(x)| = 2$, luego cada punto de $\mathbb{C}^\infty$ es divisible entre dos divisores primos de V con multiplicidad 1 o por uno solo con multiplicidad 2. Sabemos que el único punto singular de V es $(0, 0)$, sobre el cual puede haber más de un primo.

Si $a \in \mathbb{C}$, $a \neq 0$, entonces los divisores primos de a en V son los primos situados sobre las antiimágenes de a por x. Como entre dichas antiimágenes no está $(0, 0)$, se trata simplemente de las antiimágenes de a.

Si $a \neq -1$ entonces hay dos antiimágenes distintas, a saber $(a, \pm\sqrt{a^2(a + 1)})$, luego son no ramificadas.

Si $a = -1$ hay una única antiimagen, a saber $(-1, 0)$, luego este punto tiene índice de ramificación igual a 2.

Por otra parte, V tiene un único punto en el infinito, donde x toma el valor ∞, luego dicho punto también tiene índice de ramificación igual a 2.

La única antiimagen de $a = 0$ es el punto $(0, 0)$, pero hay dos posibilidades: o bien está situado bajo dos primos distintos con multiplicidad 1 o bien bajo un único primo con multiplicidad 2. La fórmula de Hurwitz excluye esta última posibilidad, pues entonces sería

$$2 - 2g = 2 \cdot 2 + (1 - 2) + (1 - 2) + (1 - 2),$$

lo cual es imposible. Concluimos que sobre $(0, 0)$ hay dos divisores primos distintos y que el género de V es $g = 0$. En realidad ya habíamos obtenido esto en el último ejemplo de la página 141. (Recordemos que la aplicación $\Sigma_V \longrightarrow V$ es equivalente a la regularización de V.) ■

Ejemplo *Para cada número natural $g \geq 1$, la curva V dada por*

$$Y^2 = X(X^2 - 1) \cdots (X^2 - g^2)$$

tiene género g.

En efecto, es fácil ver que V es irreducible y que todos sus puntos finitos son regulares. Su único punto infinito es $(0, 1, 0)$, que es singular si $g \geq 2$. Sea $K = \mathbb{C}(V) = \mathbb{C}(x, y)$ y consideremos la aplicación $x : V \longrightarrow \mathbb{C}$.

Como en el ejemplo anterior razonamos que los únicos puntos finitos ramificados son los puntos $(a, 0)$, con $a = 0, \pm 1, \ldots, \pm g$, cuyo índice de ramificación es $e = 2$.

La fórmula de Hurwitz implica que el número de primos ramificados ha de ser par, luego sobre el punto infinito no puede haber más que un divisor primo, también con $e = 2$, y así obtenemos que el género $\bar{g}$ de V cumple

$$2 - 2\bar{g} = 2 \cdot 2 + (2g + 2)(1 - 2) = 2 - 2g,$$

luego $\bar{g} = g$. ■

Ahora vamos a probar un teorema que nos permitirá aplicar toda la teoría sobre cuerpos de funciones algebraicas a superficies de Riemann arbitrarias. Para ello necesitamos algunos resultados adicionales sobre el cuerpo $\mathcal{M}(X)$ de las funciones meromorfas sobre una superficie de Riemann X. Como ya comentamos en el capítulo IV, siempre existen funciones meromorfas no constantes, por lo que el teorema 1.63 implica que $\mathcal{M}(X)$ tiene grado de trascendencia 1 sobre $\mathbb{C}$. Sin embargo, se cumple algo más fuerte:[5] Fijada una función meromorfa $x \in \mathcal{M}(X)$ de grado n, cualquier otra función meromorfa es raíz de un polinomio de grado n con coeficientes en $\mathbb{C}(x)$. Esto prueba que $\mathcal{M}(X)$ es una extensión finita de $\mathbb{C}(x)$, por lo que $\mathcal{M}(X)$ es un cuerpo de funciones algebraicas. Más aún:

Teorema 6.29 *Si V es una superficie de Riemann, entonces el cuerpo de funciones meromorfas $K = \mathcal{M}(V)$ es un cuerpo de funciones algebraicas complejas y existe una transformación conforme $\phi : V \longrightarrow \Sigma_K$ tal que, para cada $f \in K$ y cada $P \in V$, se cumple que $f(P) = f(\phi(P))$.*

[5] Ver el teorema 14.20 de mi libro de *Funciones de variable compleja.*

DEMOSTRACIÓN: Según acabamos de observar, K es un cuerpo de funciones algebraicas. Si $P \in V$, la aplicación $v_P : K^* \longrightarrow \mathbb{Z}$ que a cada función meromorfa le asigna su orden en P es un homomorfismo de grupos no trivial, luego su imagen es un subgrupo $n\mathbb{Z}$, para cierto $n > 0$ (veremos que $n = 1$). La aplicación v_P/n es claramente una valoración en K. Llamemos $\phi(P)$ al divisor primo correspondiente.

Si $\alpha \in K$, entonces α es regular en P si y sólo si $v_P(\alpha) \geq 0$, si y sólo si $v_{\phi(P)}(\alpha) \geq 0$, si y sólo si α es regular en $\phi(P)$ y, en tal caso, si $\alpha(P) = a$, entonces $v_P(\alpha - a) > 0$, luego $v_{\phi(P)}(\alpha - a) > 0$, luego $\alpha(\phi(P)) = a = \alpha(P)$.

Ahora es claro que ϕ es continua, pues la antiimagen por ϕ de un abierto básico de los considerados en el teorema 6.25 es un conjunto de la misma forma en V, donde claramente es abierto.

Dado $P \in V$, sea $\alpha \in K$ tal que $v_{\phi(P)}(\alpha) = 1$. Esto implica que α se restringe a una carta en un entorno de $\phi(P)$, luego α es inyectiva en un entorno de P, lo cual implica que $v_P(\alpha) = 1$. Así pues, $v_P = v_{\phi(P)}$ (el n que aparecía en la definición es igual a 1, como anunciábamos). Más aún, la lectura de ϕ respecto de las cartas de V y Σ_K formadas por la restricción de α a un entorno de P es la identidad, luego ϕ es holomorfa en V. En particular es abierta y, como V es compacta, también es cerrada. Así pues ϕ es suprayectiva.

Por último, si P, Q son puntos distintos en V, tomamos $\alpha \in K$ tal que $\alpha(P) \neq \alpha(Q)$, según el teorema anterior. Podemos suponer que $\alpha(P) \neq \infty$, con lo que $\beta = \alpha - \alpha(P)$ cumple $\beta(P) = 0$, $\beta(Q) \neq 0$ o, lo que es lo mismo, $v_P(\beta) > 0 \geq v_Q(\beta)$. Esto prueba que $v_P \neq v_Q$, es decir, $\phi(P) \neq \phi(Q)$ y así ϕ es biyectiva, luego es una transformación conforme. ■

Como en el caso de las curvas proyectivas, si V es una superficie de Riemann llamaremos *divisores primos de* V a los divisores primos de su cuerpo de funciones meromorfas, y llamaremos Σ_V al conjunto de todos ellos, que según el teorema anterior es una superficie de Riemann conformemente equivalente a V. Más concretamente, la prueba del teorema nos muestra que podemos identificar cada punto $P \in V$ con la valoración v_P que a cada función meromorfa le asigna su orden en P (en el sentido de la teoría de funciones de variable compleja).

Ahora es claro que toda superficie de Riemann V es conformemente equivalente a una curva proyectiva regular (pues $\mathcal{M}(V)$ es $\mathbb{C}$-isomorfo al cuerpo de funciones racionales de una curva proyectiva regular $\overline{V}$, luego V es conformemente equivalente a Σ_V, que es conformemente equivalente a $\Sigma_{\overline{V}}$, que es conformemente equivalente a $\overline{V}$).

Si $\phi : V \longrightarrow W$ es una aplicación holomorfa no constante, entonces podemos definir una aplicación holomorfa suprayectiva (luego regular) $\psi : \overline{V} \longrightarrow \overline{W}$ que conmute con las transformaciones conformes entre V, $\overline{V}$ y W, $\overline{W}$. Entonces los $\mathbb{C}$-monomorfismos $\overline{\phi} : \mathcal{M}(W) \longrightarrow \mathcal{M}(V)$ y $\overline{\psi} : \mathbb{C}(\overline{W}) \longrightarrow \mathbb{C}(\overline{V})$ conmutan con los $\mathbb{C}$-isomorfismos $\mathcal{M}(V) \cong \mathbb{C}(\overline{V})$ y $\mathcal{M}(W) \cong \mathbb{C}(\overline{W})$. Esto implica la conmutatividad del cuadrado central del diagrama siguiente:

$$\begin{tikzcd}
V \arrow[r] \arrow[d, "\phi"'] & \Sigma_V \arrow[r] \arrow[d] & \Sigma_{\overline{V}} \arrow[r] \arrow[d] & \overline{V} \arrow[d, "\psi"] \\
W \arrow[r] & \Sigma_W \arrow[r] & \Sigma_{\overline{W}} \arrow[r] & \overline{W}
\end{tikzcd}$$

Todas las flechas horizontales son transformaciones conformes, el rectángulo exterior es conmutativo por definición de ψ y sabemos que el tercer cuadrado conmuta porque $\overline{V}$ y $\overline{W}$ son variedades proyectivas. Concluimos que el primer cuadrado también conmuta, es decir, que los divisores en V de un punto de W son precisamente sus antiimágenes.

A partir de aquí, todo lo que sabemos sobre ψ vale también para ϕ. Por ejemplo, el grado de ϕ en sentido analítico coincide con su grado algebraico, y lo mismo sucede con los índices de ramificación.

Similarmente, si partimos de un $\mathbb{C}$-monomorfismo $\overline{\phi} : \mathcal{M}(W) \longrightarrow \mathcal{M}(V)$, podemos construir otro $\overline{\psi} : \mathbb{C}(\overline{W}) \longrightarrow \mathbb{C}(\overline{V})$ que defina una $\psi : \overline{V} \longrightarrow \overline{W}$ y, a partir del diagrama anterior, definir $\phi : V \longrightarrow W$. La conclusión es la siguiente:

Teorema 6.30 *Las aplicaciones holomorfas no constantes $\phi : V \longrightarrow W$ entre dos superficies de Riemann se corresponden biunívocamente con los $\mathbb{C}$-monomorfismos $\overline{\phi} : \mathcal{M}(W) \longrightarrow \mathcal{M}(V)$ mediante la relación $\overline{\phi}(\alpha) = \phi \circ \alpha$. En particular, dos superficies de Riemann son conformemente equivalentes si y sólo si sus cuerpos de funciones meromorfas son $\mathbb{C}$-isomorfos.*

6.4 La aritmética de los divisores primos

Vamos a profundizar en las propiedades y el comportamiento de los divisores primos de un cuerpo de funciones algebraicas. En primer lugar vamos a demostrar que la hipótesis de separabilidad en el teorema 6.18 se puede sustituir por otra hipótesis más conveniente. Para ello probamos un par de resultados previos.

Teorema 6.31 *Sea k_0 un cuerpo perfecto de característica p y sea $k = k_0(x)$, donde x es trascendente sobre k_0. Si K es una extensión finita inseparable de k, entonces $x^{1/p} \in K$.*

DEMOSTRACIÓN: Sea $y \in K$ un elemento no separable sobre k. Entonces $|k(y) : k| = mp$ y existe un polinomio

$$F(X,Y) = \sum_{j=0}^{m} \Big(\sum_i a_{ij} X^i\Big) Y^{jp} \in k_0[X,Y]$$

tal que $f(x,y) = 0$. Como k_0 es perfecto,

$$g(X,Y) = \sum_{j=0}^{m} \Big(\sum_i a_{ij}^{1/p} X^i\Big) Y^{j} \in k_0[X,Y]$$

y $g(x^{1/p}, y) = f(x, y)^{1/p} = 0$, luego $|k_0(x^{1/p}, y) : k_0(x^{1/p})| \leq m$. Puesto que $|k_0(x^{1/p}) : k_0(x)| \leq p$, vemos que

$$mp \geq |k_0(x^{1/p}, y) : k_0(x)| \geq |k_0(x, y) : k_0(x)| = mp.$$

Por consiguiente, $k_0(x^{1/p}, y) = k(y) \subset K$, luego $x^{1/p} \in K$. ■

Teorema 6.32 *Sea K/k una extensión puramente inseparable de grado n de cuerpos de funciones algebraicas sobre un cuerpo de constantes perfecto k_0. Entonces cada primo $\mathfrak{p}$ de k es divisible entre un único primo $\mathfrak{P}$ de K, el grado de inercia es $f = 1$ y el índice de ramificación es $e = n$.*

DEMOSTRACIÓN: Sea p la característica de los cuerpos. La extensión puede descomponerse en una cadena de extensiones de grado p, luego podemos suponer que $|K : k| = p$. Como el único k-monomorfismo $K \longrightarrow \mathbb{K}_\mathfrak{p}$ es la identidad, el teorema 6.17 nos da que $\mathfrak{p}$ sólo tiene un divisor primo $\mathfrak{P}$ en K. Cada $y \in \mathfrak{O}_\mathfrak{P}$ cumple que $y^p \in k$, luego cada $y \in \overline{K}_\mathfrak{P}$ cumple que $y^p \in \overline{k}_\mathfrak{p}$. Ahora bien, los cuerpos de restos son extensiones finitas de k_0, luego son perfectos, de donde se sigue que $\overline{K}_\mathfrak{p} = \overline{k}_\mathfrak{p}$, es decir, $f = 1$. Sólo falta probar que $e = p$. Sabemos que $e = ef = |K_\mathfrak{p} : k_\mathfrak{p}| = n(\mathfrak{P}/\mathfrak{p})$. Si $K = k(y)$, entonces $y^p \in k$ y $K_\mathfrak{p} = k_\mathfrak{p}(y)$, con $y^p \in k_\mathfrak{p}$, luego el grado local $n(\mathfrak{P}/\mathfrak{p})$ será 1 o p según si y está o no en $k_\mathfrak{p}$. Supongamos que es 1.

Sea $x = y^p \in k$. Se cumple que x es trascendente sobre k_0, pues si fuera algebraico $k_0(x)$ sería perfecto y tendríamos que $y \in k_0(x) \subset k$. Sea $k' = k_0(x)$ y $K' = k'(y)$. Vamos a ver que la extensión K'/k' también es un contraejemplo al teorema. Sea $\mathfrak{p}'$ el primo de k' al cual divide $\mathfrak{p}$ y sea $\mathfrak{P}'$ el único primo de K' que lo divide.

Como $y \notin k$, el teorema anterior nos da que k/k' es separable. Por lo tanto $k_\mathfrak{p}/k'_{\mathfrak{p}'}$ también lo es. Estamos suponiendo que $y \in k_\mathfrak{p}$ e $y^p = x \in k'_{\mathfrak{p}'}$, luego por la separabilidad de la extensión ha de ser $y \in k'_{\mathfrak{p}'}$, luego $K'_{\mathfrak{P}'} = k'_{\mathfrak{p}'}(y) = k'_{\mathfrak{p}'}$ y $n(\mathfrak{P}'/\mathfrak{p}') = 1$.

En otras palabras, si K/k es un contraejemplo, hemos encontrado otro en el que el cuerpo base es un cuerpo de fracciones algebraicas. Equivalentemente, podemos suponer que $k = k_0(x)$. Observemos que $K = k(y) = k_0(y)$ es también un cuerpo de fracciones algebraicas. Cambiando x por $1/x$ si es preciso, podemos suponer que el primo $\mathfrak{p}$ es finito, digamos el asociado a un polinomio irreducible $p(x) = \sum\limits_i a_i x^i \in k_0[x]$. Si definimos $\mathfrak{P}$ como el divisor primo de K asociado a

$$f(y) = p(x)^{1/p} = \sum_i a_i^{1/p} y^i \in k_0[y],$$

es claro que $v_\mathfrak{P}(p(x)) = v_\mathfrak{P}(f(x)^p) = p = pv_\mathfrak{p}(p(x))$, de donde $v_\mathfrak{P}|_k = pv_\mathfrak{p}$, luego este $\mathfrak{P}$ es precisamente el divisor de $\mathfrak{p}$ en k y el grado de inercia es $e = p$. ■

Mediante técnicas analíticas hemos visto que para $k_0 = \mathbb{C}$ el número de primos de un cuerpo k ramificados en una extensión es finito. Más adelante veremos que si el cuerpo de constantes es arbitrario esto sigue siendo cierto para extensiones separables. Sin embargo, acabamos de probar que es falso para extensiones inseparables, pues en ellas todos los primos se ramifican (notemos que toda extensión inseparable contiene una extensión intermedia puramente inseparable). Por otra parte, el teorema anterior afirma que las extensiones puramente inseparables (sobre un cuerpo de constantes perfecto) también cumplen el teorema 6.18. Ahora es fácil unir ambos teoremas en un enunciado común:

Teorema 6.33 *Si K/k es una extensión de cuerpos de funciones algebraicas sobre un cuerpo de constantes perfecto k_0, la tesis del teorema* 6.18 *se cumple igualmente.*

Demostración: Podemos suponer que k tiene característica prima p. Sea $\mathfrak{p}$ un divisor primo de k y consideremos la clausura puramente inseparable K_p de k en K. Sea $|K : K_p| = n_s$ y $|K_p : k| = p^m$.

Por el teorema anterior sólo existe un primo $\mathfrak{p}'$ en K_p que divida a $\mathfrak{p}$. Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ los divisores primos de K que dividen a $\mathfrak{p}'$ (que son los mismos que dividen a $\mathfrak{p}$) y sea $n_i' = n(\mathfrak{P}_i/\mathfrak{p}')$. Como la extensión K/K_p es separable, cumple 6.18 y tenemos que $n_s = n_1' + \cdots + n_r'$. Por el teorema anterior tenemos que $n(\mathfrak{p}'/\mathfrak{p}) = p^m$, luego

$$n = p^m n_s = p^m n_1' + \cdots + p^m n_r' = n_1 + \cdots + n_r.$$

■

La hipótesis de que k_0 sea perfecto incluye a todos los cuerpos de característica 0, a todos los cuerpos finitos y a todos los cuerpos algebraicamente cerrados, por lo que no nos va a suponer ninguna restricción seria.

NOTA: *En lo sucesivo supondremos tácitamente que el cuerpo de constantes k_0 de los cuerpos de funciones algebraicas que consideremos será siempre un cuerpo perfecto.*

Por ejemplo, bajo esta hipótesis podemos probar:

Teorema 6.34 *Si K/k es una extensión finita de Galois de cuerpos de funciones algebraicas, $\mathfrak{P}$ es un divisor primo en K y $\mathfrak{p}$ es el primo de k al cual divide, entonces la extensión de cuerpos de restos $\overline{K}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}}$ también es finita de Galois.*

Demostración: Como estamos suponiendo que k_0 es perfecto, es claro que la extensión es separable. Veamos que es normal.

Tomamos $[\alpha] \in \overline{K}_{\mathfrak{P}}$. Por el teorema de aproximación 5.5 podemos encontrar $\alpha' \in K$ tal que $|\alpha' - \alpha|_{\mathfrak{P}} < 1$ y $|\alpha'|_{\mathfrak{P}'} < 1$ para todo divisor $\mathfrak{P}'$ de $\mathfrak{p}$ en K distinto de $\mathfrak{P}$. La primera condición hace que $[\alpha] = [\alpha']$, luego podemos suponer que $v_{\mathfrak{P}'}(\alpha) \geq 0$ para todo $\mathfrak{P}'$. Equivalentemente, podemos suponer que $v_{\mathfrak{P}}(\sigma(\alpha)) \geq 0$ para todo $\sigma \in G$.

Si $p(x) = \operatorname{pol\,mín}(\alpha, k)$ acabamos de probar que $p(x)$ se escinde en $\mathfrak{O}_{\mathfrak{P}}[x]$, luego podemos tomar clases módulo $\mathfrak{p}$ y así obtenemos un polinomio $\bar{p}(x) \in \overline{k}_{\mathfrak{p}}[x]$ que tiene a $[\alpha]$ por raíz y que se escinde en $\overline{K}_{\mathfrak{P}}[x]$. De aquí se sigue que el polinomio mínimo de $[\alpha]$ se escinde también en $\overline{K}_{\mathfrak{P}}[x]$, luego la extensión es normal. ■

El comportamiento de los divisores primos en las extensiones normales es especialmente simple. Ello es consecuencia del siguiente hecho obvio:

Teorema 6.35 *Sea $\sigma : K \longrightarrow L$ un k-isomorfismo entre dos extensiones finitas de un cuerpo de funciones algebraicas k y sea $\mathfrak{p}$ un divisor primo de k. Entonces, para cada divisor primo $\mathfrak{P}$ de K que divide a $\mathfrak{p}$ existe un único divisor primo $\sigma(\mathfrak{P})$ de L que divide a $\mathfrak{p}$ tal que para todo $\alpha \in K$ se cumple $v_{\mathfrak{P}}(\alpha) = v_{\sigma(\mathfrak{P})}(\sigma(\alpha))$. Además $e(\mathfrak{P}/\mathfrak{p}) = e(\sigma(\mathfrak{P})/\mathfrak{p})$ y $f(\mathfrak{P}/\mathfrak{p}) = f(\sigma(\mathfrak{P})/\mathfrak{p})$.*

DEMOSTRACIÓN: Basta definir $v_{\sigma(\mathfrak{P})}(\alpha) = v_{\mathfrak{P}}(\sigma^{-1}(\alpha))$. ■

En particular, si K/k es una extensión normal de cuerpos de funciones algebraicas y $G = G(K/k)$ es el grupo de los k-automorfismos de K, entonces G actúa (por la derecha) sobre el conjunto de los divisores primos de K que dividen a un primo dado $\mathfrak{p}$ de k, es decir, para cada uno de estos divisores $\mathfrak{P}$ y cada $\sigma \in G$ está definido $\sigma(\mathfrak{P})$ según el teorema anterior, y además $(\sigma\tau)(\mathfrak{P}) = \tau(\sigma(\mathfrak{P}))$ y $1(\mathfrak{P}) = \mathfrak{P}$. Más aún:

Teorema 6.36 *Sea K/k una extensión normal de cuerpos de funciones algebraicas y sea $G = G(K/k)$ el grupo de todos los k-automorfismos de K. Sea $\mathfrak{p}$ un divisor primo de k. Entonces G actúa transitivamente sobre los divisores primos de K que dividen a $\mathfrak{p}$, es decir, dados dos cualesquiera de ellos $\mathfrak{P}$ y $\mathfrak{P}'$, existe $\sigma \in G$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

DEMOSTRACIÓN: Sean $\tau_{\mathfrak{P}} : K \longrightarrow \mathbb{K}_{\mathfrak{p}}$ y $\tau_{\mathfrak{P}'} : K \longrightarrow \mathbb{K}_{\mathfrak{p}}$ dos k-monomorfismos según el teorema 6.17. Podemos suponer que $K \subset \mathbb{K}_{\mathfrak{p}}$, y entonces, por la normalidad de K/k, se ha de cumplir que $\tau_{\mathfrak{P}}[K] = \tau_{\mathfrak{P}'}[K] = K$. Es claro entonces que $\sigma = \tau_{\mathfrak{P}} \circ \tau_{\mathfrak{P}'}^{-1} \in G$ cumple $|\alpha|_{\mathfrak{P}} = |\sigma(\alpha)|_{\mathfrak{P}'}$ (para un par de valores absolutos que extiendan a uno dado de $\mathfrak{p}$), de donde se sigue claramente que $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{P}'}(\sigma(\alpha))$ para todo $\alpha \in K$, luego $\mathfrak{P}' = \sigma(\mathfrak{P})$. ■

Combinando los dos últimos teoremas concluimos que si K/k es una extensión normal de cuerpos de funciones algebraicas y $\mathfrak{p}$ es un divisor primo en k, entonces todos sus divisores en K tienen el mismo grado de inercia y el mismo índice de ramificación (luego también el mismo grado local). En otras palabras, $e(\mathfrak{P}/\mathfrak{p})$, $f(\mathfrak{P}/\mathfrak{p})$ y $n(\mathfrak{P}/\mathfrak{p})$ no dependen de $\mathfrak{P}$. La relación del teorema 6.18 (o de 6.33) se reduce a $n = efr$.

Para el caso de una extensión finita de Galois podemos decir mucho más:

Definición 6.37 Sea K/k una extensión finita de Galois de cuerpos de funciones algebraicas, sea $\mathfrak{P}$ un divisor primo de K y sea $\mathfrak{p}$ el primo de k al cual divide. Definimos el *grupo de descomposición* de $\mathfrak{p}$ sobre $\mathfrak{P}$ como

$$G_{\mathfrak{P}} = \{\sigma \in G(K/k) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Claramente $G_{\mathfrak{P}}$ es un subgrupo del grupo de Galois $G = G(K/k)$. Además, para todo $\sigma \in G$ se cumple $G_{\sigma(\mathfrak{P})} = G_{\mathfrak{P}}^{\sigma}$. Es fácil biyectar el conjunto cociente $G/G_{\mathfrak{P}}$ con el número r de divisores primos de $\mathfrak{p}$ en K, con lo que $|G_{\mathfrak{P}}| = ef$. Más concretamente, los efr automorfismos de G se dividen en r clases de ef automorfismos cada una, de modo que los automorfismos de cada clase llevan $\mathfrak{P}$ a cada uno de sus conjugados (a cada uno de los divisores de $\mathfrak{p}$).

El cuerpo L fijado por $G_{\mathfrak{P}}$ se llama *cuerpo de descomposición* de $\mathfrak{p}$ sobre $\mathfrak{P}$. Claramente $|L : k| = r$.

Como $K_{\mathfrak{P}} = k_{\mathfrak{p}}K$, es claro que la extensión $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ también es finita de Galois. La restricción induce un monomorfismo de grupos $G(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \longrightarrow G_{\mathfrak{P}}$ que, de hecho, es un isomorfismo porque ambos grupos tienen el mismo orden.

Sea $\mathfrak{p}'$ el primo de L divisible entre $\mathfrak{P}$. Así $k \subset L \subset K$ y $k_{\mathfrak{p}} \subset L_{\mathfrak{p}'} \subset K_{\mathfrak{P}}$. Ahora bien, $G_{\mathfrak{P}} = G(K/L)$, y es fácil ver que $G_{\mathfrak{P}}$ es también el grupo de descomposición de $\mathfrak{P}$ sobre $\mathfrak{p}'$. Por consiguiente,

$$|K_{\mathfrak{P}} : L_{\mathfrak{p}'}| = |G_{\mathfrak{P}}| = |K_{\mathfrak{P}} : k_{\mathfrak{p}}|,$$

es decir, $L_{\mathfrak{p}'} = k_{\mathfrak{p}}$. Esto implica que $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$. Como la extensión local $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ es la misma que $K_{\mathfrak{P}}/L_{\mathfrak{p}'}$, resulta que el grado de inercia y el índice de ramificación son los mismos para $\mathfrak{P}/\mathfrak{p}$ que para $\mathfrak{P}/\mathfrak{p}'$. En particular es claro que $\mathfrak{P}$ es el único primo en K que divide a $\mathfrak{p}'$ (pues $|K : L| = ef$).

Cada automorfismo $\sigma \in G_{\mathfrak{P}}$ se restringe a un automorfismo $\sigma : \mathfrak{O}_{\mathfrak{P}} \longrightarrow \mathfrak{O}_{\mathfrak{P}}$ que deja fijos a los elementos de $\mathfrak{o}_{\mathfrak{p}}$, el cual induce a su vez un $\overline{k}_{\mathfrak{p}}$-automorfismo $\bar{\sigma} : \overline{K}_{\mathfrak{P}} \longrightarrow \overline{K}_{\mathfrak{P}}$ de forma natural ($\bar{\sigma}([\alpha]) = [\sigma(\alpha)]$). Recogemos esto y un poco más en el teorema siguiente:

Teorema 6.38 *Sea K/k una extensión finita de Galois de cuerpos de funciones algebraicas. Sea $\mathfrak{P}$ un divisor primo en K y sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$. Entonces cada $\sigma \in G_{\mathfrak{P}}$ induce de forma natural un automorfismo $\overline{\sigma} \in G(\overline{K}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}})$ y la aplicación $\sigma \mapsto \bar{\sigma}$ es un epimorfismo de grupos $G_{\mathfrak{P}} \longrightarrow G(\overline{K}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}})$.*

DEMOSTRACIÓN: Sólo falta probar la suprayectividad. Notemos que si L es el cuerpo de descomposición de $\mathfrak{p}$ sobre $\mathfrak{P}$ y $\mathfrak{p}'$ es el primo intermedio, se cumple que $\overline{L}_{\mathfrak{p}'} = \overline{k}_{\mathfrak{p}}$, luego podemos sustituir k por L y suponer, pues, que $G = G_{\mathfrak{P}}$. Como $\overline{K}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}}$ es separable, tiene un elemento primitivo, digamos $[\alpha]$. Al igual que en la prueba de 6.34, podemos suponer que $p(x) = \operatorname{pol\,mín}(\alpha, k)$ se escinde en $\mathfrak{O}_{\mathfrak{P}}[x]$. Dado $\tau \in G(\overline{K}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}})$, tenemos que $\tau([\alpha])$ es raíz de $\bar{p}[x]$, luego $\tau([\alpha]) = [\alpha']$, donde α' es un conjugado de α. Existe $\sigma \in G = G_{\mathfrak{P}}$ tal que $\sigma(\alpha) = \alpha'$, con lo que $\bar{\sigma}([\alpha]) = [\sigma(\alpha)] = [\alpha'] = \tau([\alpha])$ y, por consiguiente, $\tau = \bar{\sigma}$. ■

Esto nos lleva a la definición siguiente:

Definición 6.39 Sea K/k una extensión finita de Galois de cuerpos de funciones algebraicas, sea $\mathfrak{P}$ un primo de K y $\mathfrak{p}$ el primo de k al cual divide. Llamaremos *grupo de inercia* de $\mathfrak{p}$ sobre $\mathfrak{P}$ al núcleo $T_{\mathfrak{P}} \leq G_{\mathfrak{P}}$ del epimorfismo descrito en el teorema anterior. Llamaremos *cuerpo de inercia* de $\mathfrak{p}$ sobre $\mathfrak{P}$ al cuerpo fijado por $T_{\mathfrak{P}}$.

Según el teorema anterior, tenemos un isomorfismo $G_{\mathfrak{P}}/T_{\mathfrak{P}} \cong G(\overline{K}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}})$. En particular $|T_{\mathfrak{P}}| = f$. Si L es el cuerpo de descomposición de $\mathfrak{p}$ sobre $\mathfrak{P}$ y M es el cuerpo de inercia, tenemos las inclusiones $k \subset L \subset M \subset K$. Los grados de estas extensiones son

$$|L : k| = r, \qquad |M : L| = f, \qquad |K : M| = e.$$

Como $T_{\mathfrak{P}}$ es un subgrupo normal de $G_{\mathfrak{P}}$, tenemos que la extensión M/L es de Galois. Sea $\mathfrak{p}'$ el primo intermedio en L y $\mathfrak{p}''$ el primo intermedio en M. Como $G(K/M) = T_{\mathfrak{P}}$, es claro que el epimorfismo $\sigma \mapsto \bar{\sigma}$ para la extensión K/M es trivial, luego $G(\overline{K}_{\mathfrak{P}}/\overline{M}_{\mathfrak{p}''}) = 1$, luego $f(\mathfrak{P}/\mathfrak{p}'') = 1$. De aquí se sigue que $f(\mathfrak{p}''/\mathfrak{p}') = f = |M : L|$.

El teorema siguiente recoge todo lo que hemos probado:

Teorema 6.40 *Sea K/k una extensión finita de Galois de cuerpos de funciones algebraicas, sea $\mathfrak{P}$ un primo en K y $\mathfrak{p}$ el primo de k al cual divide. Sea L el cuerpo de descomposición y M el cuerpo de inercia, sean $\mathfrak{p}'$ y $\mathfrak{p}''$ los primos divisibles por $\mathfrak{P}$ en cada uno de estos cuerpos. Sea r el número de divisores primos de $\mathfrak{p}$ en K, $f = f(\mathfrak{P}/\mathfrak{p})$ y $e = e(\mathfrak{P}/\mathfrak{p})$. Entonces se tienen los datos indicados en la tabla siguiente:*

Grado		r		f		e	
Cuerpo	k		L		M		K
Primo	$\mathfrak{p}$		$\mathfrak{p}'$		$\mathfrak{p}''$		$\mathfrak{P}$
Ramificación		1		1		e	
Inercia		1		f		1	

Probamos ahora un teorema sencillo sobre normas y trazas que necesitaremos más adelante:

Teorema 6.41 *Sea K/k una extensión de cuerpos de funciones algebraicas y sea $\mathfrak{p}$ un divisor primo en k. Para cada divisor primo $\mathfrak{P}$ de K que divida a $\mathfrak{p}$, sean $\mathrm{N}_{\mathfrak{P}} : K_{\mathfrak{P}} \longrightarrow k_{\mathfrak{p}}$ y $\mathrm{Tr}_{\mathfrak{P}} : K_{\mathfrak{P}} \longrightarrow k_{\mathfrak{p}}$ la norma y la traza locales. Entonces, para todo $\alpha \in K$,*

$$\mathrm{N}_k^K(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{\mathfrak{P}}(\alpha), \qquad \mathrm{Tr}_k^K(\alpha) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_{\mathfrak{P}}(\alpha).$$

Demostración: Supongamos primero que la extensión es separable. Entonces, $\mathrm{N}_k^K(\alpha)$ es el producto de las imágenes de α por todos los k-monomorfismos de K en una clausura algebraica de $k_{\mathfrak{p}}$. Al agrupar los que se extienden a cada compleción $K_{\mathfrak{P}}$ obtenemos la norma $\mathrm{N}_{\mathfrak{P}}(\alpha)$, luego se cumple la fórmula del enunciado, e igualmente con las trazas.

En el caso general, sea L la clausura puramente inseparable de k en K. Por el teorema 6.32 sabemos que $\mathfrak{p}$ tiene un único divisor $\mathfrak{p}'$ en L. Así como que $|L_{\mathfrak{p}'} : k_{\mathfrak{p}}| = |L : k|$. La extensión K/L es separable, luego, por la parte ya probada,

$$\mathrm{N}_L^K(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}'} \mathrm{N}'_{\mathfrak{P}}(\alpha),$$

donde $\mathrm{N}'_{\mathfrak{P}}$ es la norma de la extensión $K_{\mathfrak{P}}/L_{\mathfrak{p}'}$. Elevando ambos miembros a $|L:k|$ obtenemos la relación para K/k. El caso de las trazas es trivial, pues la traza de una extensión inseparable es nula. ■

Para terminar estudiamos la estructura de las compleciones de los divisores primos. Todos son isomorfos a cuerpos de series formales de potencias.

Teorema 6.42 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0, sea $\mathfrak{p}$ un divisor primo de K, sea π un primo en $K_{\mathfrak{p}}$ y sea $k_{0\mathfrak{p}}$ la clausura algebraica de k_0 en $K_{\mathfrak{p}}$. Entonces $K_{\mathfrak{p}} = k_{0\mathfrak{p}}((\pi))$, es decir, todo elemento de $K_{\mathfrak{p}}$ se expresa de forma única como*

$$\alpha = \sum_{-\infty \ll n} a_n \pi^n, \qquad \text{con } a_n \in k_{0\mathfrak{p}}.$$

En particular $k_{0\mathfrak{p}} \cong \overline{K}_{\mathfrak{p}}$.

Demostración: Tenemos que $\overline{K}_{\mathfrak{p}}$ es una extensión finita de k_0. Como ha de ser separable, se cumple $\overline{K}_{\mathfrak{p}} = k_0(c)$, para cierta clase c. Sea $p(x)$ el polinomio mínimo de c sobre k_0. Entonces, $p(x)$ factoriza módulo $\mathfrak{p}$ como $(x-c)q(x)$, y los factores son primos entre sí porque la extensión de cuerpos de restos es separable. Por el lema de Hensel 5.20 el polinomio p tiene una raíz $\alpha \in K_{\mathfrak{p}}$, de modo que $\overline{K}_{\mathfrak{p}} = k_0([\alpha])$.

La aplicación natural $k_0(\alpha) \longrightarrow \overline{K}_{\mathfrak{p}}$ es suprayectiva, luego es un isomorfismo de cuerpos, pero lo mismo podemos decir de la aplicación natural $k_{0\mathfrak{p}} \longrightarrow \overline{K}_{\mathfrak{p}}$ (notemos que todos los elementos de $k_{0\mathfrak{p}}$ son enteros en $K_{\mathfrak{p}}$, pues la valoración es trivial en k_0 y, por 6.9, también en $k_{0\mathfrak{p}}$). Consecuentemente $k_{0\mathfrak{p}} = k_0(\alpha) \cong \overline{K}_{\mathfrak{p}}$. Ahora basta aplicar el teorema 5.17. ■

Una ligera variante del argumento que acabamos de emplear nos da el siguiente resultado:

Teorema 6.43 *Sea $k = k_0((x))$ un cuerpo de series formales de potencias sobre un cuerpo de constantes (perfecto) k_0 y sea K una extensión finita de k. Sea k_1 la clausura algebraica de k_0 en K. Entonces k_1 es una extensión finita de k_0 y $K = k_1((y))$ para cierto $y \in K$.*

El teorema 6.42 generaliza la noción de serie de Taylor de una función racional sobre una curva algebraica. En efecto, sea V una curva algebraica sobre un cuerpo (algebraicamente cerrado) k_0, sea $K = k_0(V)$ su cuerpo de funciones racionales y sea $P \in V$ un punto regular. Si $\pi \in \mathcal{O}_P(V)$ es un parámetro local en P, esto significa que $v_P(\pi) = 1$, lo cual sigue siendo cierto en la compleción K_P. Esto significa que π es primo en K_P y el teorema 6.42 nos da que $K_P = k_0((\pi))$. En particular, todo $\alpha \in \mathcal{O}_P(V)$ admite un desarrollo de la forma

$$\alpha = \sum_{m=0}^{\infty} a_m \pi^m, \qquad a_m \in k_0. \tag{6.2}$$

Es inmediato que la serie de potencias

$$F(X) = \sum_{m=0}^{\infty} a_m X^m$$

es precisamente la serie de Taylor de α en P respecto al parámetro π, pues, para todo $n \geq 0$, se cumple que

$$\pi^{n+1} \mid \alpha - \sum_{m=0}^{n} a_m \pi^m,$$

luego

$$\alpha - \sum_{m=0}^{n} a_m \pi^m \in \mathfrak{m}_P^{n+1},$$

tal y como exige la definición de serie de Taylor.

En particular, si $k_0 = \mathbb{C}$, el teorema 4.7 nos da que la serie (6.2) no sólo converge a α formalmente en K_P, sino que también converge (a α) como serie funcional en un entorno de P.

Más aún, si $\alpha \in \mathbb{C}(V)$ es una función racional no nula no necesariamente regular en P, entonces $\pi^n \alpha$ es regular en P, para $n = v_P(\alpha)$, y la convergencia de la serie de Taylor de $\pi^n \alpha$ en un entorno de P implica inmediatamente que la serie de Laurent de α como elemento de K_P converge a α en un entorno de P excepto en el propio punto P si α no es regular.

Capítulo VII

Funciones algebraicas II

En el capítulo anterior nos hemos ocupado esencialmente del comportamiento local de los divisores primos, es decir, el comportamiento de cada uno de ellos con independencia de los demás. Ahora sentaremos las bases del estudio de su comportamiento global, es decir, de aquellos resultados que dependen simultáneamente de todos ellos. Por ejemplo, en el caso complejo conocemos dos resultados globales: uno es que el número de primos ramificados en una extensión es necesariamente finito, y otro es la fórmula de Hurwitz. En este capítulo —entre otras cosas— generalizaremos el primero de ellos a extensiones separables de cuerpos de funciones algebraicas sobre un cuerpo de constantes arbitrario, mientras que la versión general de la fórmula de Hurwitz tendrá que esperar al capítulo siguiente, donde daremos una definición algebraica de género que extienda a la que ya tenemos para el caso complejo.

7.1 Divisores

El estudio global de los cuerpos de funciones algebraicas se apoya en la noción de divisor que introducimos a continuación:

Definición 7.1 Sea K un cuerpo de funciones algebraicas. Definimos el grupo de los *divisores* de K como el grupo abeliano libre $\mathcal{D}$ generado por los divisores primos de K. Usaremos notación multiplicativa, de modo que cada divisor de K se expresa de forma única como

$$\mathfrak{a} = \prod_{\mathfrak{P}} \mathfrak{P}^{n_{\mathfrak{P}}},$$

donde los exponentes $n_{\mathfrak{P}}$ son enteros y casi todos nulos.

Definimos $v_{\mathfrak{P}}(\mathfrak{a}) = n_{\mathfrak{P}}$. Un divisor es *entero* si todos sus exponentes son no negativos. Diremos que un divisor $\mathfrak{a}$ *divide* a un divisor $\mathfrak{b}$ (y lo representaremos por $\mathfrak{a} \mid \mathfrak{b}$) si $v_{\mathfrak{P}}(\mathfrak{a}) \leq v_{\mathfrak{P}}(\mathfrak{b})$ para todo divisor primo $\mathfrak{P}$ de K. Equivalentemente, si $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, donde $\mathfrak{c}$ es un divisor entero.

Es claro que un conjunto finito de divisores tiene un máximo común divisor y un mínimo común múltiplo, que se forman elevando cada primo al menor (respectivamente, al mayor) exponente con que aparece en los divisores dados.

En virtud del teorema 6.19, cada $\alpha \in K^*$ determina un divisor, a saber,

$$(\alpha) = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\alpha)}.$$

A los divisores de esta forma los llamaremos *divisores principales* de K. Notemos que, por definición, $v_{\mathfrak{P}}((\alpha)) = v_{\mathfrak{P}}(\alpha)$.

Las propiedades de las valoraciones nos dan que $(\alpha)(\beta) = (\alpha\beta)$, así como que $(\alpha^{-1}) = (\alpha)^{-1}$. En otras palabras, el conjunto P_K de los divisores principales de K es un subgrupo de $\mathcal{D}$ y tenemos un epimorfismo

$$K^* \longrightarrow P_K.$$

Según el teorema 6.22, el núcleo de este homomorfismo es k_1^*, donde k_1 es el cuerpo exacto de constantes de K. Así pues, $P_K \cong K^*/k_1^*$. Al pasar de K^* a P_K estamos identificando a dos funciones cuando se diferencian en un factor constante de k_1^*.

Conviene pensar en los divisores de K como en distribuciones posibles de ceros y polos de una función algebraica. Si un divisor $\mathfrak{a}$ es principal, eso significa que la distribución asociada a $\mathfrak{a}$ se realiza en K, es decir, existe realmente una función $\alpha \in K^*$ (única salvo una constante) tal que $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{P}}(\mathfrak{a})$ para todo divisor primo $\mathfrak{P}$ de K.

Si K/k es una extensión de cuerpos de funciones algebraicas, identificamos cada divisor primo $\mathfrak{p}$ de k con el divisor

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \in \mathcal{D}_K, \tag{7.1}$$

donde $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ son los divisores de $\mathfrak{p}$ en K y $e_1, \ldots, e_r$ son los índices de ramificación correspondientes. Esta aplicación —obviamente inyectiva— se extiende de forma única por linealidad a un monomorfismo de grupos

$$\mathcal{D}_k \longrightarrow \mathcal{D}_K,$$

que nos permite identificar a cada divisor de k con un divisor de K.

La transitividad de los índices de ramificación se traduce inmediatamente en que si tenemos una cadena de extensiones $k \subset K \subset L$, entonces la composición de las identificaciones $\mathcal{D}_k \longrightarrow \mathcal{D}_K \longrightarrow \mathcal{D}_L$ es la identificación correspondiente a la extensión K/k. Así mismo, tenemos el diagrama conmutativo

$$\begin{tikzcd} K^* \arrow[r] & \mathcal{D}_K \\ k^* \arrow[r] \arrow[u] & \mathcal{D}_k \arrow[u] \end{tikzcd}$$

En efecto, si $\alpha \in k^*$ y $\mathfrak{P}$ es un primo de K, sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$ y sea $e = e(\mathfrak{P}/\mathfrak{p})$. Entonces

$$v_{\mathfrak{P}}((\alpha)_K) = v_{\mathfrak{P}}(\alpha) = ev_{\mathfrak{p}}(\alpha) = ev_{\mathfrak{p}}((\alpha)_k) = v_{\mathfrak{P}}((\alpha)_k),$$

luego $(\alpha)_K = (\alpha)_k$.

La identificación (7.1) nos permite hablar de la descomposición en primos en K de un divisor primo $\mathfrak{p}$ de k, de modo que lo que hasta ahora llamábamos divisores de $\mathfrak{p}$ en K son precisamente los primos de K que aparecen en dicha factorización con exponente no nulo.

Por ejemplo, el teorema 6.32 afirma que si K/k es una extensión puramente inseparable de grado n, entonces cada primo $\mathfrak{p}$ de k se descompone en la forma $\mathfrak{p} = \mathfrak{P}^n$, para cierto primo $\mathfrak{P}$ de K.

Similarmente, las observaciones tras el teorema 6.36 equivalen a que si K/k es una extensión normal, cada primo $\mathfrak{p}$ de k factoriza en K en la forma

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

de modo que, además, todos los factores tienen el mismo grado de inercia. Conviene introducir algunas definiciones:

Definición 7.2 Sea K/k una extensión de grado n de cuerpos de funciones algebraicas. Sea $\mathfrak{P}$ un primo en K y $\mathfrak{p}$ el primo de k al cual divide. Diremos que

a) $\mathfrak{p}$ se *escinde* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$.

b) $\mathfrak{p}$ se *escinde completamente* en K si $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_n$ (de modo que todos los factores tienen necesariamente $e = f = 1$).

c) $\mathfrak{p}$ se *conserva primo* en K si $\mathfrak{p} = \mathfrak{P}$ (de modo que $e(\mathfrak{P}/\mathfrak{p}) = 1$, $f(\mathfrak{P}/\mathfrak{p}) = n$).

d) $\mathfrak{p}$ se *ramifica* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) > 1$.

e) $\mathfrak{p}$ se *ramifica completamente* en K si $\mathfrak{p} = \mathfrak{P}^n$ (de modo que $e(\mathfrak{P}/\mathfrak{p}) = n$, $f(\mathfrak{P}/\mathfrak{p}) = 1$).

En estos términos, el teorema 6.40 afirma que una extensión finita de Galois K/k de cuerpos de funciones algebraicas se puede descomponer en una cadena de extensiones $k \subset L \subset M \subset K$ (relativa a primos dados $\mathfrak{P}$ y $\mathfrak{p}$), de modo que $\mathfrak{p}$ se escinda en L en un primo $\mathfrak{p}'$, el cual a su vez se conserva primo en M y luego se ramifica completamente en K.

Un caso especialmente simple se da cuando la extensión es abeliana, pues entonces el grupo de descomposición $G_{\mathfrak{P}}$ es normal y todos los divisores de $\mathfrak{p}$ en K tienen el mismo grupo de descomposición, por lo que el cuerpo de descomposición L es el mismo para todos. En tal caso, $\mathfrak{p}$ se escinde completamente en L, en la forma $\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Similarmente, el cuerpo de inercia M es el mismo para todos los divisores de $\mathfrak{p}$, y todos los $\mathfrak{p}_i$ se conservan primos en M, mientras que se ramifican completamente en K, en la forma $\mathfrak{p}_i = \mathfrak{P}_i^e$.

Introducimos ahora la noción de norma de un divisor:

Definición 7.3 Si K/k es una extensión de cuerpos de funciones algebraicas, definimos la *norma*

$$\mathrm{N}_k^K : \mathcal{D}_K \longrightarrow \mathcal{D}_k$$

como el homomorfismo que sobre los primos viene dado por $\mathrm{N}_k^K(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$, donde $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$.

La transitividad de grado de inercia implica la transitividad de la norma, es decir, dada una cadena $k \subset K \subset L$, se cumple que $\mathrm{N}_k^L = \mathrm{N}_K^L \circ \mathrm{N}_k^K$.

Para cada primo $\mathfrak{p}$ de k se cumple

$$\mathrm{N}_k^K(\mathfrak{p}) = \mathrm{N}(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}) = \mathfrak{p}^{f_1 e_1 + \cdots + f_r e_r} = \mathfrak{p}^{|K:k|}.$$

Por linealidad esto es cierto para todo divisor $\mathfrak{a} \in \mathcal{D}_k$, es decir,

$$\mathrm{N}_k^K(\mathfrak{a}) = \mathfrak{a}^{|K:k|}.$$

Ahora probamos que la norma que acabamos de definir es consistente con la norma usual de la extensión K/k:

Teorema 7.4 *Si K/k es una extensión de cuerpos de funciones algebraicas, el diagrama siguiente es conmutativo:*

$$\begin{tikzcd} K^* \arrow[r] \arrow[d, "\mathrm{N}_k^K"'] & \mathcal{D}_K \arrow[d, "\mathrm{N}_k^K"] \\ k^* \arrow[r] & \mathcal{D}_k \end{tikzcd}$$

Demostración: Hemos de probar que para todo $\alpha \in K^*$ se cumple

$$(\mathrm{N}_k^K(\alpha)) = \mathrm{N}_k^K((\alpha)).$$

Sea K_i la clausura puramente inseparable de k en K. Así tenemos la cadena $k \subset K_i \subset K$, de modo que la primera extensión es puramente inseparable y la segunda es separable. Teniendo en cuenta que las dos normas son transitivas, es claro que basta probar el teorema para cada una de estas extensiones por separado. Alternativamente, basta probar el teorema en el supuesto de que K/k es puramente inseparable y en el supuesto de que es separable.

Si K/k es puramente inseparable de grado n, entonces, según el teorema 6.32, cada primo $\mathfrak{p}$ de k se corresponde con un único primo $\mathfrak{P}$ de K y su factorización es $\mathfrak{p} = \mathfrak{P}^n$ (con $f = 1$). Por lo tanto:

$$\mathrm{N}_k^K((\alpha)) = \prod_{\mathfrak{P}} \mathrm{N}_k^K(\mathfrak{P}^{v_{\mathfrak{P}}(\alpha)}) = \prod_{\mathfrak{P}} \mathfrak{p}^{v_{\mathfrak{P}}(\alpha)} = \prod_{\mathfrak{P}} \mathfrak{P}^{n v_{\mathfrak{P}}(\alpha)} = (\alpha)^n = (\alpha^n) = (\mathrm{N}_k^K(\alpha)).$$

Supongamos ahora que K/k es separable de grado n. En primer lugar, consideremos el caso en que además es normal, es decir, es finita de Galois. Sea $G = G(K/k)$ el grupo de Galois y sea $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$ un primo de k. Tenemos que

$$\mathrm{N}_k^K(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Puesto que $v_{\mathfrak{p}} = (1/e)v_{\mathfrak{P}_1}$, se cumple que

$$v_{\mathfrak{p}}(\mathrm{N}_k^K(\alpha)) = \frac{1}{e}\sum_{\sigma\in G} v_{\mathfrak{P}_1}(\sigma(\alpha)) = \frac{1}{e}\sum_{\sigma\in G} v_{\sigma(\mathfrak{P}_1)}(\alpha).$$

Cuando σ recorre G, tenemos que $\sigma(\mathfrak{P}_1)$ recorre ef veces cada primo $\mathfrak{P}_i$, luego

$$v_{\mathfrak{p}}(\mathrm{N}_k^K(\alpha)) = f\sum_{i=1}^{r} v_{\mathfrak{P}_i}(\alpha) = v_{\mathfrak{p}}(\mathrm{N}_k^k((\alpha))).$$

Por consiguiente, $(\mathrm{N}_k^K(\alpha)) = \mathrm{N}_k^K((\alpha))$.

Consideremos ahora el caso general en que K/k es separable. Sea L la clausura normal de K sobre k. Tenemos $k \subset K \subset L$ y la extensión L/k es de Galois, luego cumple el teorema. Si $\alpha \in K^*$, tenemos que

$$(\mathrm{N}_k^L(\alpha)) = (\mathrm{N}_k^K(\alpha)^{|L:K|}) = (\mathrm{N}_k^K(\alpha))^{|L:K|}.$$

Por otro lado,

$$(\mathrm{N}_k^L(\alpha)) = \mathrm{N}_k^L((\alpha)) = \mathrm{N}_k^K((\alpha))^{|L:K|}.$$

Así, si $\mathfrak{p}$ es un primo de k, tenemos que

$$|L:K|v_{\mathfrak{p}}(\mathrm{N}_k^K(\alpha)) = |L:K|v_{\mathfrak{p}}(\mathrm{N}_k^K((\alpha))),$$

con lo que, tras simplificar $|L:K|$, concluimos que $(\mathrm{N}_k^K(\alpha)) = \mathrm{N}_k^K((\alpha))$. ■

En particular, si $\phi : V \longrightarrow W$ es una aplicación regular no constante entre curvas proyectivas regulares, entonces la norma de un punto $P \in V$ es simplemente $\phi(P)$, luego la aplicación norma $\phi : \mathcal{D}_V \longrightarrow \mathcal{D}_W$ es simplemente la extensión lineal de ϕ al grupo de divisores. Por ello, la seguiremos llamando ϕ.

Definición 7.5 Si K es un cuerpo de funciones algebraicas, la aplicación que a cada divisor primo le asigna su grado se extiende por linealidad a un homomorfismo

$$\operatorname{grad} : \mathcal{D} \longrightarrow \mathbb{Z},$$

con lo que tenemos definido el *grado* de un divisor arbitrario, de modo que

$$\operatorname{grad} \mathfrak{ab} = \operatorname{grad} \mathfrak{a} + \operatorname{grad} \mathfrak{b}, \qquad \operatorname{grad} \mathfrak{a}^{-1} = -\operatorname{grad} \mathfrak{a}.$$

Si $\mathfrak{P}$ es un primo en K, la relación (6.1) puede escribirse ahora en la forma

$$\operatorname{grad}_K \mathfrak{P} = f(\mathfrak{P}/\mathfrak{p}) \operatorname{grad}_k \mathfrak{p} = \operatorname{grad}_k \mathfrak{p}^f = \operatorname{grad}_k \mathrm{N}_k^K(\mathfrak{P}).$$

Como el primer y el último término son ambos multiplicativos, esta relación es válida por linealidad para todo divisor, es decir, para todo $\mathfrak{a} \in \mathcal{D}$ se cumple que

$$\operatorname{grad}_K \mathfrak{a} = \operatorname{grad}_k \mathrm{N}_k^K(\mathfrak{a}). \tag{7.2}$$

En particular, si $\mathfrak{a} \in \mathcal{D}_k$ tenemos que

$$\operatorname{grad}_K \mathfrak{a} = |K : k| \operatorname{grad}_k \mathfrak{a},$$

de modo que el grado de un divisor depende de la extensión en que lo consideremos.

Ahora podemos dar una condición necesaria para que una distribución posible de ceros y polos sea realizable en un cuerpo de funciones algebraicas, es decir, para que un divisor sea principal:

Teorema 7.6 *Si K es un cuerpo de funciones algebraicas, entonces los divisores principales de K tienen grado 0. Si $K = k_0(x)$ es un cuerpo de fracciones algebraicas, entonces los divisores principales son exactamente los de grado 0.*

Demostración: Consideremos primero el caso de un cuerpo de fracciones algebraicas $k = k_0(x)$. Si $\alpha \in k^*$ es constante, entonces $(\alpha) = 1$, luego por definición $\operatorname{grad}(\alpha) = 0$. Por otra parte, todo $\alpha \in k^*$ no constante se expresa de forma única como

$$\alpha = p_1(x)^{r_1} \cdots p_n(x)^{r_n},$$

donde $p_i(x)$ son polinomios irreducibles y los exponentes son enteros no nulos. Si llamamos $\mathfrak{p}_i = (p_i(x))$, tenemos que $(\alpha) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \infty^r$, donde

$$r = v_\infty(\alpha) = -\operatorname{grad} \alpha = -\sum_{i=1}^n r_i \operatorname{grad} p_i(x) = -\sum_{i=1}^n r_i \operatorname{grad} \mathfrak{p}_i.$$

Por lo tanto, teniendo en cuenta que $\operatorname{grad} \infty = 1$, concluimos que

$$\operatorname{grad}(\alpha) = \sum_{i=1}^n r_i \operatorname{grad} \mathfrak{p}_i + r \operatorname{grad} \infty = 0,$$

luego todos los divisores principales de k tienen grado 0.

Recíprocamente, si $\operatorname{grad} \mathfrak{a} = 0$, para cada primo finito $\mathfrak{p}$, tomamos un polinomio $p_\mathfrak{p}(x) \in k_0[x]$ tal que $\mathfrak{p} = (p_\mathfrak{p}(x))$ y definimos

$$\alpha = \prod_\mathfrak{p} p_\mathfrak{p}(x)^{v_\mathfrak{p}(\mathfrak{a})}.$$

El producto es finito, luego $\alpha \in k^*$. Por construcción $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\mathfrak{a})$ para todo primo finito $\mathfrak{p}$ y, del hecho de que tanto (α) como $\mathfrak{a}$ tienen grado 0, se sigue fácilmente que $v_\infty(\alpha) = v_\infty(\mathfrak{a})$, luego $\mathfrak{a} = (\alpha)$. Así pues, todo divisor de grado 0 es principal.

Si K es un cuerpo arbitrario y $x \in K$ es trascendente sobre k_0, tenemos que $k = k_0(x) \subset K$ y, por la parte ya probada, todos los divisores principales de k tienen grado 0. Ahora basta aplicar la fórmula (7.2) junto con el hecho de que la norma de un divisor principal es principal. ■

Por ejemplo, si el cuerpo de constantes es algebraicamente cerrado (y, por consiguiente, todos los divisores primos tienen grado 1), vemos que la suma de los órdenes de una función algebraica en todos los puntos ha de ser nula. Más precisamente:

Teorema 7.7 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 algebraicamente cerrado y $x \in K$ una función no constante. Entonces el número de ceros de x es igual al número de polos (contados ambos con sus multiplicidades) y además dicho número es $|K : k_0(x)|$.*

DEMOSTRACIÓN: Teniendo en cuenta que los divisores primos de K tienen todos grado 1, el grado de (α) es precisamente el número de ceros de α menos el número de polos, luego dicha diferencia es nula.

Como elemento de $k = k_0(x)$, se cumple $(x) = \mathfrak{p}/\mathfrak{q}$, donde $\mathfrak{p}$ es el divisor asociado al primo x de $k_0[x]$ y $\mathfrak{q}$ es el primo infinito. El número de ceros de x es el número de factores primos de $\mathfrak{p}$ en K, es decir, el grado de $\mathfrak{p}$ en K. Ahora basta aplicar la relación $\operatorname{grad}_K \mathfrak{p} = |K : k| \operatorname{grad}_k(\mathfrak{p}) = |K : k|$. ■

El teorema siguiente muestra que tener grado 0 no es suficiente en general para que un divisor sea principal:

Teorema 7.8 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes algebraicamente cerrado. Si todos los divisores de grado 0 de K son principales, entonces K es un cuerpo de fracciones algebraicas.*

DEMOSTRACIÓN: Sean $\mathfrak{P}$ y $\mathfrak{Q}$ dos divisores primos distintos en K. Como el cuerpo de constantes k_0 es algebraicamente cerrado, $\operatorname{grad} \mathfrak{P} = \operatorname{grad} \mathfrak{Q} = 1$, luego $\operatorname{grad} \mathfrak{P}/\mathfrak{Q} = 0$ y, por hipótesis, existe $x \in K$ tal que $\mathfrak{P}/\mathfrak{Q} = (x)$. La función x tiene un único cero y un único polo, luego el teorema anterior nos da que $K = k_0(x)$. ■

Definición 7.9 Sea K un cuerpo de funciones algebraicas, sea $\mathcal{D}$ su grupo de divisores y P el grupo de los divisores principales. Llamaremos *grupo de clases* de K al grupo cociente $\mathcal{H} = \mathcal{D}/P$. Diremos que dos divisores $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{D}$ son *equivalentes* si son congruentes módulo P, es decir, si $\mathfrak{a} = (\alpha)\mathfrak{b}$, para cierto $\alpha \in K^*$. Cuando hablemos de *clases* de divisores, se entenderá que nos referimos a clases de congruencia módulo P.

Como los divisores principales tienen todos grado 0, resulta que dos divisores equivalentes tienen el mismo grado, por lo que podemos hablar del grado de una clase de divisores. En otros términos, tenemos el homomorfismo

$$\operatorname{grad} : \mathcal{H} \longrightarrow \mathbb{Z}.$$

Si K/k es una extensión de cuerpos de funciones algebraicas, la inclusión $\mathcal{D}_k \longrightarrow \mathcal{D}_K$ induce un homomorfismo de grupos $\mathcal{H}_k \longrightarrow \mathcal{H}_K$. Así mismo, el teorema 7.4 nos da que la norma induce un homomorfismo $\mathrm{N}_k^K : \mathcal{H}_K \longrightarrow \mathcal{H}_k$.

7.2 Intersección de curvas

Hacemos un paréntesis en la teoría general para mostrar algunas aplicaciones interesantes de los conceptos que acabamos de introducir al estudio de las curvas planas. Sabemos que dos curvas proyectivas planas se cortan necesariamente, y ahora vamos a determinar en cuántos puntos se cortan. Por ejemplo, el hecho de que el cuerpo de constantes sea algebraicamente cerrado significa que todo polinomio $Y = F(X)$ de grado n corta al eje $X = 0$ exactamente en n puntos, siempre y cuando contemos cada corte tantas veces como indica la multiplicidad de la raíz correspondiente de F. Vamos a ver que la situación general es muy parecida. En primer lugar asignaremos una “multiplicidad” a cada punto en el que se cortan dos curvas planas, y después probaremos el teorema de Bezout, según el cual, dos curvas de grados m y n respectivamente se cortan en mn puntos, contados con sus multiplicidades. A partir de aquí obtendremos numerosas consecuencias.

Números de intersección Consideremos dos curvas proyectivas planas distintas V y W y un punto $P \in V \cap W$. Fijemos un sistema de referencia proyectivo, respecto al cual $W = V(G)$, donde $G \in k_0[X, Y, Z]$ es una forma de grado m. Elijamos una forma lineal L que no se anule en P y llamemos $g = G/L^m \in \mathcal{O}_P(V)$. Notemos que $g \neq 0$, pues en caso contrario G se anularía en V y sería $V = W$. El hecho de que $P \in W$ se traduce en que $g(P) = 0$.

Definición 7.10 En las condiciones anteriores, llamaremos *número de intersección* de V y W en P al número natural

$$I_P(V \cap W) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(g),$$

donde $\mathfrak{P}$ recorre los divisores primos de V situados sobre P.

Claramente $I_P(V \cap W) > 0$, pues $g \in \mathfrak{m}_P \subset \mathfrak{P}$ para todo primo situado sobre P, luego $v_{\mathfrak{P}}(g) \geq 1$. Convenimos en definir $I_P(V \cap W) = 0$ para puntos $P \notin V \cap W$. Así mismo es útil considerar que $I_P(V \cap V) = +\infty$.

Observemos que la definición del número de intersección no depende de la elección de L, pues si tomamos otra forma lineal L' que no se anule en P, con ella obtenemos otra función $g' = (L/L')^m g$, y L/L' es una unidad de $\mathcal{O}_P(V)$, luego también de cada anillo $\mathfrak{O}_{\mathfrak{P}}$, para cada $\mathfrak{P}$ situado sobre P, luego $v_{\mathfrak{P}}(g') = v_{\mathfrak{P}}(g)$. Una comprobación rutinaria muestra que el número de intersección tampoco depende del sistema de referencia respecto al que se calcula.

Si tomamos un sistema de referencia respecto al cual P sea finito, podemos tomar como L la recta del infinito Z, con lo que g es, en coordenadas afines, la deshomogeneización de G.

En vista de esto, definimos el número de intersección de dos curvas afines V y $W = V(G)$ (donde ahora $G \in k_0[X, Y]$) en un punto $P \in V \cap G$, como

$$I_P(V \cap W) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(g),$$

donde $g = [G] \in \mathcal{O}_P(V)$. Sucede entonces que el número de intersección en un punto de dos curvas proyectivas coincide con el de las correspondientes curvas afines según esta definición, luego en los problemas locales podemos trabajar siempre con curvas afines.

Para que la definición de número de intersección sea razonable ha de cumplir una condición que no es en absoluto evidente, pero que probamos a continuación:

Teorema 7.11 *Si V y W son dos curvas proyectivas y $P \in V \cap W$, entonces*

$$I_P(V \cap W) = I_P(W \cap V).$$

DEMOSTRACIÓN: Tomemos un sistema de referencia en el que $P = (0, 0, 1)$ y el punto $(0, 1, 0)$ no esté ni en V ni en W. Respecto a este sistema, sean $V = V(F)$ y $W = V(G)$, donde F, $G \in k_0[X, Y]$. Sean $f = [F] \in \mathcal{O}_P(W)$ y $g = [G] \in \mathcal{O}_P(V)$. Hemos de probar que

$$\sum_{\mathfrak{P}} v_{\mathfrak{P}}(g) = \sum_{\mathfrak{Q}} v_{\mathfrak{Q}}(f),$$

donde $\mathfrak{P}$ y $\mathfrak{Q}$ recorren los primos de $k_0(V)$ y $k_0(W)$ situados sobre P. El hecho de que el punto infinito $(0, 1, 0)$ no esté en las curvas se traduce en que los polinomios $F(X, Y)$ y $G(X, Y)$, como elementos de $k_0(X)[Y]$, son mónicos.

Sea $K = k_0(V) = k_0(x, y)$, donde x e y son las funciones coordenadas, y sea $k = k_0(x)$. Notemos que los primos $\mathfrak{P}$ de K situados sobre P están determinados por las condiciones $x(\mathfrak{P}) = y(\mathfrak{P}) = 0$. Además, $x(\mathfrak{P}) = 0$ equivale a $v_{\mathfrak{P}}(x) > 0$ y también a que $\mathfrak{P}$ divide al primo $\mathfrak{p}$ de k situado sobre 0. Así pues, los primos de K situados sobre P son los divisores $\mathfrak{P}$ de $\mathfrak{p}$ en K que cumplen $|y|_{\mathfrak{P}} < 1$.

Según 6.17, los divisores de $\mathfrak{p}$ en K se corresponden con los K-monomorfismos $\sigma : K \longrightarrow \mathbb{K}$, donde $\mathbb{K}$ es una clausura algebraica de $k_{\mathfrak{p}} = k_0((X))$.

Sea $F = F_1 \cdots F_r$ la descomposición en factores irreducibles de F en $k_{\mathfrak{p}}[Y]$. Para cada i, sea $F_i = (Y - y_{i1}) \cdots (y - y_{ie_i})$ la factorización de F_i en $\mathbb{K}$ (podría haber raíces repetidas si F_i no es separable). Cada y_{ij} determina un K-monomorfismo que, a su vez, determina un divisor primo $\mathfrak{P}_i$. La j no influye, pues existe un $k_{\mathfrak{p}}$-isomorfismo (en particular, una isometría) entre cada $k_{\mathfrak{p}}(y_{ij})$ y cada $k_{\mathfrak{p}}(y_{ij'})$, por lo que ambas raíces determinan el mismo divisor. Además $e(\mathfrak{P}_i/\mathfrak{p}) = |k_{\mathfrak{p}}(y_{ij}) : k_{\mathfrak{p}}| = e_i$.

Nos interesan los primos $\mathfrak{P}_i$ tales que $|y|_{\mathfrak{P}_i} = |y_{ij}| < 1$ (el último valor absoluto es el de $\mathbb{K}$). Observemos que, como cada F_i es mónico, las raíces y_{ij} son enteros algebraicos, luego en cualquier caso cumplen $|y_{ij}| \leq 1$.

Queremos calcular $v_{\mathfrak{P}_i}(g)$. Claramente,

$$|g(x, y)|_{\mathfrak{P}_i} = |G(x, y)|_{\mathfrak{P}_i} = |G(X, y_i)| = \Big| \prod_{j=1}^{e_i} G(X, y_{ij}) \Big|^{1/e_i}.$$

El producto es la norma de $G(X, y_{i1})$, luego está en $k_{\mathfrak{p}}$ y

$$v_{\mathfrak{P}_i}(g) = \frac{1}{e_i} v_{\mathfrak{P}_i}\Big(\prod_{j=1}^{e_i} G(X, y_{ij}) \Big) = v_{\mathfrak{p}}\Big(\prod_{j=1}^{e_i} G(X, y_{ij}) \Big) = v_{\mathfrak{p}}\Big(\prod_{ji'j'} (y_{ij} - y'_{i'j'}) \Big),$$

donde hemos factorizado $G = G_1 \cdots G_s$ en $k_{\mathfrak{p}}[Y]$ y a su vez cada

$$G_{i'} = (Y - y'_{i'1}) \cdots (Y - y'_{i'e'_i})$$

en $\mathbb{K}$. Como en el caso de F, sabemos que $|y'_{i'j'}| \leq 1$, y claramente el valor absoluto no depende de j'. Si $|y'_{i'j'}| = 1$ entonces $|y_{ij} - y'_{i'j'}| = 1$, luego el producto sobre j' (que está en $k_{\mathfrak{p}}$) tiene valor $v_{\mathfrak{p}}$ nulo. Al eliminar estos factores queda que

$$v_{\mathfrak{P}_i}(g) = v_{\mathfrak{p}}\Big(\prod_{j\, i'j'} (y_{ij} - y'_{i'j'})\Big), \tag{7.3}$$

donde los índices recorren sólo las raíces de F y G con valor absoluto < 1. Así pues,

$$I_P(V \cap W) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(g) = v_{\mathfrak{p}}\Big(\prod_{ij\, i'j'} (y_{ij} - y'_{i'j'})\Big).$$

El miembro derecho no se altera si intercambiamos los papeles de F y G, por lo que también es igual a $I_P(W \cap V)$. ■

En lo sucesivo calcularemos $I_P(V \cap W)$ considerando divisores de V o de W según convenga. Por ejemplo, vamos a estudiar ahora la intersección de una curva arbitraria $V = V(F)$ con una recta L. Puesto que L es regular, es más fácil trabajar con divisores de L.

Sea $(X, Y) = (a + uT, b + vT)$ una parametrización de L, de modo que su ecuación será $v(X - a) - u(Y - b) = 0$. Los puntos (finitos) de $V \cap L$ están en correspondencia con las raíces del polinomio

$$F(T) = F(a + uT, b + vT) = c \prod_{i=1}^{r} (T - t_i)^{e_i}.$$

Concretamente, $V \cap L$ consta de los puntos $P_i = (a + ut_i, b + vt_i)$. Vamos a ver que $I_{P_i}(V \cap L) = e_i$. Para ello consideramos $f = [F] \in \mathcal{O}_{P_i}(L)$. Podemos definir

$$t = \frac{x - a}{u} = \frac{y - b}{v} \in k_0[L].$$

(Notemos que puede ser $u = 0$ o $v = 0$, pero una de las dos definiciones siempre será posible y, en cualquier caso, en $k_0[L]$ se cumple $x = a + ut$, $y = b + vt$.)

Tenemos que $f = F(a + ut, b + vt) = c \prod\limits_{i=1}^{r} (t - t_i)^{e_i}$. Por otra parte, teniendo en cuenta la ecuación de L, es fácil ver que $d_{P_i}(t - t_i) \neq 0$, por lo que $t - t_i$ es un parámetro local en P_i y, en consecuencia,

$$I_{P_i}(V \cap L) = v_{P_i}\left(c \prod_{j=1}^{r} (t - t_j)^{e_j}\right) = \sum_{j=1}^{r} e_j v_{P_i}(t - t_j) = e_i.$$

Para probar el teorema de Bezout demostramos primero un caso particular:

Teorema 7.12 *Sea V una curva proyectiva plana de grado m y L una recta (distinta de V). Entonces*

$$\sum_{P \in \mathrm{P}^2} I_P(V \cap L) = m.$$

En otras palabras, V y L se cortan exactamente en m puntos, contados con su multiplicidad.

DEMOSTRACIÓN: Podemos tomar un sistema de referencia proyectivo en el que $L = V(Y)$ y en el que la recta $Z = 0$ no pase por ningún punto de $V \cap L$. Así, al deshomogeneizar respecto de Z tenemos que todos los puntos de $V \cap L$ son finitos.

Sea $V = V(F)$, con $F \in k_0[X, Y]$. Sea $F = F_0 + \cdots + F_m$ la descomposición de F en formas. Así, la ecuación de V en coordenadas homogéneas es

$$F_0(X, Y)Z^m + F_1(X, Y)Z^{m-1} + \cdots + F_m(X, Y) = 0.$$

El punto infinito $(1, 0, 0)$ está en L, luego no está en V, luego $F_m(1, 0) \neq 0$. De aquí se sigue que $F_m(X, 0)$ no es el polinomio nulo, luego es un polinomio de grado m y, a su vez, esto implica que $F(X, 0)$ es un polinomio de grado m.

La parametrización de L considerada en la discusión precedente es ahora $(X, Y) = (T, 0)$, luego para calcular $V \cap L$ hemos de considerar el polinomio

$$F(T, 0) = c \prod_{i=1}^{r} (T - t_i)^{e_i}.$$

Según acabamos de ver, tiene grado m, con lo que

$$\sum_{P \in \mathrm{P}^2} I_P(V \cap L) = \sum_{i=1}^{r} e_i = m.$$

■

Teorema 7.13 (Teorema de Bezout) *Sean V y W dos curvas proyectivas planas distintas de grados m y n. Entonces*

$$\sum_P I_P(V \cap W) = mn,$$

donde P recorre todos los puntos de P^2 (o, equivalentemente, todos los puntos de $V \cap W$).

DEMOSTRACIÓN: Sea $V = V(F)$, $W = V(G)$, donde F y G son formas en $k_0[X, Y, Z]$. Para cada punto $P \in V \cap W$ elegimos una forma lineal L_P tal que $L_P(P) \neq 0$, construimos $g_P = [F]/[L_P^n] \in \mathcal{O}_P$ y, por definición,

$$I_P(V \cap W) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(g_P),$$

donde $\mathfrak{P}$ recorre los primos de $K = k_0(V)$ situados sobre P.

Por lo tanto,

$$\sum_P I_P(V\cap W) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(g_P),$$

donde ahora $\mathfrak{P}$ recorre todos los primos de K y P es el punto sobre el que está situado el primo $\mathfrak{P}$ correspondiente.

Tomemos ahora una forma lineal arbitraria L y observemos que

$$g_P = \frac{[G]}{[L_P^n]} = \frac{[G]}{[L^n]}\frac{[L^n]}{[L_P^n]} = g_0\, l_P^n,$$

donde hemos llamado $g_0 = [G]/[L^n] \in K$ y $l_P = [L]/[L_P] \in \mathcal{O}_P$. Así pues,

$$\sum_P I_P(V\cap W) = \sum_{\mathfrak{P}} (v_{\mathfrak{P}}(g_0) + n v_{\mathfrak{P}}(l_P)) = \operatorname{grad}(g_0) + nI_P(V\cap L) = nm,$$

donde hemos usado que los divisores principales tienen grado 0 y el teorema anterior. ■

Tangentes y multiplicidades Observemos que las tangentes a una curva pueden caracterizarse por su número de intersección:

Teorema 7.14 *Si P es un punto regular de una curva plana V, entonces la tangente L a V en P es la única recta que cumple $I_P(V\cap L)\geq 2$.*

Demostración: Sea $L = V(F)$, donde F es un polinomio de grado 1 y sea $f = [F] \in \mathcal{O}_P(V)$. Es claro entonces que $d_Pf = F|_{T_PV}$. Así, L es la recta tangente T_PV si y sólo si $d_Pf = 0$, si y sólo si f no es un parámetro local de V en P, si y sólo si $I_P(V\cap L) = v_P(f) \geq 2$. ■

Notemos que si V es una recta, entonces su tangente en cualquier punto P es $L = V$ y, de acuerdo con el convenio que hemos adoptado, $I_P(V\cap L) = +\infty$. En lo sucesivo nunca nos detendremos en este caso particular, en el que todos los resultados que discutiremos se cumplirán trivialmente.

El teorema anterior permite extender la noción de recta tangente a los puntos singulares de una curva. En efecto, sea P un punto de una curva V. Fijemos un sistema de referencia respecto al cual $P = (0, 0)$ y sea $F(X, Y) = 0$ la ecuación de V en dicho sistema de referencia. Sea

$$F = F_m + F_{m+1} + \cdots + F_n, \qquad 1\leq m\leq n,$$

la descomposición de F en formas. Sea L una recta que pase por P. Su ecuación paramétrica será $(X, Y) = (uT, vT)$, con lo que

$$F(T) = F(uT, vT) = T^mF_m(u, v) + \cdots + T^nF_n(u, v).$$

Podemos descomponer $F_m = \prod\limits_{i=0}^{r} L_i^{e_i}$ en producto de formas lineales (basta deshomogeneizar F_m a $F_m(X, 1)$, factorizar el polinomio resultante y volver a homogeneizar). Es claro entonces que $F_m(u, v) = 0$ si y sólo si $L = L_i$ para algún i. Concluimos que $I_P(V, L) = m$ para todas las rectas excepto para un número finito de ellas.

Definición 7.15 Si P es un punto de una curva plana V de grado n, llamaremos *multiplicidad* de P en V al mínimo número natural $m \leq n$ tal que existen rectas L tales que $I_P(V \cap L) = m$. La representaremos por $m_P(V)$. Según acabamos de probar, la igualdad $I_P(V \cap L) = m_P(V)$ se cumple para todas las rectas que pasan por P salvo para un número finito de ellas, a las que llamaremos *rectas tangentes* a V en P. Según su multiplicidad, los puntos se clasifican en *simples dobles, triples, etc.*

Con la notación anterior, los coeficientes de F_1 son las derivadas de F en P, luego $F_1 = 0$ si y sólo si P es un punto singular de V. En otras palabras, un punto P es regular en V si y sólo si es simple. En tal caso, la única recta tangente según la definición anterior es la de ecuación $F_1 = 0$, pero ésta es la recta tangente que ya teníamos definida. Por lo tanto, la nueva definición incluye a la anterior como un caso particular.

Notemos que si V es una curva plana de grado $n > 1$, se ha de cumplir que $m_P(V) < n$, pues en caso contrario el polinomio que define a V sería la forma F_n y sería reducible. En particular, las cónicas no pueden tener singularidades.

Ejemplos El punto $(0, 0)$ es un punto doble de la curva "alfa", dada por la ecuación $Y^2 = X^2(X + 1)$. Sus tangentes son los factores de $F_2 = X^2 - Y^2$, es decir, las rectas $Y = \pm X$.

Igualmente, $(0, 0)$ es un punto doble de la curva $Y^2 = X^3$, pero ahora $F_2 = Y^2$, luego la curva tiene sólo una tangente (doble) en $(0, 0)$, a saber, la recta $Y = 0$. ■

Veamos ahora que podemos asignar una tangente a cada divisor primo de una curva. En efecto, sea $\mathfrak{P}$ un divisor primo de una curva V situado sobre un punto P. Fijemos un sistema de referencia afín en el que $P = (0, 0)$. Sea $m_0 = \operatorname{mín}\{v_{\mathfrak{P}}(x), v_{\mathfrak{P}}(y)\} > 0$. Supongamos, por ejemplo, que el mínimo se alcanza en x, es decir, $v_{\mathfrak{P}}(x) = m_0$. Fijado un primo π en $\mathfrak{O}_{\mathfrak{P}}$, tenemos que $v_{\mathfrak{P}}(x/\pi^{m_0}) = 0$, luego existe un $a \in k_0$ no nulo tal que $x/\pi^{m_0} \equiv a \pmod{\mathfrak{P}}$. Multiplicando π por una raíz m_0-ésima de a podemos suponer que $a = 1$. Así $x = \pi^{m_0} + \alpha\pi^{m_0+1}$, para cierto $\alpha \in \mathfrak{O}_{\mathfrak{P}}$. Similarmente, $y = a\pi^{m_0} + \beta\pi^{m_0+1}$, con $a \in k_0$ y $\beta \in \mathfrak{O}_{\mathfrak{P}}$ (tal vez $a = 0$). Si $L = uX + vY$ es cualquier recta que pasa por P y $l = ux + vy = [L] \in \mathfrak{O}_P$, tenemos que

$$v_{\mathfrak{P}}(l) = v_{\mathfrak{P}}((u + va)\pi^{m_0} + \gamma\pi^{m_0+1}).$$

Claramente, $v_{\mathfrak{P}}(l) = m_0$ excepto si $u + va = 0$, en cuyo caso $v_{\mathfrak{P}}(l) > m_0$. Esto determina una única recta L. Hemos probado el teorema siguiente:

Teorema 7.16 *Sea V una curva plana y $\mathfrak{P}$ un divisor primo de V situado sobre un punto P. Si L es una recta que pasa por P y $l = [L] \in \mathfrak{O}_{\mathfrak{P}}$, entonces $v_{\mathfrak{P}}(l)$ toma el mismo valor m_0 para todas las rectas L excepto para una de ellas.*

Definición 7.17 En las condiciones del teorema anterior, diremos que m_0 es la *multiplicidad* de $\mathfrak{P}$ en V, y la representaremos por $m_{\mathfrak{P}}(V)$. Llamaremos *tangente* a V en $\mathfrak{P}$ a la única recta L tal que $v_{\mathfrak{P}}(l) > m_{\mathfrak{P}}(V)$.

Las tangentes que acabamos de definir son las que ya teníamos definidas:

Teorema 7.18 *Si P es un punto de una curva plana V, las tangentes a V en P son las tangentes a V en los primos situados sobre P y la multiplicidad $m_P(V)$ es la suma de las multiplicidades $m_{\mathfrak{P}}(V)$ de estos primos.*

DEMOSTRACIÓN: Si L es una recta que pasa por P distinta de todas las tangentes a V en P y de todas las tangentes a V en los primos situados sobre P, entonces

$$m_P(V) = I_P(V \cap L) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(l) = \sum_{\mathfrak{P}} m_{\mathfrak{P}}(V).$$

Una recta L es tangente a V en P si y sólo si

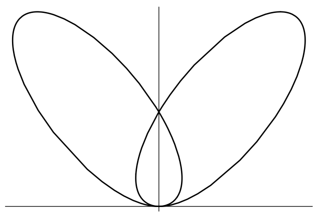
$$\sum_{\mathfrak{P}} v_{\mathfrak{P}}(l) = I_P(V \cap L) > m_P(V) = \sum_{\mathfrak{P}} m_{\mathfrak{P}}(V).$$

Como, en cualquier caso, $v_{\mathfrak{P}}(l) \geq m_{\mathfrak{P}}(V)$, la desigualdad anterior equivale a que $v_{\mathfrak{P}}(l) > m_{\mathfrak{P}}(V)$ para algún $\mathfrak{P}$, es decir, a que L sea tangente a L en un primo $\mathfrak{P}$. ■

En particular, el teorema anterior implica que el número de primos situados sobre un punto P es mayor o igual que el número de tangentes a V en P y menor o igual que $m_P(V)$. Ninguna de estas dos desigualdades tiene por qué ser una igualdad. La curva $Y^2 = X^3$ tiene una singularidad con un solo primo y multiplicidad 2, mientras que la curva del ejemplo siguiente tiene una singularidad en $(0,0)$ con una tangente y dos primos.

Ejemplo Consideremos la curva V dada por la ecuación

$$Y^4 - 2Y^3 + Y^2 - 3X^2Y + 2X^4 = 0$$



Para probar que es irreducible homogeneizamos respecto de Z y deshomogeneizamos respecto de Y, con lo que tenemos el polinomio

$$Z^2 - (3X^2 + 2)Z + 2X^4 + 1.$$

Es fácil ver que no tiene raíces en $\mathbb{C}[X]$, luego es irreducible.

Una simple comprobación muestra que la intersección de V con la recta $X = 0$ la forman los puntos $(0,0)$ y $(0,1)$. El punto $(0,0)$ es doble y tiene una única tangente, $Y = 0$. Para estudiar el punto $(0,1)$ hacemos el cambio $Y \mapsto Y + 1$, con lo que obtenemos la ecuación

$$Y^4 + 2X^4 + 2Y^3 - 3X^2 + Y^2 - 3X^2 = 0.$$

Vemos que $(0,1)$ es doble con dos tangentes distintas, $Y = \pm\sqrt{3}X$.

Sea $K = \mathbb{C}(V) = \mathbb{C}(x,y)$ y $k = \mathbb{C}(x)$. Los primos de $K = \mathbb{C}(V)$ que dividen al primo $\mathfrak{p}$ de k situado sobre 0 son los situados sobre las antiimágenes de 0 por x, es decir, sobre los puntos $(0,0)$ o $(0,1)$.

Sobre $(0,1)$ hay exactamente dos primos, pues la multiplicidad es 2 y hay dos tangentes. Sobre $(0,0)$ puede haber uno o dos primos. Esto deja dos posibilidades: $0 = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4$ o bien $0 = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3^2$. Si se da la primera — y vamos a ver que éste es el caso— entonces sobre $(0,0)$ hay exactamente dos primos y una sola tangente.

Hemos de excluir la posibilidad de que 0 se escinda completamente. Lo haremos mediante un argumento indirecto a través de la fórmula del género. En primer lugar estudiamos la ramificación en infinito.

La curva V tiene cuatro puntos distintos en el infinito, cuyas coordenadas homogéneas cumplen $Y^4 + 2X^4 = 0$. No puede ser $X = 0$, por lo que la función x tiene un polo sobre cada uno de ellos. Así pues, todos dividen al primo infinito de k. Como éste tiene a lo sumo cuatro divisores, concluimos que, de hecho tiene cuatro, $\infty = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4$, luego no hay ramificación en el infinito.

Ahora observamos que la aplicación $(X,Y) \mapsto (-X,Y)$ es un isomorfismo de V en sí misma que induce un automorfismo de K. Su restricción a k es el automorfismo inducido por el isomorfismo $X \mapsto -X$ de $\mathbb{C}^\infty$. Es claro entonces que los índices de ramificación del primo de k situado sobre un $\zeta \in \mathbb{C}$ son los mismos que los del primo situado sobre $-\zeta$. Por consiguiente, en la fórmula

$$2 - 2g = 8 - \sum_i (e_i - 1),$$

el sumatorio es de la forma $2a + b$, donde $2a$ es la aportación de los primos distintos de 0 e ∞ y b es la aportación de 0 (pues ya hemos visto que en ∞ no hay ramificación). Las posibilidades para b son $b = 0$ si 0 se escinde completamente y $b = 1$ si hay ramificación. Ahora bien, la relación $2 - 2g = 8 - 2a - b$ muestra que b ha de ser par, luego $b = 0$ y concluimos que 0 se escinde completamente. ■

El teorema siguiente muestra que los números de intersección se reducen casi siempre a las multiplicidades:

Teorema 7.19 *Sean V y W dos curvas planas distintas y $P \in V \cap W$. Entonces*

$$I_P(V \cap W) \geq m_P(V) m_P(W).$$

La igualdad se da si y sólo si V y W no tienen tangentes comunes en P.

Demostración: Tomemos un sistema de referencia tal que $P = (0,0)$ y la recta $X = 0$ no sea tangente a V ni a W en P. Sea $V = V(F)$, $W = V(G)$. Basta probar que

$$v_{\mathfrak{P}}(g) \geq m_{\mathfrak{P}}(V) m_P(W),$$

y que se da la igualdad si y sólo si ninguna tangente a V en $\mathfrak{P}$ es tangente a W. La prueba se basa en la expresión para $v_{\mathfrak{P}}(g)$ que hemos encontrado en la demostración del teorema 7.11.

El hecho de que la recta $X = 0$ no sea tangente a V en $\mathfrak{P}$ implica que $v_{\mathfrak{P}}(x) = m_{\mathfrak{P}}(V) \leq v_{\mathfrak{P}}(y)$. Llamemos $r = m_{\mathfrak{P}}(V)$. Podemos tomar un primo π en $\mathfrak{O}_{\mathfrak{P}}$ tal que $x = \pi^r + \alpha\pi^{r+1}$, con $\alpha \in \mathfrak{O}_{\mathfrak{P}}$. Sea $y = a\pi^r + \beta\pi^{r+1}$, con $\beta \in \mathfrak{O}_{\mathfrak{P}}$. Así la tangente a V en $\mathfrak{P}$ es la recta $-aX + Y$.

Similarmente, si $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ son los primos de W situados sobre P, llamamos $r_i = v_{\mathfrak{Q}_i}(x)$ y elegimos un primo π_i en $\mathfrak{O}_{\mathfrak{Q}_i}$ de modo que

$$x = \pi_i^{r_i} + \alpha_i \pi_i^{r_i+1}, \qquad y = a_i \pi_i^{r_i} + \beta_i \pi_i^{r_i+1}.$$

La tangente a W en $\mathfrak{Q}_i$ es $-a_i X + Y$, luego la hipótesis de que la tangente a V en $\mathfrak{P}$ no sea tangente a W equivale a que $a \neq a_i$ para todo i. Además tenemos que

$$r_1 + \cdots + r_s = m_{\mathfrak{Q}_1}(W) + \cdots + m_{\mathfrak{Q}_s}(W) = m_P(W).$$

Sea $K = k_0(V)$, sea $k = k_0(x)$ y sea $\mathfrak{p}$ el primo de k situado sobre 0 (que es el primo al que divide $\mathfrak{P}$). Sea $k_{\mathfrak{p}} = k_0((X))$ y $\mathbb{K}$ una clausura algebraica de $k_{\mathfrak{p}}$. En el teorema 7.11 hemos obtenido la igualdad (7.3), en virtud de la cual $v_{\mathfrak{P}}(g)$ es el valor $v_{\mathfrak{p}}$ del producto de todos los $y_j - y'_{i'j'}$, donde y_{ij} varía entre las raíces de $F(X,Y)$ en $\mathbb{K}$ que inducen el primo $\mathfrak{P}$ e $y'_{i'j'}$ recorre las raíces de $G(X,Y)$ en $\mathbb{K}$ que inducen cada primo $\mathfrak{Q}_{i'}$. (Hemos suprimido el índice i porque aquí $\mathfrak{P}$ está fijo.)

Como $v_{\mathfrak{p}}(x) = 1$, tenemos que $r = e(\mathfrak{P}/\mathfrak{p})$, luego hay r raíces y_j, cada una de las cuales es imagen de y por un $k_{\mathfrak{p}}$-monomorfismo $\sigma_j : K_{\mathfrak{P}} \longrightarrow \mathbb{K}$. Todas las raíces que estamos considerando estarán en una extensión finita E de $k_{\mathfrak{p}}$, donde podemos trabajar con una valoración v. Sea $e = e(E/k_{\mathfrak{p}})$, de modo que $v = e v_{\mathfrak{p}}|_{k_{\mathfrak{p}}}$. Tenemos que

$$x = \sigma_j(x) = \sigma_j(\pi)^r + \sigma_j(\alpha)\sigma_j(\pi)^{r+1}, \quad y_j = \sigma_j(y) = a\sigma_i(\pi)^r + \sigma_j(\alpha)\sigma_j(\pi)^{r+1},$$

luego $y_j = ax + \delta_j \rho^{e+1}$, donde ρ es un primo en E y $v(\delta_j) \geq 0$.

Similarmente, $y'_{i'j'} = a_{i'} x + \delta_{i'j'} \rho^{e+1}$. Así pues,

$$v_{\mathfrak{P}}(g) = v_{\mathfrak{p}}\Big(\prod_{j\,i'j'} \big((a - a_{i'})x + (\delta_j - \delta_{i'j'})\rho^{e+1}\big)\Big)$$

$$= \frac{1}{e} \sum_{j\,i'j'} v_{\mathfrak{P}}\big((a - a_{i'})x + (\delta_j - \delta_{i'j'})\rho^{e+1}\big) \geq \frac{1}{e} \sum_{j\,i'j'} e = r(r_1 + \cdots + r_s)$$

$$= m_{\mathfrak{P}}(V) m_P(W).$$

Se cumple que $v_{\mathfrak{P}}((a - a_{i'})x + (\delta_j - \delta_{i'j'}\rho^{e+1})) > e$ si y sólo si $a = a_{i'}$, luego la igualdad $v_{\mathfrak{P}}(g) = m_{\mathfrak{P}}(V) m_P(W)$ se da exactamente cuando $a \neq a_{i'}$ para todo i'. ■

Ahora podemos dar una caracterización geométrica del grado de una curva plana:

Teorema 7.20 *Si V es una curva plana de grado n, existen infinitas rectas que cortan a V en n puntos distintos.*

DEMOSTRACIÓN: Observemos que las rectas de P^2 están en correspondencia biunívoca con los puntos de P^2 mediante $aX + bY + cZ = 0 \leftrightarrow (a, b, c)$. Sea

$V = V(F)$, sea V_0 la subvariedad formada por los puntos regulares de V y consideremos la aplicación $\phi : V_0 \longrightarrow \mathrm{P}^2$ dada por

$$\phi(P) = \left(\left.\frac{\partial F}{\partial X}\right|_P, \left.\frac{\partial F}{\partial Y}\right|_P, \left.\frac{\partial F}{\partial Z}\right|_P \right).$$

Obviamente es regular y $\phi[V_0]$ contiene todos los puntos correspondientes a las rectas de P^2 tangentes a V en algún punto regular. Sea $W = \overline{\phi[V_0]}$ que es una subvariedad de P^2, pues si $W = C_1 \cup C_2$, con C_1 y C_2 cerrados, entonces $V_0 = \phi^{-1}[C_1] \cup \phi^{-1}[C_2]$, luego $V_0 = \phi^{-1}[C_i]$, $\phi[V_0] \subset C_i$ y $W = \overline{\phi[V_0]} \subset C_i$.

Tenemos que $\phi : V_0 \longrightarrow W$ es densa, luego podemos identificar $k_0(W)$ con un subcuerpo de $k_0(V)$ y, por lo tanto, $\dim W \leq \dim V_0 = 1$.

Fijado un punto $P \in V$ regular, el conjunto de rectas que pasan por P se corresponde con una recta L de P^2 a través de la correspondencia que hemos indicado. Cambiando P por otro punto si fuera preciso, podemos suponer que $L \neq W$. Así, $L \cap W$ es finito, luego hay infinitos puntos en $L \setminus W$, cada uno de los cuales se corresponde con una recta que pasa por P y no es tangente a V en ningún punto regular.

Eliminando las rectas que pasan por P y por un punto singular de V (que son un número finito), nos quedan todavía infinitas rectas R que pasan por P y que sólo cortan a V en puntos regulares (sin ser tangentes). Entonces $I_Q(V \cap R) = 1$ para cada $Q \in V \cap R$. Por el teorema de Bezout, R corta a V en n puntos distintos. ■

Teniendo en cuenta el teorema de Bezout, vemos que el grado de una curva plana V es el máximo número n tal que existe una recta que corta a V en n puntos distintos.

Numeros de intersección entre formas Fijado un sistema de referencia en P^2, para cada par de formas F, $G \in k_0[X, Y, Z]$, consideramos sus descomposiciones en formas irreducibles[1] $F = F_1 \cdots F_r$, $G = G_1 \cdots G_s$ y definimos el *número de intersección*

$$I_P(F \cap G) = \sum_{ij} I_P(V_i \cap W_j),$$

donde $V_i = V(F_i)$, $W_j = V(G_j)$. Este número será infinito si y sólo si F y G tienen un factor común. Así mismo, definimos la *multiplicidad* de P en F como

$$m_P(F) = \sum_i m_P(V_i).$$

Igualmente podemos definir multiplicidades y multiplicidades para polinomios de $k_0[X, Y]$. Incluso podemos hablar de números de intersecciones mixtos $I_P(V \cap G)$, donde $V = V(F)$ es una curva (y F es una forma irreducible) y G una forma arbitraria.

[1] Es fácil ver que los factores irreducibles de las formas son formas: basta deshomogeneizar respecto a una variable, factorizar y volver a homogeneizar.

Todos los teoremas que hemos probado para curvas se generalizan trivialmente a polinomios. Por ejemplo, el teorema de Bezout para formas afirma que $I_P(F \cap G) = (\operatorname{grad} F)(\operatorname{grad} G)$. Para probarlo basta descomponer F y G y aplicar el teorema de Bezout a las curvas definidas por cada par de factores.

Notemos que si $F \in k_0[X, Y]$ es un polinomio, entonces su forma de menor grado es el producto de las formas de menor grado de sus factores, por lo que la multiplicidad en F de $(0, 0)$ sigue siendo este grado mínimo. Así mismo, las tangentes a F en $(0, 0)$ siguen siendo los factores de esta forma de grado mínimo. Todas las comprobaciones son inmediatas. Observemos que la relación

$$I_P(V \cap G) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(g)$$

sigue siendo válida aunque G no sea irreducible, pues la función g es el producto de las funciones g_i asociadas a los factores de G. De aquí se sigue una propiedad adicional que simplifica mucho el cálculo de números de intersección:

$$I_P(F \cap G) = I_P(F \cap (G + HF)),$$

pues $f = 0$ en $\mathcal{O}_P(V_i)$, luego $g = g + hf$.

Puntos de inflexión Estudiamos ahora una noción relacionada con el número de intersección de una curva con su tangente. Como aplicación obtendremos algunos resultados sobre cúbicas regulares que nos harán falta más adelante.

Definición 7.21 un *punto de inflexión* de una curva plana V es un punto regular P de V tal que existe una recta L (que necesariamente ha de ser la tangente a V en P) para la cual $I_P(V \cap L) \geq 3$. La inflexión se llama *ordinaria* si $I_P(V \cap L) = 3$.

Obviamente una cónica no puede tener inflexiones. Teniendo en cuenta el ejemplo de la página 119, es fácil ver que toda cúbica singular tiene una única inflexión. Vamos a probar que las cúbicas regulares también tienen inflexiones. Para ello nos basaremos en una caracterización de los puntos de inflexión.

Consideremos un punto regular P de una curva V. Podemos tomar un sistema de referencia respecto al cual $P = (0, 0)$. Sea $F = F_1 + \cdots + F_n$ el polinomio que define a F.

Una recta L parametrizada por $(X, Y) = (uT, vT)$ cumplirá $I_P(V \cap L) \geq 3$ si $F_1(u, v) = F_2(u, v) = 0$. Así pues, P será un punto de inflexión de V si y sólo si existe $(u, v) \in k_0^2$, $(u, v) \neq (0, 0)$, tal que $F_1(u, v) = F_2(u, v) = 0$.

En primer lugar probamos que esto equivale a que el polinomio $F_1 + F_2$ sea reducible (o bien $F_2 = 0$).

En efecto, suponiendo $v \neq 0$ y llamando $t = u/v$ tenemos que $F_1(t, 1) = F_2(t, 1) = 0$, luego $F_1(X, 1) \mid F_2(X, 1)$ y, sustituyendo X por X/Y, concluimos que $F_1(X, Y) \mid F_2(X, Y)$.

Recíprocamente, Si $F_1 + F_2 = RS$ y $F_2 \neq 0$, entonces ambos factores tienen grado 1, y uno de ellos, digamos R, ha de cumplir $R(0, 0) = 0$. Entonces F_1

es R por el término independiente de S, luego $F_1 \mid F_2$ y cualquier raíz no nula (u,v) de F_1 lo es de F_2.

A partir de aquí supondremos que la característica de k_0 es distinta de 2, con lo que la forma F_2 (que, de momento, supondremos no nula) es

$$F_2(X,Y) = \frac{1}{2}\left(\frac{\partial^2 F}{\partial X^2}\bigg|_P X^2 + 2\,\frac{\partial^2 F}{\partial X \partial Y}\bigg|_P XY + \frac{\partial^2 F}{\partial Y^2}\bigg|_P X^2 \right).$$

La condición que hemos encontrado es la reducibilidad del polinomio

$$\frac{\partial F}{\partial X}\bigg|_P X + \frac{\partial F}{\partial Y}\bigg|_P Y + \frac{1}{2}\,\frac{\partial^2 F}{\partial X^2}\bigg|_P X^2 + \frac{\partial^2 F}{\partial X \partial Y}\bigg|_P XY + \frac{1}{2}\,\frac{\partial^2 F}{\partial Y^2}\bigg|_P X^2.$$

Esta ecuación determina una cónica afín, que será reducible si y sólo si lo es su clausura proyectiva, determinada por la forma

$$\frac{\partial F}{\partial X}\bigg|_P XZ + \frac{\partial F}{\partial Y}\bigg|_P YZ + \frac{1}{2}\,\frac{\partial^2 F}{\partial X^2}\bigg|_P X^2 + \frac{\partial^2 F}{\partial X \partial Y}\bigg|_P XY + \frac{1}{2}\,\frac{\partial^2 F}{\partial Y^2}\bigg|_P X^2.$$

Matricialmente es:

$$(X,Y,Z)\begin{pmatrix} \frac{\partial^2 F}{\partial X^2}\Big|_P & \frac{\partial^2 F}{\partial X \partial Y}\Big|_P & \frac{\partial F}{\partial X}\Big|_P \\ \frac{\partial^2 F}{\partial X \partial Y}\Big|_P & \frac{\partial^2 F}{\partial Y^2}\Big|_P & \frac{\partial F}{\partial Y}\Big|_P \\ \frac{\partial F}{\partial X}\Big|_P & \frac{\partial F}{\partial Y}\Big|_P & 0 \end{pmatrix}\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

Es conocido que una cónica es irreducible si y sólo si el rango de su matriz es 3 (ver el ejemplo de la página 73). Así pues, P será un punto de inflexión si y sólo si

$$\begin{vmatrix} \frac{\partial^2 F}{\partial X^2}\Big|_P & \frac{\partial^2 F}{\partial X \partial Y}\Big|_P & \frac{\partial F}{\partial X}\Big|_P \\ \frac{\partial^2 F}{\partial X \partial Y}\Big|_P & \frac{\partial^2 F}{\partial Y^2}\Big|_P & \frac{\partial F}{\partial Y}\Big|_P \\ \frac{\partial F}{\partial X}\Big|_P & \frac{\partial F}{\partial Y}\Big|_P & 0 \end{vmatrix} = 0.$$

(Esta condición recoge también el caso en que $F_2 = 0$). Todavía podemos obtener una condición formalmente más simple. Llamemos $F(X,Y,Z)$ a la homogeneización de F, de modo que $F(X,Y) = F(X,Y,1)$. Es claro que ambos polinomios tienen las mismas derivadas respecto de X e Y, luego podemos considerar que la F que aparece en el determinante anterior es $F(X,Y,Z)$. Ahora usamos la relación

$$\frac{\partial F}{\partial X}X + \frac{\partial F}{\partial Y}Y + \frac{\partial F}{\partial Z}Z = nF$$

y las que resultan de aplicar esta misma propiedad a las parciales de F:

$$\frac{\partial^2 F}{\partial X^2}X + \frac{\partial^2 F}{\partial X \partial Y}Y + \frac{\partial^2 F}{\partial X \partial Z}Z = (n-1)\frac{\partial F}{\partial X},$$

$$\frac{\partial^2 F}{\partial X \partial Y}X + \frac{\partial^2 F}{\partial Y^2}Y + \frac{\partial^2 F}{\partial Y \partial Z}Z = (n-1)\frac{\partial F}{\partial Y}.$$

Multiplicamos la tercera columna del determinante por $n-1$ y le restamos las dos primeras (usando que $F(P)=0$) y luego repetimos las operaciones con las filas. El determinante resulta ser igual a

$$H(F)(P) = \begin{vmatrix} \left.\frac{\partial^2 F}{\partial X^2}\right|_P & \left.\frac{\partial^2 F}{\partial X \partial Y}\right|_P & \left.\frac{\partial^2 F}{\partial X \partial Z}\right|_P \\ \left.\frac{\partial^2 F}{\partial X \partial Y}\right|_P & \left.\frac{\partial^2 F}{\partial Y^2}\right|_P & \left.\frac{\partial^2 F}{\partial Y \partial Z}\right|_P \\ \left.\frac{\partial^2 F}{\partial X \partial Z}\right|_P & \left.\frac{\partial^2 F}{\partial Y \partial Z}\right|_P & \left.\frac{\partial^2 F}{\partial Z^2}\right|_P \end{vmatrix}.$$

El determinante $H(F)(P)$ se llama *hessiano* de F en P y es fácil ver que la condición $H(F)(P)=0$ no depende del sistema de referencia elegido, pues un cambio de sistema de referencia proyectivo multiplica la matriz hessiana por una matriz regular.

Teorema 7.22 *Un punto regular P de una curva plana $V=V(F)$ es un punto de inflexión si y sólo si $H(F)(P)=0$.*

Notemos que si V tiene grado n entonces $H(F)(X,Y,Z)$ es una forma de grado $3(n-2)$, luego, si $n \geq 3$, define una curva proyectiva (salvo que sea la forma nula). El teorema 3.24 implica que existe un punto $P \in V$ tal que $H(F)(P)=0$. Si P es regular será un punto de inflexión. Así pues:

Teorema 7.23 *Toda curva proyectiva plana regular de grado ≥ 3 (sobre un cuerpo de característica distinta de 2) tiene un punto de inflexión.*

Consideremos por ejemplo una cúbica regular $V=V(F)$. Podemos tomar un sistema de referencia afín en el que el punto de inflexión sea $(X,Z)=(0,0)$. Si $F(X,Z)=F_1(X,Z)+F_2(X,Z)+F_3(X,Z)$, hemos visto que el hecho de que $(0,0)$ sea un punto de inflexión equivale a que la cónica $F_1(X,Z)+F_2(X,Z)$ sea reducible (o bien $F_2=0$). Así pues,

$$F(X,Z) = (uX+vZ)(1+aX+bZ)+cX^3+dX^2Z+eXZ^2+fZ^3,$$

donde $(u,v) \neq (0,0)$, o de lo contrario $(0,0)$ sería un punto singular. Supongamos $v \neq 0$. El cambio de coordenadas dado por $X'=X$, $Z'=uX+vZ$ nos da un polinomio de la forma

$$F(X,Z) = Z(1+aX+bZ)+cX^3+dX^2Z+eXZ^2+fZ^3.$$

Si homogeneizamos con Y y deshomogeneizamos respecto de Z (con lo que el punto de inflexión pasa a estar en el infinito) obtenemos que V está determinada por la ecuación

$$Y^2+(aX+b)Y+cX^3+dX^2+eX+f=0.$$

Ahora el cambio de coordenadas $Y=Y'-(aX'+b)/2$ reduce la ecuación a

$$Y^2 = aX^3+bX^2+cX+d,$$

donde $a \neq 0$, pues V es una cúbica (por ejemplo, si fuera $a = 0$ no podría haber un punto de inflexión). En este cambio hemos supuesto que la característica de k_0 es distinta de 2. Si suponemos además que es distinta de 3 podemos hacer el cambio

$$X = aX' - \frac{b}{3a}, \qquad Y = \frac{a^2}{2}Y'$$

y la ecuación se reduce a

$$Y^2 = 4X^3 - g_2X - g_3, \qquad g_2,\ g_3 \in k_0.$$

Por último notamos que si a fuera una raíz múltiple del polinomio de la derecha, entonces $(a, 0)$ sería un punto singular de V. Así pues, hemos probado el teorema siguiente:

Teorema 7.24 *Toda cúbica regular sobre un cuerpo k_0 de característica distinta de 2 o 3 es proyectivamente equivalente a una cúbica de ecuación*

$$Y^2 = 4X^3 - g_2X - g_3, \qquad g_2,\ g_3 \in k_0,$$

donde el polinomio de la derecha no tiene raíces múltiples.

Una ecuación en las condiciones del teorema anterior se llama *forma normal de Weierstrass* de la cúbica regular V. La notación g_2, g_3 para las constantes es la acostumbrada en la teoría de funciones elípticas, en la que ahora no vamos a entrar.

Es fácil probar que, recíprocamente, toda ecuación en forma normal determina una cúbica regular (la irreducibilidad se sigue del criterio de Eisenstein aplicado a un factor primo del miembro derecho).

7.3 Diferentes

En esta sección probaremos que el número de primos ramificados en una extensión separable de cuerpos de funciones algebraicas es finito. Se trata de un resultado global, pero empezaremos estudiando más a fondo la ramificación desde un punto de vista local.

Si K/k es una extensión finita de cuerpos, la aplicación $(\alpha, \beta) \mapsto \operatorname{Tr}(\alpha\beta)$ es una forma bilineal en K. Su matriz en una k-base de K dada, digamos $w_1, \ldots, w_n$, es claramente $\bigl(\operatorname{Tr}(w_iw_j)\bigr)$. En la prueba del teorema 1.19 vimos que si la extensión K/k es separable entonces esta matriz tiene determinante no nulo, por lo que la forma bilineal es regular e induce un isomorfismo entre K y su k-espacio vectorial dual (el espacio de las aplicaciones lineales de K en k). En general, cada base de un espacio vectorial de dimensión finita tiene asociada una base en su espacio dual. En nuestro caso podemos considerar su antiimagen por el isomorfismo inducido por la traza y obtenemos así otra k-base de K, a la que llamamos base dual de la base de partida.

El teorema siguiente recoge los hechos que vamos a necesitar en la práctica sobre todo lo dicho.

Teorema 7.25 *Sea K/k una extensión de cuerpos finita separable, consideremos la traza* $\mathrm{Tr} : K \longrightarrow k$ *y sea* $w_1, \ldots, w_n$ *una* k*-base de* K*. Entonces*

a) La matriz $\big(\mathrm{Tr}(w_i w_j)\big)$ *tiene determinante no nulo.*

b) Existen unos únicos elementos $z_1, \ldots, z_n$ *en* K *de modo que*

$$\mathrm{Tr}(w_i z_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Estos elementos forman una k*-base de* K *a la que llamaremos* base dual *de la base dada.*

Demostración: El apartado a) está probado en la demostración del teorema 1.19. También vimos allí la existencia de los elementos $z_1, \ldots, z_n$, y es clara su unicidad, pues las coordenadas de los z_i en la base w_j son la solución de un sistema de n ecuaciones lineales con n incógnitas cuya matriz de coeficientes es la del apartado a). Esto mismo implica que $z_1, \ldots, z_n$ forman una k-base de K. ■

Definición 7.26 Sea K/k una extensión finita separable de cuerpos métricos discretos completos, sea $\mathfrak{o}$ el anillo de enteros de k y $\mathrm{Tr} : K \longrightarrow k$ la traza de la extensión. Para cada $L \subset K$, definimos su *complementario* como el conjunto

$$L' = \{\alpha \in K \mid \mathrm{Tr}[\alpha L] \subset \mathfrak{o}\} \subset K.$$

Teorema 7.27 *Sea K/k una extensión separable de cuerpos métricos discretos completos, sean* $\mathfrak{o}$ *y* $\mathfrak{O}$ *sus respectivos anillos de enteros y sean* L *y* M *subgrupos aditivos de* K*. Entonces*

a) L' *es un subgrupo aditivo de* K*.*

b) Si L *es un* $\mathfrak{o}$*-módulo (o un* $\mathfrak{O}$*-módulo) entonces* L' *también lo es.*

c) Si $L \subset M$ *entonces* $M' \subset L'$*.*

d) Si $w_1, \ldots, w_n$ *es una* k*-base de* K *y* $w'_1, \ldots, w'_n$ *es su base dual, entonces el módulo complementario de* $L = \langle w_1, \ldots, w_n\rangle_{\mathfrak{o}}$ *es* $L' = \langle w'_1, \ldots, w'_n\rangle_{\mathfrak{o}}$*.*

Demostración: a) Si α_1, $\alpha_2 \in L'$ entonces

$$\mathrm{Tr}\big((\alpha_1 - \alpha_2)\beta\big) = \mathrm{Tr}(\alpha_1\beta) - \mathrm{Tr}(\alpha_2\beta) \in \mathfrak{o}$$

para todo $\beta \in L$.

b) Si $\alpha \in L'$ y $d \in \mathfrak{o}$ (o $d \in \mathfrak{O}$) entonces $d\beta \in L$ para todo $\beta \in L$, luego $\mathrm{Tr}(d\alpha\beta) = \mathrm{Tr}\big(\alpha(d\beta)\big) \in \mathfrak{o}$ para todo $\beta \in L$.

c) es evidente.

d) Sea $\alpha \in L'$. Entonces $\alpha = a_1 w'_1 + \cdots a_n w'_n$ para ciertos elementos $a_i \in K$. Pero sucede que $a_i = \mathrm{Tr}(\alpha w_i) \in \mathfrak{o}$, luego $\alpha \in \langle w'_1, \ldots, w'_n\rangle_{\mathfrak{o}}$.

Recíprocamente, si $\alpha = a_1 w_1' + \cdots + a_n w_n'$, para ciertos elementos $a_i \in \mathfrak{o}$, entonces $\mathrm{Tr}(\alpha w_i) = a_i \in \mathfrak{o}$, y por linealidad es claro que $\mathrm{Tr}(\alpha\beta) \in \mathfrak{o}$ para todo $\beta \in L$, luego $\alpha \in L'$. ■

En la situación del teorema anterior, estamos principalmente interesados en el $\mathfrak{O}$-módulo $\mathfrak{O}'$. Observemos que de 5.35 se sigue que $\mathrm{Tr}[\mathfrak{O}] \subset \mathfrak{o}$ (la traza de un entero es entera). Esto implica que $\mathfrak{O} \subset \mathfrak{O}'$.

Por otra parte, la separabilidad de la extensión implica que existe un $\alpha \in K$ con $\mathrm{Tr}(\alpha) = a \neq 0$. Si π es un primo en $\mathfrak{o}$, tenemos que $\mathrm{Tr}(\alpha/\pi^i) = a/\pi^i$, que no está en $\mathfrak{o}$ para i suficientemente grande. Concluimos que $\mathfrak{O}' \neq K$.

Si $\alpha \in \mathfrak{O}'$, entonces $\alpha\mathfrak{O} \subset \mathfrak{O}'$, es decir, $\mathfrak{O}'$ contiene a todos $\beta \in K$ con $v(\beta) \geq v(\alpha)$. Por consiguiente, el conjunto $I = \{v(\alpha) \mid \alpha \in \mathfrak{O}'\}$ está acotado inferiormente en $\mathbb{Z}$ (o de lo contrario sería $\mathfrak{O}' = K$). Como $\mathfrak{O} \subset \mathfrak{O}'$ tenemos que $\mathbb{N} \subset I$, luego $-i = \min I \leq 0$. Es claro entonces que

$$\mathfrak{O}' = \{\alpha \in K \mid v(\alpha) \geq -i\} = \Pi^{-i}\mathfrak{O},$$

donde Π es cualquier primo en K.

Definición 7.28 Sea K/k una extensión finita separable de cuerpos métricos discretos completos. Con la notación anterior, definimos el *diferente* de la extensión como el ideal $\mathfrak{D}_{K/k} = \mathfrak{P}^i$, donde $\mathfrak{P}$ es el ideal primo de $\mathfrak{O}$. En lo sucesivo representaremos por $\mathfrak{D}_{K/k}^{-1}$ al módulo $\mathfrak{O}'$.

Demostraremos que la extensión K/k es no ramificada si y sólo si $\mathfrak{D}_{K/k} = 1$. Para ello necesitamos algunos resultados previos, que a su vez nos servirán para relacionar los diferentes locales de una extensión de cuerpos de funciones algebraicas. En primer lugar probamos la transitividad de los diferentes:

Teorema 7.29 *Sea $k \subset K \subset L$ una cadena de extensiones finitas separables de cuerpos métricos discretos completos. Entonces*

$$\mathfrak{D}_{L/k} = \mathfrak{D}_{L/K}\mathfrak{D}_{K/k}.$$

Demostración: En el enunciado hay que entender que —al igual que hacemos en los cuerpos de funciones algebraicas— cada ideal $\mathfrak{P}^i$ de $\mathfrak{O}_K$ se identifica con el ideal $\mathfrak{Q}^{ei}$ de $\mathfrak{O}_L$, donde $\mathfrak{P}$ es el primo de $\mathfrak{O}_K$, $\mathfrak{Q}$ es el primo de $\mathfrak{O}_L$ y $e = e(L/K)$. En otras palabras, si

$$\mathfrak{D}_{L/k} = \mathfrak{Q}^i, \quad \mathfrak{D}_{L/K} = \mathfrak{Q}^j, \quad \mathfrak{D}_{K/k} = \mathfrak{P}^r,$$

hemos de probar que $i = j + er$.

En efecto, dado $\alpha \in L$ arbitrario, tenemos que

$$\alpha \in \mathfrak{D}_{L/k}^{-1} \leftrightarrow \mathrm{Tr}_k^L[\alpha\mathfrak{O}_L] \subset \mathfrak{o} \leftrightarrow \mathrm{Tr}_k^K[\mathrm{Tr}_K^L[\alpha\mathfrak{O}_L]] \subset \mathfrak{o} \leftrightarrow \mathrm{Tr}_k^K[\mathrm{Tr}_K^L[\alpha\mathfrak{O}_L]\mathfrak{O}_K] \subset \mathfrak{o}.$$

Aquí hemos usado que Tr_K^L es K-lineal. Llegamos, pues, a que

$$\alpha \in \mathfrak{D}_{L/k}^{-1} \leftrightarrow \mathrm{Tr}_K^L[\alpha\mathfrak{O}_L] \subset \mathfrak{D}_{K/k}^{-1}.$$

Sea $\mathfrak{D}_{K/k}^{-1} = \delta^{-1}\mathfrak{O}_K$, con $\delta \in \mathfrak{O}_K$. Entonces

$$\alpha \in \mathfrak{D}_{L/k}^{-1} \leftrightarrow \mathrm{Tr}_K^L[\delta\alpha\mathfrak{O}_L] \subset \mathfrak{O}_K \leftrightarrow \delta\alpha \in \mathfrak{D}_{L/K}^{-1}.$$

Así pues,

$$v_L(\alpha) \geq -i \leftrightarrow v_L(\delta) + v_L(\alpha) \geq -j \leftrightarrow v_L(\alpha) \geq -j - er.$$

Como $v_L(\alpha)$ es un entero arbitrario, esto implica que $i = j + er$. ■

El teorema siguiente está probado en la demostración de 5.32:

Teorema 7.30 *Sea K/k una extensión finita de cuerpos métricos discretos completos, sea $\omega_1, \ldots, \omega_f$ una $\overline{k}$-base de $\overline{K}$ y π un primo de K. Entonces $\omega_i\pi^j$, para $i = 1, \ldots, f$, $j = 0, \ldots, e-1$ es una $\mathfrak{o}$-base de $\mathfrak{O}$.*

Para calcular el diferente de una extensión nos basaremos en el teorema siguiente:

Teorema 7.31 *Sea $K = k(\alpha)$ una extensión de cuerpos separable de grado n, sea $f \in k[x]$ el polinomio mínimo de α y sea*

$$\frac{f(x)}{x-\alpha} = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}.$$

Entonces la base dual de $1, \alpha, \ldots, \alpha^{n-1}$ es

$$\frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)}.$$

Demostración: Sean $\alpha_1, \ldots, \alpha_n$ las raíces de f. Si $0 \leq r \leq n-1$ se cumple que

$$\sum_{i=1}^n \frac{f(x)}{x-\alpha_i}\,\frac{\alpha_i^r}{f'(\alpha_i)} = x^r.$$

En efecto, la diferencia entre ambos miembros es un polinomio de grado menor o igual que $n-1$ y tiene por raíces a todos los α_i, luego es idénticamente nulo. Los sumandos del miembro izquierdo son todos los conjugados del polinomio

$$\frac{f(x)}{x-\alpha}\,\frac{\alpha^r}{f'(\alpha)},$$

luego la suma tiene por coeficientes a las trazas de los coeficientes de este último polinomio.

El coeficiente i-ésimo es $f'(\alpha)^{-1}b_i\alpha^r$, luego hemos obtenido que

$$\mathrm{Tr}\left(\frac{b_i}{f'(\alpha)}\,\alpha^r\right) = \begin{cases} 1 & \text{si } i = r, \\ 0 & \text{si } i \neq r. \end{cases}$$

■

Como consecuencia:

Teorema 7.32 *Sea K/k una extensión separable de grado n de cuerpos métricos discretos completos. Sea $\alpha \in \mathfrak{O}$ tal que $K = k(\alpha)$, sea $f(x)$ el polinomio mínimo de α y $L = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\mathfrak{o}}$. Entonces $L' = L/f'(\alpha)$. Además $f'(\alpha) \in \mathfrak{D}_{K/k}$ y si $\mathfrak{O} = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\mathfrak{o}}$ entonces $\mathfrak{D}_{K/k} = (f'(\alpha))$.*

Demostración: Por 7.27 y el teorema anterior (con la notación de éste último),

$$L' = \left\langle \frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)} \right\rangle_{\mathfrak{o}}.$$

Ahora bien, 5.35 implica que $f(x) \in \mathfrak{o}[x]$. Si

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n, \qquad a_i \in \mathfrak{o},$$

entonces la igualdad

$$f(x) = (x - \alpha)(b_0 + b_1 x + \cdots + b_{n-1} x^{n-1})$$

nos da las relaciones

$$a_i = b_{i-1} - \alpha b_i, \quad i = 1, \ldots, n-1, \qquad b_{n-1} = 1.$$

Por recurrencia resulta

$$\begin{array}{lcl} b_{n-1} & = & 1 \\ b_{n-2} & = & a_{n-1} + \alpha \\ b_{n-3} & = & a_{n-1} + a_{n-2}\alpha + a_{n-1}\alpha^2 \\ \cdots & & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ b_0 & = & a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n \end{array}$$

De aquí se sigue que

$$L' = \frac{1}{f'(\alpha)} \langle b_0, b_1, \ldots, b_{n-1} \rangle_{\mathfrak{o}} = \frac{1}{f'(\alpha)} \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_{\mathfrak{o}} = \frac{1}{f'(\alpha)} L.$$

Como $\alpha \in \mathfrak{O}$, tenemos que $L \subset \mathfrak{O}$, luego $\mathfrak{O}' \subset L' = L/f'(\alpha)$. Pongamos que $\mathfrak{D}_{K/k} = \mathfrak{P}^i$ y sea $\mathfrak{P} = (\pi)$. Entonces $\pi^{-i} \in \mathfrak{O}'$, luego $\pi^{-i} = \beta/f'(\alpha)$, para cierto $\beta \in L \subset \mathfrak{O}$. Por lo tanto $f'(\alpha) = \beta\pi^i \in \mathfrak{D}_{K/k}$.

La hipótesis de la última parte es que $L = \mathfrak{O}$, con lo que $\mathfrak{O}' = \mathfrak{O}/f'(\alpha)$. Así pues, $f'(\alpha)\pi^{-i}\mathfrak{O} = \mathfrak{O}$, de donde se sigue claramente que $(f'(\alpha)) = (\pi^i) = \mathfrak{D}_{K/k}$. ■

El teorema siguiente muestra la relación entre el diferente de una extensión separable y la ramificación de sus primos:

Teorema 7.33 *Sea K/k una extensión finita separable de cuerpos métricos discretos completos tal que el cuerpo de restos $\overline{k}$ sea perfecto, sea $e = e(K/k)$, sea $\mathfrak{D}$ el diferente de la extensión y $\mathfrak{P}$ el ideal primo de $\mathfrak{O}_K$. Entonces:*

a) Si $\mathfrak{P} \nmid e$*, entonces* $\mathfrak{D} = \mathfrak{P}^{e-1}$.

b) Si $\mathfrak{P} \mid e$*, entonces* $\mathfrak{P}^e \mid \mathfrak{D}$.

c) En particular $e > 1$ *si y sólo si* $\mathfrak{P} \mid \mathfrak{D}$.

DEMOSTRACIÓN: Veamos en primer lugar que si $e = 1$ entonces $\mathfrak{D} = 1$ (notemos que esto es un caso particular de a). Sea $\alpha \in \mathfrak{O}$ tal que $\overline{K} = \overline{k}(\alpha)$. Si $e = 1$, el teorema 7.30 nos da que $\mathfrak{O} = \langle 1, \alpha, \ldots \alpha^{n-1} \rangle_{\mathfrak{o}}$ y 7.32 nos da entonces que $\mathfrak{D} = (f'(\alpha))$, donde $f(x) \in \mathfrak{o}[x]$ es el polinomio mínimo de α. Puesto que $|K : k| = |\overline{K} : \overline{k}|$, la imagen de f en $\overline{k}[x]$ ha de ser el polinomio mínimo de $[\alpha]$, en particular es irreducible y, por la separabilidad, $f'(\alpha) \not\equiv 0 \pmod{\mathfrak{P}}$, es decir, $\mathfrak{P} \nmid \mathfrak{D}$, luego $\mathfrak{D} = 1$.

Supongamos ahora que $e > 1$. Por el teorema 5.33 podemos tomar un cuerpo intermedio $k \subset L \subset K$ de modo que $|K : L| = e(K/L) = e$ y, por consiguiente $e(L/k) = 1$. Por la parte ya probada sabemos que $\mathfrak{D}_{L/k} = 1$, luego $\mathfrak{D} = \mathfrak{D}_{K/L}$. Así pues, basta probar el resto del teorema para la extensión K/L o, equivalentemente, podemos suponer que $|K : k| = e$. Así, podemos aplicar el teorema 5.34, según el cual $K = k(\pi)$, donde π es un primo en K cuyo polinomio mínimo en k es un polinomio de Eisenstein

$$f(x) = x^e + a_{e-1}x^{e-1} + \cdots + a_1 x + a_0, \qquad \pi^e \mid a_i.$$

El teorema 7.30 nos da que $\mathfrak{O} = \langle 1, \pi, \ldots, \pi^{e-1} \rangle_{\mathfrak{o}}$, luego por 7.32 tenemos que $\mathfrak{D} = (f'(\pi))$. Ahora basta observar que

$$f'(\pi) = e\pi^{e-1} + (e-1)a_{e-1}\pi^{e-2} + \cdots + a_1.$$

Si $\mathfrak{P} \nmid e$, entonces todos los términos menos el primero son divisibles entre π^e, luego $v_{\mathfrak{P}}(f'(\pi)) = e-1$ y $\mathfrak{D} = \mathfrak{P}^{e-1}$. En cambio, si $\mathfrak{P} \mid e$, entonces todos los términos son divisibles entre π^e, luego $\mathfrak{P}^e \mid \mathfrak{D}$. Esto prueba a) y b), de donde c) es inmediato. ■

La condición $\mathfrak{p} \mid e$ puede darse exactamente por dos motivos: que exista un primo $p \mid e$ tal que $\mathfrak{P} \mid p$ (lo cual no sucede con los cuerpos que nosotros estamos manejando, ya que las constantes son unidades) o bien porque K tenga característica prima p y $p \mid e$ (en cuyo caso $e = 0$ como elemento de K).

Con esta caracterización de la ramificación, ya podemos demostrar el resultado que perseguíamos:

Teorema 7.34 *El número de primos ramificados de una extensión separable de cuerpos de funciones algebraicas es finito.*

DEMOSTRACIÓN: Sea K/k una extensión separable de cuerpos de funciones algebraicas. Por el teorema 1.32 existe $x \in k$ tal que la extensión $k/k_0(x)$ es finita separable. Basta probar que el número de primos de $k_0(x)$ ramificados en K es finito. Equivalentemente, podemos suponer que $k = k_0(x)$.

Sea $K = k(\alpha)$. Por 1.18 podemos suponer que α es entero sobre $k_0[x]$. Si $\mathfrak{P}$ es un primo de K que divide a un primo finito $\mathfrak{p}$ de k, en particular tenemos que α es entero sobre $\mathfrak{o}_\mathfrak{p}$, luego $\alpha \in \mathfrak{O}_\mathfrak{P}$ por 5.35.

Se cumple que $K_\mathfrak{P} = k_\mathfrak{p}(\alpha)$, luego podemos aplicar el teorema 7.32 para concluir que $g'(\alpha) \in \mathfrak{D}_{K_\mathfrak{P}/k_\mathfrak{p}}$, donde $g(x)$ es el polinomio mínimo de α en $k_\mathfrak{p}[x]$. Puesto que $g(x) \mid f(x)$, es claro que $g'(\alpha) \mid f'(\alpha)$. Así pues, $f'(\alpha) \in \mathfrak{D}_{K_\mathfrak{P}/k_\mathfrak{p}}$. Si $\mathfrak{D}_{K_\mathfrak{P}/k_\mathfrak{p}} \neq 1$, esto implica que $v_\mathfrak{P}(f'(\alpha)) > 0$.

Teniendo en cuenta que $f'(\alpha) \in K^*$, concluimos que $\mathfrak{D}_{K_\mathfrak{P}/k_\mathfrak{p}} \neq 1$ a lo sumo para un número finito de primos (los divisores del primo infinito de k y los que cumplan $v_\mathfrak{P}(f'(\alpha)) > 0$). Por el teorema anterior, el número de primos ramificados es finito. ■

Definición 7.35 Sea K/k una extensión separable de cuerpos de funciones algebraicas. Para cada primo $\mathfrak{P}$ de K definimos el *diferente local* en $\mathfrak{P}$ como $\mathfrak{D}_\mathfrak{P} = \mathfrak{D}_{K_\mathfrak{P}/k_\mathfrak{p}}$, donde $\mathfrak{p}$ es el primo de k divisible entre K. Podemos identificar a $\mathfrak{D}_\mathfrak{P}$ con un divisor de K (potencia de $\mathfrak{P}$). Por el teorema anterior se cumple que $\mathfrak{D}_\mathfrak{P} = 1$ salvo a lo sumo para una cantidad finita de primos, luego podemos definir el *diferente* de la extensión como el divisor

$$\mathfrak{D}_{K/k} = \prod_{\mathfrak{P}} \mathfrak{D}_\mathfrak{P} \in \mathcal{D}_K.$$

Se trata de un divisor entero cuyos factores primos son los primos de K ramificados sobre k. El teorema 7.29 implica inmediatamente que si $k \subset K \subset L$ es una cadena de extensiones separables de cuerpos de funciones algebraicas entonces

$$\mathfrak{D}_{L/k} = \mathfrak{D}_{L/K}\mathfrak{D}_{K/k}.$$

El teorema 7.33 nos permite calcular el discriminante de una extensión de cuerpos de funciones algebraicas bajo una restricción mínima:

Teorema 7.36 *Sea K/k una extensión de cuerpos de funciones algebraicas tal que* $\operatorname{car} k = 0$ *o bien* $\operatorname{car} k = p$ *es un primo que no divide al índice de ramificación de ningún divisor primo de K. Entonces*

$$\mathfrak{D}_{K/k} = \prod_{\mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P})-1}.$$

DEMOSTRACIÓN: Sea $\mathfrak{P}$ un divisor primo de K y $\mathfrak{p}$ el primo de k al cual divide. Según la definición de diferente, basta probar que $\mathfrak{D}_\mathfrak{P} = \mathfrak{P}^{e(\mathfrak{P})-1}$, donde $\mathfrak{D}_\mathfrak{P}$ es el diferente de la extensión local $K_\mathfrak{P}/k_\mathfrak{p}$. Según el teorema 7.33 esto sucede si $\mathfrak{P} \nmid e(\mathfrak{P})$. Ahora bien, $e(\mathfrak{P})$ (visto como elemento de $K_\mathfrak{P}$) es una constante, luego sólo podría ser múltiplo de $\mathfrak{P}$ si fuera nula, pero esta posibilidad la excluye la hipótesis del teorema. ■

7.4 Extensiones de constantes

Terminamos el capítulo estudiando una clase particularmente simple de extensiones de cuerpos de funciones algebraicas. Su interés radica en que en muchas ocasiones sus propiedades nos permiten reducir problemas al caso en que el cuerpo de constantes es algebraicamente cerrado.

Definición 7.37 Si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0, una *extensión (finita) de constantes* de K es un cuerpo L obtenido adjuntando a K un conjunto (finito) de elementos algebraicos sobre k_0.

Puesto que estamos suponiendo que k_0 es perfecto, las extensiones de constantes son separables. Comencemos estudiando las extensiones finitas. Sea, pues, $L = K(A)$, donde A es un conjunto finito de elementos algebraicos sobre k_0. Entonces $k_1 = k_0(A) = k_0(\alpha)$, para un cierto α (algebraico sobre k_0), y es claro que $L = K(\alpha)$. Tenemos que L es también un cuerpo de funciones algebraicas sobre k_0. Si éste es el cuerpo de constantes exacto de K, entonces el polinomio mínimo de α sobre K tiene sus coeficientes en k_0, pues éstos dependen polinómicamente de sus raíces, luego son algebraicos sobre k_0. Por consiguiente $|L : K| = |k_1 : k_0|$.

Más concretamente, las potencias de α son a la vez una k_0-base de k_1 y una K-base de L. De aquí se sigue fácilmente que cualquier k_0-base de k_1 es una K-base de L.

Se cumple que k_1 es el cuerpo de constantes exacto de L, pues si éste fuera un cuerpo mayor $k_2 = k_0(\beta)$, el mismo razonamiento nos daría que

$$|L : K| \geq |K(\beta) : K| = |k_2 : k_0| > |k_1 : k_0| = |L : K|,$$

lo cual es absurdo. Con esto es inmediato el teorema siguiente:

Teorema 7.38 *Sea K un cuerpo de funciones algebraicas sobre el cuerpo de constantes exacto k_0. Si fijamos una clausura algebraica de K y, en ella, la clausura algebraica de k_0, la correspondencia $k_1 \mapsto Kk_1$ es una biyección entre las extensiones finitas de k_0 y las extensiones finitas de constantes de K. Esta correspondencia conserva los grados de las extensiones y su inversa asigna a cada extensión finita de constantes L de K su cuerpo de constantes exacto.*

Si K es un cuerpo de funciones algebraicas y L es una extensión finita de constantes, cuando consideramos un divisor de K como divisor de L, su grado se multiplica por $|L : K|$, pero si pasamos a considerar el grado respecto al cuerpo de constantes exacto de L, éste de divide de nuevo entre $|L : K|$, luego vuelve a ser el grado inicial. Llamaremos *grado absoluto* de un divisor en un cuerpo de funciones a su grado respecto al cuerpo de constantes exacto. De este modo, acabamos de ver que el grado absoluto de un divisor se conserva al extender las constantes. El teorema siguiente describe las descomposiciones de los primos en las extensiones de constantes.

Teorema 7.39 *Sea K un cuerpo de funciones algebraicas y L una extensión finita de constantes de K. Sean k_0 y k_1 los respectivos cuerpos exactos de constantes. Entonces:*

a) El grado absoluto de los divisores de K se conserva al considerarlos como divisores de L.

b) Si $\mathfrak{P}$ es un primo de L y $\mathfrak{p}$ es el primo de K divisible entre $\mathfrak{P}$, entonces $\overline{L}_{\mathfrak{P}} = \overline{K}_{\mathfrak{p}} k_1$.

c) Ningún primo de K se ramifica en L.

d) Los primos de grado 1 de K se conservan primos en L.

e) Si $\mathfrak{p}$ es un primo de K de grado r, existe una extensión de constantes L de K donde $\mathfrak{p}$ se descompone en r primos de grado 1.

DEMOSTRACIÓN: Ya hemos probado que el grado absoluto se conserva. Tomemos ahora un primo $\mathfrak{P}$ de L y sea $\mathfrak{p}$ el primo de K divisible entre $\mathfrak{P}$. Si $k_1 = k_0(\alpha)$, entonces $L = K(\alpha)$ y $L_{\mathfrak{P}} = K_{\mathfrak{p}}(\alpha)$. Sea $k_{0\mathfrak{p}}$ la clausura algebraica de k_0 en $K_{\mathfrak{p}}$. Según 6.42, tenemos que $k_{0\mathfrak{p}}$ es isomorfo a $\overline{K}_{\mathfrak{p}}$. El polinomio mínimo de α sobre $K_{\mathfrak{p}}$ tiene sus coeficientes en $k_{0\mathfrak{p}}$, luego

$$n_{\mathfrak{P}} = |L_{\mathfrak{P}} : K_{\mathfrak{p}}| \geq |\overline{L}_{\mathfrak{P}} : \overline{K}_{\mathfrak{p}}| \geq |k_{0\mathfrak{p}}(\alpha) : k_{0\mathfrak{p}}| = n_{\mathfrak{P}}.$$

Así pues, $n_{\mathfrak{P}} = f(\mathfrak{P}/\mathfrak{p})$ y el índice de ramificación ha de ser trivial. Esto prueba c). Además $\overline{L}_{\mathfrak{P}} = K_{\mathfrak{p}}(\alpha) = K_{\mathfrak{p}} k_1$, lo que prueba b).

Si $\operatorname{grad} \mathfrak{p} = 1$, entonces $k_{0\mathfrak{p}} = k_0$, con lo que

$$f(\mathfrak{P}/\mathfrak{p}) = n_{\mathfrak{P}} = |k_0(\alpha) : k_0| = |k_1 : k_0| = |L : K|,$$

de donde se sigue que $\mathfrak{p}$ se conserva primo en L.

Por otra parte, si $\mathfrak{p}$ es un primo de K de grado r, tendremos que $k_{0\mathfrak{p}} = k_0(\beta)$, para cierto β. Adjuntándole a k_0 las raíces del polinomio mínimo de β sobre k_0 obtenemos una extensión k_1 de k_0 que a su vez determina una extensión de constantes L de K. Si $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en L entonces, por b) tenemos que $\overline{L}_{\mathfrak{P}}$ es la adjunción a $\overline{K}_{\mathfrak{p}} = k_0(\beta)$ de las raíces del polinomio mínimo de β, o también la adjunción a k_0 de estas raíces, luego $\overline{L}_{\mathfrak{P}} = k_1$, de donde se sigue que los divisores de $\mathfrak{p}$ en L tienen grado (absoluto) 1. Como $\mathfrak{p}$ tiene grado r respecto de k_1, tenemos que $\mathfrak{p}$ se descompone en L en r factores de grado 1. ■

Terminamos la sección mostrando que todos estos hechos se generalizan fácilmente a extensiones infinitas de constantes.

En primer lugar, si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 y k_1 es una extensión algebraica de k_0, la extensión de constantes $L = Kk_1$ es un cuerpo de funciones algebraicas sobre k_1. En efecto, si $K = k_0(\alpha_1, \ldots, \alpha_n)$, entonces $L = k_1(\alpha_1, \ldots, \alpha_n)$, luego L es finitamente generado sobre k_1 y, como las extensiones algebraicas no alteran el grado de trascendencia, tenemos que L sigue teniendo grado de trascendencia 1 sobre k_0 y también sobre k_1.

Es importante tener presente que si la extensión k_1/k_0 es infinita entonces L no es un cuerpo de funciones algebraicas sobre k_0. No obstante, es claro que L es la unión de todas las extensiones finitas de constantes de K contenidas en L, y esto es la clave para generalizar a extensiones infinitas de constantes todos los resultados que conocemos para extensiones finitas. Por ejemplo, si k_0 es el cuerpo de constantes exacto de K, entonces k_1 es el cuerpo de constantes exacto de L. Para probarlo basta tener en cuenta que si $\alpha \in L$ es algebraico sobre k_1, entonces también lo es sobre k_0 y está en una extensión finita de constantes Kk_2, donde $k_0 \subset k_2 \subset k_1$, luego $\alpha \in k_2$ por la propiedad correspondiente para extensiones finitas.

Consideremos el caso particular en que k_1 es la clausura algebraica de k_0. Cada primo $\mathfrak{p}$ de K se descompone en primos de grado 1 en una extensión finita de constantes, los cuales se conservan primos en todas las extensiones mayores. Esto significa que la valoración $v_{\mathfrak{p}}$ tiene un número finito de extensiones al cuerpo $L = Kk_1$ (las cuales se anulan en k_1). Por consiguiente lo mismo es válido para cualquier extensión de constantes de K (que es un subcuerpo de L).

En resumen, si L es cualquier extensión de constantes de K y $\mathfrak{p}$ es un primo en K, existe un número finito de primos $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ de L cuyas valoraciones extienden a la de $\mathfrak{p}$. Esto nos permite identificar a $\mathfrak{p}$ con el divisor de L dado por $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$. A su vez, esta identificación induce un monomorfismo del grupo de los divisores de K en el de los divisores de L (si la extensión es finita se trata de la identificación usual).

Es fácil ver que esta identificación es consistente con la identificación de los divisores de K con los de las extensiones intermedias. Así mismo es claro que las correspondencias $\alpha \mapsto (\alpha)$ conmutan con la inclusión $K \longrightarrow L$ y con la identificación de divisores. El grado absoluto se conserva por extensiones de constantes arbitrarias.

Veamos por ejemplo la prueba de esto último. Tomemos una extensión de constantes L/K y veamos en primer lugar que si $\mathfrak{p}$ es un primo de K de grado absoluto 1 entonces $\mathfrak{p}$ tiene también grado absoluto 1 en L. Sabemos que $\mathfrak{p}$ se conserva primo en todas las extensiones finitas de constantes de K y que en todas tiene grado absoluto 1, es decir, todo elemento de una extensión finita de constantes de K es congruente módulo $\mathfrak{p}$ con una constante. Por consiguiente todo elemento de L cumple esto mismo, luego $\mathfrak{p}$ tiene grado absoluto 1 en L.

En segundo lugar observamos que si $\overline{K}$ es la adjunción a K de una clausura algebraica de k_0, de modo que $K \subset L \subset \overline{K}$, entonces el grado absoluto de un primo $\mathfrak{p}$ en K se conserva en $\overline{K}$. En efecto, sabemos que $\mathfrak{p}$ se descompone en r primos de grado absoluto 1 en una extensión finita intermedia de $\overline{K}/K$, todos los cuales siguen teniendo grado absoluto 1 en $\overline{K}$ por la parte ya probada, luego $\mathfrak{p}$ tiene grado absoluto r en $\overline{K}$. Aplicando esto mismo a los divisores de $\mathfrak{p}$ en L concluimos que la suma de sus grados absolutos (es decir, el grado absoluto de $\mathfrak{p}$ en L) es igual a la suma de los grados absolutos de sus divisores primos en $\overline{K}$, que son los divisores de $\mathfrak{p}$ en $\overline{K}$, luego dicha suma es r.

Capítulo VIII

El teorema de Riemann-Roch

En este capítulo probaremos un resultado profundo sobre cuerpos de funciones algebraicas. Son tantas sus consecuencias que dedicaremos todo el capítulo siguiente a mostrar las más inmediatas. En este capítulo veremos la más importante: la posibilidad de definir una noción algebraica de género de un cuerpo de funciones que en el caso complejo coincide con el que ya teníamos definido. El género algebraico es un invariante que determina fuertemente las características de un cuerpo. Como preparación al teorema de Riemann-Roch conviene estudiar primero el concepto de forma diferencial, a lo cual dedicamos las dos primeras secciones.

8.1 Diferenciales de series de potencias

Vamos a trabajar con cuerpos de series formales de potencias. Como en el caso de los cuerpos de funciones algebraicas, supondremos siempre que el cuerpo de constantes k_0 es perfecto.

Derivadas Partiremos del concepto de derivada formal de una serie de potencias, a partir del cual introduciremos después el de forma diferencial. La definición es la generalización obvia de la derivada formal de un polinomio.

Definición 8.1 Sea $k = k_0((x))$ el cuerpo de series formales de potencias con coeficientes en k_0. Si π es cualquier primo del anillo $k_0[[x]]$, entonces, el teorema 5.17 muestra que todo elemento de k se expresa de forma única como

$$\alpha = \sum_{-\infty \ll n} a_n \pi^n, \qquad \text{con } a_n \in k_0.$$

Definimos

$$\frac{d\alpha}{d\pi} = \sum_{-\infty \ll n} n a_n \pi^{n-1}.$$

Esta definición extiende a la definición de derivada parcial en un anillo se series formales de potencias de varias variables que dimos en en capítulo I. El teorema siguiente recoge las propiedades básicas de esta derivada formal:

Teorema 8.2 *Sea $k = k_0((x))$ un cuerpo de series formales de potencias y π un primo en k. Entonces:*

a) Para todo α, $\beta \in k$ y todo a, $b \in k_0$, se cumple:

$$\frac{d(a\alpha + b\beta)}{d\pi} = a\,\frac{d\alpha}{d\pi} + b\,\frac{d\beta}{d\pi}.$$

b) Si α, $\beta \in k$, se cumple

$$\frac{d(\alpha\beta)}{d\pi} = \frac{d\alpha}{d\pi}\,\beta + \alpha\,\frac{d\beta}{d\pi}.$$

En particular

$$\frac{d\alpha^n}{d\pi} = n\alpha^{n-1}\frac{d\alpha}{d\pi}, \qquad \textit{para todo } n \in \mathbb{Z}.$$

c) La función

$$\frac{d}{d\pi} : k \longrightarrow k$$

es continua.

d) Si π_1 es otro primo de k y $\alpha \in k$, entonces

$$\frac{d\alpha}{d\pi_1} = \frac{d\alpha}{d\pi}\,\frac{d\pi}{d\pi_1}.$$

e) Si $f(u, v) \in k_0[u, v]$ y α, $\beta \in k$, entonces

$$\frac{df(\alpha, \beta)}{d\pi} = \frac{\partial f}{\partial u}(\alpha, \beta)\frac{d\alpha}{d\pi} + \frac{\partial f}{\partial v}(\alpha, \beta)\frac{d\beta}{d\pi},$$

donde las derivadas parciales de f se entienden en el sentido usual para polinomios.

Demostración: La propiedad a) es inmediata. Para probar b) tomamos

$$\alpha = \sum_{-\infty \ll n} a_n\pi^n, \qquad \beta = \sum_{-\infty \ll n} b_n\pi^n.$$

Entonces

$$\begin{aligned} \frac{d\alpha}{d\pi}\,\beta + \alpha\,\frac{d\beta}{d\pi} \quad = \quad & \sum_{-\infty \ll n} (n+1)a_{n+1}\pi^n \sum_{-\infty \ll n} b_n\pi^n \\ & + \sum_{-\infty \ll n} a_n\pi^n \sum_{-\infty \ll n} (n+1)b_{n+1}\pi^n \end{aligned}$$

$$\begin{aligned}
&= \sum_{-\infty\ll n}\Big(\sum_{r+s=n}(r+1)a_{r+1}b_s + \sum_{r+s=n}(s+1)a_r b_{s+1}\Big)\pi^n \\
&= \sum_{-\infty\ll n}\Big(\sum_{r+s=n}(r+1)a_{r+1}b_s + \sum_{r+s=n} s a_{r+1}b_s\Big)\pi^n \\
&= \sum_{-\infty\ll n}(n+1)\Big(\sum_{r+s=n}a_{r+1}b_s\Big)\pi^n \\
&= \sum_{-\infty\ll n}(n+1)\Big(\sum_{r+s=n+1}a_r b_s\Big)\pi^n \\
&= \frac{d}{d\pi}\Big(\sum_{-\infty\ll n}\Big(\sum_{r+s=n}a_r b_s\Big)\pi^n\Big) = \frac{d(\alpha\beta)}{d\pi}.
\end{aligned}$$

La fórmula para la derivada de α^n para $n \geq 0$ se prueba fácilmente por inducción. Para exponentes negativos derivamos $\alpha^{-n}\alpha^n = 1$ y despejamos la derivada de α^n.

c) La continuidad de la derivación es inmediata. De hecho

$$v\left(\frac{d\alpha}{d\pi}\right) \geq v(\alpha) - 1.$$

Para probar d) llamamos $\alpha_m = \sum\limits_{n\leq m} a_n\pi^n$. Entonces

$$\frac{d\alpha_m}{d\pi_1} = \sum_{n\leq m} a_n\frac{d\pi^n}{d\pi_1} = \sum_{n\leq m} na_n\pi^{n-1}\frac{d\pi}{d\pi_1} = \frac{d\alpha_m}{d\pi}\frac{d\pi}{d\pi_1}.$$

Tomando límites obtenemos la fórmula buscada.

e) Es fácil ver que si la fórmula se cumple para $f(u,v) = u^i v^j$ entonces se cumple para todo polinomio. Ahora bien, este caso se comprueba fácilmente a partir de b) ■

Estamos interesados en obtener propiedades relacionadas con las derivadas que no dependan del primo respecto al cual derivamos. Como primera observación a este respecto notemos que, si π y π_1 son primos de k, entonces

$$\pi = \sum_{n=1}^{\infty} a_n\pi_1^n, \qquad \text{con } a_1 \neq 0,$$

luego

$$\frac{d\pi}{d\pi_1} = a_1 + a_2\pi_1 + a_3\pi_1^2 + \cdots$$

es una unidad de $k_0[[x]]$. El apartado d) del teorema anterior prueba en particular que la propiedad $\dfrac{d\alpha}{d\pi} = 0$ es independiente del primo π. Más concretamente, es fácil probar:

Teorema 8.3 *Sea $k = k_0((x))$ un cuerpo de series formales de potencias, sea $\alpha \in k$ y π un primo en $k_0[[x]]$. Se cumple* *a) Si* $\operatorname{car} k = 0$ *entonces* $\dfrac{d\alpha}{d\pi} = 0$ *si y sólo si* $\alpha \in k_0$.

b) Si $\operatorname{car} k = p > 0$ *entonces* $\dfrac{d\alpha}{d\pi} = 0$ *si y sólo si* $\alpha = \sum_{-\infty \ll n} a_n \pi^{pn}$, *es decir, si y sólo si* $\alpha \in k^p$.

Definición 8.4 Sea $k = k_0((x))$ un cuerpo de series formales de potencias y sean α, $\beta \in k$ tales que $\dfrac{d\alpha}{d\pi} \neq 0$ (para cualquier primo π). Definimos

$$\frac{d\beta}{d\alpha} = \frac{\dfrac{d\beta}{d\pi}}{\dfrac{d\alpha}{d\pi}},$$

para cualquier primo π. Del teorema 8.2 se sigue que la definición no depende de la elección de π, así como que si α es primo esta definición coincide con la que ya teníamos.

También es inmediato comprobar que, cuando las derivadas que intervienen están definidas, se cumplen las igualdades siguientes:

$$\frac{d\gamma}{d\alpha} = \frac{d\gamma}{d\beta}\,\frac{d\beta}{d\alpha}, \qquad \frac{d\beta}{d\alpha} = \left(\frac{d\alpha}{d\beta}\right)^{-1}.$$

Más en general, las propiedades del teorema 8.2 son válidas aunque π no sea primo.

Diferenciales Supongamos, como hasta ahora, que k es un cuerpo de series de potencias. En el conjunto de todos los pares $(\beta, \alpha) \in k \times k$ tales que $\dfrac{d\alpha}{d\pi} \neq 0$ definimos la relación de equivalencia

$$(\beta_1, \alpha_1)\, R\, (\beta_2, \alpha_2) \quad \text{si y sólo si} \quad \beta_1 = \beta_2 \, \frac{d\alpha_2}{d\alpha_1}.$$

A las clases de equivalencia respecto a esta relación las llamaremos *formas diferenciales* en k. La forma diferencial determinada por el par (β, α) se representa por $\beta\, d\alpha$. De este modo, se cumple que

$$\beta_1\, d\alpha_1 = \beta_2\, d\alpha_2 \quad \text{si y sólo si} \quad \beta_1 = \beta_2 \, \frac{d\alpha_2}{d\alpha_1}.$$

Es inmediato que la forma diferencial $0\, d\alpha$ está formada por todos los pares $(0, \alpha)$ tales que $\dfrac{d\alpha}{d\pi} \neq 0$. A esta forma la llamaremos *forma nula* y la representaremos simplemente por 0.

Definimos la suma de dos formas diferenciales como

$$\beta_1\, d\alpha_1 + \beta_2\, d\alpha_2 = \Big(\beta_1 \frac{d\alpha_1}{d\alpha} + \beta_2 \, \frac{d\alpha_2}{d\alpha}\Big) d\alpha, \tag{8.1}$$

donde α es cualquier elemento de k con derivadas no nulas.

Es claro que esta definición no depende de la elección de α ni de los representantes de las formas diferenciales. Con esta operación, el conjunto de las formas diferenciales es claramente un grupo abeliano (el elemento neutro es la forma nula).

También podemos definir el producto escalar

$$\gamma(\beta\, d\alpha) = (\gamma\beta)\, d\alpha, \tag{8.2}$$

con el cual el conjunto de las formas diferenciales de k resulta ser un k-espacio vectorial.

Si representamos por $d\alpha$ la forma $1\, d\alpha$, entonces una forma cualquiera $\beta\, d\alpha$ es el producto escalar de β por $d\alpha$ en el sentido que acabamos de definir.

En lo sucesivo adoptaremos el convenio de que $d\alpha = 0$ cuando (y sólo cuando) $\dfrac{d\alpha}{d\pi} = 0$. Según el teorema 8.3, esto sucede cuando α es constante si $\operatorname{car} k = 0$ o cuando $\alpha \in k^p$ si $\operatorname{car} k = p$. Ahora la expresión $\beta\, d\alpha$ está definida para todo par de elementos de k, y es fácil ver que las fórmulas (8.1) y (8.2) siguen siendo válidas bajo este convenio.

Con esta notación, la derivada $\dfrac{d\beta}{d\alpha}$ está definida para todo par de elementos α y $\beta \in K$ tales que $d\alpha \neq 0$ y entonces

$$d\beta = \frac{d\beta}{d\alpha}\, d\alpha.$$

Esta fórmula muestra que cualquier forma no nula es una base del espacio de todas las formas, luego este espacio tiene dimensión 1.

Toda forma diferencial puede expresarse en la forma $\omega = \beta\, d\pi$, donde π es un primo de k. Como la derivada de un primo respecto de otro es una unidad, es claro que podemos definir el *orden* de ω como $v(\omega) = v(\beta)$ sin que éste dependa del primo elegido. Más en general, es claro que

$$v(\beta\, d\alpha) = v\Big(\beta\, \frac{d\alpha}{d\pi}\Big),$$

para cualquier primo π. Por consiguiente podemos hablar de si una diferencial tiene un cero o un polo de un orden dado.

El operador de Cartier Introducimos ahora un concepto de utilidad para tratar con diferenciales en cuerpos de característica prima. Sea, pues, k un cuerpo de series de potencias sobre un cuerpo de constantes (perfecto) k_0 de característica p. Es inmediato comprobar que $|k : k^p| = p$. De hecho, si π es un primo en k, entonces $k^p = k_0((\pi^p))$, $k = k_0(\pi)$ y las potencias $1, \pi, \ldots, \pi^{p-1}$ forman una k^p-base de k. Notemos que π^p es un primo de k^p.

Estos hechos implican que toda forma diferencial ω de k se expresa de forma única como

$$\omega = u\, \frac{d\pi}{\pi} = (u_0 + u_1\pi + \cdots + u_{p-1}\pi^{p-1})\, \frac{d\pi}{\pi}, \qquad u_i \in k^p. \tag{8.3}$$

Definimos

$$C_\pi(\omega) = u_0 \, \frac{d\pi^p}{\pi^p},$$

donde el miembro derecho ha de entenderse como una forma diferencial en el cuerpo $k^p = k((\pi^p))$. Es claro que C_π es una aplicación k^p-lineal del espacio de las formas diferenciales de k en el espacio de las formas diferenciales de k^p. Vamos a probar que no depende de π.

Sea $E = \{d\alpha \mid \alpha \in k\}$ el espacio de las *diferenciales exactas* de k. Se cumple que $C_\pi(d\alpha) = 0$, pues si

$$\alpha = a_0 + a_1\pi + \cdots + a_{p-1}\pi^{p-1}, \qquad a_i \in k^p,$$

entonces

$$d\alpha = (a_1\pi + \cdots + (p-1)a_{p-1}\pi^{p-1}) \, \frac{d\pi}{\pi},$$

luego, en efecto, $C_\pi(d\alpha) = 0$.

Recíprocamente, si $C_\pi(\omega) = 0$ entonces ω es una forma exacta. Para probarlo la expresamos en la forma (8.3) y observamos que si $i > 0$

$$d\Big(\frac{u_i}{i}\,\pi^i\Big) = u_i\pi^i \, \frac{d\pi}{\pi},$$

es decir, todos los términos de (8.3) son exactos salvo a lo sumo el correspondiente a $i = 0$. Basta probar que $u_0 = 0$, pero es que

$$C_\pi(\omega) = u_0 \, \frac{d\pi^p}{\pi^p} = 0,$$

mientras que $d\pi^p$ no es nula como forma diferencial de k^p porque π^p es un primo de k^p. Por consiguiente ha de ser $u_0 = 0$.

Con esto tenemos probado que el núcleo de C_π es exactamente E. Para demostrar que C_π no depende de π basta ver que si $\alpha \in k$ es no nulo, entonces

$$C_\pi\Big(\frac{d\alpha}{\alpha}\Big) = \frac{d\alpha^p}{\alpha^p}.$$

Para ello expresamos

$$\frac{d\alpha}{\alpha} = \frac{\pi}{\alpha}\,\frac{d\alpha}{d\pi}\,\frac{d\pi}{\pi}, \qquad \frac{\pi}{\alpha}\,\frac{d\alpha}{d\pi} = g_0 + g_1\pi + \cdots + g_{p-1}\pi^{p-1}, \quad g_i \in k^p.$$

Por otra parte sea $\alpha = a_0 + a_1\pi + \cdots + a_n\pi^n$, con $a_i \in k^p$, $a_n \neq 0$, $n < p$. Así tenemos $\alpha = q(\pi)$, donde q es un polinomio separable sobre k^p, porque su grado es menor que p. Sea k' la adjunción a k de las raíces de q y sea k_1' la adjunción a k^p de estas mismas raíces.

Claramente $k' = kk_1' = k^p(\pi)k_1' = k_1'(\pi)$. Los elementos de k_1' son separables sobre k^p, mientras que π no lo es, luego $\pi \notin k_1'$. Sin embargo $\pi^p \in k^p \subset k_1'$, luego $|k' : k_1'| = p$.

De este modo, cada $x \in k'$ se expresa de forma única como

$$x = c_0 + c_1\pi + \cdots + c_{p-1}\pi^{p-1}, \qquad c_i \in k'_1.$$

Definimos

$$\frac{dx}{d\pi} = c_1 + \cdots + (p-1)c_{p-1}\pi^{p-2}.$$

Es claro que esta derivación extiende a la derivada respecto de π en k. También es fácil probar que satisface las reglas de derivación de la suma y el producto. En k' podemos descomponer

$$\alpha = a_n \prod_{i=1}^n (\pi - \beta_i),$$

y ahora podemos calcular

$$\frac{d\alpha}{d\pi} = a_n \sum_{i=1}^n \prod_{j\neq i} (\pi - \beta_j).$$

Claramente,

$$\frac{\pi}{\alpha}\frac{d\alpha}{d\pi} = \sum_{i=1}^n \frac{\pi}{\pi - \beta_i} = \sum_{i=1}^n \Big(1 + \frac{1}{\frac{\pi}{\beta_i} - 1}\Big)$$

$$= \sum_{i=1}^n \left(1 + \frac{1}{\left(\frac{\pi}{\beta_i}\right)^p - 1}\left(1 + \frac{\pi}{\beta_i} + \cdots + \left(\frac{\pi}{\beta_i}\right)^{p-1}\right)\right).$$

Esta fórmula muestra que

$$g_0 = \sum_{i=1}^n \left(1 + \frac{1}{\left(\frac{\pi}{\beta_i}\right)^p - 1}\right) = \left(\sum_{i=1}^n \left(1 + \frac{1}{\frac{\pi}{\beta_i} - 1}\right)\right)^p = \Big(\frac{\pi}{\alpha}\frac{d\alpha}{d\pi}\Big)^p.$$

Por consiguiente:

$$C_\pi\Big(\frac{d\alpha}{\alpha}\Big) = \frac{\pi^p}{\alpha^p}\Big(\frac{d\alpha}{d\pi}\Big)^p\frac{d\pi^p}{\pi^p} = \frac{\pi^p}{\alpha^p}\frac{d\alpha^p}{d\pi^p}\frac{d\pi^p}{\pi^p} = \frac{d\alpha^p}{\alpha^p}.$$

■

Definición 8.5 Sea k un cuerpo de series de potencias de característica prima p. El *operador de Cartier* de k es el operador del espacio de las formas diferenciales de k en el espacio de las formas diferenciales de k^p dado por

$$C\Big((u_0 + u_1\pi + \cdots + u_{p-1}\pi^{p-1})\frac{d\pi}{\pi}\Big) = u_0\frac{d\pi^p}{\pi^p},$$

donde $u_i \in k^p$ y π es cualquier primo de k.

Tenemos que el operador de Cartier es k^p-lineal, su núcleo lo constituyen las formas diferenciales exactas de k y para todo $\alpha \in k$ no nulo se cumple

$$C\Big(\frac{d\alpha}{\alpha}\Big) = \frac{d\alpha^p}{\alpha^p}.$$

Estas propiedades lo determinan completamente.

Residuos Terminamos la sección introduciendo un invariante muy importante de las formas diferenciales en un cuerpo de series de potencias.

Definición 8.6 Sea k un cuerpo de series de potencias sobre un cuerpo de constantes k_0. Definimos el *residuo* respecto a un primo π de un elemento

$$\alpha = \sum_{-\infty \ll n} c_n \pi^n \in k$$

como

$$\operatorname{Res}_\pi \alpha = c_{-1}.$$

Es claro que $\operatorname{Res} : k \longrightarrow k_0$ es una aplicación k_0-lineal y además es continua si en k_0 consideramos la topología discreta. Así mismo,

$$\operatorname{Res}_\pi \Big(\frac{d\alpha}{d\pi}\Big) = 0$$

y

$$\operatorname{Res}_\pi(c\pi^n) = \begin{cases} c & \text{si } n = -1, \\ 0 & \text{si } n \neq -1, \end{cases} \qquad c \in k_0.$$

Definimos el *residuo* de una forma diferencial como

$$\operatorname{Res}_\pi(\beta\, d\alpha) = \operatorname{Res}_\pi \Big(\beta\, \frac{d\alpha}{d\pi}\Big).$$

Teorema 8.7 *Sea k un cuerpo de series de potencias y π, π_1 dos primos de k. Entonces, para toda forma diferencial ω de k se cumple*

$$\operatorname{Res}_\pi \omega = \operatorname{Res}_{\pi_1}(\omega).$$

Demostración: Basta probar que para todo $\beta \in k$ se cumple

$$\operatorname{Res}_\pi \beta = \operatorname{Res}_{\pi_1} \Big(\beta\, \frac{d\pi}{d\pi_1}\Big), \tag{8.4}$$

pues entonces

$$\begin{aligned} \operatorname{Res}_{\pi_1}(\beta\, d\alpha) &= \operatorname{Res}_{\pi_1}\Big(\beta\, \frac{d\alpha}{d\pi_1}\Big) = \operatorname{Res}_{\pi_1}\Big(\beta\, \frac{d\alpha}{d\pi}\, \frac{d\pi}{d\pi_1}\Big) \\ &= \operatorname{Res}_\pi\Big(\beta\, \frac{d\alpha}{d\pi}\Big) = \operatorname{Res}_\pi(\beta\, d\alpha). \end{aligned}$$

Como las aplicaciones Res_π y $\operatorname{Res}_{\pi_1}$ son lineales y continuas, basta probar el teorema cuando $\beta = \pi^n$. Supongamos primero que k tiene característica 0. Entonces, si $n \neq -1$, tenemos que el miembro izquierdo vale 0, y el derecho también, porque

$$\pi^n\, \frac{d\pi}{d\pi_1} = \frac{d}{d\pi_1}\Big(\frac{\pi^{n+1}}{n+1}\Big).$$

Si $n = -1$, desarrollamos

$$\pi = c_1\pi_1 + c_2\pi_1^2 + \cdots,$$

con lo que

$$\frac{d\pi}{d\pi_1} = c_1 + 2c_2\pi_1 + \cdots,$$

de donde

$$\frac{1}{\pi}\,\frac{d\pi}{d\pi_1} = \frac{c_1 + 2c_2\pi_1 + \cdots}{c_1\pi_1 + c_2\pi_1^2 + \cdots} = \frac{1}{\pi_1} + \cdots,$$

y los dos miembros de la fórmula valen 1.

Consideremos ahora el caso en que k tiene característica prima p. Usaremos el operador de Cartier C. En primer lugar observamos que si ω es una forma diferencial arbitraria de k, entonces

$$\operatorname{Res}_\pi(\omega) = \operatorname{Res}_{\pi^p}(C(\omega)).$$

En efecto, descompongamos ω en la forma (8.3), donde $u = \sum c_n\pi^n$. Entonces

$$u_i\pi^i = \sum_{n\equiv i \ (\text{mód } p)} c_n\pi^n, \qquad 0 \leq i < p,$$

con lo que

$$C(\omega) = u_0\,\frac{d\pi^p}{\pi^p} = \Big(\sum_n c_{np}(\pi^p)^n\Big)\,\frac{d\pi^p}{\pi^p},$$

luego ω y $C(\omega)$ tienen ambas residuo c_0.

Más aún, de los cálculos que acabamos de realizar se sigue que si $v(\omega) \geq 0$ entonces $v(C(\omega)) \geq 0$, y que si $v(\omega) = r-1 \leq 0$ entonces $v(C(\omega)) \geq r/p-1$. Por lo tanto, aplicando repetidas veces el operador de Cartier podemos restringirnos al caso en que $v(\omega) \geq -1$. Más concretamente, basta probar (8.4) cuando $v(\beta) \geq -1$ o, más concretamente, cuando $\beta = \pi^n$, con $n \geq -1$. Ahora bien, si $n \geq 0$ ambos miembros valen 0, y si $n = -1$ vale el mismo razonamiento que en el caso de característica 0. ■

Definición 8.8 Sea k un cuerpo de series de potencias sobre un cuerpo de coeficientes k_0. Llamaremos *residuo* de una forma diferencial $\omega = \beta\,d\alpha$ de k a

$$\operatorname{Res}\omega = \operatorname{Res}_\pi\Big(\beta\,\frac{d\alpha}{d\pi}\Big),$$

para cualquier primo π de k.

La aplicación Res es k_0-lineal. Las formas enteras tienen residuo nulo. También conviene recordar que en la prueba del teorema anterior hemos visto que el operador de Cartier conserva los residuos.

Recordemos que, por el teorema 6.43, una extensión finita K de un cuerpo de series de potencias $k = k_0((\pi))$ es de la forma $K = k_1((\rho))$, donde k_1 es la clausura algebraica de k_0 en K.

Teorema 8.9 *Sea $K = k_1((\rho))$ una extensión finita separable de un cuerpo de series formales de potencias $k = k_0((\pi))$. Entonces, para todo $\alpha \in k$ y todo $\beta \in K$, se cumple*

$$\operatorname{Tr}_{k_0}^{k_1}(\operatorname{Res}_K(\beta\, d\alpha)) = \operatorname{Res}_k(\operatorname{Tr}_k^K(\beta)\, d\alpha).$$

DEMOSTRACIÓN: Sea $L = k_1((\pi))$. Basta probar

a) $\operatorname{Tr}_{k_0}^{k_1}(\operatorname{Res}_L(\beta\, d\alpha)) = \operatorname{Res}_k(\operatorname{Tr}_k^L(\beta)\, d\alpha)$, para $\alpha \in k$, $\beta \in L$,

b) $\operatorname{Res}_K(\beta\, d\alpha) = \operatorname{Res}_L(\operatorname{Tr}_L^K(\beta)\, d\alpha)$, para $\alpha \in L$, $\beta \in K$.

Para probar a) observamos que $L = kk_1$, por lo que $|L : k| \leq |k_1 : k_0|$. Por otra parte, cada k_0-monomorfismo de k_1 (en una clausura algebraica) se extiende claramente a un k-monomorfismo de L. Esto prueba la igualdad de los índices y, además, si

$$\beta = \sum_i a_i \pi^i, \qquad a_i \in k_1,$$

entonces

$$\operatorname{Tr}_k^L(\beta) = \sum_i \operatorname{Tr}_{k_0}^{k_1}(a_i)\pi^i.$$

Sea

$$\frac{d\alpha}{d\pi} = \sum_j b_j \pi^j, \qquad b_j \in k_0.$$

Entonces

$$\operatorname{Tr}_{k_0}^{k_1}(\operatorname{Res}_L(\beta\, d\alpha)) = \operatorname{Tr}_{k_0}^{k_1}(\operatorname{Res}_\pi(\beta\, \frac{d\alpha}{d\pi})) = \operatorname{Tr}_{k_0}^{k_1}\Big(\sum_{i+j=-1} a_i b_j\Big)$$

$$= \sum_{i+j=-1} \operatorname{Tr}_{k_0}^{k_1}(a_i) b_j = \operatorname{Res}_\pi\Big(\operatorname{Tr}_k^L(\beta)\, \frac{d\alpha}{d\pi}\Big) = \operatorname{Res}_K(\operatorname{Tr}_k^L(\beta)\, d\alpha).$$

Para probar b) vemos que $f(L/k) = |k_1 : k_0| = f(K/k)$, luego $f(K/L) = 1$ y, por lo tanto, la extensión K/L está totalmente ramificada. Por el teorema 5.34 el polinomio mínimo de ρ sobre L es un polinomio de Eisenstein. En particular, si ρ_i son los conjugados de ρ en una extensión de K tenemos que

$$\prod_{i=1}^{e} \rho_i = c(\pi) = c_1\pi + c_2\pi^2 + \cdots, \qquad c_i \in k_1, \quad c_1 \neq 0. \tag{8.5}$$

Basta probar que

$$\operatorname{Res}_K(\beta\, d\pi) = \operatorname{Res}_L(\operatorname{Tr}_L^K(\beta)\, d\pi), \qquad \beta \in K,$$

pues b) se sigue de este hecho aplicado a $\beta\, \dfrac{d\alpha}{d\pi}$ en lugar de β. A su vez basta probar que

$$\operatorname{Res}_K(\beta\, d\rho) = \operatorname{Res}_L\Big(\operatorname{Tr}_L^K\Big(\beta\, \frac{d\rho}{d\pi}\Big) d\pi\Big), \qquad \beta \in K,$$

pues la igualdad anterior se sigue de esta aplicada a $\beta \, \dfrac{d\pi}{d\rho}$ en lugar de β. Ambos miembros son k_1-lineales y continuos en β, luego podemos tomar $\beta = \rho^{n-1}$, para un $n \in \mathbb{Z}$, es decir, hemos de probar que

$$\operatorname{Res}_K\Big(\rho^n \, \frac{d\rho}{\rho}\Big) = \operatorname{Res}_L\Big(\operatorname{Tr}_L^K\Big(\rho^{n-1} \, \frac{d\rho}{d\pi}\Big) d\pi\Big), \qquad n \in \mathbb{Z}. \tag{8.6}$$

Las derivadas siguientes las calculamos en la adjunción a K de los elementos ρ_i (que es un cierto cuerpo de series de potencias):

$$\frac{dc}{d\pi} = \sum_{i=1}^{e} \prod_{j\neq i} \rho_i \frac{d\rho_i}{d\pi},$$

luego

$$\frac{1}{c} \, \frac{dc}{d\pi} = \sum_{i=1}^{e} \frac{1}{\rho_i} \, \frac{d\rho_i}{d\pi} = \operatorname{Tr}_L^K\Big(\frac{1}{\rho} \, \frac{d\rho}{d\pi}\Big).$$

Ahora bien, de (8.5) se sigue inmediatamente que el residuo del miembro izquierdo es 1, luego

$$\operatorname{Res}_L\Big(\operatorname{Tr}_L^K\Big(\rho^{-1} \, \frac{d\rho}{d\pi}\Big)\Big) = 1 = \operatorname{Res}_K(\rho^{-1} \, d\rho).$$

Observemos que la derivada $\dfrac{d\rho}{d\pi}$ es la misma calculada en K o en la extensión en la que estábamos trabajando. En efecto, en ambos cuerpos es la inversa de la derivada $\dfrac{d\pi}{d\rho}$, y ésta está determinada por la expresión de π como serie de potencias de ρ.

Hemos probado (8.6) para $n = 0$. Supongamos ahora que $\operatorname{car} k \nmid n$, $n \neq 0$. Entonces

$$\operatorname{Tr}_L^K\Big(\rho^{n-1} \, \frac{d\rho}{d\pi}\Big) = \frac{1}{n} \operatorname{Tr}_L^K\Big(\frac{d\rho^n}{d\pi}\Big) = \frac{1}{n}\sum_{i=1}^{e} \frac{d\rho_i^n}{d\pi} = \frac{1}{n} \, \frac{d}{d\pi} \sum_{i=1}^{e} \rho_i^n = \frac{1}{n} \, \frac{d}{d\pi} \, \operatorname{Tr}_L^K(\rho^n).$$

Ahora basta tener en cuenta que las derivadas tienen residuo nulo, luego se cumple (8.6). Nos queda el caso en que $\operatorname{car} k = p \mid n$, $n \neq 0$. Digamos que $n = pn'$. Veremos que el operador de Cartier nos reduce este caso a los anteriores. En primer lugar expresamos (8.6) en la forma equivalente

$$\operatorname{Res}_K\Big(\rho^n \, \frac{d\rho}{\rho}\Big) = \operatorname{Res}_L\Big(\operatorname{Tr}_L^K\Big(\rho^n \, \frac{\pi}{\rho} \, \frac{d\rho}{d\pi}\Big) \, \frac{d\pi}{\pi}\Big).$$

Sean C_K y C_L los operadores de Cartier de K y L respectivamente. Puesto que éstos conservan los residuos, basta probar que

$$\operatorname{Res}_{K^p}\Big(C_K\Big(\rho^n \, \frac{d\rho}{\rho}\Big)\Big) = \operatorname{Res}_{L^p}\Big(C_L\Big(\operatorname{Tr}_L^K\Big(\rho^n \, \frac{\pi}{\rho} \, \frac{d\rho}{d\pi}\Big) \, \frac{d\pi}{\pi}\Big)\Big). \tag{8.7}$$

Para ello vamos a ver que C_L conmuta con la traza, de modo que esto será equivalente a

$$\operatorname{Res}_{K^p}\Big((\rho^p)^{n'}\,\frac{d\rho^p}{\rho^p}\Big) = \operatorname{Res}_{L^p}\Big(\operatorname{Tr}_{L^p}^{K^p}\Big((\rho^p)^{n'}\,\frac{\pi^p}{\rho^p}\,\frac{d\rho^p}{d\pi^p}\Big)\frac{d\pi^p}{\pi^p}\Big), \tag{8.8}$$

pero esto es (8.6) para $n' = n/p$. Por consiguiente, aplicando un número finito de veces los operadores de Cartier reducimos el problema a los casos ya probados.

Así pues, sólo falta comprobar la igualdad de los miembros derechos de (8.7) y (8.8). Para ello observamos que $|K : K^p| = p$ y que $\pi \notin K^p$ (pues si $\pi = \alpha^p$ entonces $\alpha \notin L$ y la extensión $L(\alpha)/L$ sería inseparable). Por consiguiente $K = K^p(\pi)$. Esto nos permite expresar

$$\frac{\pi}{\rho}\,\frac{d\rho}{d\pi} = \sum_{i=0}^{p-1} g_i\pi^i, \qquad g_i \in K^p.$$

Entonces

$$\operatorname{Tr}_L^K\Big(\rho^n\,\frac{\pi}{\rho}\,\frac{d\rho}{d\pi}\Big) = \sum_{i=0}^{p-1}\operatorname{Tr}_L^K(\rho^n g_i)\pi^i,$$

y como $\rho^n g_i \in K^p$, resulta que $\operatorname{Tr}_L^K(\rho^n g_i) \in L^p$, de donde

$$C_L\Big(\operatorname{Tr}_L^K\Big(\rho^n\,\frac{\pi}{\rho}\,\frac{d\rho}{d\pi}\Big)\,\frac{d\pi}{\pi}\Big) = \operatorname{Tr}_L^K(\rho^n g_0)\,\frac{d\pi^p}{\pi^p} = \operatorname{Tr}_{L^p}^{K^p}(\rho^n g_0)\,\frac{d\pi^p}{\pi^p}$$

$$= \operatorname{Tr}_{L^p}^{K^p}\Big(\frac{\pi^p}{d\pi^p}C_K\Big(\rho^n\frac{\pi}{\rho}\,\frac{d\rho}{d\pi}\,\frac{d\pi}{\pi}\Big)\Big)\,\frac{d\pi^p}{\pi^p} = \operatorname{Tr}_{L^p}^{K^p}\Big(\frac{\pi^p}{d\pi^p}\,\rho^n C_K\Big(\frac{d\rho}{\rho}\Big)\Big)\,\frac{d\pi^p}{\pi^p}$$

$$= \operatorname{Tr}_{L^p}^{K^p}\Big(\frac{\pi^p}{d\pi^p}\,\rho^n\,\frac{d\rho^p}{\rho^p}\Big)\,\frac{d\pi^p}{\pi^p} = \operatorname{Tr}_{L^p}^{K^p}\Big((\rho^p)^{n'}\,\frac{\pi^p}{\rho^p}\,\frac{d\rho^p}{d\pi^p}\Big)\frac{d\pi^p}{\pi^p},$$

como había que probar. ■

8.2 Diferenciales de funciones algebraicas

Nos ocupamos ahora de la teoría global correspondiente a la teoría local que acabamos de desarrollar. Necesitamos un resultado previo sobre separabilidad. El teorema 1.32 implica como caso particular que si K es un cuerpo de funciones algebraicas, existe un $x \in K$ tal que la extensión $K/k_0(x)$ es finita separable. Vamos a dar otra prueba de este teorema para cuerpos de funciones algebraicas que en añadidura caracteriza los x que cumplen esto:

Definición 8.10 Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0. Diremos que un elemento $x \in K$ es *separador* si la extensión $K/k_0(x)$ es separable.

Es claro que un elemento separador de K ha de ser trascendente sobre k_0 (o de lo contrario la extensión K/k_0 sería algebraica). Si los cuerpos tienen característica 0, ser separador equivale a ser trascendente. Más aún, si k_0 es el cuerpo exacto de constantes de K entonces ser separador equivale a no ser constante.

Para probar la existencia de elementos separadores en cuerpos de característica prima (independientemente de 1.32) nos apoyaremos en el teorema siguiente:

Teorema 8.11 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 de característica prima p. Sea $x \in K$ trascendente sobre k_0. Entonces la clausura separable de $k_0(x)$ en K es de la forma $K_s = K^{p^n}$, para cierto natural $n \geq 0$.*

DEMOSTRACIÓN: Como K/K_s es puramente inseparable, $|K : K_s| = p^n$, para cierto natural n. También es claro que $K^{p^n} \subset K_s$ pues, si $\alpha \in K$, su polinomio mínimo sobre K_s ha de ser de la forma $x^{p^i} - \alpha^{p^i}$, con $i \leq n$, luego $\alpha^{p^n} \in K_s$. Basta probar que $|K : K^{p^n}| = p^n$.

Puesto que k_0 es perfecto, tenemos que $k^{p^n} = k_0(x^{p^n})$. Llamemos $k_1 = k^{p^n}$ y $x_1 = x^{p^n}$. Así $k_1 = k_0(x_1)$, $k = k_1(x)$ y x es raíz del polinomio $t^{p^n} - x_1$, que es irreducible en $k_1[t]$, pues un factor propio sería de la forma $(t-x)^{p^i} = t^{p^i} - x^{p^i}$, para $i < n$, con lo que $x^{p^{n-1}} \in k_0(x^{p^n}) = k_0(x)^{p^n}$, de donde $x \in k_0(x)^p$, pero esto es claramente falso.

Así pues, $|k : k^{p^n}| = p^n$. Ahora basta observar que

$$\begin{aligned} |K : k^{p^n}| &= |K : K^{p^n}|\,|K^{p^n} : k^{p^n}| = |K : K^{p^n}|\,|K : k|, \\ |K : k^{p^n}| &= |K : k|\,|k : k^{p^n}| = |K : k|\,p^n, \end{aligned}$$

donde hemos usado que la aplicación $u \mapsto u^{p^n}$ es un isomorfismo entre las extensiones K/k y K^{p^n}/k^{p^n}, luego tienen el mismo grado. Igualando ambas líneas concluimos que $|K : K^{p^n}| = p^n$, como queríamos probar. ■

Teorema 8.12 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 de característica prima p. Un elemento $x \in K$ trascendente sobre k_0 es separador si y sólo si $x \notin K^p$.*

DEMOSTRACIÓN: Sea $x \in K$ trascendente sobre k_0. Entonces la extensión $K/k_0(x)$ es finita. Sea K_s la clausura separable de $k_0(x)$ en K. Por el teorema anterior $K_s = K^{p^n}$, para cierto $n \geq 0$.

Puesto que $x \in K_s$, tenemos que $\sqrt[p^n]{x} \in K$. La aplicación $u \mapsto u^{p^n}$ es un isomorfismo entre las extensiones $K \,/\, k_0\big(\sqrt[p^n]{x}\big)$ y $K_s/k_0(x)$, luego la primera es separable, ya que la segunda lo es.

De aquí se sigue que n es el mayor número natural tal que $\sqrt[p^n]{x} \in K$, pues si $\sqrt[p^{n+1}]{x} \in K$, éste sería puramente inseparable sobre $k_0\big(\sqrt[p^n]{x}\big)$, por lo que $\sqrt[p^{n+1}]{x} \in k_0\big(\sqrt[p^n]{x}\big)$, y esto lleva fácilmente a una contradicción.

En resumen, x es separador si y sólo si $n = 0$, si y sólo si $x \notin K^p$. ■

Pasemos ya a investigar la noción de diferencial de una función algebraica. Si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0, el teorema 6.42 afirma que para cada divisor primo $\mathfrak{P}$ de K, su compleción es $K_{\mathfrak{P}} = k_{0\mathfrak{P}}((\pi))$, donde π es cualquier primo de $K_{\mathfrak{P}}$ y $k_{0\mathfrak{p}}$ es la clausura algebraica de k_0 en $K_{\mathfrak{P}}$. Por consiguiente, si α y $\beta \in K$, tenemos definida la forma diferencial $(\beta\, d\alpha)_{\mathfrak{P}}$ de $K_{\mathfrak{P}}$.

Definición 8.13 Si K es un cuerpo de funciones algebraicas y α, $\beta \in K$, definimos la *forma diferencial* $\beta\, d\alpha$ de K como el elemento del producto de todos los espacios de formas diferenciales de todas las compleciones de K cuya componente $\mathfrak{P}$-ésima es $(\beta\, d\alpha)_{\mathfrak{P}}$.

El conjunto de las formas diferenciales de K tiene estructura de espacio vectorial (es un subespacio del espacio producto de los espacios de formas diferenciales locales), de modo que $\beta\, d\alpha$ es el producto escalar de β por $d\alpha = 1\, d\alpha$. Escribiremos $d_{\mathfrak{P}}\alpha$ en lugar de $(d\alpha)_{\mathfrak{P}}$. De este modo $(\beta\, d\alpha)_{\mathfrak{P}} = \beta\, d_{\mathfrak{P}}\alpha$.

Seguidamente determinamos las funciones con diferencial nula:

Teorema 8.14 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 y sea $x \in K$. Entonces $dx \neq 0$ si y sólo si x es separador, y en tal caso todas las componentes de dx son no nulas.*

Demostración: Podemos suponer que k_0 es el cuerpo de constantes exacto de K. Supongamos que x no es separador. Si $\operatorname{car} K = 0$, esto sólo puede ocurrir si $x \in k_0$. Si $\operatorname{car} k = p > 0$, por el teorema 8.12 puede ocurrir también que $x \in K^p$. En cualquiera de estos casos, el teorema 8.3 nos da que las componentes de dx son nulas, luego $dx = 0$.

Supongamos ahora que x es separador. Sea $\mathfrak{P}$ un divisor primo de K y sea $\pi \in K$ tal que $v_{\mathfrak{P}}(\pi) = 1$. De este modo tenemos un primo π de $K_{\mathfrak{P}}$ que pertenece a K. Sea $f(x,t)$ su polinomio mínimo sobre $k_0(x)$. Por el teorema 8.2 tenemos que

$$0 = \frac{df(x,\pi)}{d\pi} = \frac{\partial f}{\partial x}(x,\pi)\frac{dx}{d\pi} + \frac{\partial f}{\partial t}(x,\pi).$$

Ahora bien, como π es separable sobre $k_0(x)$, el último término es no nulo, luego la derivada de x tampoco puede ser nula. Por consiguiente $d_{\mathfrak{P}}x \neq 0$. ■

Más en general, una forma diferencial $\beta\, d\alpha \neq 0$ cumple $\beta \neq 0$ y $d\alpha \neq 0$, luego tiene todas sus componentes no nulas. Como consecuencia, dos formas diferenciales de un cuerpo K de funciones algebraicas son iguales si y sólo si coinciden en una componente.

De este modo, si K es un cuerpo de funciones algebraicas, α, $x \in K$, x es separador y $\mathfrak{P}$ es un divisor primo de K, tenemos definida la derivada

$$\frac{d\alpha}{dx} \in K_{\mathfrak{P}}.$$

Si $f(x,t)$ es el polinomio mínimo de α sobre $k_0(x)$, se cumple

$$0 = \frac{\partial f}{\partial x}(x,\alpha) + \frac{\partial f}{\partial t}(x,\alpha)\frac{d\alpha}{dx}.$$

Como f es separable, podemos despejar

$$\frac{d\alpha}{dx} = -\frac{\dfrac{\partial f}{\partial x}(x,\alpha)}{\dfrac{\partial f}{\partial t}(x,\alpha)} \in K. \tag{8.9}$$

Así pues, la derivada $\dfrac{d\alpha}{dx}$ es un elemento de K independiente de $\mathfrak{P}$. Además se cumple la relación

$$d\alpha = \frac{d\alpha}{dx}\, dx. \tag{8.10}$$

Esto prueba que el espacio de las formas diferenciales de K es un K-espacio vectorial de dimensión 1.

En la sección anterior hemos definido el orden de una forma diferencial local. En el caso global tenemos un orden en cada primo. Concretamente, si $x \in K$ es un elemento separador, definimos

$$v_{\mathfrak{P}}(\beta\, dx) = v_{\mathfrak{P}}(\beta\, d_{\mathfrak{P}}x) = v_{\mathfrak{P}}\left(\beta\, \frac{dx}{d\pi}\right),$$

donde π es un primo cualquiera de $K_{\mathfrak{P}}$. Vamos a probar que $v_{\mathfrak{P}}(\beta\, dx) = 0$ para casi todo primo $\mathfrak{P}$. Esto nos permitirá asignar un divisor de K a cada diferencial.

Sea $\mathfrak{p}$ el divisor primo de $k = k_0(x)$ divisible entre $\mathfrak{P}$. Sea $p(x) \in k_0[x]$ el polinomio mónico irreducible que cumple $\mathfrak{p} = (p(x))$ si es que $\mathfrak{p} \neq \infty$ o bien $p(x) = 1/x$ si $\mathfrak{p} = \infty$. En cualquier caso $v_{\mathfrak{p}}(p(x)) = 1$, luego $p(x)$ es primo en $k_{\mathfrak{p}}$. Según el teorema 6.42, sabemos que $K_{\mathfrak{P}} = k_{0\mathfrak{P}}((\pi))$, donde $k_{0\mathfrak{P}}$ es la clausura algebraica de k_0 en $K_{\mathfrak{P}}$.

Sea $L = k_{0\mathfrak{P}}((p))$. Así el cuerpo de restos de L es el mismo que el de $K_{\mathfrak{P}}$, mientras que p sigue siendo primo en L. Esto implica que $f(L/k_{\mathfrak{p}}) = f(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ y $e(L/k_{\mathfrak{p}}) = 1$. Concluimos que la extensión $L/k_{\mathfrak{p}}$ es no ramificada y $K_{\mathfrak{P}}/L$ es totalmente ramificada.

Por el teorema 5.34, el polinomio mínimo de π sobre L es un polinomio de Eisenstein, digamos

$$f(p,\pi) = \pi^e + pf_{e-1}(p)\pi^{e-1} + \cdots + pf_1(p)\pi + pf_0(p) = 0,$$

donde los coeficientes $f_i(p)$ son series enteras con coeficientes en $k_{0\mathfrak{P}}$ y $f_0(p)$ es una unidad. Derivando esta igualdad tenemos

$$\frac{\partial f}{\partial p}(p,\pi)\frac{dp}{d\pi} + \frac{\partial f}{\partial \pi}(p,\pi) = 0.$$

Por una parte,

$$\begin{aligned} \frac{\partial f}{\partial p}(p,\pi) &= (f_{e-1}(p) + pf'_{e-1}(p))\pi^{e-1} + \cdots + (f_0(p) + pf'_0(p)) \\ &\equiv f_0(p) \not\equiv 0 \ (\text{mód } \mathfrak{P}). \end{aligned}$$

Por otro lado, el teorema 7.30 implica que las potencias $1, \pi, \ldots, \pi^{e-1}$ generan el anillo de enteros de $K_{\mathfrak{P}}$ sobre el de L, y entonces 7.32 nos da que $\dfrac{\partial f}{\partial \pi}(p, \pi)$ genera el diferente de la extensión $K_{\mathfrak{P}}/L$, que es el mismo que el de la extensión $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, ya que el tramo inferior es no ramificado. Si llamamos $\mathfrak{D}$ al diferente de la extensión K/k, entonces el diferente de $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ es su componente $\mathfrak{D}_{\mathfrak{P}}$, y hemos probado que

$$v_{\mathfrak{P}}\left(\frac{dp}{d\pi}\right) = v_{\mathfrak{P}}\left(\frac{\partial f}{\partial \pi}(p, \pi)\right) = v_{\mathfrak{P}}(\mathfrak{D}_{\mathfrak{P}}) = v_{\mathfrak{P}}(\mathfrak{D}).$$

Por otra parte,

$$\frac{dp}{d\pi} = \frac{dp}{dx}\frac{dx}{d\pi},$$

y

$$\frac{dp}{dx} = \begin{cases} p'(x) & \text{si } \mathfrak{p} \neq \infty, \\ -1/x^2 & \text{si } \mathfrak{p} = \infty. \end{cases}$$

Si $\mathfrak{P} \mid \infty$, entonces $v_{\mathfrak{P}}(-1/x^2) = v_{\mathfrak{P}}(\infty^2)$, mientras que si $\mathfrak{P} \nmid \infty$ tenemos igualmente que $v_{\mathfrak{P}}(p'(x)) = 0 = v_{\mathfrak{P}}(\infty^2)$. En cualquier caso tenemos que

$$v_{\mathfrak{P}}(dx) = v_{\mathfrak{P}}\left(\frac{dx}{d\pi}\right) = v_{\mathfrak{P}}\left(\frac{\mathfrak{D}}{\infty^2}\right).$$

En particular tenemos que, ciertamente, $v_{\mathfrak{P}}(dx) = 0$ para casi todo primo $\mathfrak{P}$. Lo mismo vale obviamente para cualquier forma diferencial $\alpha\, dx$ no nula. Esto justifica la definición siguiente:

Definición 8.15 Sea K un cuerpo de funciones algebraicas y $\alpha\, dx$ una forma diferencial no nula en K. Llamaremos *divisor diferencial* asociado a $\alpha\, dx$ al divisor

$$(\alpha\, dx) = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\alpha\, dx)},$$

donde

$$v_{\mathfrak{P}}(\alpha\, dx) = v_{\mathfrak{P}}\left(\alpha\,\frac{dx}{d\pi}\right),$$

para cualquier primo π.

Hemos demostrado el teorema siguiente:

Teorema 8.16 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0. Sea dx una forma diferencial no nula en K, con lo que x es un elemento separador y la extensión $K/k_0(x)$ es separable. Sea $\mathfrak{D}$ el diferente de esta extensión. Entonces*

$$(dx) = \frac{\mathfrak{D}}{\infty^2}.$$

La fórmula (8.10) muestra que todos los divisores diferenciales son equivalentes. De hecho, los divisores diferenciales constituyen una clase de equivalencia de divisores de K.

Definición 8.17 Si K es un cuerpo de funciones algebraicas, llamaremos *clase diferencial* o *clase canónica* de K a la clase de divisores de K formada por los divisores diferenciales.

Vamos a calcular el grado de la clase canónica de una curva proyectiva bajo una restricción: diremos que un punto P de una curva proyectiva V es *ordinario* si V tiene $m_P(V)$ tangentes distintas en P. El teorema 7.18 implica (ver la observación posterior) que en tal caso V tiene $m_P(V)$ primos sobre P. Es claro que todo punto regular es ordinario.

Teorema 8.18 *Sea V una curva proyectiva plana de grado n cuyas singularidades sean todas ordinarias. Entonces el grado de su clase canónica es $2g-2$, con*

$$g = \frac{(n-1)(n-2)}{2} - \sum_P \frac{m_P(V)(m_P(V)-1)}{2},$$

donde P recorre los puntos (singulares) de V

DEMOSTRACIÓN: Por el teorema 7.20, podemos tomar una recta que corte a V en n puntos distintos. Podemos tomar un sistema de referencia respecto al cual esta recta sea $Z=0$. Así mismo podemos exigir que la recta $Y=0$ corte a la anterior en un punto (que tendrá coordenadas $(1,0,0)$) que no esté en V ni en ninguna de las tangentes a V por puntos singulares.

El teorema de Bezout implica que en los n puntos donde V corta a la recta infinita $Z=0$ el número de intersección es 1, luego todos estos puntos han de ser regulares. En otras palabras, V no tiene singularidades en el infinito.

Consideramos las coordenadas afines $x=X/Z$ e $y=Y/Z$. El grado de la clase canónica es, por ejemplo, el grado del divisor (dx), que es el que vamos a calcular. Sea $V=F(F)$, con $F\in k_0[X,Y]$.

Sea $P=(a,b)$ un punto finito de V. Si $\frac{\partial F}{\partial Y}\big|_P \neq 0$ entonces P es un punto regular, y ciertamente $X=a$ no es la recta tangente a V en P, luego si $\mathfrak{P}$ es el único primo de V situado sobre P, se cumple que $\pi = x-b$ es primo en $\mathfrak{O}_{\mathfrak{P}}$ y $dx = d(x-b) = 1d\pi$, luego $v_{\mathfrak{P}}(dx) = v_{\mathfrak{P}}(1) = 0$.

Supongamos ahora que $\frac{\partial F}{\partial Y}\big|_P = 0$. Distinguimos dos casos: si $\frac{\partial F}{\partial X}\big|_P \neq 0$ entonces P es regular e $Y=b$ no es la tangente a V en P; si $\frac{\partial F}{\partial X}\big|_P = 0$ entonces P es singular y la recta $Y=b$ tampoco es tangente a V en P porque contiene al punto $(1,0,0)$.

Así pues, en cualquier caso tenemos que la recta $Y=b$ no es tangente a V en P. Consecuentemente $I_P(V\cap Y-b) = m_P(V)$. Puesto que este número de intersección es la suma de los valores $v_{\mathfrak{P}}(y-b)$ para todos los primos $\mathfrak{P}$ situados sobre P y hay $m_P(V)$ tales primos (ya que P es ordinario), concluimos que $v_{\mathfrak{P}}(y-b)=1$ para todo primo $\mathfrak{P}$. Así pues, $\pi = y-b$ es primo en $\mathfrak{O}_{\mathfrak{P}}$. Además $d\pi = dy$.

Ahora usamos que $F(x,y)=0$, por lo que

$$\frac{\partial F}{\partial X}(x,y)\,dx + \frac{\partial F}{\partial Y}(x,y)\,dy = 0. \tag{8.11}$$

Despejando,

$$dx = -\frac{\frac{\partial F}{\partial Y}}{\frac{\partial F}{\partial X}}\, dy = -\frac{\frac{\partial F}{\partial Y}}{\frac{\partial F}{\partial X}}\, d\pi.$$

Por consiguiente $v_{\mathfrak{P}}(dx) = v_{\mathfrak{P}}\left(\frac{\partial F}{\partial Y}\right) - v_{\mathfrak{P}}\left(\frac{\partial F}{\partial X}\right)$. Si sumamos sobre todos los primos situados sobre P tenemos que

$$\sum_{\mathfrak{P}} v_{\mathfrak{P}}(dx) = I_P\left(V \cap \frac{\partial F}{\partial Y}\right) - I_P\left(V \cap \frac{\partial F}{\partial X}\right).$$

Vamos a calcular el segundo número de intersección. Sea

$$F = F_m(X-a, Y-b) + F_{m+1}(X-a, Y-b) + \cdots$$

la descomposición en formas de F alrededor de P, donde $m = m_P(V)$. El hecho de que $Y-b$ no sea tangente a V en P se traduce en que $Y - b \nmid F_m(X-a, Y-b)$ o, equivalentemente, en que $Y \nmid F_m(X, Y)$. En particular $F_m \neq Y^m$, luego las tangentes a V en P se corresponden con las raíces de $F_m(X, 1)$, las cuales son simples (pues P es ordinario).

Esto implica que $\frac{\partial F_m}{\partial X}(X, 1)$ sea un polinomio no nulo sin raíces en común con F_m. Dichas raíces se corresponden con las tangentes en P de $\frac{\partial F}{\partial X}$, luego concluimos que F y $\frac{\partial F}{\partial X}$ no tienen tangentes comunes en P (y además P tiene multiplicidad $m-1$ en la derivada). Esto implica que $I_P\left(V \cap \frac{\partial F}{\partial X}\right) = m_P(V)(m_P(V)-1)$. En total:

$$\sum_{\mathfrak{P}} v_{\mathfrak{P}}(dx) = I_P\left(V \cap \frac{\partial F}{\partial Y}\right) - m_P(V)(m_P(V)-1),$$

donde $\mathfrak{P}$ recorre los primos de V situados sobre P. Notemos que esta fórmula es válida incluso en el caso en que $\frac{\partial F}{\partial Y}\big|_P \neq 0$, pues entonces ambos miembros son nulos.

Supongamos ahora que P es un punto infinito. Por la elección del sistema de referencia tenemos que $P = (a, 1, 0)$, P es regular y la recta $Z = 0$ no es tangente a V en P. Sea $\mathfrak{P}$ el único primo de V situado sobre P.

Llamando $z = Z/Y$, tenemos que $1 = I_P(V \cap Z) = v_{\mathfrak{P}}(z)$, luego $\pi = z$ es primo en $\mathfrak{O}_{\mathfrak{P}}$. Además $y = 1/z$, luego $dy = (-1/z^2)dz = -\pi^{-2}\, d\pi$, luego $v_{\mathfrak{P}}(dy) = -2$. Despejando dx en (8.11) concluimos que

$$v_{\mathfrak{P}}(dx) = v_{\mathfrak{P}}\left(\frac{\partial F}{\partial Y}\right) - v_{\mathfrak{P}}\left(\frac{\partial F}{\partial X}\right) - 2.$$

Ahora hemos de tener cuidado con el hecho de que las derivadas representan funciones en coordenadas afines y $\mathfrak{P}$ es un primo infinito. Para calcular las valoraciones hemos de homogeneizar las derivadas.

Sea $F(X, Y, Z)$ la homogeneización del polinomio $F(X, Y)$, de modo que $F(X, Y) = F(X, Y, 1)$. Claramente $\frac{\partial F}{\partial Y}(X, Y) = \frac{\partial F}{\partial Y}(X, Y, 1)$, y a su vez

$$\frac{\partial F}{\partial Y}(x, y) = \frac{\partial F}{\partial Y}(x, y, 1) = \frac{\frac{\partial F}{\partial Y}(X, Y, Z)}{Z^{n-1}}.$$

Podemos hablar del número de intersección $I_P\big(V \cap \frac{\partial F}{\partial Y}(X,Y)\big)$, siendo la derivada una curva afín y P un punto infinito, entendiendo que con ello nos referimos al número de intersección en P de V con la clausura proyectiva de la curva, es decir, a $I_P(V \cap \frac{\partial F}{\partial Y}(X,Y,Z))$, pero este número de intersección no puede calcularse dividiendo $\frac{\partial F}{\partial Y}$ entre Z^{n-1}, porque Z se anula en P. Una forma que no se anula en P es Y, luego

$$v_{\mathfrak{P}}\left(\frac{\partial F}{\partial Y}(x,y)\right) = v_{\mathfrak{P}}\left(\frac{\frac{\partial F}{\partial Y}(X,Y,Z)}{Z^{n-1}}\right) = v_{\mathfrak{P}}\left(\frac{\frac{\partial F}{\partial Y}}{Y^{n-1}}\right) + v_{\mathfrak{P}}\left(\frac{Y^{n-1}}{Z^{n-1}}\right)$$

$$= I_P\left(V \cap \frac{\partial F}{\partial Y}\right) + v_{\mathfrak{P}}(z^{-n-1}) = I_P\left(V \cap \frac{\partial F}{\partial Y}\right) - (n-1).$$

Igualmente

$$v_{\mathfrak{P}}\left(\frac{\partial F}{\partial X}(x,y)\right) = v_{\mathfrak{P}}\left(\frac{\frac{\partial F}{\partial X}(X,Y,Z)}{Z^{n-1}}\right) = v_{\mathfrak{P}}\left(\frac{\frac{\partial F}{\partial X}}{Y^{n-1}}\right) + v_{\mathfrak{P}}\left(\frac{Y^{n-1}}{Z^{n-1}}\right),$$

pero ahora observamos que $\frac{\partial F}{\partial X}\big|_P \neq 0$, con lo que el primer término del miembro derecho es nulo. En efecto, si la derivada fuera nula, evaluando en $P = (a, 1, 0)$ la relación

$$\frac{\partial F}{\partial X}X + \frac{\partial F}{\partial Y}Y + \frac{\partial F}{\partial Z}Z = nF$$

concluiríamos que $\frac{\partial F}{\partial X}\big|_P = \frac{\partial F}{\partial Y}\big|_P = 0$ y, como P es regular, la derivada respecto de Z sería no nula, pero entonces $Z = 0$ sería tangente a V en P, lo cual es falso. Así pues, tenemos que

$$v_{\mathfrak{P}}\left(\frac{\partial F}{\partial X}(x,y)\right) = -(n-1).$$

En total,

$$v_{\mathfrak{P}}(dx) = I_P\left(V \cap \frac{\partial F}{\partial Y}\right) - 2.$$

Ahora sólo hemos de sumar para todos los primos y aplicar el teorema de Bezout:

$$\begin{aligned}\operatorname{grad}(dx) &= \sum_P I_P\left(V \cap \frac{\partial F}{\partial Y}\right) - 2n - \sum_P m_P(V)(m_P(V)-1)\\ &= n(n-1) - 2n - \sum_P m_P(V)(m_P(V)-1)\\ &= (n-1)(n-2) - 2 - \sum_P m_P(V)(m_P(V)-1) = 2g-2.\end{aligned}$$

■

La razón para expresar el grado en términos de g es que g será lo que más adelante llamaremos género de V, de modo que en el caso $k_0 = \mathbb{C}$ coincidirá con el género topológico que ya tenemos definido.

Nos ocupamos ahora de los residuos de una forma diferencial. Si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0, α, $\beta \in K$ y $\mathfrak{p}$ es un primo de K, tenemos definido

$$\operatorname{Res}_{\mathfrak{p}}(\beta\, d\alpha) = \operatorname{Res}_{K_{\mathfrak{p}}}(\beta\, d_{\mathfrak{p}}\alpha) \in k_{0\mathfrak{p}},$$

donde $k_{0\mathfrak{p}}$ es la clausura algebraica de k_0 en $K_{\mathfrak{p}}$. En general estos residuos no están en el cuerpo de constantes k_0. El teorema 8.9 muestra que las trazas conectan bien los residuos entre extensiones, por lo que resulta conveniente definir

$$\oint_{\mathfrak{p}} \beta\, d\alpha = \operatorname{Tr}_{k_0}^{k_{0\mathfrak{p}}}(\operatorname{Res}_{\mathfrak{p}}(\beta\, d\alpha)).$$

Notemos que esto tiene sentido para todo α, $\beta \in K_{\mathfrak{p}}$. Claramente esta integral es k_0-lineal en α y en β. Del teorema 8.9 deducimos ahora la siguiente versión global:

Teorema 8.19 *Sea L/K una extensión separable de cuerpos de funciones algebraicas sobre un cuerpo de constantes k_0. Sea $\alpha \in K$ y $\beta \in L$. Entonces, para cada primo $\mathfrak{p}$ de K se cumple*

$$\oint_{\mathfrak{p}} \operatorname{Tr}_K^L(\beta)\, d\alpha = \sum_{\mathfrak{P}|\mathfrak{p}} \oint_{\mathfrak{P}} \beta\, d\alpha.$$

Demostración: Basta usar que la traza global es la suma de las trazas locales (teorema 6.41):

$$\begin{aligned}
\oint_{\mathfrak{p}} \operatorname{Tr}_K^L(\beta)\, d\alpha &= \sum_{\mathfrak{P}|\mathfrak{p}} \oint_{\mathfrak{p}} \operatorname{Tr}_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(\beta)\, d\alpha = \sum_{\mathfrak{P}|\mathfrak{p}} \operatorname{Tr}_{k_0}^{k_{0\mathfrak{p}}}(\operatorname{Res}_{\mathfrak{p}}(\operatorname{Tr}_{K_{\mathfrak{p}}}^{L_{\mathfrak{P}}}(\beta)\, d\alpha) \\
&= \sum_{\mathfrak{P}|\mathfrak{p}} \operatorname{Tr}_{k_0}^{k_{0\mathfrak{p}}}(\operatorname{Tr}_{k_{0\mathfrak{p}}}^{k_{0\mathfrak{P}}}(\operatorname{Res}_{\mathfrak{P}}(\beta\, d\alpha))) = \sum_{\mathfrak{P}|\mathfrak{p}} \operatorname{Tr}_{k_0}^{k_{0\mathfrak{P}}}(\operatorname{Res}_{\mathfrak{P}}(\beta\, d\alpha)) \\
&= \sum_{\mathfrak{P}|\mathfrak{p}} \oint_{\mathfrak{P}} \beta\, d\alpha.
\end{aligned}$$

■

Es importante observar que la integral local de una forma diferencial depende del cuerpo de constantes que estemos considerando. Concretamente, si cambiamos el cuerpo de constantes por otro mayor, la integral respecto al cuerpo menor es la traza de la integral respecto al cuerpo mayor. La igualdad del teorema anterior se cumple si las integrales de ambos miembros se calculan respecto al mismo cuerpo de constantes, al contrario de lo que ocurre en el teorema siguiente:

Teorema 8.20 *Sea K un cuerpo de funciones algebraicas sobre el cuerpo exacto de constantes k_0. Sea L una extensión finita de constantes de K. Entonces, para todo α, $\beta \in K$ y todo primo $\mathfrak{p}$ de K se cumple que*

$$\oint_{\mathfrak{p}} \beta\, d\alpha = \sum_{\mathfrak{P}|\mathfrak{p}} \oint_{\mathfrak{P}} \beta\, d\alpha,$$

donde las integrales del miembro derecho se calculan respecto al cuerpo exacto de constantes de L.

DEMOSTRACIÓN: Podemos suponer que la extensión L/K es finita de Galois y que los divisores de $\mathfrak{p}$ en L tienen grado 1. En efecto, siempre existe una extensión L' de K en estas condiciones y que contiene a L, y el teorema para L/K se sigue inmediatamente del teorema para L'/K y L'/L.

Sea k_1 el cuerpo de constantes exacto de L y sea $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ la factorización de $\mathfrak{p}$ en L. Tomando grados en ambos miembros concluimos que $r = \operatorname{grad} \mathfrak{p}$.

Sea $n = |L : K| = |k_1 : k_0|$. Es fácil ver que la restricción determina un isomorfismo $G(L/K) \cong G(k_1/k_0)$. Cada $\sigma \in G(L/K)$ determina un isomorfismo topológico $\sigma : L_{\mathfrak{P}_1} \longrightarrow L_{\sigma(\mathfrak{P}_1)}$. Si $\pi \in K$ cumple $v_{\mathfrak{p}}(\pi) = 1$, entonces también $v_{\mathfrak{P}_i}(\pi) = 1$, por lo que $L_{\mathfrak{P}_i} = k_1((\pi))$. El isomorfismo inducido por σ viene dado por

$$\sigma\Big(\sum_i a_i \pi^i\Big) = \sum_i \sigma(a_i)\pi^i.$$

Fijemos automorfismos σ_i tales que $\sigma_i(\mathfrak{P}_1) = \mathfrak{P}_i$. Identifiquemos a $K_{\mathfrak{p}}$, como es habitual, con la clausura de K en $L_{\mathfrak{P}_1}$, de modo que $K_{\mathfrak{p}} = k_{0\mathfrak{p}}((\pi))$, donde $k_{0\mathfrak{p}}$ es un subcuerpo de k_1 de grado r sobre k_0. En este punto es crucial observar que esta representación de $k_{0\mathfrak{p}}$ como subcuerpo de k_1 depende de la elección que hemos hecho de $\mathfrak{P}_1$, en el sentido de que si queremos identificar a $K_{\mathfrak{p}}$ con un subcuerpo de otro $L_{\mathfrak{P}_i}$ tendremos que sustituir $k_{0\mathfrak{p}}$ por su imagen por σ_i.

Si un automorfismo $\sigma \in G(L/K)$ fija a $\mathfrak{P}_1$ entonces fija a $k_{0\mathfrak{p}}$. Como el número de automorfismos que cumplen una y otra condición ha de ser igual a n/r, el recíproco es cierto y, por consiguiente, las restricciones $\sigma_i|_{k_{0\mathfrak{p}}}$ son los r monomorfismos de $k_{0\mathfrak{p}}$ sobre k_0. Sea

$$\beta\,\frac{d\alpha}{d\pi} = \sum_i a_i\pi^i, \qquad a_i \in k_{0\mathfrak{p}}.$$

Entonces $\operatorname{Res}_{\mathfrak{P}_1}(\beta\, d\alpha) = a_{-1}$ y aplicando σ_i obtenemos que $\operatorname{Res}_{\mathfrak{P}_i}(\beta\, d\alpha) = \sigma_i(a_{-1})$. Por otra parte a_{-1} es también $\operatorname{Res}_{\mathfrak{p}}(\beta\, d\alpha)$, con lo que

$$\sum_{\mathfrak{P}|\mathfrak{p}} \oint_{\mathfrak{P}} \beta\, d\alpha = \sum_{i=1}^{r} \operatorname{Res}_{\mathfrak{P}_i}(\beta\, d\alpha) = \sum_{i=1}^{r} \sigma_i(a_{-1}) = \operatorname{Tr}_{k_0}^{k_{0\mathfrak{p}}}(\operatorname{Res}_{\mathfrak{p}}(\beta\, d\alpha)) = \oint_{\mathfrak{p}} \beta\, d\alpha.$$

■

Ejercicio: Probar que el teorema anterior es válido para extensiones infinitas de constantes.

Sabemos que el orden de una forma diferencial es nulo en todos los primos salvo a lo sumo en una cantidad finita de ellos, luego el residuo correspondiente también es nulo. Por consiguiente tiene sentido la suma

$$\sum_{\mathfrak{p}} \oint_{\mathfrak{p}} \beta\, d\alpha.$$

Ahora podemos probar otro importante teorema global:

Teorema 8.21 (Teorema de los residuos) *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 y $\beta\,d\alpha$ una forma diferencial en K. Entonces*

$$\sum_{\mathfrak{p}} \oint_{\mathfrak{p}} \beta\,d\alpha = 0.$$

DEMOSTRACIÓN: Sea $x \in K$ un elemento separador y sea $k = k_0(x)$. Basta probar que

$$\sum_{\mathfrak{p}} \oint_{\mathfrak{p}} \beta\,dx = 0, \qquad \beta \in K,$$

pues el caso general se sigue de éste cambiando β por $\beta\,\dfrac{d\alpha}{dx}$. A su vez 8.19 nos da que la suma de las integrales locales de $\beta\,dx$ en K es la misma que la suma de las integrales locales de $\operatorname{Tr}_k^K(\beta)\,dx$ en k. Por consiguiente, podemos suponer que $K = k_0(x)$ es un cuerpo de funciones racionales. El teorema 8.20 nos permite sustituir k_0 por una extensión finita. Esto nos permite suponer que los divisores primos de β tienen grado 1. Entonces $\beta\,dx$ se descompone en una combinación lineal de términos de la forma

$$\frac{dx}{(x-a)^i}, \qquad x^i\,dx.$$

En efecto, si $x - a$ es un divisor del denominador de β, el desarrollo en serie de Laurent de β alrededor de este primo consta de un número finito de múltiplos de funciones $(x-a)^{-i}$ más una función racional cuyo denominador no es divisible entre $x - a$. Volviendo a aplicar este proceso de descomposición con otro primo, finalmente llegamos a una función racional cuyo denominador es constante, luego es un polinomio, luego es combinación lineal de términos x^i.

Así pues, basta probar el teorema para formas de los dos tipos indicados. Las formas $x^i\,dx$ tienen todos sus residuos nulos, al igual que las formas del primer tipo cuando $i \neq 1$. Por último,

$$\operatorname{Res}_{x-a} \frac{dx}{x-a} = 1, \qquad \operatorname{Res}_{\infty} \frac{dx}{x-a} = -1,$$

y todos los demás residuos son nulos, luego estas formas también cumplen el teorema. ■

Observemos que si el cuerpo de constantes es algebraicamente cerrado, las integrales locales son simplemente los residuos, y el teorema anterior afirma en tal caso que la suma de los residuos de una función algebraica es nula.

Diferenciales en curvas algebraicas Terminamos la sección relacionando la noción de forma diferencial que acabamos de introducir con la usual en geometría algebraica y, en particular para curvas complejas, con la de la geometría diferencial.

Ante todo observemos que si V es una curva algebraica sobre un cuerpo k_0, $\alpha \in \mathcal{O}_P(V)$ y π es un parámetro local en P, al final del capítulo VI vimos que el desarrollo en serie de α en $k_0(V)_P$ respecto al primo π es precisamente la serie de Taylor de α respecto de π, de donde se sigue que la derivada de α respecto de π que hemos definido en este capítulo coincide con la definida en 3.45 (ver los comentarios tras la definición).

Una *forma diferencial* en sentido amplio sobre una curva V sería cualquier aplicación ω que a cada punto P en un abierto U de V le asigne un elemento ω_P del espacio cotangente T_PV^*. El conjunto de todas las formas diferenciales definidas sobre un mismo abierto U tiene estructura de k_0-espacio vectorial con las operaciones definidas puntualmente. Más aún, es un módulo sobre el anillo de todas las funciones de U en k_0. Si ω es una forma en un abierto U, su restricción $\omega|_{U'}$ a un abierto menor U' es una forma en U'.

Por ejemplo, si U es un abierto en V y $\alpha \in k_0[U]$, entonces podemos considerar a $d\alpha$ como una forma diferencial en U, que a cada punto $P \in U$ le asigna $d_P\alpha \in T_PV^*$.

Sea ω una forma diferencial definida en un entorno U de un punto P y sea π un parámetro local en P. Entonces el teorema 3.34 nos da que, para todo Q en un entorno $U' \subset U$ de P, la función $\pi - \pi(Q)$ es también un parámetro local en Q, por lo que $d_Q\pi$ es una base de T_QV^* y existe una función $\alpha : U' \longrightarrow k_0$ tal que $\omega|_{U'} = \alpha\, d\pi$.

Si $\pi' \in k_0(V)$ es otro parámetro local alrededor de P, entonces

$$d\pi|_{U\cap U'} = \frac{d\pi}{d\pi'}\, d\pi'|_{U\cap U'}.$$

Hemos visto que $d\pi/d\pi' \in k_0[U \cap U']$. En vista de esto, podemos definir una forma *regular* en un punto P como una forma ω tal que $\omega|_U = \alpha\, d\pi$, donde $\pi - \pi(Q)$ es un parámetro local en todos los puntos de un entorno U de P y $\alpha \in k_0[U]$, sin que importe el parámetro con que se comprueba la regularidad.

Es fácil ver que si dos formas son regulares en un abierto U y coinciden en un abierto menor, entonces coinciden en todo U. Esto nos permite definir una *forma racional* en V como una forma que es regular en un abierto U de V, no está definida fuera de U y no admite una extensión regular a ningún abierto mayor. Claramente, toda forma regular en un abierto de V se extiende a una única forma racional en V. Toda forma racional en V es (la extensión de una forma) de tipo $\alpha\, d\pi$, para una cierta función $\pi \in k_0(V)$.

Más aún, si $\alpha, \beta \in k_0(V)$ son funciones arbitrarias, entonces para cada punto P donde ambas son regulares podemos tomar un parámetro local π y expresar

$$\alpha\, d\beta = \alpha\, \frac{d\beta}{d\pi}\, d\pi,$$

lo que prueba que toda forma $\alpha\, d\beta$ es (o se extiende a) una forma diferencial racional en V. Ahora ya es fácil comprobar que las formas diferenciales del cuerpo $k_0(V)$ pueden identificarse con las formas racionales en V.

Si $k_0 = \mathbb{C}$ o, más en general, si V es una superficie de Riemann, en los razonamientos anteriores podemos cambiar "parámetro local" por "carta", "regular" por "holomorfa" y "racional" por "meromorfa" y así es fácil concluir que las formas diferenciales en $\mathcal{M}(V)$ son las formas diferenciales meromorfas en V, es decir, las formas diferenciales (en el sentido de la geometría diferencial) definidas en V salvo en un número finito de polos y de modo que en cada abierto coordenado U (dominio de una carta z) se expresan como $f\,dz$, donde f es una función meromorfa en U.

8.3 La dimensión de un divisor

El teorema de Riemann-Roch es esencialmente una fórmula que relaciona el grado de un divisor con otro invariante asociado que introducimos a continuación.

Definición 8.22 Sea K un cuerpo de fracciones algebraicas y $\mathfrak{a}$ un divisor de K. Llamaremos *múltiplos* de $\mathfrak{a}$ a los elementos del conjunto

$$m(\mathfrak{a}) = \{\alpha \in K \mid v_{\mathfrak{P}}(\alpha) \geq v_{\mathfrak{P}}(\mathfrak{a}) \text{ para todo } \mathfrak{P}\}.$$

Notemos que un $\alpha \in K^*$ es múltiplo de $\mathfrak{a}$ si y sólo si $\mathfrak{a} \mid (\alpha)$, pero en la definición de $m(\mathfrak{a})$ admitimos también al 0. Así, por las propiedades de las valoraciones, los conjuntos de múltiplos son claramente k_0-espacios vectoriales.

Si $\alpha \in m(\mathfrak{a})$ es no nulo, entonces

$$0 = \operatorname{grad}(\alpha) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(\alpha) \operatorname{grad} \mathfrak{P} \geq \sum_{\mathfrak{P}} v_{\mathfrak{P}}(\mathfrak{a}) \operatorname{grad} \mathfrak{P} = \operatorname{grad} \mathfrak{a}.$$

Así pues, si $\operatorname{grad} \mathfrak{a} > 0$ necesariamente $m(\mathfrak{a}) = 0$. Para trabajar con divisores de grado positivo es costumbre definir la dimensión de un divisor como la del espacio de múltiplos de su inverso:

Definición 8.23 Sea $\mathfrak{a}$ un divisor de un cuerpo de funciones algebraicas K sobre el cuerpo de constantes k_0. Definimos la *dimensión* de $\mathfrak{a}$ como

$$\dim \mathfrak{a} = \dim_{k_0} m(\mathfrak{a}^{-1}).$$

No es evidente que la dimensión de un divisor sea finita, pero lo es:

Teorema 8.24 *Si K es un cuerpo de funciones algebraicas, todos los divisores de K tienen dimensión finita.*

DEMOSTRACIÓN: Sea $\mathfrak{a}$ un divisor de K (podemos suponer $\operatorname{grad} \mathfrak{a} \geq 0$) y sea $\mathfrak{P}$ un divisor primo de K tal que $v_{\mathfrak{P}}(\mathfrak{a}) = 0$. Llamemos $g = \operatorname{grad} \mathfrak{P}$. Sea r un número natural no nulo tal que $\dim m(\mathfrak{a}^{-1}) > rg$.

Todo $\alpha \in m(\mathfrak{a}^{-1})$ cumple $v_{\mathfrak{P}}(\alpha) \geq v_{\mathfrak{P}}(\mathfrak{a}^{-1}) = 0$, luego $m(\mathfrak{a}^{-1}) \subset \mathfrak{O}_{\mathfrak{P}}$. Observemos ahora que

$$\dim_{k_0} \mathfrak{O}_{\mathfrak{P}}/\mathfrak{P}^r \leq rg.$$

En efecto, consideramos la sucesión de subespacios vectoriales

$$0 = \mathfrak{P}^r/\mathfrak{P}^r \leq \mathfrak{P}^{r-1}/\mathfrak{P}^r \leq \cdots \leq \mathfrak{P}/\mathfrak{P}^r \leq \mathfrak{O}_{\mathfrak{P}}/\mathfrak{P}^r.$$

Basta ver que cada cociente de dos espacios consecutivos tiene dimensión g. Para el último tenemos que $(\mathfrak{O}_{\mathfrak{P}}/\mathfrak{P}^r)\big/(\mathfrak{P}/\mathfrak{P}^r) \cong \mathfrak{O}_{\mathfrak{P}}/\mathfrak{P} = \overline{K}_{\mathfrak{P}}$, que ciertamente tiene dimensión g sobre k_0.

Para los restantes tenemos que $(\mathfrak{P}^i/\mathfrak{P}^r)\big/(\mathfrak{P}^{i+1}/\mathfrak{P}^r) \cong \mathfrak{P}^i/\mathfrak{P}^{i+1}$. Tomando $\pi \in K$ tal que $v_{\mathfrak{P}}(\pi) = 1$, podemos definir un isomorfismo

$$\overline{K}_{\mathfrak{P}} \longrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1}$$

mediante $[\alpha] \mapsto [\alpha\pi^i]$.

Así pues, si $\alpha_0, \ldots, \alpha_{rg} \in m(\mathfrak{a}^{-1})$ son k_0-linealmente independientes, sus clases módulo $\mathfrak{P}^r$ no pueden serlo, luego existen constantes no todas nulas tales que

$$\theta = a_0\alpha_0 + \cdots + a_{rg}\alpha_{rg} \equiv 0 \ (\text{mód}\ \mathfrak{P}^r).$$

Por lo tanto, $v_{\mathfrak{P}}(\theta) \geq r$. Tenemos que $\theta \in m(\mathfrak{a}^{-1})$ y como los α_i son linealmente independientes, se cumple que $\theta \neq 0$. Por el teorema 7.6 resulta que

$$0 = \operatorname{grad}(\theta) = \sum_{\mathfrak{Q}} v_{\mathfrak{Q}}(\theta) \operatorname{grad} \mathfrak{Q} \geq \sum_{\mathfrak{Q} \neq \mathfrak{P}} v_{\mathfrak{Q}}(\mathfrak{a}^{-1}) \operatorname{grad} \mathfrak{Q} + r \operatorname{grad} \mathfrak{P}.$$

Teniendo en cuenta que $v_{\mathfrak{P}}(\mathfrak{a}^{-1}) = 0$, podemos añadir el término que falta al sumatorio, que pasa a ser $-\operatorname{grad} \mathfrak{a}$. Concluimos que $rg \leq \operatorname{grad} \mathfrak{a}$, luego

$$r \leq \frac{\operatorname{grad} \mathfrak{a}}{g}.$$

Por consiguiente, si r es la parte entera de $g^{-1} \operatorname{grad} \mathfrak{a} + 1$, no puede cumplir la desigualdad de partida, con lo que

$$\dim \mathfrak{a} \leq \left(\frac{\operatorname{grad} \mathfrak{a}}{g} + 1 \right) \operatorname{grad} \mathfrak{P} = \operatorname{grad} \mathfrak{a} + \operatorname{grad} \mathfrak{P}.$$

■

Otra propiedad relevante es que la dimensión del espacio de múltiplos es la misma para los divisores equivalentes. En efecto, de la propia definición se desprende que si $\alpha \in K^*$ entonces $m(\alpha\mathfrak{a}) = \alpha m(\mathfrak{a})$, por lo que la aplicación $u \mapsto \alpha u$ es un automorfismo de K como k_0-espacio vectorial que transforma $m(\mathfrak{a})$ en $m(\alpha\mathfrak{a})$. Por consiguiente podemos hablar de la dimensión de una clase de divisores, así como de la aplicación

$$\dim : \mathcal{D}/P \longrightarrow \mathbb{N}.$$

También hemos visto que las clases de grado negativo tienen dimensión nula. Vamos a calcular ahora la dimensión de las clases de grado 0. Suponemos que k_0 es el cuerpo exacto de constantes de K.

En general, si A es cualquier clase de divisores y $\mathfrak{a} \in A$, para cada $\alpha \in K^*$ se cumple $\alpha \in m(\mathfrak{a}^{-1})$ si y sólo si $(\alpha) = \mathfrak{m}/\mathfrak{a}$ para un cierto divisor entero $\mathfrak{m}$, que de hecho pertenece a la clase A. Recíprocamente, todo divisor entero $\mathfrak{m} \in A$ da lugar a un $\alpha \in m(\mathfrak{a}^{-1})$ que satisface la relación anterior. Según 6.22, dos elementos no nulos de $m(\mathfrak{a}^{-1})$ se corresponden con un mismo divisor $\mathfrak{m}$ si y sólo si se diferencian en un elemento de k_0. (Aquí usamos que k_0 es el cuerpo exacto de constantes.)

Si $\dim A = r$, podemos tomar una k_0-base $\alpha_1, \ldots, \alpha_r$ de $m(\mathfrak{a}^{-1})$ y entonces sus correspondientes divisores enteros $\mathfrak{m}_i$ son distintos dos a dos. Por consiguiente, una clase de divisores A contiene al menos $\dim A$ divisores enteros distintos dos a dos.

Ahora basta tener en cuenta que 1 es el único divisor entero de grado 0, por lo que si $A \neq 1$ es una clase de grado 0, necesariamente $\dim A = 0$. Similarmente $\dim 1 \leq 1$ y, puesto que $k_0 \subset m(1)$, de hecho se da la igualdad y $\dim 1 = 1$. En resumen:

Teorema 8.25 *Si K es un cuerpo de funciones algebraicas sobre el cuerpo exacto de constantes k_0 y $A \in \mathcal{D}/P$ es una clase de divisores de grado 0, entonces*

$$\dim A = \begin{cases} 0 & \textit{si } A \neq 1, \\ 1 & \textit{si } A = 1. \end{cases}$$

Veamos que las extensiones de constantes conservan la dimensión de los divisores (entendida, al igual que el grado, respecto al cuerpo de constantes exacto de cada cuerpo).

Teorema 8.26 *Sea K un cuerpo de funciones algebraicas y L una extensión finita de constantes de K. Sean k_0 y k_1 los respectivos cuerpos de constantes exactos. Entonces la dimensión (respecto a k_0) de un divisor de K coincide con su dimensión (respecto a k_1) como divisor de L. Más concretamente, si $\mathfrak{a}$ es un divisor de K, toda k_0-base de $m_K(\mathfrak{a})$ es una k_1-base de $m_L(\mathfrak{a})$.*

Demostración: Basta probar la última afirmación. Sea $\omega_1, \ldots, \omega_m$ una k_0-base de $m_K(\mathfrak{a})$. En primer lugar, si $\mathfrak{p}$ es un primo de K, tenemos que su descomposición en L es de la forma $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$, donde los primos $\mathfrak{P}_i$ son distintos dos a dos. Por lo tanto las valoraciones $v_{\mathfrak{P}_i}$ extienden a la valoración $v_{\mathfrak{p}}$, y así, si $\alpha \in K$, la relación $v_{\mathfrak{p}}(\alpha) \geq n$ equivale a que $v_{\mathfrak{P}_i}(\alpha) \geq n$ para todo i. De aquí se sigue que $\omega_i \in m_L(\mathfrak{a})$.

Es fácil ver que son linealmente independientes sobre k_1. En efecto, sea $k_1 = k_0(\alpha)$. Si $\sum\limits_i a_i\omega_i = 0$, con $a_i \in k_1$, entonces $a_i = \sum\limits_j b_{ij}\alpha^j$, con $b_{ij} \in k_0$, luego $\sum\limits_{ij} b_{ij}\omega_i\alpha^j = 0$, de donde $\sum\limits_i b_{ij}\omega_i = 0$ y por consiguiente todos los coeficientes b_{ij} son nulos.

Con esto hemos probado que $\dim_K \mathfrak{a} \leq \dim_L \mathfrak{a}$. Si llamamos k_2 a la clausura normal de k_1 sobre k_0 y L' a la extensión de constantes de K asociada a k_2, tendremos que $\dim_K \mathfrak{a} \leq \dim_L \mathfrak{a} \leq \dim_{L'} \mathfrak{a}$, y basta probar la igualdad de los extremos. Equivalentemente, podemos suponer que k_1 es normal sobre k_0.

Tomemos $\beta \in m_L(\mathfrak{a})$. Hemos de probar que es combinación lineal de los elementos ω_i. En principio $\beta = \sum_i a_i \alpha^i$, con $a_i \in K$. Sean $\alpha_1, \ldots, \alpha_n$ los conjugados de α sobre k_0 (y también sobre K). Entonces, las imágenes de β por los K-automorfismos de L son los elementos $\beta_j = \sum_i a_i \alpha_j^i$. Es fácil ver que todos ellos pertenecen a $m_L(\mathfrak{a})$.

La matriz (α_j^i) tiene determinante no nulo (es de Vandermonde), luego podemos despejar $a_i = \sum_i b_{ij}\beta_j$, con $b_{ij} \in k_1$. Puesto que $m_L(\mathfrak{a})$ es un k_1-espacio vectorial, concluimos que $a_i \in m_L(\mathfrak{a}) \cap K \subset m_K(\mathfrak{a})$. Consecuentemente, cada a_i es combinación lineal de los ω_i con coeficientes en k_0, y de aquí que β es combinación lineal de los ω_i con coeficientes en k_1. ■

De aquí extraemos una consecuencia interesante:

Teorema 8.27 *Sea K un cuerpo de funciones algebraicas y L una extensión finita de constantes de K. Entonces un divisor de K es principal como divisor de K si y sólo si es principal como divisor de L. Por consiguiente podemos identificar el grupo de clases de K con un subgrupo del grupo de clases de L.*

DEMOSTRACIÓN: Basta probar la primera afirmación, pero, según 8.25, un divisor $\mathfrak{a}$ es principal si y sólo si $\operatorname{grad} \mathfrak{a} = 0$ y $\dim \mathfrak{a} = 1$, y estas propiedades se conservan en las extensiones finitas de constantes. ■

Esto se generaliza inmediatamente a extensiones infinitas de constantes: todas ellas conservan la dimensión y la equivalencia de divisores, y el grupo de los divisores de una extensión es la unión de los grupos de divisores de las extensiones finitas intermedias.

8.4 El teorema de Riemann-Roch

Ya tenemos casi todos los elementos necesarios para demostrar el teorema fundamental sobre cuerpos de funciones algebraicas. Como ya hemos comentado, se trata de una fórmula que relaciona la dimensión y el grado de un divisor (o, equivalentemente, de una clase de divisores). En esta fórmula interviene una constante asociada al cuerpo que resulta ser una generalización de la noción de género que ya tenemos definida topológicamente cuando el cuerpo de constantes es $\mathbb{C}$. Vamos a seguir la prueba de André Weil, basada en el concepto de elemento ideal que introducimos a continuación.

Definición 8.28 Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0. Llamaremos *elementos ideales aditivos* de K a los elementos α del producto cartesiano de todas las compleciones $K_\mathfrak{P}$ de K que verifican $v_\mathfrak{P}(\alpha_\mathfrak{P}) \geq 0$ salvo a lo sumo para un número finito de primos $\mathfrak{P}$.

El conjunto V_K de todos los elementos ideales aditivos tiene estructura de anillo (con divisores de 0). Podemos identificar cada $\alpha \in K$ con el elemento ideal dado por $\alpha_\mathfrak{P} = \alpha$, para todo divisor primo $\mathfrak{P}$ de K. De este modo, K es un subcuerpo de V_K.

Para cada divisor $\mathfrak{a}$ de K definimos $\Lambda(\mathfrak{a})$ como el conjunto de los elementos ideales $\alpha \in V_K$ tales que $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) \geq -v_{\mathfrak{P}}(\mathfrak{a})$ para todo divisor primo $\mathfrak{P}$ de K.

De este modo se cumple que $\Lambda(\mathfrak{a}) \cap K = m(\mathfrak{a}^{-1})$. Tanto V_K como los conjuntos $\Lambda(\mathfrak{a})$ tienen estructura de k_0-espacio vectorial y la dimensión de la intersección $\Lambda(\mathfrak{a}) \cap K$ es lo que hemos llamado $\dim \mathfrak{a}$.

En general, si B es un espacio vectorial y $A \leq B$, representaremos por $|B : A|$ a la dimensión del espacio cociente B/A.

Es claro que $\mathfrak{a} \mid \mathfrak{b}$ si y sólo si $\Lambda(\mathfrak{a}) \subset \Lambda(\mathfrak{b})$. Vamos a calcular la dimensión del cociente $|\Lambda(\mathfrak{b}) : \Lambda(\mathfrak{a})|$ (sobre k_0).

Teorema 8.29 *Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos divisores de un cuerpo de funciones algebraicas tales que $\mathfrak{a} \mid \mathfrak{b}$. Entonces*

$$|\Lambda(\mathfrak{b}) : \Lambda(\mathfrak{a})| = \operatorname{grad} \mathfrak{b} - \operatorname{grad} \mathfrak{a}.$$

Demostración: Basta probarlo en el caso en que $\mathfrak{b} = \mathfrak{a}\mathfrak{P}$, para un cierto primo $\mathfrak{P}$. Sea K el cuerpo de funciones que estamos considerando y sea $\mathfrak{O}_{\mathfrak{P}} \subset K$ el anillo de enteros respecto a $\mathfrak{P}$. Sea $\pi \in K$ tal que $v_{\mathfrak{P}}(\pi) = 1$ y sea $n = v_{\mathfrak{P}}(\mathfrak{a})$. Consideremos la aplicación $\mathfrak{O}_{\mathfrak{P}} \longrightarrow \Lambda(\mathfrak{b})/\Lambda(\mathfrak{a})$ que a cada $\alpha \in \mathfrak{O}_{\mathfrak{P}}$ le asigna la clase del elemento ideal cuya componente $\mathfrak{P}$-ésima es $\pi^{-n-1}\alpha$ y sus otras componentes son nulas. Claramente se trata de un epimorfismo de espacios vectoriales y su núcleo es $\mathfrak{P}$. Así pues,

$$|\Lambda(\mathfrak{b}) : \Lambda(\mathfrak{a})| = \dim \mathfrak{O}_{\mathfrak{P}}/\mathfrak{P} = \operatorname{grad} \mathfrak{P} = \operatorname{grad} \mathfrak{b} - \operatorname{grad} \mathfrak{a}.$$

■

La siguiente fórmula que necesitamos se prueba más claramente en un contexto general: sean B y C dos subespacios vectoriales de un mismo espacio y $A \leq B$. Entonces

$$|B : A| = |B + C : A + C| + |B \cap C : A \cap C|.$$

En efecto, se cumple

$$\begin{aligned} |B : A| &= |B : A + (B \cap C)| + |A + (B \cap C) : A| \\ &= |B/(B \cap C) : (A + (B \cap C))/(B \cap C)| + |A + (B \cap C) : A|. \end{aligned}$$

La imagen del cociente $(A + (B \cap C))/(B \cap C)$ por el isomorfismo natural $B/(B \cap C) \cong (B + C)/C$ es claramente $(A + C)/C$, luego

$$|B : A| = |(B + C)/C : (A + C)/C| + |B \cap C : A \cap B \cap C|,$$

y de aquí se sigue la fórmula buscada. ■

Nos interesa el caso particular en que $A = \Lambda(\mathfrak{a})$, $B = \Lambda(\mathfrak{b})$ (con $\mathfrak{a} \mid \mathfrak{b}$) y $C = K$. Entonces tenemos

$$|\Lambda(\mathfrak{b}) : \Lambda(\mathfrak{a})| = |\Lambda(\mathfrak{b}) + K : \Lambda(\mathfrak{a}) + K| + |m(\mathfrak{b}^{-1}) : m(\mathfrak{a}^{-1})|.$$

Teniendo en cuenta el teorema anterior concluimos:

Teorema 8.30 *Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos divisores de un cuerpo K de funciones algebraicas tales que $\mathfrak{a} \mid \mathfrak{b}$. Entonces*

$$\operatorname{grad} \mathfrak{b} - \operatorname{grad} \mathfrak{a} = |\Lambda(\mathfrak{b}) + K : \Lambda(\mathfrak{a}) + K| + \dim \mathfrak{b} - \dim \mathfrak{a}.$$

Necesitamos descomponer el índice de esta fórmula como diferencia

$$|V_K : \Lambda(\mathfrak{b}) + K| - |V_K : \Lambda(\mathfrak{a}) + K|,$$

pero para ello hemos de probar que estos índices son finitos.

Conviene introducir la función

$$r(\mathfrak{a}) = \operatorname{grad} \mathfrak{a} - \dim \mathfrak{a},$$

de modo que si $\mathfrak{a} \mid \mathfrak{b}$ se cumple

$$0 \leq |\Lambda(\mathfrak{b}) + K : \Lambda(\mathfrak{a}) + K| = r(\mathfrak{b}) - r(\mathfrak{a}). \tag{8.12}$$

Así pues, la función r es "creciente". Vamos a probar que está acotada superiormente.

Fijemos un $x \in K$ no constante. Sea $k = k_0(x)$, sea $n = |K : k_0(x)|$ y sea $\alpha_1, \ldots, \alpha_n$ una k-base de K. Podemos suponer que los α_i son enteros sobre $k_0[x]$, es decir, que sus polos están en los primos infinitos. Por consiguiente existe un número natural s_0 tal que $\alpha_i \in m(\infty^{-s_0})$.

Tomemos un natural $s > s_0$. Si $0 \leq m \leq s - s_0$ entonces $x^m \alpha_i \in m(\infty^{-s})$. Puesto que estas funciones son linealmente independientes sobre k_0, esto prueba que $\dim \infty^s \geq (s - s_0 + 1)n$.

Llamemos $N_s = |\Lambda(\infty^s) + K : \Lambda(1) + K| \geq 0$. El teorema 8.30 para $\mathfrak{a} = 1$ y $\mathfrak{b} = \infty^s$ nos da

$$sn = \operatorname{grad} \infty^s = N_s + \dim \infty^s - 1 \geq N_s + (s - s_0 + 1)n - 1,$$

luego $N_s \leq s_0 n - n + 1$, para todo $s > s_0$. Por consiguiente

$$r(\infty^s) - r(1) \leq s_0 n - n + 1$$

y así $r(\infty^s) \leq r(1) + s_0 n - n + 1$ para todo $s > s_0$.

Ahora tomamos un divisor arbitrario $\mathfrak{b}$. Sea $p(x) \in k_0[x]$ un polinomio que tenga ceros adecuados en los divisores finitos de $\mathfrak{b}$, de modo que, para un s suficientemente grande, $\mathfrak{b} \mid p(x)\infty^s$. Ahora usamos que la función r es monótona y sólo depende de las clases de los divisores, con lo que

$$r(\mathfrak{b}) \leq r(p(x)\infty^s) = r(\infty^s) \leq r(1) + s_0 n - n + 1.$$

En resumen, tal y como queríamos probar, la función r está acotada superiormente.

El interés de esto se debe a lo siguiente: Si en la fórmula (8.12) fijamos $\mathfrak{a}$, tiene que haber un divisor $\mathfrak{b}$ tal que $\mathfrak{a} \mid \mathfrak{b}$ y el índice $|\Lambda(\mathfrak{b}) + K : \Lambda(\mathfrak{a}) + K|$ sea máximo (pues la función $r(\mathfrak{b})$ está acotada). Por otra parte, tomando $\mathfrak{b}$ suficientemente grande podemos hacer que $\Lambda(\mathfrak{b})$ contenga cualquier elemento prefijado de V_K, luego el grado máximo sólo puede alcanzarse si $\Lambda(\mathfrak{b}) + K = V_K$. Así pues:

Teorema 8.31 *Si K es un cuerpo de funciones algebraicas, existe un divisor $\mathfrak{b}$ en K tal que $V_K = \Lambda(\mathfrak{b}) + K$.*

Más aún, lo que hemos probado es que todo divisor $\mathfrak{a}$ tiene un múltiplo $\mathfrak{b}$ que cumple el teorema anterior, con lo que la fórmula (8.12) nos da que el índice

$$\delta(\mathfrak{a}) = |V_K : \Lambda(\mathfrak{a}) + K|$$

es finito.

Ahora podemos escribir la fórmula del teorema 8.30 como

$$\operatorname{grad} \mathfrak{b} - \operatorname{grad} \mathfrak{a} = \delta(\mathfrak{a}) - \delta(\mathfrak{b}) + \dim \mathfrak{b} - \dim \mathfrak{a},$$

o mejor,

$$\dim \mathfrak{a} - \operatorname{grad} \mathfrak{a} - \delta(\mathfrak{a}) = \dim \mathfrak{b} - \operatorname{grad} \mathfrak{b} - \delta(\mathfrak{b}).$$

En principio, esto se cumple si $\mathfrak{a} \mid \mathfrak{b}$, pero como todo par de divisores tiene un múltiplo común, de hecho vale para todo $\mathfrak{a}$ y todo $\mathfrak{b}$. En definitiva, hemos encontrado un invariante de K, que conviene representar de la forma siguiente:

Definición 8.32 Llamaremos *género* de un cuerpo de funciones algebraicas K al número natural g que cumple

$$\dim \mathfrak{a} - \operatorname{grad} \mathfrak{a} - \delta(\mathfrak{a}) = 1 - g,$$

para todo divisor $\mathfrak{a}$ de K.

Más adelante veremos que si el cuerpo de constantes es $k_0 = \mathbb{C}$, entonces el género que acabamos de definir coincide con el género topológico de Σ_K. De momento observemos que se trata ciertamente de un número natural, pues si tomamos $\mathfrak{a} = 1$ queda

$$g = \delta(1) = |V_K : \Lambda(1) + K|.$$

La ecuación que define a g es, equivalentemente,

$$\dim \mathfrak{a} = \operatorname{grad} \mathfrak{a} - (g - 1) + \delta(\mathfrak{a}),$$

donde $\delta(\mathfrak{a}) \geq 0$. Esta fórmula es casi el teorema de Riemann-Roch. Sólo falta sustituir $\delta(\mathfrak{a})$ por una expresión que no involucre elementos ideales.

Definición 8.33 Si K es un cuerpo de funciones algebraicas, una *diferencial* de V_K es una aplicación lineal $\lambda : V_K \longrightarrow k_0$ que se anula en un conjunto de la forma $\Lambda(\mathfrak{a}) + K$, para cierto divisor $\mathfrak{a}$ de K.

Veremos enseguida que estas diferenciales pueden identificarse con las formas diferenciales de K definidas anteriormente. Para ello necesitamos algunos hechos básicos sobre ellas que ya conocemos para formas diferenciales.

El conjunto de las diferenciales de V_K tiene estructura de k_0-espacio vectorial. El conjunto de aquellas que se anulan en un conjunto $\Lambda(\mathfrak{a}) + K$ fijo es un subespacio vectorial, isomorfo al dual del espacio cociente $V_K/(\Lambda(\mathfrak{a})+K)$, luego su dimensión es $\delta(\mathfrak{a})$.

Podemos dotar al espacio de las diferenciales de estructura de K-espacio vectorial. Para ello, si λ es una diferencial que se anula en $\Lambda(\mathfrak{a})+K$ y $x \in K$, definimos $x\lambda$ mediante $(x\lambda)(\alpha) = \lambda(x\alpha)$. Ciertamente $x\lambda$ es k_0-lineal y se anula en $\Lambda((x)\mathfrak{a})+K$.

Teorema 8.34 *Sea K un cuerpo de funciones algebraicas y λ una diferencial no nula de su espacio de elementos ideales. Entonces la familia de los conjuntos $\Lambda(\mathfrak{a})$ donde se anula λ tiene un máximo respecto a la inclusión.*

Demostración: En primer lugar observamos que si λ se anula en $\Lambda(\mathfrak{a}_1)$ y en $\Lambda(\mathfrak{a}_2)$, entonces también se anula en

$$\Lambda(\mathfrak{a}_1)+\Lambda(\mathfrak{a}_2) = \Lambda(\operatorname{mcm}(\mathfrak{a}_1,\mathfrak{a}_2)).$$

Esta igualdad se prueba fácilmente a partir de la relación (en $K_{\mathfrak{P}}$)

$$\mathfrak{P}^m + \mathfrak{P}^n = \mathfrak{P}^{\min\{\mathrm{m,n}\}}.$$

En vista de esto basta demostrar que el grado de los divisores $\mathfrak{a}$ tales que λ se anula en $\Lambda(\mathfrak{a})$ está acotado, pues si $\mathfrak{a}$ tiene grado máximo, entonces $\Lambda(\mathfrak{a})$ cumple lo pedido.

Sea, pues, $\mathfrak{a}$ un divisor tal que λ se anula en $\Lambda(\mathfrak{a})$ y sea $\mathfrak{b}$ un divisor arbitrario. Tomemos $x \in m(\mathfrak{b}^{-1})$. Entonces $x\lambda$ se anula en $\Lambda((x)\mathfrak{a})$ y, como $\mathfrak{a}\mathfrak{b}^{-1} \mid (x)\mathfrak{a}$, también en $\Lambda(\mathfrak{a}\mathfrak{b}^{-1})$. Si $x_1,\ldots,x_n \in m(\mathfrak{b}^{-1})$ son linealmente independientes sobre k_0, lo mismo les sucede a $x_1\lambda,\ldots,x_n\lambda$ (ya que por hipótesis $\lambda \neq 0$), luego $\delta(\mathfrak{a}\mathfrak{b}^{-1}) \geq \dim \mathfrak{b}$.

La definición del género de K nos da que

$$\begin{aligned}\dim(\mathfrak{a}\mathfrak{b}^{-1}) - \operatorname{grad}\mathfrak{a} + \operatorname{grad}\mathfrak{b} + (g-1) = \delta(\mathfrak{a}\mathfrak{b}^{-1}) &\geq \dim \mathfrak{b}\\ &= \operatorname{grad}\mathfrak{b} - (g-1) + \delta(\mathfrak{b}),\end{aligned}$$

luego

$$\operatorname{grad}\mathfrak{a} \leq \dim(\mathfrak{a}\mathfrak{b}^{-1}) + 2g - 2 - \delta(\mathfrak{b}) \leq \dim(\mathfrak{a}\mathfrak{b}^{-1}) + 2g - 2.$$

Ahora basta tomar un divisor $\mathfrak{b}$ de grado suficientemente grande como para que $\operatorname{grad}(\mathfrak{a}\mathfrak{b}^{-1}) \leq 0$, con lo que $\dim(\mathfrak{a}\mathfrak{b}^{-1}) = 0$ y concluimos que $\operatorname{grad}\mathfrak{a} \leq 2g-2$.

■

En las condiciones de este teorema, es claro que el divisor $\mathfrak{a}$ está completamente determinado por $\Lambda(\mathfrak{a})$ y por lo tanto por λ.

Definición 8.35 Sea K un cuerpo de funciones algebraicas y λ una diferencial no nula de V_K. Llamaremos *divisor asociado* a λ al mayor divisor $\mathfrak{a}$ de K tal que λ se anula en $\Lambda(\mathfrak{a})$. Lo representaremos por (λ).

Teorema 8.36 *Sea K un cuerpo de funciones algebraicas. El espacio de las diferenciales de V_K tiene dimensión 1 sobre K.*

DEMOSTRACIÓN: Supongamos que λ y μ son dos diferenciales linealmente independientes sobre K. Entonces, si $x_1, \ldots, x_n \in K$ son linealmente independientes sobre el cuerpo de constantes k_0, se cumple que $x_1\lambda, \ldots, x_n\lambda, x_1\mu, \ldots, x_n\mu$ son linealmente independientes sobre k_0, pues si

$$\sum a_i x_i \lambda + \sum b_i x_i \mu = 0, \qquad \text{con } a_i, b_i \in k_0,$$

la independencia de λ y μ obliga a que $\sum a_i x_i = \sum b_i x_i = 0$, luego $a_i = b_i = 0$ para todo i.

Sea $\mathfrak{a}$ un divisor tal que λ y μ se anulen en $\Lambda(\mathfrak{a})$. Podemos tomar el mismo pues, claramente, $\Lambda(\mathfrak{a}) \cap \Lambda(\mathfrak{b}) = \Lambda(\operatorname{mcd}(\mathfrak{a}, \mathfrak{b}))$.

Sea $\mathfrak{b}$ un divisor arbitrario. Si $x \in m(\mathfrak{b}^{-1})$ entonces $x\lambda$ se anula en $\Lambda((x)\mathfrak{a})$, que contiene a $\Lambda(\mathfrak{a}\mathfrak{b}^{-1})$. Similarmente, $x\mu$ se anula en $\Lambda(\mathfrak{a}\mathfrak{b}^{-1})$, luego podemos concluir que $\delta(\mathfrak{a}\mathfrak{b}^{-1}) \geq 2 \dim \mathfrak{b}$. Ahora la definición de género nos da que

$$\dim(\mathfrak{a}\mathfrak{b}^{-1}) - \operatorname{grad} \mathfrak{a} + \operatorname{grad} \mathfrak{b} + (g-1) \geq 2 \dim \mathfrak{b}$$

$$= 2(\operatorname{grad} \mathfrak{b} - (g-1) + \delta(\mathfrak{b})) \geq 2 \operatorname{grad} \mathfrak{b} - 2(g-1).$$

Tomamos $\mathfrak{b}$ de grado suficientemente grande como para que $\dim(\mathfrak{a}\mathfrak{b}^{-1}) = 0$, la fórmula anterior nos da que el grado de $\mathfrak{b}$ está acotado superiormente, lo cual es absurdo, pues $\mathfrak{b}$ es arbitrario. ■

Ahora ya podemos interpretar las diferenciales de V_K en términos de formas diferenciales de K. Para ello observemos que si ω es una forma diferencial de K, para cada elemento ideal $\alpha \in V_K$ podemos definir

$$\int \alpha\omega = \sum_{\mathfrak{P}} \oint_{\mathfrak{P}} \alpha_{\mathfrak{P}} \omega_{\mathfrak{P}}.$$

Este operador integral es claramente k_0-lineal. Por el teorema de los residuos se anula en K y claramente también se anula en $\Lambda(\omega)$. Por consiguiente este operador integral es una diferencial de V_K en el sentido de 8.33. La aplicación que a cada forma ω le asigna su operador integral en V_K es K-lineal y no nula. Como el espacio de formas diferenciales de K y el de diferenciales de V_K tienen ambos dimensión 1, de hecho tenemos un isomorfismo entre ellos.

Más aún, se cumple que (ω) es el mayor divisor $\mathfrak{a}$ tal que la diferencial asociada a ω se anula en $\Lambda(\mathfrak{a})$, pues si $(\omega) \mid \mathfrak{a}$ y $v_{\mathfrak{P}}(\mathfrak{a}) > v_{\mathfrak{P}}(\omega)$ para un primo $\mathfrak{P}$, podemos tomar $\alpha \in \Lambda(\mathfrak{a})$ de modo que $v_{\mathfrak{P}}(\alpha) = -v_{\mathfrak{P}}(\omega) - 1$ y $v_{\mathfrak{Q}}(\alpha) = -v_{\mathfrak{Q}}(\omega)$ para $\mathfrak{Q} \neq \mathfrak{P}$ y entonces

$$\int \alpha\omega = \oint_{\mathfrak{P}} \alpha_{\mathfrak{P}} \omega_{\mathfrak{P}} = \operatorname{Tr}_{k_0}^{k_{0\mathfrak{P}}}(\operatorname{Res}_{\mathfrak{P}}(\alpha_{\mathfrak{P}} \omega_{\mathfrak{P}})).$$

Como $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}} \omega_{\mathfrak{P}}) = -1$, se cumple que $\operatorname{Res}_{\mathfrak{P}}(\alpha_{\mathfrak{P}} \omega_{\mathfrak{P}}) \neq 0$ y multiplicando $\alpha_{\mathfrak{P}}$ por un elemento adecuado de $k_{0\mathfrak{P}}$ podemos exigir que la traza sea también no nula (porque la traza de una extensión separable no puede ser nula).

Esto prueba que el divisor asociado a una forma diferencial es el mismo que el asociado a su operador integral. Por consiguiente, los divisores asociados a las diferenciales de V_K son precisamente los divisores de la clase canónica de K.

Finalmente podemos probar:

Teorema 8.37 (Riemann-Roch) *Si K es un cuerpo de funciones algebraicas y A es una clase de divisores de K, entonces*

$$\dim A = \operatorname{grad} A - (g-1) + \dim(W/A),$$

donde W es la clase canónica y g es el género de K.

DEMOSTRACIÓN: Sea $\mathfrak{c}$ un divisor de la clase canónica. Sólo hemos de probar que, para todo divisor $\mathfrak{a}$ de K, se cumple $\delta(\mathfrak{a}) = \dim(\mathfrak{c}\mathfrak{a}^{-1})$. Sea λ una diferencial tal que $(\lambda) = \mathfrak{c}$.

Si $\mathfrak{b}$ es un divisor arbitrario y $x \in m(\mathfrak{b}^{-1})$, entonces $(x\lambda) = (\mathfrak{c}\mathfrak{b}^{-1})$, es decir, $x\lambda$ se anula en $\Lambda(\mathfrak{c}\mathfrak{b}^{-1})$. Recíprocamente, si $x\lambda$ es una diferencial que se anula en $\Lambda(\mathfrak{c}\mathfrak{b}^{-1})$ entonces $\mathfrak{c}\mathfrak{b}^{-1} \mid (x\lambda) = (x)\mathfrak{c}$, luego $x \in m(\mathfrak{b}^{-1})$.

Hemos probado que $\delta(\mathfrak{c}\mathfrak{b}^{-1}) = \dim \mathfrak{b}$. Esto vale para todo divisor $\mathfrak{b}$. Tomando $\mathfrak{b} = \mathfrak{c}\mathfrak{a}^{-1}$ resulta $\delta(\mathfrak{a}) = \dim(\mathfrak{c}\mathfrak{a}^{-1})$. ■

Es imposible explicar aquí la trascendencia de este teorema. Ésta empezará a ponerse de manifiesto en el capítulo siguiente, dedicado por completo a mostrar sus consecuencias más destacadas. Ahora veremos únicamente las más inmediatas, que nos terminan de perfilar el concepto de género.

El género y la clase canónica En primer lugar veamos que el teorema de Riemann-Roch nos permite caracterizar el género de un cuerpo de funciones en términos más naturales y operativos que la definición que hemos dado. Así, el teorema siguiente muestra que el género puede definirse como la dimensión de la clase canónica, o también en función de su grado. Recíprocamente, la clase canónica puede caracterizarse en términos del género:

Teorema 8.38 *Sea K un cuerpo de funciones algebraicas de género g. Entonces la clase canónica de K es la única clase W que cumple*

$$\dim W = g, \qquad \operatorname{grad} W = 2g-2.$$

DEMOSTRACIÓN: La primera igualdad se obtiene haciendo $A = 1$ en el teorema de Riemann-Roch. La segunda con $A = W$. Si otra clase W' cumple esto mismo, entonces el teorema de Riemann-Roch nos da que $\dim(W/W') = 1$ y, por otra parte, $\operatorname{grad}(W/W') = 0$, luego 8.25 implica que $W/W' = 1$, y así $W' = W$. ■

También podemos caracterizar el género en términos de la dimensión y el grado de divisores sin involucrar la clase canónica. Para ello observamos que si $\operatorname{grad} A > 2g-2$, entonces $\operatorname{grad}(W/A) < 0$, luego $\dim(W/A) = 0$ y así, el teorema de Riemann-Roch se reduce a

$$\dim A = \operatorname{grad} A - (g-1), \qquad (\text{si } \operatorname{grad} A > 2g-2).$$

Esto se conoce como la *parte de Riemann* del teorema de Riemann-Roch, y permite definir el género de un cuerpo de funciones algebraicas como el valor

$$g = \operatorname{grad} A - \dim A + 1,$$

para cualquier clase A de grado suficientemente grande.

Por ejemplo, de aquí se sigue que el género se conserva en las extensiones de constantes (calculado respecto al cuerpo exacto de constantes de cada cuerpo). Basta tener el cuenta que las extensiones de constantes conservan la dimensión y el grado de los divisores. Más en general, ahora vemos la forma en que el género depende del cuerpo de constantes:

Teorema 8.39 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 y sea $k_1 \subset K$ una extensión finita de k_0. Sean g_0 y g_1 el género de K respecto a k_0 y k_1 respectivamente, entonces*

$$2g_0 - 2 = |k_1 : k_0|(2g_1 - 2).$$

DEMOSTRACIÓN: Basta tener en cuenta que $2g - 2 = 2 \operatorname{grad} A - 2 \dim A$ para toda clase de grado suficientemente grande. ■

Otra consecuencia sencilla es que los cuerpos de fracciones algebraicas tienen género 0. En efecto, según el teorema 8.16, la clase canónica es $W = [\infty^{-2}]$, luego $\dim W = -2$, y el teorema 8.38 implica entonces que el género es $g = 0$.

Relación entre el grado y la dimensión La importancia del teorema de Riemann-Roch reside esencialmente en que permite expresar explícitamente la dimensión de una clase de divisores en función de su grado, salvo para las clases con grado $0 < n < 2g - 2$. Basta tener presente que $\dim A = 0$ si $\operatorname{grad} A < 0$ (y por lo tanto $\dim(W/A) = 0$ si $\operatorname{grad} A > 2g - 2$), así como el teorema 8.25 para las clases de grado 0. El teorema siguiente es una comprobación rutinaria:

Teorema 8.40 *Sea K un cuerpo de funciones algebraicas de género g. Sea W su clase canónica y sea A_n una clase de divisores de K de grado n. Entonces*

- *Si $g = 0$,*
$$\dim A_n = \begin{cases} 0 & \text{si } n < 0, \\ n+1 & \text{si } n \geq 0. \end{cases}$$

- *Si $g = 1$,*
$$\dim A_n = \begin{cases} 0 & \text{si } n < 0, \\ n & \text{si } n > 0, \end{cases} \qquad \dim A_0 = \begin{cases} 1 & \text{si } A_0 = 1, \\ 0 & \text{si } A_0 \neq 1. \end{cases}$$

- *Si $g \geq 2$,*
$$\dim A_n = \begin{cases} 0 & \text{si } n < 0, \\ n - (g-1) & \text{si } n > 2g-2, \end{cases}$$
$$\dim A_0 = \begin{cases} 1 & \text{si } A_0 = 1, \\ 0 & \text{si } A_0 \neq 1, \end{cases} \qquad \dim A_{2g-2} = \begin{cases} g & \text{si } A_{2g-2} = W, \\ g-1 & \text{si } A_{2g-2} \neq W. \end{cases}$$

La fórmula del género de Hurwitz Para terminar probaremos que el género de un cuerpo de funciones algebraicas sobre $\mathbb{C}$ coincide con el que ya teníamos definido. Para ello probaremos una fórmula general que se particulariza a la que ya conocíamos para calcular el género en el caso complejo.

Teorema 8.41 (Fórmula de Hurwitz) *Sea K/k una extensión separable de cuerpos de funciones algebraicas. Sean g_K y g_k los géneros respectivos y sea $\mathfrak{D}_{K/k}$ el diferente de la extensión. Entonces*

$$2g_K - 2 = |K:k|(2g_k - 2) + \operatorname{grad}_K \mathfrak{D}_{K/k}.$$

Demostración: Sea $\mathfrak{c}$ un divisor de la clase canónica de k. De 8.16 se sigue que $\mathfrak{D}_{K/k}\mathfrak{c}$ está en la clase canónica de K. Así,

$$\begin{aligned} 2g_K - 2 &= \operatorname{grad}_K(\mathfrak{D}_{K/k}\mathfrak{c}) = \operatorname{grad}_K \mathfrak{D}_{K/k} + \operatorname{grad}_K \mathfrak{c} \\ &= \operatorname{grad}_K \mathfrak{D}_{K/k} + |K:k|(2g_k - 2). \end{aligned}$$

■

Teniendo en cuenta el teorema 7.36 (y la forma en que 7.33 se usa en la prueba) podemos dar una versión más explícita de la fórmula de Hurwitz:

Teorema 8.42 (Fórmula de Hurwitz) *Sea K/k una extensión separable de cuerpos de funciones algebraicas y sean g_K, g_k sus géneros respectivos. Entonces*

$$2g_K - 2 \geq |K:k|(2g_k - 2) + \sum_{\mathfrak{P}} (e_{\mathfrak{P}} - 1) \operatorname{grad}_K \mathfrak{P},$$

y la igualdad se da exactamente si $\operatorname{car} k = 0$ *o bien* $\operatorname{car} k = p$ *es un primo que no divide a ningún índice de ramificación* $e_{\mathfrak{P}}$.

En particular, si k_0 es un cuerpo algebraicamente cerrado de característica 0 y $k = k_0(x)$, la fórmula de Hurwitz se reduce a

$$2 - 2g = 2|K:k| - \sum_{\mathfrak{P}} (e_{\mathfrak{P}} - 1),$$

Comparando con 6.28 podemos concluir lo que ya habíamos anunciado:

Teorema 8.43 *Si K es un cuerpo de funciones algebraicas sobre $\mathbb{C}$, entonces el género definido en* 8.32 *coincide con el género topológico de la superficie de Riemann Σ_K.*

En particular, si definimos el género de una curva cuasiproyectiva como el de su cuerpo de funciones racionales, tenemos que esta definición extiende a la que ya teníamos para el caso complejo.

Ejercicio: Sea $\phi : S \longrightarrow T$ una aplicación holomorfa no constante entre superficies de Riemann (compactas). Demostrar que el género de T es menor o igual que el de S. Si S y T tienen el mismo género $g \geq 2$, entonces ϕ es biyectiva. Si ambas tienen género $g = 1$, entonces ϕ es localmente inyectiva (no tiene puntos de ramificación).

Capítulo IX

Consecuencias del teorema de Riemann-Roch

En el capítulo anterior hemos demostrado el teorema de Riemann-Roch, que a primera vista es una fórmula técnica no muy sugerente. No obstante, ya hemos podido vislumbrar su importancia en cuanto que nos ha permitido dar una definición puramente algebraica del género de un cuerpo de funciones, con lo cual hemos caracterizado y generalizado la noción topológica de género que conocíamos para curvas algebraicas complejas. Aunque esta noción algebraica de género va a ser fundamental en el estudio de los cuerpos de funciones algebraicas, lo cierto es que con ello no hemos visto más que una mínima parte de las posibilidades del teorema de Riemann-Roch.

9.1 Consecuencias inmediatas

Recogemos en esta primera sección algunas aplicaciones variadas del teorema de Riemann-Roch.

El grado mínimo En el capítulo anterior hemos visto que los cuerpos de fracciones algebraicas tienen género 0. El recíproco es cierto casi siempre, pero no siempre. Para entender la situación definimos el *grado mínimo* f_0 de un cuerpo de funciones algebraicas K como el menor grado positivo de un divisor de K.

Puesto que el grado es un homomorfismo de grupos, el grado de todo divisor es múltiplo de f_0 y todo múltiplo de f_0 es el grado de un divisor. Si g es el género de K, la clase canónica tiene grado $2g-2$, luego $f_0 \mid 2g-2$. Esto limita las posibilidades para el grado mínimo de un cuerpo de género g excepto si $g = 1$. Puede probarse que existen cuerpos de género $g = 1$ con grado mínimo arbitrariamente grande.

Si K es un cuerpo de fracciones algebraicas o el cuerpo de constantes es algebraicamente cerrado, se cumple trivialmente que $f_0 = 1$. El teorema 9.29

(más abajo) prueba que también es éste el caso si el cuerpo de constantes es finito.

El teorema siguiente muestra que el género y el grado mínimo determinan lo "lejos" que está un cuerpo de funciones algebraicas de ser un cuerpo de fracciones:

Teorema 9.1 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes exacto k_0, sea g su género y f_0 su grado mínimo. Entonces existe un $x \in K$ separador tal que $|K : k_0(x)| \leq g + f_0$.*

DEMOSTRACIÓN: Del teorema de Riemann-Roch se sigue que toda clase A con $\operatorname{grad} A \geq g + 1$ cumple $\dim A \geq 2$. Podemos tomar, pues, una clase A de grado mínimo rf_0 tal que $\dim A \geq 2$. Ciertamente $r > 0$ y por la minimalidad, una clase B con $\operatorname{grad} B = (r-1)f_0$ cumple $\dim B < 2$, luego $(r-1)f_0 < g+1$, luego $(r-1)f_0 \leq g$ y así $rf_0 \leq g + f_0$.

Sea $\mathfrak{b}$ un divisor entero contenido en la clase A (ver las observaciones previas al teorema 8.25). Tomamos $x \in m(\mathfrak{b}^{-1})$ no constante. Entonces $(x) = \mathfrak{a}/\mathfrak{b}$, donde $\mathfrak{a}$ es un divisor entero en A. Además $\mathfrak{a} \neq \mathfrak{b}$. Simplificando divisores comunes llegamos a $(x) = \mathfrak{a}'/\mathfrak{b}'$, donde $\operatorname{grad} \mathfrak{a}' = \operatorname{grad} \mathfrak{b}' \leq rf_0 \leq g + f_0$.

Respecto al cuerpo $k = k_0(x)$, el divisor $\mathfrak{b}'$ es ∞, luego es un divisor de k de grado 1. Por consiguiente

$$|K : k_0(x)| = \operatorname{grad}_K \mathfrak{b}' \leq g + f_0.$$

Falta probar que x es separador. Si no lo fuera, según el teorema 8.12 podríamos expresarlo como $x = t^p$, donde p es la característica de K. Entonces $(t) = \mathfrak{a}''/\mathfrak{b}''$, donde $\operatorname{grad} \mathfrak{b}'' < \operatorname{grad} \mathfrak{b} \leq rf_0$, pero entonces $t \in m(\mathfrak{b}''^{-1})$, y también $1 \in m(\mathfrak{b}''^{-1})$, pues $(1) = \mathfrak{b}''/\mathfrak{b}''$, luego $\dim \mathfrak{b}'' \geq 2$, en contradicción con la minimalidad de r. ∎

En particular tenemos la siguiente caracterización de los cuerpos de fracciones algebraicas:

Teorema 9.2 *Un cuerpo de funciones algebraicas K sobre un cuerpo de constantes exacto k_0 es un cuerpo de fracciones algebraicas si y sólo si tiene género 0 y tiene un divisor de grado 1 (es decir, si $f_0 = 1$).*

En particular, sobre un cuerpo de constantes algebraicamente cerrado o finito los cuerpos de fracciones algebraicas son exactamente los de género 0.

Una cota para el género Vamos a estimar el género de un cuerpo de funciones algebraicas en términos del grado de una ecuación entre sus generadores.

Teorema 9.3 *Sea $K = k_0(x, y)$ un cuerpo de funciones algebraicas tal que sus generadores satisfagan una ecuación polinómica irreducible $F(x, y) = 0$ de grado n. Entonces el género g de K satisface la desigualdad*

$$g \leq \frac{(n-1)(n-2)}{2}.$$

En particular, el género de una curva plana de grado n satisface esta relación.

DEMOSTRACIÓN: Podemos suponer que k_0 es algebraicamente cerrado, pues las extensiones de constantes conservan el género. Es fácil ver que el polinomio F sigue siendo irreducible tras la extensión, aunque no necesitamos este hecho, pues si F fuera reducible, pasaríamos a un factor de menor grado.

También podemos suponer que el coeficiente de y^n en $F(x, y)$ es 1. En caso contrario, sea F_n la forma de grado n de F. El cambio $x = x' + ay'$, $y = y'$ nos da un nuevo polinomio $F(x' + ay', y')$ en el que el coeficiente de y'^n es $F_n(a, 1)$. El polinomio $F_n(x, 1)$ no puede ser idénticamente nulo, luego existe $a \in k_0$ tal que $F_n(a, 1) \neq 0$ y así los nuevos generadores x', y' cumplen que el coeficiente de y'^n es no nulo. Dividiendo la ecuación entre este coeficiente lo convertimos en 1.

Sea ∞ el primo infinito de $k = k_0(x)$. Dividiendo $F(x, y) = 0$ entre x^n obtenemos un polinomio mónico con coeficientes en $\mathfrak{o}_\infty$ con raíz y/x. Así pues, y/x es entero sobre $\mathfrak{o}_\infty$, luego el teorema 5.35 implica que $v_{\mathfrak{P}}(y/x) \geq 0$, para todo primo $\mathfrak{P}$ de K que divida a ∞. Equivalentemente, $v_{\mathfrak{P}}(y) \geq v_{\mathfrak{P}}(x)$.

Similarmente, $F(x, t)$ es un polinomio con coeficientes en $\mathfrak{o}_{\mathfrak{p}}$ para todo primo finito $\mathfrak{p}$ de k y tiene a y por raíz, luego $v_{\mathfrak{P}}(y) \geq 0$ para todo primo $\mathfrak{P}$ de K que divida a un primo finito de k.

Ahora es claro que $m(\infty^{-s})$ contiene todas las funciones de la forma

$$f_s(x), \quad y f_{s-1}(x), \quad \ldots, \quad y^{n-1} f_{s-n+1}(x),$$

donde $f_i(x)$ es cualquier polinomio en x de grado i. Por consiguiente,

$$\dim \infty^s \geq (s+1) + s + \cdots + (s-n+2) = ns + 1 - \frac{(n-1)(n-2)}{2}.$$

Por otro lado, $\operatorname{grad} \infty^s = ns$ y, para s suficientemente grande,

$$g = \operatorname{grad} \infty^s - \dim \infty^s + 1 \leq \frac{(n-1)(n-2)}{2}.$$

■

En particular vemos que las rectas y las cónicas tienen género 0, mientras que las cúbicas tienen género ≤ 1. El teorema del apartado siguiente muestra que las cúbicas regulares tienen, de hecho, género 1.

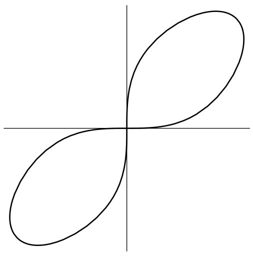
Curvas algebraicas El teorema 8.18 nos proporciona un refinamiento del teorema anterior que nos proporciona el valor exacto del género de muchas curvas planas:

Teorema 9.4 *Sea V una curva proyectiva plana de grado n cuyas singularidades sean todas ordinarias. Entonces su género es*

$$g = \frac{(n-1)(n-2)}{2} - \sum_P \frac{m_P(V)(m_P(V)-1)}{2},$$

donde P recorre los puntos (singulares) de V.

Ejemplo *La curva $X^4 + Y^4 = XY$ tiene género 2, luego no es birracionalmente equivalente a ninguna curva plana regular.*



En efecto, es fácil ver que su única singularidad es el punto $P = (0, 0)$, que es un punto doble ordinario con tangentes $X = 0$ e $Y = 0$. Podemos aplicar el teorema anterior y concluir que el género es

$$g = \frac{(4-1)(4-2)}{2} - \frac{2(2-1)}{2} = 2.$$

El teorema implica también que el género de una curva plana regular ha de ser $g = 0, 1, 3, 6, \ldots$ luego la regularización de esta curva no puede sumergirse en P^2. ■

Por otra parte, el ejemplo de la página 234 se generaliza trivialmente a cuerpos de constantes arbitrarios, por lo que existen curvas (planas) de todos los géneros:

Teorema 9.5 *Si $g \geq 0$, las curvas $Y^2 = F(X)$, donde $F(X) \in k_0[X]$ es un polinomio de grado $2g + 1$ o $2g + 2$ sin raíces múltiples, tienen género g.*

Observemos de paso que la fórmula del teorema 9.4 no es aplicable a curvas con singularidades no ordinarias. Por ejemplo, la curva

$$Y^2 = (X-1)(X-2)(X-3)(X-4)$$

tiene una única singularidad en el infinito (no ordinaria) de orden 2. El teorema anterior implica que tiene género $g = 1$, mientras que la fórmula del teorema 9.4 daría $g = 2$.

Cuerpos elípticos e hiperelípticos Las curvas del teorema anterior constituyen una familia un poco más general de lo que podría parecer: sus cuerpos de funciones se caracterizan por ser extensiones cuadráticas de un cuerpo de fracciones algebraicas. Antes de probarlo conviene introducir algunos conceptos:

Definición 9.6 Un cuerpo K de funciones algebraicas es *elíptico* (resp. *hiperelíptico*) si tiene género $g = 1$ (resp. $g \geq 2$) y es una extensión cuadrática de un cuerpo de fracciones algebraicas. Una curva proyectiva regular es *elíptica* o *hiperelíptica* si lo es su cuerpo de funciones racionales.

Equivalentemente, un cuerpo K de género $g > 0$ es elíptico o hiperelíptico si y sólo si tiene una función x cuyos polos formen un divisor de grado 2. En efecto, si existe tal x, consideramos $k = k_0(x)$ y llamamos ∞ al primo infinito de k. Entonces ∞ es el único polo de x en k, luego sus polos en K son los divisores de ∞. La hipótesis es, pues, que ∞ tiene grado 2 en K, luego ha de ser $|K : k| = 2$. Esto implica que K es elíptico o hiperelíptico, según su género. Recíprocamente, si $|K : k| = 2$, donde $k = k_0(x)$, entonces la función x tiene por polos en K a los divisores de ∞, el cual tiene grado 2 en K.

Observemos que este mismo razonamiento prueba que un cuerpo que contenga una función con un único polo de grado 1 ha de ser un cuerpo de fracciones algebraicas.

Teorema 9.7 *Todo cuerpo de género $g = 1$ y grado mínimo $f_0 = 1$ es elíptico. Todo cuerpo de género $g = 2$ es hiperelíptico.*

DEMOSTRACIÓN: Si K es un cuerpo de género 1 y tiene un divisor $\mathfrak{a}$ de grado 1, entonces el teorema de Riemann-Roch implica que $\dim \mathfrak{a} = 1$, luego $\mathfrak{a}$ es equivalente a un divisor entero $\mathfrak{P}$ también de grado 1, luego $\mathfrak{P}$ es primo.

Por otra parte $\dim \mathfrak{P}^2 = 2$, luego existe una función $x \in m(\mathfrak{P}^{-2})$ no constante. Esto significa que x tiene a lo sumo un polo doble en $\mathfrak{P}$, pero no puede tener un polo simple porque entonces K tendría género 0, luego, en efecto, K es elíptico.

Supongamos ahora que K tiene género $g = 2$. Podemos tomar un divisor entero $\mathfrak{a}$ en la clase canónica W. Entonces $\operatorname{grad} \mathfrak{a} = 2g - 2 = 2$ y $\dim \mathfrak{a} = g = 2$. Tomamos una función $x \in m(\mathfrak{a}^{-1})$ no constante y llamamos $k = k_0(x)$. Es claro que $\mathfrak{a}$ es el primo infinito de k, luego $|K : k| = 2$ y así K es hiperelíptico. ■

Más adelante veremos que hay cuerpos de género 3 que no son hiperelípticos.

Supongamos ahora que el cuerpo k_0 es algebraicamente cerrado y sea K un cuerpo elíptico o hiperelíptico. Entonces $K = k_0(x, u)$, donde u satisface una ecuación

$$u^2 + R(x)u + S(x) = 0, \qquad R(x),\ S(x) \in k_0(x).$$

Cambiando u por $u' = u + R(x)/2$ tenemos igualmente $K = k_0(x, u')$ pero ahora u' satisface una ecuación

$$u'^2 = T(x), \qquad T(x) \in k_0(x).$$

Digamos que

$$T(x) = \frac{a_0(x - a_1) \cdots (x - a_m)}{(x - b_1) \cdots (x - b_n)}, \qquad a_i,\ b_i \in k_0.$$

Cambiando u' por $u'' = u'(x - b_1) \cdots (x - b_m)$ tenemos igualmente que $K = k_0(x, u'')$ y ahora

$$u''^2 = a_0(x - a_1) \cdots (x - a_m)(x - b_1) \cdots (x - b_n).$$

Dividiendo u'' entre una raíz cuadrada de a_0 podemos suponer $a_0 = 1$. Si dos raíces del polinomio de la derecha son iguales, digamos $a_1 = a_2$, sustituimos u'' por $u''/(x-a_1)$, con lo que se sigue cumpliendo $K = k_0(x, u'')$ y la raíz doble desaparece de la ecuación. Repitiendo este proceso llegamos a que $K = k_0(x, y)$, donde y satisface una ecuación $y^2 = F(x)$ y $F(X) \in k_0[X]$ es un polinomio mónico sin raíces múltiples.

Más aún, podemos exigir que F tenga grado impar, pues si

$$y^2 = (x - a_1) \cdots (x - a_k),$$

con $k = 2m + 2$, cambiamos x por $x' = 1/(x - a_k)$ e y por

$$y' = \frac{x'^{m+1}y}{\sqrt{\prod_{i=1}^{k-1}(a_i - a_k)}},$$

de modo que se sigue cumpliendo $K = k_0(x', y')$ y además

$$y'^2 = (x' - b_1) \cdots (x' - b_{k-1}),$$

donde los $b_i \in k_0$ son distintos dos a dos. Con esto hemos probado:

Teorema 9.8 *Si K es un cuerpo elíptico o hiperelíptico de género g sobre un cuerpo de constantes k_0 algebraicamente cerrado, entonces $K = k_0(x, y)$, donde x, y satisfacen una ecuación de la forma $y^2 = F(x)$, para un cierto polinomio $F[X] \in k_0[X]$ mónico con raíces distintas dos a dos. Más aún, podemos exigir que F tenga grado impar.*

El teorema 9.5 nos da que si F tiene grado $2g + 1$ o $2g + 2$, entonces un cuerpo K en las condiciones del teorema anterior tiene género g, luego si $g > 0$ es elíptico o hiperelíptico. Vemos así que hay cuerpos hiperelípticos de todos los géneros $g \geq 2$.

9.2 Cuerpos de funciones elípticas

En la sección anterior hemos definido los cuerpos elípticos como los cuerpos de género 1 que son extensiones cuadráticas de cuerpos de fracciones algebraicas. El teorema 9.7 afirma que todo cuerpo de género 1 y grado mínimo 1 es elíptico. Ahora vamos a estudiar más a fondo estos cuerpos. Por comodidad incluiremos en la definición la hipótesis sobre el grado mínimo. Así ésta se reduce a la siguiente:

Definición 9.9 Un *cuerpo de funciones elípticas* es un cuerpo de funciones algebraicas de género $g = 1$ y grado mínimo $f_0 = 1$. Una *curva elíptica* es una curva proyectiva regular de género $g = 1$.

Lo primero que obtenemos del teorema de Riemann-Roch para estos cuerpos es que la clase canónica cumple $\operatorname{grad} W = 0$, $\dim W = 1$, luego 8.25 nos da:

> *En un cuerpo de funciones elípticas la clase canónica es la clase principal.*

Por otra parte, el teorema de Riemann-Roch implica también que, para divisores de grado positivo, la dimensión es igual al grado. En particular, en la clase de un divisor de grado 1 podemos tomar un representante entero, que por consiguiente será primo. En definitiva:

> *Todo cuerpo de funciones elípticas tiene un primo de grado* 1.

Otra consecuencia notable del teorema de Riemann-Roch es que los cuerpos de funciones elípticas son definibles mediante ecuaciones cúbicas en forma normal de Weierstrass. En primer lugar, el teorema siguiente nos da que son definibles por cúbicas:

Teorema 9.10 *Sea K un cuerpo de funciones elípticas. Entonces $K = k_0(x, y)$ donde x, y satisfacen una ecuación (no nula) con coeficientes en k_0 de la forma*

$$y^2 + (ax + b)y + cx^3 + dx^2 + ex + f = 0.$$

DEMOSTRACIÓN: Sea $\mathfrak{p}$ un divisor primo de grado 1 (cuya existencia acabamos de justificar). Entonces $\dim \mathfrak{p}^2 = \operatorname{grad} \mathfrak{p}^2 = 2$, luego $m(\mathfrak{p}^{-2})$ contiene dos funciones linealmente independientes 1, x. Tenemos que $(x) = \mathfrak{a}/\mathfrak{p}^2$, donde $\mathfrak{a}$ es un divisor entero. Así $\mathfrak{p}^2$ es el primo infinito de $k = k_0(x)$, luego $|K : k| = \operatorname{grad} \mathfrak{p}^2 = 2$. (Notemos que x no puede tener un polo simple en $\mathfrak{p}$, pues entonces 1, $x \in m(\mathfrak{p}^{-1})$, cuando $\dim \mathfrak{p} = 1$.)

Como $\dim \mathfrak{p}^3 = \operatorname{grad} \mathfrak{p}^3 = 3$, tenemos que $m(\mathfrak{p}^{-3})$ contiene tres funciones linealmente independientes 1, x, y. No puede ser que $y \in k_0(x)$, pues entonces 1, x, $y \in m_k(\mathfrak{p}^{-2})$, mientras que $\dim_k(\mathfrak{p}^2) = \operatorname{grad}_k(\mathfrak{p}^2) + 1 = 2$ (ya que k tiene género 0). Así pues, $K = k_0(x, y)$.

Ahora observamos que 1, x, x^2, x^3, xy, y, $y^2 \in m(\mathfrak{p}^{-6})$, pero $\dim \mathfrak{p}^6 = 6$, luego estas siete funciones son linealmente dependientes sobre k_0, lo que nos da una ecuación como indica el enunciado. (El coeficiente de y^2 ha de ser no nulo, o cada sumando tendría un polo de orden distinto en $\mathfrak{p}$, lo cual es imposible.)

■

Para pasar a una ecuación de Weierstrass hemos de suponer que la característica del cuerpo de constantes k_0 es distinta de 2 y 3 (comparar con la prueba del teorema 7.24). Cambiando y por $y - (ax + b)/2$ obtenemos una ecuación de la forma

$$y^2 = ax^3 + bx^2 + cx + d.$$

Ha de ser $a \neq 0$ o, de lo contrario, K tendría género 0 por el teorema 9.3. Ahora sustituimos

$$x \mapsto ax - \frac{b}{3a}, \qquad y \mapsto \frac{a^2}{2}\, y$$

y la ecuación se reduce a

$$y^2 = 4x^3 - g_2 x - g_3, \qquad g_2,\ g_3 \in k_0. \tag{9.1}$$

El polinomio $4x^3 - g_2x - g_3$ no puede tener raíces múltiples (en una clausura algebraica de k_0), pues si a fuera una raíz múltiple, el cuerpo $K(a)$ sería también un cuerpo elíptico (pues las extensiones de constantes no alteran el género) y su grado mínimo seguiría siendo 1. Además estaría generado por elementos x e y que cumplirían la misma ecuación, pero ahora podríamos cambiar x por $x - a$, con lo que la ecuación pasaría a ser $y^2 = 4x^3 + cx^2$ (pues el miembro izquierdo ha de tener a 0 como raíz doble). Ahora bien, esto implica que $4x = (y/x)^2 - c$, de donde $K(a) = k_0(y/x)$ sería un cuerpo de fracciones algebraicas, luego tendría género 0, contradicción.

Una forma conveniente de expresar que un polinomio no tiene raíces múltiples es a través de su discriminante. Para un polinomio de grado 3

$$ax^3 + bx^2 + cx + d = a(x - \alpha)(x - \beta)(x - \gamma),$$

el *discriminante* se define como

$$\Delta = \big(a(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)\big)^2.$$

La definición para un polinomio de grado arbitrario es la generalización obvia de ésta. La teoría de Galois muestra fácilmente que Δ pertenece al mismo cuerpo que los coeficientes del polinomio, y es claro que un polinomio tiene raíces simples si y sólo si su discriminante es no nulo. Un cálculo laborioso muestra que, para un polinomio de grado 3,

$$\Delta = -\frac{4db^3}{a^2} + \frac{b^2c^2}{a^2} + 18\frac{bcd}{a} - \frac{4c^3}{a} - 27d^2.$$

En particular, el discriminante del miembro derecho de (9.1) resulta ser $\Delta = g_2^3 - 27g_3^2$. El teorema siguiente recoge lo que hemos probado:

Teorema 9.11 *Sea K un cuerpo de funciones elípticas sobre un cuerpo de constantes k_0 de característica distinta de 2 y 3. Entonces $K = k_0(x, y)$, donde x, y satisfacen una ecuación de la forma*

$$y^2 = 4x^3 - g_2x - g_3, \qquad g_2,\ g_3 \in k_0, \qquad g_2^3 - 27g_3^2 \neq 0.$$

Recordemos que las ecuaciones de este tipo son las que hemos llamado ecuaciones en forma normal de Weierstrass. En particular, del teorema anterior se desprende que toda curva elíptica (es decir, toda curva proyectiva regular de género 1) es birracionalmente equivalente —y, por lo tanto, isomorfa— a una cúbica (plana) regular. Recíprocamente, el teorema 9.4 implica que todas las cúbicas regulares son curvas elípticas.

En las condiciones del teorema anterior, si tomamos $x' = t^2x$, $y' = t^3y$, con $t \in k_0^*$, obtenemos dos nuevos generadores que satisfacen una ecuación de Weierstrass con coeficientes $g_2' = t^4g_2$ y $g_3' = t^6g_3$. Recíprocamente, vamos a probar que si $K = k_0(x, y) = k_0(x', y')$ y ambos pares de generadores satisfacen sendas ecuaciones de Weierstrass, entonces los coeficientes de éstas están relacionados en la forma $g_2' = t^4g_2$ y $g_3' = t^6g_3$, para cierto $t \in k_0^*$. Para ello necesitamos el teorema siguiente:

Teorema 9.12 *Si K es un cuerpo de funciones elípticas y $\mathfrak{p}$, $\mathfrak{p}'$ son dos divisores primos de grado 1, entonces existe un k_0-automorfismo σ de K que cumple $\sigma(\mathfrak{p}) = \mathfrak{p}'$.*

DEMOSTRACIÓN: La clase $[\mathfrak{p}\mathfrak{p}']$ tiene grado 2, luego también tiene dimensión 2, luego contiene un divisor entero $\mathfrak{a}$ distinto de $\mathfrak{p}\mathfrak{p}'$. Así, $\mathfrak{a}/\mathfrak{p}\mathfrak{p}' = (x)$, donde $x \in K$ no es constante. Es claro entonces que $\mathfrak{p}\mathfrak{p}'$ es el primo infinito del cuerpo $k = k_0(x)$.

Comparando el grado de $\mathfrak{p}\mathfrak{p}'$ en k y en K concluimos que $|K:k|=2$. Si la característica de k_0 no es 2, es claro que la extensión ha de ser separable y, por tener grado 2, también normal. Esto también es cierto si la característica es 2. Si la extensión fuera inseparable sería $K=k_0(x,\sqrt{\alpha}\,)$, donde $\alpha\in k_0(x)$. Usando que k_0 es perfecto, concluimos que $\sqrt{\alpha}\in k_0(\sqrt{x})$, luego $k_0(x)\subset K\subset k_0(\sqrt{x}\,)$. Teniendo en cuenta los grados, resulta que $K=k_0(\sqrt{x}\,)$ y llegamos a que K tiene género 0, contradicción.

Así pues, en cualquier caso K/k es una extensión de Galois de grado 2 y $\mathfrak{p}$, $\mathfrak{p}'$ son los divisores en K del primo infinito de k. Ahora basta aplicar 6.36. ■

Teorema 9.13 *Sea K un cuerpo de funciones elípticas sobre un cuerpo de constante k_0 de característica distinta de 2 y 3. Si $K=k_0(x,y)=k_0(x',y')$ y los generadores satisfacen ecuaciones*

$$y^2=4x^3-g_2x-g_3,\qquad y'^2=4x'^3-g_2'x'-g_3',$$

entonces existe un $t\in k_0^*$ tal que $g_2'=t^4g_2$ y $g_3'=t^6g_3$.

Demostración: Si ∞ es el primo infinito de $k=k_0(x)$ y $\mathfrak{p}$ es un divisor primo de ∞ en K, entonces

$$2v_{\mathfrak{p}}(y)=v_{\mathfrak{p}}(y^2)=e(\mathfrak{p}/\infty)v_\infty(4x^3-g_2x-g_3)=-3e(\mathfrak{p}/\infty).$$

Por consiguiente, $2\mid e(\mathfrak{p}/\infty)$ y, como $|K:k|=2$, ha de ser $e(\mathfrak{p}/\infty)=2$. Así pues, $\infty=\mathfrak{p}^2$. Es claro también que $\mathfrak{p}$ tiene grado 1. Por otra parte, $1,x,x^3\in m(\mathfrak{p}^{-6})$, luego la ecuación de Weierstrass implica que $y^2\in m(\mathfrak{p}^{-6})$ y así $y\in m(\mathfrak{p}^{-3})$.

Todo esto lo hemos deducido del mero hecho de que x e y satisfacen una ecuación en forma normal. Por lo tanto, lo mismo es válido para x', y' con otro divisor primo $\mathfrak{p}'$ de grado 1.

Por el teorema anterior existe un k_0-automorfismo de K que transforma $\mathfrak{p}'$ en $\mathfrak{p}$. Al aplicarlo sobre los generadores x', y' obtenemos dos nuevos generadores que satisfacen la misma ecuación, pero ahora $\mathfrak{p}'=\mathfrak{p}$.

Así pues, 1, x, $x'\in m(\mathfrak{p}^{-2})$. Como $\dim\mathfrak{p}^2=2$, ha de ser $x'=a+bx$, para ciertos a, $b\in k_0$, $b\neq 0$. Por otra parte, 1, x, y, $y'\in m(\mathfrak{p}^{-3})$ y, como $\dim\mathfrak{p}^3=3$, ha de ser $y'=c+dx+ey$, para ciertas constantes c, d, $e\in k_0$, $e\neq 0$. Sustituyendo en la ecuación de x', y' obtenemos la igualdad de polinomios

$$(c+dx+ey)^2-4(a+bx)^3+g_2'(a+bx)+g_3'=f(y^2-4x^3+g_2x+g_3),$$

para cierta constante $f\in k_0$.

Igualando los términos en x^3 vemos que $f=b^3$. Igualando los términos en y^2 sale que $f=e^2$. Igualando los términos en xy concluimos que $d=0$. Los términos en x^2 nos dan $a=0$. De los términos en y sale $c=0$, luego tenemos que $x'=bx$, $y'=ey$ con $b^3=e^2$. Llamando $t=e/b\in k_0^*$ tenemos que $x'=t^2x$, $y'=t^3y$, de donde $g_2'=t^4g_2$ y $g_3'=t^6g_3$. ■

Así pues, no podemos asociar unívocamente a cada cuerpo K de funciones elípticas unos coeficientes g_2, g_3, pero el teorema anterior muestra que de ellos sí se deriva un invariante:

Teorema 9.14 *Sea K un cuerpo de funciones elípticas y sobre un cuerpo de constantes k_0 de característica distinta de 2 o 3. Entonces, el elemento*

$$J(K) = \frac{g_2^3}{g_2^3 - 27g_3^2} \in k_0,$$

donde $K = k_0(x, y)$ con $y^2 = 4x^4 - g_2x - g_3$, es independiente de la elección de los generadores x, y.

Es claro que cuerpos k_0-isomorfos han de tener el mismo invariante $J(K)$. El recíproco es casi cierto, salvo por el hecho de que, obviamente, $J(K)$ se conserva por extensiones de constantes.

Teorema 9.15 *Sean K y K' dos cuerpos elípticos sobre un cuerpo de constantes k_0 de característica distinta de 2 o 3 y tales que $J(K) = J(K')$. Entonces existe una extensión finita k_1 de k_0 tal que las extensiones $K_1 = Kk_1$ y $K_1' = K'k_1$ son k_1-isomorfas. Más aún, la extensión k_1 puede elegirse tal que $|k_1 : k_0| \leq 2$, 4, 6 según si $1 \neq J \neq 0$, $J = 1$ o $J = 0$, respectivamente.*

Demostración: Fijemos generadores de K y K' que satisfagan ecuaciones en forma normal de Weierstrass con coeficientes g_2, g_3 y g_2', g_3' respectivamente. Se cumple que g_2 y g_2' son ambos nulos o ambos no nulos según si J es nulo o no. Si $J \neq 0$, tomamos $t = (g_2'/g_2)^{1/4}$ en una extensión de k_0 y así, mediante el cambio de generadores $x \mapsto t^2x$, $y \mapsto t^3y$ obtenemos generadores (en una extensión de constantes de K) que cumplen una ecuación en forma normal con $g_2 = g_2'$. La igualdad de los invariantes implica entonces que $g_3 = \pm g_3'$. Si se da el signo negativo tomamos $t' = \sqrt{-1}$ y al cambiar de nuevo los generadores, obtenemos $g_2 = g_2'$, $g_3 = g_3'$.

Así pues, hemos encontrado una extensión finita k_1 de k tal que los cuerpos K_1 y K_1' admiten pares de generadores que satisfacen la misma ecuación en forma normal, con lo que ciertamente son k_1-isomorfos. En definitiva, hemos encontrado un cuerpo k_1 en el cual tienen solución las ecuaciones $g_2' = t^4g_2$, $g_3' = t^6g_3$. Podemos suponer que $k_1 = k_0(t)$. Ahora bien, si $J \neq 0$, 1, entonces g_2, g_2', g_3, g_3' son todos no nulos y $t^2 = t^6/t^2 = g_3'g_2/g_3g_2'$, luego $|k_1 : k_0| \leq 2$. Si $J = 1$ entonces $g_3 = g_3' = 0$ y $t^4 = g_2'/g_2$, luego $|k_1 : k_0| \leq 4$. Finalmente, si $J = 0$ entonces $g_2 = g_2' = 0$ y $t^6 = g_3'/g_3$, luego $|k_1 : k_0| \leq 6$. ■

En particular, si k_0 es algebraicamente cerrado, dos cuerpos de funciones elípticas son k_0-isomorfos si y sólo si tienen el mismo invariante. Igualmente, si definimos el invariante de una curva elíptica como el de su cuerpo de funciones racionales, tenemos que dos curvas elípticas son isomorfas si y sólo si tienen el mismo invariante.

Ahora probaremos que existen cuerpos elípticos con cualquier invariante prefijado. Primeramente demostramos que las ecuaciones en forma canónica siempre definen cuerpos elípticos:

Teorema 9.16 *Sea $K = k_0(x, y)$ un cuerpo de funciones algebraicas sobre un cuerpo de constantes k_0 de característica distinta de 2 y 3 cuyos generadores satisfagan una ecuación en forma normal de Weierstrass. Entonces K es un cuerpo de funciones elípticas.*

DEMOSTRACIÓN: En la prueba de 9.13 hemos visto que el primo infinito de $k = k_0(x)$ se descompone como $\infty = \mathfrak{p}^2$ en K, donde $\mathfrak{p}$ es un primo de grado 1. Así pues, el grado mínimo de K es $f_0 = 1$. Sólo hemos de probar que el género de K es igual a 1. Extendiendo el cuerpo de constantes podemos suponerlo algebraicamente cerrado, pues esto no altera el género de K. Entonces podemos ver a K como el cuerpo de funciones racionales de la cúbica proyectiva V determinada por la ecuación $Y^2 = 4X^3 - g_2X - g_3$. Se trata de una cúbica regular y, por el teorema 9.4, tiene género 1. ■

Ahora es fácil probar:

Teorema 9.17 *Si la característica de k_0 es distinta de 2 y 3 y $c \in k_0$, entonces existe un cuerpo K de funciones elípticas sobre k_0 con invariante $J(K) = c$.*

DEMOSTRACIÓN: Si $c = 1$ sirve el cuerpo definido por $y^2 = 4(x^3 - x)$. Para $c = 0$ tomamos $y^2 = 4(x^3 - 1)$ y para $c \neq 0$, 1 tomamos

$$y^2 = 4x^3 - 3c(c-1)x - c(c-1)^2.$$

■

En particular vemos que existen infinitas cúbicas regulares no isomorfas dos a dos (una para cada invariante posible). Si $k_0 = \mathbb{C}$, esto nos lleva a que existen curvas regulares homeomorfas (es decir, del mismo género) que no son isomorfas.

Ya sabemos que un cuerpo de funciones elípticas tiene necesariamente primos de grado 1. El teorema siguiente prueba que tiene muchos:

Teorema 9.18 *Sea K un cuerpo de funciones elípticas y sea $\mathfrak{p}$ un divisor primo de grado 1 en K. Entonces la aplicación que a cada divisor primo $\mathfrak{P}$ de grado 1 de K le asigna la clase de divisores $[\mathfrak{P}/\mathfrak{p}]$ es una biyección entre el conjunto de los primos de grado 1 y el grupo de las clases de grado 0 de K.*

DEMOSTRACIÓN: Si $[\mathfrak{P}/\mathfrak{p}] = [\mathfrak{P}'/\mathfrak{p}]$, entonces $\mathfrak{P}/\mathfrak{P}'$ es principal. Si fuera $\mathfrak{P} \neq \mathfrak{P}'$, entonces $\mathfrak{P}/\mathfrak{P}' = (x)$, donde $x \in K$ sería no constante. Así $\mathfrak{P}'$ sería el primo infinito de $k = k_0(x)$, pero como el grado de $\mathfrak{P}'$ sería 1 tanto respecto de k como respecto de K, concluiríamos que $K = k$, pero entonces K tendría género 0. Así pues, la correspondencia es inyectiva.

Dada una clase C de grado 0, tenemos que $\dim C[\mathfrak{p}] = \operatorname{grad} C[\mathfrak{p}] = 1$, luego la clase $C[\mathfrak{p}]$ contiene un divisor entero $\mathfrak{P}$, que será primo por tener grado 1, y así $\mathfrak{P}/\mathfrak{p} \in C$, luego la correspondencia es también suprayectiva. ■

La biyección del teorema anterior nos permite trasladar la estructura de grupo de las clases de grado 0 al conjunto de los primos de grado 1:

Definición 9.19 Sea K un cuerpo de funciones elípticas y sea $\mathfrak{p}$ un divisor primo de K de grado 1. Para cada par $\mathfrak{P}$, $\mathfrak{Q}$ de divisores primos de grado 1 definimos $\mathfrak{P} + \mathfrak{Q} = \mathfrak{R}$ como el divisor primo de grado 1 que cumple

$$[\mathfrak{P}/\mathfrak{p}][\mathfrak{Q}/\mathfrak{p}] = [\mathfrak{R}/\mathfrak{p}].$$

Es claro que esta operación convierte al conjunto de los divisores de grado 1 de K en un grupo abeliano, de modo que la aplicación $\mathfrak{P} \mapsto [\mathfrak{P}/\mathfrak{p}]$ es un isomorfismo de grupos. Notemos que la definición depende de la elección de $\mathfrak{p}$, que resulta ser el elemento neutro, pero dos elecciones distintas dan lugar a grupos isomorfos, pues ambos son isomorfos al grupo de clases de grado 0 de K.

En particular, si V es una curva elíptica sobre un cuerpo de constantes k_0, los divisores primos de grado 1 de V son todos los divisores primos de su cuerpo de funciones racionales $k_0(V)$, que se corresponden biunívocamente con los puntos de V, luego tenemos definida una estructura de grupo sobre la propia curva V. En el caso concreto de una cúbica regular $V \subset \mathrm{P}^2$ esta estructura de grupo tiene una interpretación geométrica sencilla:

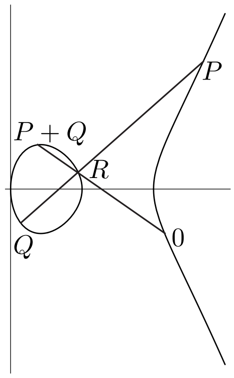
Consideremos un sistema de referencia proyectivo respecto al cual la ecuación de V esté en forma normal de Weierstrass. Esto significa que las funciones coordenadas afines x, $y \in K$ satisfacen la ecuación y, por supuesto, generan K.

En la prueba del teorema 9.13 hemos visto que el primo infinito de $k_0(x)$ es de la forma $\mathfrak{p}^2$, y se cumple $x \in m(\mathfrak{p}^{-2})$, $y \in m(\mathfrak{p}^{-3})$. Más precisamente, las funciones 1, x, y forman una base de $m(\mathfrak{p}^{-3})$. Notemos que $\mathfrak{p}$ es el único punto donde x e y tienen polos, es decir, el único punto infinito de V, de coordenadas homogéneas $(0, 1, 0)$, que además es un punto de inflexión. Su recta tangente es la recta del infinito. Con la representación geométrica usual, las rectas que pasan por $\mathfrak{p}$ son las rectas verticales.

Consideremos una recta en P^2 determinada por la forma $L = aX + bY + cZ$. Sea $l = L/Z = ax + by + c \in K$. Claramente $l \in m(\mathfrak{p}^{-3})$, luego $(l) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3/\mathfrak{p}^3$, para ciertos primos (no necesariamente distintos) $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$. Es fácil ver que éstos son los tres puntos (no necesariamente distintos) en que L corta a V según el teorema de Bezout. En efecto, si $\mathfrak{q} \neq \mathfrak{p}$ entonces Z no se anula en $\mathfrak{q}$, luego $I_{\mathfrak{q}}(V \cap L) = v_{\mathfrak{q}}(l)$ es el número de veces que $\mathfrak{q}$ figura entre los $\mathfrak{p}_i$. Para calcular $I_{\mathfrak{p}}(V \cap L)$ no hemos de dividir L entre Z, sino entre Y, con lo que $I_{\mathfrak{p}}(V \cap L) = v_{\mathfrak{p}}(l(Z/Y)) = v_{\mathfrak{p}}(ly^{-1})$. Como $y \in m(\mathfrak{p}^{-3})$, es $(y) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3/\mathfrak{p}^3$, donde los $\mathfrak{q}_i$ son los puntos (finitos) donde $Y = 0$ corta a V. Concluimos que $I_{\mathfrak{p}}(V \cap L) = v_{\mathfrak{p}}(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3/\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3)$ es el número de veces que $\mathfrak{p}$ aparece entre los $\mathfrak{p}_i$.

En resumen, hemos probado que tres puntos de V (no necesariamente distintos) $\mathfrak{p}_1$, $\mathfrak{p}_2$ y $\mathfrak{p}_3$ están alineados (en el sentido de que hay una recta que corta a V en tales puntos contando multiplicidades) si y sólo si el divisor $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3/\mathfrak{p}^3$ es principal. Aquí hay que entender que $\mathfrak{q}$, $\mathfrak{q}$ y $\mathfrak{r}$ están alineados si la tangente a V por $\mathfrak{q}$ pasa por $\mathfrak{r}$, así como que $\mathfrak{q}$, $\mathfrak{q}$ y $\mathfrak{q}$ están alineados si la tangente a V por $\mathfrak{q}$ no corta a V en más puntos, es decir, $\mathfrak{q}$ es un punto de inflexión de L.

Consideremos ahora la estructura de grupo en V que resulta de elegir arbitrariamente un primo 0 como elemento neutro. Dados dos puntos $\mathfrak{p}_1$ y $\mathfrak{p}_2$ de V, no necesariamente distintos, consideramos la recta L que pasa por ellos y sea $\mathfrak{p}_3$ el tercer punto donde esta recta corta a V, es decir, el punto para el cual se cumple $(l) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3/\mathfrak{p}^3$. Sea L' la recta que une 0 con $\mathfrak{p}_3$ y sea $\mathfrak{s}$ su tercer punto de corte. Tenemos entonces que $0\mathfrak{p}_3\mathfrak{s}/\mathfrak{p}^3 = (l')$. Por consiguiente: $[\mathfrak{p}_1\mathfrak{p}_2] = [\mathfrak{p}^3/\mathfrak{p}_3] = [0\mathfrak{s}]$, de donde $[(\mathfrak{p}_1/0)(\mathfrak{p}_2/0)] = [\mathfrak{s}/0]$, luego $\mathfrak{s} = \mathfrak{p}_1 + \mathfrak{p}_2$. En resumen:



Teorema 9.20 *Sea $V \subset \mathrm{P}^2$ una cúbica regular sobre un cuerpo de característica distinta de 2 y 3. Entonces, la suma de dos puntos P y Q de V respecto de un punto 0 elegido como neutro se calcula como sigue: se traza la recta que pasa por P y Q y se toma el tercer punto R donde esta recta corta a V, luego se traza la recta que une R con 0 y la suma es el tercer punto donde ésta corta a V.*

La situación es especialmente simple si tomamos como neutro un punto de inflexión. En tal caso, $-P$ es el único punto Q que cumple que el tercer punto de la recta que pasa por R y 0 es 0, luego dicha recta es la tangente a V por 0, pero dicha tangente sólo corta a V en 0, luego $R = 0$. En definitiva, $-P$ es el tercer punto en que la recta que une P con 0 corta a V. Por consiguiente, el punto R intermedio que calculamos para obtener $P+Q$ es $-P-Q$. De aquí se sigue fácilmente que $P+Q+R=0$ equivale a que los puntos P, Q y R están alineados.

La relación entre dos sumas respecto a neutros distintos es ahora fácil de expresar: si 0 es un punto de inflexión y $0'$ es un punto arbitrario, para sumar $P +_{0'} Q$ calculamos la recta que pasa por P y Q, que corta a V en $R = -P-Q$, y luego la recta que une R con $0'$, que corta a V en $P +_{0'} Q$, de modo que $(P +_{0'} Q) + 0' - P - Q = 0$. Así pues,

$$P +_{0'} Q = P + Q - 0'.$$

Si consideramos el sistema de coordenadas en que la ecuación de la cúbica está en forma normal, entonces las rectas que pasan por 0 son las rectas verticales, luego la aplicación $P \mapsto -P$ es simplemente $(X,Y) \mapsto (X,-Y)$.

El teorema siguiente prueba que las cúbicas regulares son que se conoce como *variedades abelianas* (variedades proyectivas con una estructura de grupo compatible con su estructura algebraica).

Teorema 9.21 *Si V es una cúbica regular sobre un cuerpo de característica distinta de 2 o 3, entonces las aplicaciones $\phi : V \times V \longrightarrow V$ y $\psi : V \longrightarrow V$ dadas por $\phi(P,Q) = P+Q$ y $\psi(P) = -P$ son regulares.*

Demostración: Tomamos un sistema de referencia en el que la ecuación de V esté en forma normal de Weierstrass. Podemos suponer que el neutro 0 es el punto del infinito, pues para otra elección $0'$ tenemos que $P +_{0'} Q = P + Q - 0'$, luego $\phi_{0'}(P,Q) = \phi(\phi(P,Q), -0')$. Similarmente, $-P_{0'} = 0' + 0' - P$, luego $\psi_{0'}(P) = \phi(0'+0', \psi(P))$.

La aplicación ψ es obviamente regular pues, según hemos visto, se cumple $\psi(X,Y) = (X,-Y)$. Respecto a ϕ, consideremos dos puntos (X_1,Y_1), (X_2,Y_2) tales que $X_1 \neq X_2$. Esto significa que no son opuestos. La recta que los une es

$$Y - Y_1 = \left(\frac{Y_2 - Y_1}{X_2 - X_1}\right)(X - X_1),$$

y esta recta corta a la cúbica en los puntos cuya coordenada X cumple

$$\left(Y_1 + \left(\frac{Y_2 - Y_1}{X_2 - X_1}\right)(X - X_1)\right)^2 = 4X^3 - g_2X - g_3.$$

Puesto que dos de ellos son X_1 y X_2 y la suma de las tres raíces es el coeficiente de X^2 cambiado de signo, vemos que la tercera raíz es

$$X_3 = \left(\frac{Y_2 - Y_1}{X_2 - X_1}\right)^2 - X_1 - X_2.$$

La ecuación de la recta nos da Y_3, y entonces la suma es el punto de coordenadas $(X_3, -Y_3)$. Ahora es claro que ϕ es una función racional regular en el abierto de $V \times V$ determinado por $X_1 \neq X_2$. Hemos de probar que es regular en un punto arbitrario $(P, Q) \in V \times V$.

Para cada $P \in V$ sea $\tau_P : V \longrightarrow V$ la traslación dada por $\tau_P(Q) = P + Q$. Es claro que τ_P es una aplicación racional, luego por la regularidad de V es —de hecho— regular. Además su inversa es τ_{-P}, que también es regular, pues es otra traslación. Concluimos que las traslaciones son isomorfismos.

Ahora observamos que si (P, Q), $(P', Q') \in V^2$, se cumple

$$\phi(P, Q) = (P + P') + (Q + Q') - (P' + Q') = \tau_{-P'-Q'}(\phi(\tau_{P'}(P), \tau_{Q'}(Q))),$$

luego $\phi = (\tau_{P'} \times \tau_{Q'}) \circ \phi \circ \tau_{-P'-Q'}$.

Así, para probar que ϕ es regular en un par (P, Q) tomamos un par (P_0, Q_0) donde sí lo sea (un par que cumpla $X_1 \neq X_1'$) y llamamos $P' = P_0 - P$, $Q' = Q_0 - Q$, con lo que $(\tau_{P'} \times \tau_{Q'})$ es regular en (P, Q) (es un isomorfismo), ϕ es regular en (P_0, Q_0) y $\tau_{-P'-Q'}$ es regular en $P_0 + Q_0$, luego la composición es regular en (P, Q). ■

9.3 Formas diferenciales

Si K es un cuerpo de funciones algebraicas, el término $\dim W/A$ en la fórmula del teorema de Riemann-Roch está estrechamente relacionado con las formas diferenciales de K. Esto está implícito en la demostración, pero es más fácil verlo directamente:

Definición 9.22 Si K es un cuerpo de funciones algebraicas sobre un cuerpo de constantes (exacto) k_0 y $\mathfrak{a}$ es un divisor en K, llamaremos $\Omega(\mathfrak{a})$ al k_0-espacio vectorial de todas las formas diferenciales ω en K tales que $v_{\mathfrak{P}}(\omega) \geq v_{\mathfrak{P}}(\mathfrak{a})$, para todo primo $\mathfrak{P}$ de K.

Teorema 9.23 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes (exacto) k_0. Sea W la clase canónica y $A = [\mathfrak{a}]$ una clase de divisores arbitraria. Entonces*

$$\dim \Omega(\mathfrak{a}) = \dim(W/A).$$

DEMOSTRACIÓN: Sea ω una forma diferencial no nula en K. Entonces, cualquier otra forma diferencial en K es de la forma $\alpha\omega$, con $\alpha \in K$. Se cumplirá que $\alpha\omega \in \Omega(\mathfrak{a})$ si y sólo si $v_{\mathfrak{P}}(\alpha) + v_{\mathfrak{P}}(\omega) \geq v_{\mathfrak{P}}(\mathfrak{a})$ para todo primo $\mathfrak{P}$ de K. Si llamamos $\mathfrak{c}$ al divisor de ω, tenemos que $[\mathfrak{c}] = W$ y $\alpha\omega \in \Omega(\mathfrak{a})$ si y sólo si $v_{\mathfrak{P}}(\alpha) \geq v_{\mathfrak{P}}(\mathfrak{a}/\mathfrak{c})$ para todo primo $\mathfrak{P}$, lo cual equivale a que $\alpha \in m(\mathfrak{a}/\mathfrak{c})$.

Es claro entonces que la aplicación $m(\mathfrak{a}/\mathfrak{c}) \longrightarrow \Omega(\mathfrak{a})$ dada por $\alpha \mapsto \alpha\omega$ es un k_0-isomorfismo, luego $\dim \Omega(\mathfrak{a}) = \dim(W/A)$. ■

A partir de aquí podemos usar el teorema de Riemann-Roch para justificar la existencia de formas diferenciales con ciertas propiedades sobre sus ceros y polos. Antes conviene introducir una clasificación que resultará natural en el capítulo siguiente, cuando nos ocupemos de la integración en superficies de Riemann.

Definición 9.24 Si K es un cuerpo de funciones algebraicas, llamaremos *diferenciales de primera clase* en K a las formas diferenciales en K que no tienen polos, las *diferenciales de segunda clase* son las formas diferenciales cuyos residuos son todos nulos y las *diferenciales de tercera clase* son las formas diferenciales que tienen a lo sumo polos de orden 1.

Es claro que una forma diferencial es de primera clase si y sólo si es a la vez de segunda y tercera clase. Lo más notable sobre las diferenciales de primera clase es que existen. Recordemos que las únicas funciones algebraicas sin polos son las constantes. Por el contrario, (salvo en los cuerpos de fracciones algebraicas) siempre existen diferenciales de primera clase no nulas. En efecto, el espacio de las diferenciales de primera clase es simplemente $\Omega(1)$, luego el teorema siguiente se sigue inmediatamente del teorema anterior, junto con el hecho de que la clase canónica tiene dimensión g:

Teorema 9.25 *Si K es un cuerpo de funciones algebraicas de género g, su espacio de formas diferenciales de primera clase tiene dimensión g.*

Si el cuerpo de constantes k_0 es algebraicamente cerrado, el teorema de los residuos 8.21 afirma que la suma de los residuos de una forma diferencial ha de ser nula. Ahora probamos que, salvo por esta restricción, existen diferenciales de tercera clase con cualquier distribución de residuos prefijada. En particular, toda forma diferencial es suma de una de segunda clase más otra de tercera clase:

Teorema 9.26 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes algebraicamente cerrado k_0, sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ divisores primos de K y $\alpha_1, \ldots, \alpha_n$ constantes no nulas tales que $\alpha_1 + \cdots + \alpha_n = 0$. Entonces existe una diferencial de tercera clase η en K cuyos polos son exactamente $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ y $\operatorname{Res}_{\mathfrak{P}_k} \eta = \alpha_k$, para $k = 1, \ldots, n$.*

DEMOSTRACIÓN: Basta probar el teorema para dos primos, pues si tenemos n primos $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$, podemos tomar otro más $\mathfrak{P}$ y aplicar el caso $n = 2$ para obtener formas η_k cuyos únicos polos polos (simples) estén en $\mathfrak{P}_k$ y $\mathfrak{P}$ de modo que $\operatorname{Res}_{\mathfrak{P}_k} \eta_k = \alpha_k$, $\operatorname{Res}_{\mathfrak{P}} \eta_k = -\alpha_k$. La forma $\eta = \eta_1 + \cdots + \eta_n$ cumple el teorema.

Suponemos, pues $n = 2$. Aplicamos el teorema de Riemann-Roch a la clase A del divisor $\mathfrak{a} = \mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1}$, que nos da

$$0 = \dim A = \operatorname{grad} A - (g-1) + \dim(W/A) = -(g+1) + \dim(W/A),$$

donde W es la clase canónica.

Así pues, $\dim \Omega(\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1}) = \dim(W/A) = g+1$. Por otra parte, el espacio de las diferenciales de primera clase tiene dimensión g, luego ha de existir una forma diferencial $\omega \in \Omega(\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1})$ que no sea de primera clase, es decir, que tenga al menos un polo y a lo sumo dos polos simples en los puntos $\mathfrak{P}_1$ y $\mathfrak{P}_2$. Como la suma de los residuos ha de ser nula, de hecho tiene un polo simple en ambos. Multiplicando ω por una constante tenemos la forma buscada. ■

Así pues, a toda diferencial se le puede restar una diferencial de tercera clase adecuada para que el resultado sea una diferencial de segunda clase. Evidentemente, dicha diferencial es única salvo diferenciales de primera clase.

Ejemplo Vamos a mostrar explícitamente las diferenciales de primera clase de los cuerpos elípticos e hiperelípticos sobre un cuerpo de constantes k_0 algebraicamente cerrado. Según el teorema 9.8 un cuerpo K en estas condiciones es de la forma $K = k_0(x, y)$, donde x e y satisfacen una ecuación de la forma

$$y^2 = (x - e_1) \cdots (x - e_{2g+1}), \tag{9.2}$$

donde los $e_i \in k_0$ son distintos dos a dos. Hemos de suponer además que x es separador, es decir, que $dx \neq 0$. Esto se cumple en particular si los cuerpos tienen característica 0. Vamos a probar que, en tal caso, una base del espacio de las diferenciales de primera clase la forman las diferenciales

$$\frac{dx}{y}, \quad \frac{x\,dx}{y}, \quad \ldots \quad , \quad \frac{x^{g-1}dx}{y}.$$

Sea $\omega = x^m y^{-1}\,dx$ y veamos que no tiene polos. Tomemos un primo $\mathfrak{P}$ en K y sea $\mathfrak{p}$ el primo de $k = k_0(x)$ al cual divide. Hemos de probar que $v_{\mathfrak{P}}(\omega) \geq 0$.

Supongamos en primer lugar que $v_{\mathfrak{P}}(x) \geq 0$ y sea $e = x(\mathfrak{P}) = x(\mathfrak{p}) \in k_0$. Si $e \neq e_j$ para $j = 1, \ldots, 2g+1$, entonces $y(\mathfrak{P}) \neq 0$, luego $v_{\mathfrak{P}}(y) = 0$ y claramente también $v_{\mathfrak{P}}(dx) \geq 0$, luego $v_{\mathfrak{P}}(\omega) \geq 0$. Supongamos, pues, que $e = e_j$.

Como $x - e$ se anula en $\mathfrak{P}$, ha de ser $x - e = \epsilon\pi^r$, donde ϵ es una unidad en $K_{\mathfrak{P}}$ y π un primo. Por otra parte, $x - e_i$ no se anula en $\mathfrak{P}$ para $i \neq j$, luego es una unidad. De (9.2) obtenemos que

$$2v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(x - e_j) = r.$$

Notemos que r es el índice de ramificación de $\mathfrak{P}$, que ha de ser 1 o 2, luego concluimos que es 2. Por lo tanto, $v_{\mathfrak{P}}(y) = 1$ y

$$dx = d(x - e) = \left(\frac{d\epsilon}{d\pi}\,\pi^2 + 2\epsilon\,\pi\right) d\pi,$$

de donde concluimos que $v_{\mathfrak{P}}(dx) \geq 1$. Ahora es claro que $v_{\mathfrak{P}}(\omega) \geq 0$.

Supongamos, por último, que $v_{\mathfrak{P}}(x) < 0$, de modo que $x = \epsilon\pi^{-r}$, donde de nuevo ϵ es una unidad en $K_{\mathfrak{P}}$ y π es un primo. El exponente r es así mismo el índice de ramificación de $\mathfrak{P}$, luego ha de ser 1 o 2. Llamando $t = 1/x$ tenemos que

$$y^2 = \left(\frac{1}{t} - e_1\right)\cdots\left(\frac{1}{t} - e_{2g+1}\right) = \frac{1}{t^{2g+1}}(1 - te_1)\cdots(1 - te_{2g+1}).$$

Los factores de la derecha son unidades en $K_{\mathfrak{P}}$, ya que valen 1 en $\mathfrak{P}$. Por consiguiente,

$$2v_{\mathfrak{P}}(y) = -r(2g + 1).$$

De aquí se sigue que $r = 2$, con lo que $v_{\mathfrak{P}}(y) = -2g - 1$ y $v_{\mathfrak{P}}(x) = -2$. Por otra parte,

$$dx = \left(\frac{d\epsilon}{d\pi}\,\pi^{-2} - 2\epsilon\pi^{-3}\right) d\pi,$$

con lo que $v_{\mathfrak{P}}(dx) \geq -3$. En total,

$$v_{\mathfrak{P}}(\omega) = mv_{\mathfrak{P}}(x) - v_{\mathfrak{P}}(y) + v_{\mathfrak{P}}(dx) \geq -2(g - 1) + 2g + 1 - 3 = 0.$$

Tenemos, pues que las g formas diferenciales consideradas son de primera clase. Una relación de dependencia lineal entre ellas daría lugar a una relación de dependencia lineal entre las funciones $1, x, \ldots, x^{g-1}$, lo cual es absurdo, luego ciertamente son linealmente independientes.

Veamos una aplicación:

Ejemplo *Si V es la curva proyectiva determinada por $Y^4 = X^4 - 1$, entonces V es regular y tiene género 3. Si el cuerpo de constantes k_0 es algebraicamente cerrado, entonces el cuerpo $K = k_0(V)$ no es hiperelíptico.*

En efecto, es fácil ver que no V tiene puntos singulares, luego el teorema 9.4 implica que su género es 3.

Vamos a probar que una base de las diferenciales de primera clase de K está constituida por las formas

$$\omega_1 = \frac{dx}{y^3}, \qquad \omega_2 = \frac{x\,dx}{y^3}, \qquad \omega_3 = \frac{y\,dx}{y^3}.$$

Llamemos $k = k_0(x)$. Sabemos que la extensión K/k se corresponde con la aplicación regular $x : V \longrightarrow \mathrm{P}^1$.

Sea $P \in V$ un punto finito tal que $x(P) = a$ no sea una raíz cuarta de la unidad. Así $v_P(x) \geq 0$, $v_P(y) = 0$. Además el punto $a \in A^1$ tiene cuatro divisores (antiimágenes) en V, uno de los cuales es P, luego $e_x(P) = 1$. Así pues, $v_P(x - a) = v_a(x - a) = 1$, luego $x - a$ es primo en K_P. Por consiguiente,

$$v_P(dx) = v_P(d(x - a)) = v_P(1) = 0.$$

Con esto es claro que las tres formas ω_i son regulares en P.

Supongamos ahora que $x(P) = a$ cumple $a^4 = 1$. En tal caso a tiene a P como único divisor en V, luego $e_x(P) = 4$. Tenemos que $v_P(x) = 0$ y $v_P(y) \geq 0$. Más aún, el polinomio $x^4 - 1$ factoriza en k como producto de cuatro polinomios distintos, uno de las cuales es $x - a$, luego

$$4v_P(y) = v_P(y^4) = 4v_a(y^4) = 4v_a(x^4 - 1) = 4.$$

Así pues, $v_P(y) = 1$, luego y es primo en K_P. Diferenciando la relación $y^4 = x^4 - 1$ obtenemos que $dx = (y/x)^3\, dy$, luego $v_P(dx) = 3$. De nuevo concluimos que las formas ω_i son regulares en P.

Consideremos, por último, el caso en que P es un punto infinito de K. Es claro que $\infty \in \mathrm{P}^1$ tiene cuatro divisores en V, luego $e_x(P) = 1$. En consecuencia, $v_P(x) = v_\infty(x) = -1$. Si recordamos que v_∞ en $k_0(x)$ es el grado cambiado de signo, resulta que

$$4v_P(y) = v_p(y^4) = v_\infty(x^4 - 1) = -4,$$

luego también $v_P(y) = -1$. Como primo en K_P podemos tomar $\pi = 1/x$, con lo que

$$v_P(dx) = v_P(d\pi^{-1}) = v_P(-\pi^{-2}\, d\pi) = -2.$$

Una vez más, vemos que las tres formas ω_i son regulares en P. En definitiva, son tres diferenciales de primera clase en V. Además son linealmente independientes sobre k_0, pues en caso contrario las funciones 1, x, y, serían linealmente dependientes.

Ahora observamos que

$$\frac{\omega_2}{\omega_1} = x, \qquad \frac{\omega_3}{\omega_1} = y,$$

luego $K = k_0(\omega_2/\omega_1, \omega_3/\omega_1)$. Además, este hecho se cumple para cualquier base de las diferenciales de primera clase de K, pues si $\omega_1', \omega_2', \omega_3'$ es otra base, se cumplirá que

$$\begin{aligned}
\omega_1 &= a_{11}\omega_1' + a_{12}\omega_2' + a_{13}\omega_3', \\
\omega_2 &= a_{21}\omega_1' + a_{22}\omega_2' + a_{23}\omega_3', \\
\omega_3 &= a_{31}\omega_1' + a_{32}\omega_2' + a_{33}\omega_3',
\end{aligned}$$

para ciertos $a_{ij} \in k_0$. Por lo tanto,

$$x = \frac{\omega_2}{\omega_1} = \frac{a_{21} + a_{22}\,\omega_2'/\omega_1' + a_{23}\,\omega_3'/\omega_1'}{a_{11} + a_{12}\,\omega_2'/\omega_1' + a_{13}\,\omega_3'/\omega_1'} \in k_0\left(\frac{\omega_2'}{\omega_1'}, \frac{\omega_3'}{\omega_1'}\right),$$

e igualmente $y \in k_0(\omega_2'/\omega_1', \omega_3'/\omega_1')$. Por lo tanto $k_0(\omega_2'/\omega_1', \omega_3'/\omega_1') = K$.

Esto prueba que K no es hiperelíptico, ya que si lo fuera podríamos expresar $K = k_0(x, y)$, para ciertos generadores x, y respecto a los cuales una base del espacio de diferenciales de primera clase lo constituyen las formas

$$\omega_1' = \frac{dx}{y}, \qquad \omega_2' = \frac{x\,dx}{y}, \qquad \omega_3' = \frac{x^2\,dx}{y},$$

de modo que $K = k_0(\omega_2'/\omega_1', \omega_3'/\omega_1') = k_0(x, x^2) = k_0(x)$, contradicción. ■

9.4 Cuerpos de constantes finitos

En esta sección veremos varias aplicaciones del teorema de Riemann-Roch a los cuerpos de funciones algebraicas sobre cuerpos finitos. Empezamos por una muy simple pero muy importante.

Teorema 9.27 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo de constantes finito k_0. Entonces el grupo de las clases de grado 0 tiene orden finito h.*

DEMOSTRACIÓN: Si $g = 0$ sabemos que los únicos divisores de grado 0 son los principales, luego $h = 1$. Supongamos que $g \geq 1$. Fijemos un divisor $\mathfrak{b}$ de K tal que $\operatorname{grad} \mathfrak{b} = m \geq 1$. Sea A una clase de grado 0 no principal. Entonces $\operatorname{grad} A[\mathfrak{b}]^g = mg \geq g$, y por el teorema de Riemann-Roch se cumple $\dim A[\mathfrak{b}]^g \geq 1$. En consecuencia, esta clase contiene un divisor entero $\mathfrak{a}$, de modo que $\mathfrak{a}\mathfrak{b}^{-g} \in A$. En particular $\operatorname{grad} \mathfrak{a} = mg$.

Es claro que A contiene un número finito de divisores enteros de grado menor o igual que mg (esto es cierto para cuerpos de fracciones algebraicas y se conserva por extensiones finitas). Por consiguiente hay un número finito de clases de grado 0. ■

Definición 9.28 Se llama *número de clases* de un cuerpo de funciones algebraicas sobre un cuerpo de constantes finito al número h de clases de divisores de grado 0.

Claramente, h es también el número de clases de grado n de K, para todo entero n (supuesto que existan clases de grado n, lo cual es cierto, aunque aún no lo hemos probado).

Funciones dseta Sea K un cuerpo de funciones algebraicas sobre un cuerpo exacto de constantes k_0 de cardinal finito q. Otra consecuencia del teorema de Riemann-Roch es la convergencia de la función dseta asociada a K. Concretamente, podemos definir la *norma absoluta* de un divisor $\mathfrak{a}$ de K como $\mathrm{N}(\mathfrak{a}) = q^{\operatorname{grad} \mathfrak{a}}$. Claramente es multiplicativa. La función dseta de K es la función

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde $\mathfrak{a}$ recorre los divisores enteros de K.

Vamos a probar que esta serie converge para todo número real $s > 1$ y por consiguiente, al ser una serie de Dirichlet, para todo número complejo con $\operatorname{Re} z > 1$.

Llamemos f al grado mínimo de un divisor de K. Precisamente estudiando la función dseta probaremos que $f = 1$, pero de momento no disponemos de este hecho. Puesto que todos los términos son positivos, podemos agruparlos adecuadamente:

$$\zeta_K(s) = \sum_{n=0}^{\infty} \sum_{\operatorname{grad} A = fn} \sum_{\mathfrak{a} \in A} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

donde A recorre las clases de divisores de K. Enseguida veremos que las dos sumas internas son finitas y, si probamos que la serie de la izquierda converge, lo mismo valdrá para la serie completa $\zeta_K(s)$, y la suma será la misma.

Sabemos que los divisores enteros de una clase A están en correspondencia con los elementos no nulos del espacio $m(\mathfrak{a}^{-1})$, para un $\mathfrak{a} \in A$ prefijado, de modo que dos elementos se corresponden con un mismo divisor si y sólo si se diferencian en un factor constante. Si $\dim A = m$, entonces $m(\mathfrak{a}^{-1})$ tiene $q^m - 1$ elementos no nulos. Si los agrupamos en clases de múltiplos, cada clase contiene $q-1$ elementos, luego el número de divisores enteros en la clase A es

$$\frac{q^m - 1}{q-1}, \qquad m = \dim A.$$

Así pues,

$$\zeta_K(s) = \frac{1}{q-1} \sum_{n=0}^{\infty} \sum_{\operatorname{grad} A = fn} \frac{q^{m_A} - 1}{q^{fns}}, \qquad m_A = \dim A.$$

Distingamos el caso en que el género de K es $g = 0$. Entonces hay una única clase A de cada grado fn y su dimensión es $fn + 1$, luego tenemos dos series geométricas que convergen cuando $s > 1$:

$$\zeta_K(s) = \frac{1}{q-1} \sum_{n=0}^{\infty} (q^{1+f(1-s)n} - q^{-fsn}) = \frac{1}{q-1} \left(\frac{q}{1 - q^{f(1-s)}} - \frac{1}{1 - q^{-fs}} \right).$$

Operando llegamos a

$$\zeta_K(s) = \frac{1}{q-1} \frac{q - 1 + q^{f(1-s)} - q^{1-fs}}{(1 - q^{-fs})(1 - q^{f(1-s)})}. \tag{9.3}$$

Cuando hayamos probado que $f = 1$ tendremos de hecho que

$$\zeta_K(s) = \frac{1}{(1 - q^{-s})(1 - q^{(1-s)})}.$$

Consideremos ahora el caso en que $g > 0$ y sea h el número de clases de K. Cuando $fn > 2g - 2$, el teorema de Riemann-Roch nos da que las h clases de grado nf tienen dimensión $fn - g + 1$. Separamos los sumandos correspondientes a estos términos:

$$\zeta_2(s) = \frac{h}{q-1} \sum_{fn > 2g-2} \frac{q^{fn-g+1} - 1}{q^{fsn}} = \frac{h}{q-1} \sum_{fn > 2g-2} (q^{1-g+f(1-s)n} - q^{-fsn})$$

$$= \frac{h}{q-1} \frac{q^{1-g+(2g-2+f)(1-s)}}{1 - q^{f(1-s)}} - \frac{h}{q-1} \frac{q^{-(2g-2+f)s}}{1 - q^{-fs}}.$$

Con esto ya tenemos la convergencia de la serie, pues el trozo que falta es una función entera. De todos modos vamos a desarrollarlo:

$$\begin{aligned}
\zeta_1(s) &= \frac{1}{q-1}\sum_{n=0}^{(2g-2)/f}\sum_{\operatorname{grad} A=fn}(q^{m_A-fsn}-q^{-fsn})\\
&= \frac{1}{q-1}\sum_{n=0}^{(2g-2)/f}\sum_{\operatorname{grad} A=fn}q^{m_A-fsn}-\frac{h}{q-1}\sum_{n=0}^{(2g-2)/f}q^{-fsn}\\
&= P(q^{-s})-\frac{h}{q-1}\,\frac{1-q^{-(2g-2+f)s}}{1-q^{-fs}},
\end{aligned}$$

donde P es un polinomio con coeficientes en $\mathbb{Q}$. Al sumar las dos partes se cancela un término y queda

$$\zeta_K(s)=P(q^{-s})+\frac{h}{q-1}\left(\frac{q^{1-g+(2g-2+f)(1-s)}}{1-q^{f(1-s)}}-\frac{1}{1-q^{-fs}}\right) \tag{9.4}$$

Al operar obtenemos una expresión de la forma

$$\zeta_K(s)=\frac{L(q^{-s})}{(1-q^{-fs})(1-q^{f(1-s)})}, \tag{9.5}$$

donde $L(x)$ es un polinomio con coeficientes en $\mathbb{Q}$. Notemos que (9.3) es también de esta forma. El denominador del último término de (9.4) tiene ceros simples en los puntos $s_r=-2r\pi i/(f\log q)$, para $r\in\mathbb{Z}$. Es claro entonces que

$$L(q^{-s_r})=\frac{h(q^f-1)}{q-1}.$$

Por lo tanto $\zeta_K(s)$ tiene polos simples en estos puntos. Cuando hayamos probado que $f=1$ tendremos que $L(1)=h$. Es fácil ver que todo esto vale igualmente en el caso $g=0$.

Productos de Euler Una vez probada la convergencia de la función dseta, es fácil probar la fórmula de Euler:

$$\zeta_K(s)=\prod_{\mathfrak{p}}\frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}},\qquad s>1, \tag{9.6}$$

donde $\mathfrak{p}$ recorre los divisores primos de K.

Para demostrar que $f=1$ compararemos la función dseta de K con la de la única extensión de constantes de K de grado n. Sea k_1 la única extensión de k_0 de grado n. Llamemos $K_n=Kk_1$. Sea $\mathfrak{p}$ un primo en K y $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K_n. Entonces

$$f(\mathfrak{P}/\mathfrak{p})=|(\overline{K}_n)_{\mathfrak{P}}:\overline{K}_{\mathfrak{p}}|=|k_1\overline{K}_{\mathfrak{p}}:\overline{K}_{\mathfrak{p}}|.$$

El cuerpo $\overline{K}_{\mathfrak{p}}$ tiene q^m elementos, donde $m = \operatorname{grad} \mathfrak{p}$, mientras que k_1 tiene q^n elementos. La teoría de cuerpos finitos nos da que

$$f(\mathfrak{P}/\mathfrak{p}) = \frac{\operatorname{mcm}(m,n)}{m} = \frac{n}{\operatorname{mcd}(m,n)},$$

luego $\mathfrak{p}$ se descompone en $t = (m,n)$ primos de K_n. Para calcular la función $\zeta_{K_n}(s)$ hemos de trabajar con el cuerpo de constantes k_1. Como el grado de $\mathfrak{p}$ respecto de k_1 sigue siendo m, el de sus divisores será m/t. Por otra parte el número de elementos de k_1 es q^n.

En la fórmula del producto de Euler agrupamos los factores (iguales) correspondientes a los divisores de un mismo primo de K, con lo que obtenemos que

$$\zeta_{K_n}(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{q^{(\operatorname{grad} \mathfrak{p})sn/t}}\right)^{-t}.$$

Para operar esta expresión fijamos un primo $\mathfrak{p}$ y consideramos la raíz n-sima de la unidad $\omega_n = e^{2\pi i/n}$. Si $m = \operatorname{grad} \mathfrak{p}$, entonces ω_n^m tiene orden n/t, luego

$$x^{n/t} - q^{-msn/t} = \prod_{r=0}^{n/t-1} (x - \omega_n^{mr} q^{-ms}).$$

Si dejamos que r varíe entre 0 y $n-1$ entonces cada factor aparece t veces, luego

$$(x^{n/t} - q^{-msn/t})^t = \prod_{r=0}^{n-1} (x - \omega_n^{mr} q^{-ms}).$$

Haciendo $x = 1$ queda

$$(1 - q^{-msn/t})^t = \prod_{r=0}^{n-1} (1 - \omega_n^{mr} q^{-ms}) = \prod_{r=0}^{n-1} (1 - q^{-m(s-2r\pi i/n \log q)})$$

Usando esto vemos que

$$\zeta_{K_n}(s) = \prod_{r=0}^{n-1} \zeta_K\left(s - \frac{2r\pi i}{n \log q}\right). \tag{9.7}$$

Ahora bien, en el caso $n = f$ hemos visto que cada factor tiene un polo simple en $s = 0$, luego ζ_{K_f} tiene un polo de orden f en $s = 0$, pero lo visto anteriormente vale también para esta función, luego el polo ha de ser simple y por consiguiente ha de ser $f = 1$.

Teorema 9.29 *Los cuerpos de funciones algebraicas sobre cuerpos de constantes finitos tienen divisores de todos los grados.*

El polinomio *L(x)* Ahora que sabemos que $f = 1$ podemos hacer algunas precisiones adicionales sobre el polinomio $L(x)$ que hemos introducido en (9.5). La expresión explícita de $\zeta_K(s)$ es (para $g \geq 1$)

$$\zeta_K(s) = \frac{1}{q-1}\sum_{n=0}^{2g-2}\sum_{\operatorname{grad} A=n} q^{m_A - sn} + \frac{h}{q-1}\left(\frac{q^{1-g+(2g-1)(1-s)}}{1-q^{1-s}} - \frac{1}{1-q^{-s}}\right),$$

luego

$$L(x) = \frac{(1-qx)(1-x)}{q-1}\sum_{n=0}^{2g-2}\sum_{\operatorname{grad} A=n} q^{m_A}x^n + \frac{h}{q-1}\big((1-x)q^g x^{2g-1} - (1-qx)\big).$$

Vemos así que $L(x)$ tiene grado $2g$. Más aún, el polinomio $(q-1)L(x)$ tiene coeficientes enteros, y si tomamos restos módulo $q-1$ queda

$$(q-1)L(x) \equiv (1-x)^2\sum_{n=0}^{2g-2}\sum_{\operatorname{grad} A=n} x^n + h\big((1-x)x^{2g-1} - (1-x)\big)$$

$$\equiv h(1-x)^2\sum_{n=0}^{2g-2} x^n + h(1-x)(x^{2g-1}-1) \equiv 0 \ (\text{mód } q-1).$$

Esto significa que todos los coeficientes de $(q-1)L(x)$ son múltiplos de $q-1$, luego el polinomio $L(x)$ tiene coeficientes enteros.

Ya hemos visto que $L(1) = h$, y ahora es fácil ver además que

$$L(0) = \frac{1}{q-1}\sum_{\operatorname{grad} A=0} q^{m_A} - \frac{h}{q-1} = \frac{1}{q-1}(q+h-1) - \frac{h}{q-1} = 1,$$

donde hemos usado el teorema 8.25. En resumen:

Teorema 9.30 *Sea K un cuerpo de funciones algebraicas de género g sobre un cuerpo de constantes finito (exacto) de cardinal q. Entonces la función $\zeta_K(s)$ converge en el semiplano* $\operatorname{Re} s > 1$ *a una función holomorfa que se extiende a una función meromorfa en $\mathbb{C}$ dada por*

$$\zeta_K(s) = \frac{L(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

donde $L(x) \in \mathbb{Z}[x]$ es un polinomio de grado $2g$ tal que $L(0) = 1$ y $L(1) = h$, el número de clases.

Notemos que el teorema es trivial si $g = 0$, pues entonces $L(x) = 1$. En particular, si $K = k(\alpha)$, donde k es un cuerpo de fracciones algebraicas, tenemos que $\zeta_K(s) = L(q^{-s})\zeta_k(s)$.

La ecuación funcional Con los cálculos que tenemos a nuestra disposición, es fácil probar que la función dseta satisface una ecuación funcional muy sencilla:

Teorema 9.31 *Sea K un cuerpo de funciones algebraicas de género g sobre un cuerpo de constantes finito (exacto) de cardinal q. Entonces*

$$q^{(g-1)s}\zeta_K(s) = q^{(g-1)(1-s)}\zeta_K(1-s), \qquad \textit{para todo } s \in \mathbb{C}.$$

Demostración: Consideremos el caso en que $g > 0$. El caso $g = 0$ es más simple. Según hemos visto,

$$\zeta_K(s) = \frac{1}{q-1}\sum_{n=0}^{2g-2}\sum_{\operatorname{grad} A=n} q^{m_A-ns} + \frac{h}{q-1}\left(\frac{q^{1-g+(2g-1)(1-s)}}{1-q^{(1-s)}} - \frac{1}{1-q^{-s}}\right),$$

donde m_A es la dimensión de A. Por lo tanto

$$\begin{aligned} q^{(g-1)s}\zeta_K(s) &= \frac{1}{q-1}\sum_{n=0}^{2g-2}\sum_{\operatorname{grad} A=n} q^{m_A-(n-(g-1))s} \\ &+ \frac{h}{q-1}\left(\frac{q^{g(1-s)}}{1-q^{(1-s)}} + \frac{q^{gs}}{1-q^{s}}\right). \end{aligned}$$

El segundo sumando es claramente invariante para la sustitución $s \mapsto 1-s$. Basta probar que lo mismo le sucede al primero. Si un clase A tiene grado $n \leq 2g-2$, su complementaria W/A tiene grado $2g-2-n$, luego podemos agrupar los sumandos del primer término en parejas

$$q^{m_A-(n-(g-1))s}, \qquad q^{m_{W/A}-(g-1-n)s} = q^{m_A+(g-1-n)(1-s)},$$

donde hemos usado el teorema de Riemann-Roch. Claramente la sustitución $s \mapsto 1-s$ deja invariante cada pareja. ■

Es fácil ver que en términos del polinomio $L(x)$ dado por el teorema 9.30, la ecuación funcional se expresa en la forma

$$L(x) = q^g x^{2g} L(1/qx).$$

Teniendo en cuenta que el término independiente de $L(x)$ es $L(0) = 1$, de aquí se sigue que el coeficiente director de $L(x)$ es q^g.

El logaritmo de la función dseta Tomemos logaritmos en el producto de Euler (9.6):

$$\log\zeta_K(s) = \sum_{\mathfrak{p}} \log\frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}} = \sum_{k=1}^{\infty}\sum_{\operatorname{grad}\mathfrak{p}=k}\sum_{m=1}^{\infty}\frac{1}{m}(q^{-s})^{mk}$$

$$= \sum_{m=1}^{\infty}\sum_{k|m}\sum_{\operatorname{grad}\mathfrak{p}=k}\frac{k}{m}(q^{-s})^m = \sum_{n=1}^{\infty}\frac{N_n}{n}(q^{-s})^n,$$

donde $N_n = \sum\limits_{\operatorname{grad}\mathfrak{p}|n} \operatorname{grad}\mathfrak{p}$. En particular, N_1 es el número de primos de grado 1 en K.

Sea ahora K_n la extensión de constantes de grado n de K y consideremos la fórmula (9.7). Tenemos que

$$\log\zeta_{K_n}(s) = \sum_{r=0}^{n-1} \log\zeta_K\left(s - \frac{2r\pi i}{n\log q}\right). \tag{9.8}$$

En principio, faltaría un posible término $2k\pi i$, pero enseguida veremos que no es así. En efecto, si $\omega = e^{2\pi i/n}$, el miembro derecho es

$$\sum_{r=0}^{n-1}\sum_{m=1}^{\infty} \frac{N_m}{m}(q^{-s}\omega^r)^m = \sum_{m=1}^{\infty}\frac{N_m}{m}\sum_{r=0}^{n-1}\omega^{mr}(q^{-s})^m = \sum_{n|m}\frac{N_m}{m}(q^{-s})^m.$$

Ahora es claro que ambos miembros de (9.8) son reales cuando s es real, luego son el mismo logaritmo. Por otra parte, el miembro izquierdo de (9.8) es

$$\sum_{m=1}^{\infty}\frac{N_m^{n)}}{m}(q^{-s})^{mn}.$$

Comparando ambas expresiones vemos que $N_n = N_1^{n)}$, es decir, N_n es el número de primos de grado 1 de la extensión K_n.

Si llamamos $\alpha_1, \ldots, \alpha_{2g}$ a los inversos de las raíces de $L(x)$, tenemos que

$$L(x) = \prod_{i=1}^{2g}(1 - \alpha_i x), \tag{9.9}$$

pues el coeficiente director del miembro derecho es $\alpha_1\cdots\alpha_{2g} = q^g$ (recordemos que el término independiente de $L(x)$ es 1 y su coeficiente director es q^g). Por consiguiente.

$$\zeta_K(s) = \frac{\prod\limits_{i=1}^{2g}(1-\alpha_i q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

Tomando logaritmos,

$$\sum_{n=1}^{\infty}\frac{N_n}{n}(q^{-s})^n = \sum_{n=1}^{\infty}\left(q^n + 1 - \sum_{i=1}^{2g}\alpha_i^n\right)\frac{1}{n}(q^{-s})^n.$$

Comparando ambos miembros, obtenemos la relación

$$N_n = q^n + 1 - \sum_{i=1}^{2g}\alpha_i^n.$$

La hipótesis de Riemann Citamos sin demostración un último resultado sobre la función dseta. La fórmula (9.6) muestra que $\zeta_K(s)$ no se anula en el semiplano $\operatorname{Re} s > 1$, y la ecuación funcional implica entonces que tampoco lo hace en el semiplano $\operatorname{Re} s < 0$. Así pues, todos los ceros de $\zeta_K(s)$ han de estar en la banda crítica $0 \leq \operatorname{Re} s \leq 1$. La situación es similar a la de la función dseta de Riemann clásica, es decir, la función

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \operatorname{Re} s > 1.$$

Riemann demostró que $\zeta(s)$ se extiende a todo el plano complejo con un único polo en $s = 1$, así como que satisface una cierta ecuación funcional, de la que se sigue que $\zeta(s)$ se anula en los enteros pares negativos (ceros triviales) y que cualquier otro cero ha de estar sobre la banda crítica $0 \leq \operatorname{Re} s \leq 1$. Riemann conjeturó que todos los ceros no triviales de $\zeta(s)$ se encuentran, de hecho, sobre la recta $\operatorname{Re} s = 1/2$, afirmación que se conoce como *hipótesis de Riemann* y constituye uno de los más famosos problemas abiertos en la actualidad. Sorprendentemente, André Weil demostró el análogo para las funciones dseta de los cuerpos de funciones algebraicas sobre cuerpos finitos: los únicos ceros de la función $\zeta_K(s)$ se encuentran sobre la recta $\operatorname{Re} s = 1/2$.

Observemos que s es un cero de $\zeta_K(s)$ si y sólo si q^{-s} es un cero del polinomio $L(x)$. Además $|q^{-s}| = q^{-\operatorname{Re} s}$, luego la hipótesis de Riemann equivale a que los inversos de las raíces de $L(x)$, es decir, los números que hemos llamado $\alpha_1, \ldots, \alpha_{2g}$, cumplen $|\alpha_i| = \sqrt{q}$. Por consiguiente, la hipótesis de Riemann nos da la estimación

$$|N_n - q^n - 1| = |\alpha_1^n + \cdots + \alpha_{2g}^n| \leq 2g\, q^{n/2}.$$

En particular, para $n = 1$, vemos que el número de primos de grado 1 de un cuerpo de funciones algebraicas K de género g sobre un cuerpo de constantes finito (exacto) de cardinal q satisface la estimación

$$|N_1 - q - 1| \leq 2g\sqrt{q}.$$

De hecho, la hipótesis de Riemann puede expresarse como una estimación asintótica de N_n:

Teorema 9.32 *La hipótesis de Riemann para un cuerpo de funciones algebraicas K sobre un cuerpo de constantes exacto de q elementos equivale a que*

$$N_n = q^n + O(q^{n/2}),$$

donde $O(q^{n/2})$ representa una función de n que permanece acotada cuando se divide entre $q^{n/2}$.

Demostración: Si se cumple la hipótesis de Riemann tenemos que

$$|N_n - q^n| \leq 1 + |N_n - q^n - 1| \leq 1 + 2g\, q^{n/2} \leq (2g+1)q^{n/2},$$

luego se cumple la estimación del enunciado.

Recíprocamente, tenemos que existe una constante C tal que

$$|N_n - q^n| \leq Cq^{n/2},$$

luego

$$|\alpha_1^n + \cdots + \alpha_{2g}^n| = |N_n - q^n - 1| \leq 1 + Cq^{n/2}.$$

De (9.9) se sigue que, para x en un entorno de 0,

$$\log \frac{1}{L(x)} = \sum_{n=1}^{\infty} (\alpha_1^n + \cdots + \alpha_{2g}^n) \frac{x^n}{n}.$$

Por consiguiente,

$$\left| \log \frac{1}{L(x)} \right| \leq \sum_{n=1}^{\infty} (1 + Cq^{n/2}) \frac{|x|^n}{n} \leq \log \frac{1}{1 - |x|} + C \log \frac{1}{1 - |q^{1/2}x|}.$$

De aquí se deducimos que la serie de potencias converge para todo x tal que $|x| < q^{-1/2}$, luego la función $\log L(x)^{-1}$ es holomorfa en el disco $|x| < q^{-1/2}$, luego los ceros de $L(x)$ han de cumplir $|x| \geq q^{-1/2}$, luego $|\alpha_i| \leq q^{1/2}$. Puesto que $\alpha_1 \cdots \alpha_{2g} = q^g$, en realidad ha de ser $|\alpha_i| = q^{1/2}$, como había que probar.

■

Citamos, por último, una consecuencia inmediata de la fórmula (9.7):

Teorema 9.33 *Sea K un cuerpo de funciones algebraicas sobre un cuerpo finito y sea K_n su única extensión de constantes de grado n. Entonces K cumple la hipótesis de Riemann si y sólo si la cumple K_n.*

Capítulo X

Integrales abelianas

En 1718, el conde Fagnano descubrió una curiosa propiedad sobre el arco de una lemniscata. En su sentido más general, una *lemniscata* es el conjunto de los puntos del plano complejo donde un polinomio tiene módulo constante. Las raíces del polinomio (repetidas según su multiplicidad) se llaman *focos* de la lemniscata, de modo que —factorizando el polinomio— se ve que la lemniscata está formada por los puntos del plano cuyo producto de distancias a los focos es constante. En particular, las lemniscatas de un foco (o de dos focos iguales) son circunferencias.

Consideremos una lemniscata con dos focos distintos. Aplicándole una semejanza, podemos suponer que sus focos son los puntos $\pm 1/\sqrt{2}$ (veremos que así las ecuaciones que vamos a manejar resultan ser especialmente simples).

Sea $(x, y) \in \mathbb{R}^2$ un punto de módulo $\rho = \sqrt{x^2 + y^2}$. Su distancia a cada foco es

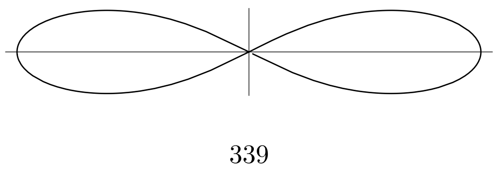
$$r_1 = (x + 1/\sqrt{2})^2 + y^2 = \rho^2 + \frac{2x}{\sqrt{2}} + \frac{1}{2},$$

$$r_2 = (x - 1/\sqrt{2})^2 + y^2 = \rho^2 - \frac{2x}{\sqrt{2}} + \frac{1}{2},$$

luego el punto está en la lemniscata si cumple

$$r_1 r_2 = (\rho^2 + 1/2)^2 - 2x^2 = \rho^4 + \rho^2 + 1/4 - 2x^2 = c^4,$$

para una constante c. Si $c^4 < 1/4$ la lemniscata consta de dos componentes conexas, cada una de las cuales rodea a un foco, mientras que si $c^4 > 1/4$ entonces hay una única componente que rodea a ambos focos. La lemniscata clásica, conocida como *lemniscata de Bernoulli,* es la correspondiente a $c^4 = 1/4$ que tiene forma de lazo, como muestra la figura e indica su nombre (el lemnisco era la cinta que adornaba las coronas con que se distinguía a los atletas en la antigua Grecia).



En este caso la ecuación se reduce a $\rho^4 + \rho^2 - 2x^2 = 0$ que, junto con la relación $\rho^2 = x^2 + y^2$ nos da una parametrización de la lemniscata:

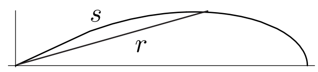
$$\begin{aligned} x &= \pm\frac{1}{\sqrt{2}}\sqrt{\rho^2 - \rho^4}, \\ y &= \pm\frac{1}{\sqrt{2}}\sqrt{\rho^2 + \rho^4}. \end{aligned}$$

Un simple cálculo nos da que el elemento de longitud es

$$ds = \frac{d\rho}{\sqrt{1-\rho^4}}.$$

Así pues, la longitud del arco de lemniscata comprendido entre el origen y un punto situado a distancia $0 < r < 1$ (unidos por el camino más corto) es

$$s(r) = \int_0^r \frac{d\rho}{\sqrt{1-\rho^4}}.$$



Probablemente, Fagnano trató de explotar la analogía entre esta integral y la bien conocida

$$\operatorname{arcsen} r = \int_0^r \frac{d\rho}{\sqrt{1-\rho^2}}.$$

Esta integral se racionaliza con el cambio de variable

$$\rho = \frac{2\tau}{1+\tau^2},$$

por lo que parece razonable aplicar a nuestra integral el cambio

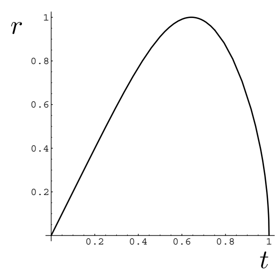
$$\rho^2 = \frac{2\tau^2}{1+\tau^4}.$$

Un simple cálculo nos da que

$$s(r) = \int_0^r \frac{d\rho}{\sqrt{1-\rho^4}} = \sqrt{2}\int_0^t \frac{d\tau}{\sqrt{1+\tau^4}}, \qquad r^2 = \frac{2t^2}{1+t^4}.$$

En lo que se refiere al cálculo de la integral no hemos ganado nada, pero Fagnano se dio cuenta de que si ahora aplicamos el mismo cambio pero con un signo negativo en el denominador, obtenemos

$$s(r) = \int_0^r \frac{d\rho}{\sqrt{1-\rho^4}} = 2\int_0^t \frac{d\tau}{\sqrt{1-\tau^4}} = 2s(t),$$



donde

$$r^2 = \frac{2\frac{2t^2}{1-t^4}}{1+\left(\frac{2t^2}{1-t^4}\right)^2} = \frac{4t^2(1-t^4)}{(1+t^4)^2}.$$

Esto tiene una interpretación geométrica: si señalamos un punto de la lemniscata a una distancia $0 < t < 1$ del origen, entonces el punto situado a la distancia r dada por la fórmula anterior determina un arco de doble longitud. (En realidad es necesario suponer que t no exceda del punto donde $r(t)$ deja de ser inyectiva, lo cual equivale a que al duplicar el arco no sobrepasemos el cuadrante). La sencilla relación entre r y t permite, por ejemplo, duplicar un arco de lemniscata con regla y compás. Así mismo podemos expresar t en función de r, lo que nos da un método para bisecar un arco de lemniscata.

En 1751, Euler llegó más lejos que Fagnano. En primer lugar, vio que la analogía con el arco seno podía aprovecharse más aún. La relación

$$\operatorname{sen}(x+y) = \operatorname{sen} x \cos y + \cos x \operatorname{sen} y$$

puede expresarse en la forma

$$u\sqrt{1-v^2} + v\sqrt{1-u^2} = \operatorname{sen}(x+y), \qquad u = \operatorname{sen} x, \quad v = \operatorname{sen} y,$$

o también,

$$\int_0^u \frac{d\rho}{\sqrt{1-\rho^2}} + \int_0^v \frac{d\rho}{\sqrt{1-\rho^2}} = \int_0^r \frac{d\rho}{\sqrt{1-\rho^2}}, \qquad r = u\sqrt{1-v^2} + v\sqrt{1-u^2}.$$

Aquí hay que entender que u y v son números positivos suficientemente pequeños. Euler consiguió probar una fórmula análoga para la lemniscata, a saber:

$$\int_0^u \frac{d\rho}{\sqrt{1-\rho^4}} + \int_0^v \frac{d\rho}{\sqrt{1-\rho^4}} = \int_0^r \frac{d\rho}{\sqrt{1-\rho^4}}, \quad r = \frac{u\sqrt{1-v^4} + v\sqrt{1-u^4}}{1+u^2v^2}.$$

Esta fórmula se particulariza a la de Fagnano cuando $u = v$, y permite sumar fácilmente dos arcos de lemniscata suficientemente pequeños como para que la suma no exceda un cuadrante.

Más aún, Euler generalizó su resultado probando que sigue siendo cierto si cambiamos el polinomio $P(u) = 1 - u^4$ por $P(u) = 1 + au^2 - u^4$, para cualquier valor de a.

Los resultados de Euler fueron notablemente generalizados por Abel, quien estudió el comportamiento de las integrales de la forma

$$\int R(x,y)\, dx,$$

donde $R(X,Y)$ es una función racional e $y(x)$ es una función algebraica determinada por una relación polinómica $P(x,y) = 0$. Estas integrales se conocen como integrales abelianas. En términos más modernos, podemos definir las integrales abelianas como las integrales curvilíneas de formas diferenciales meromorfas sobre superficies de Riemann. Por ejemplo, para interpretar como integral abeliana la integral que da la longitud de arco de la lemniscata consideramos la curva proyectiva S dada por $Y^2 = 1 - X^4$ y, en ella, la forma $\omega = dx/y$. Así,

$$s(r) = \int_\sigma \omega, \qquad \text{donde } \sigma(\rho) = (\rho, \sqrt{1-\rho^4}).$$

Dedicamos este capítulo a estudiar las integrales abelianas. Ello nos llevará a unos resultados generales de los cuales no sólo se deducen los hechos que acabamos de comentar, sino también resultados de gran interés teórico. Por ejemplo, vamos a determinar la estructura del grupo de clases de grado 0 de una curva proyectiva.

10.1 Homología y cohomología

Para trabajar con integrales sobre superficies de Riemann es imprescindible emplear los conceptos básicos de la topología algebraica. En esta primera sección recordaremos sin pruebas los hechos que vamos a necesitar.[1] Antes de entrar en materia, recordemos el comportamiento de las integrales curvilíneas sobre un abierto $U \subset \mathbb{C}$ simplemente conexo. Si $f : U \longrightarrow \mathbb{C}$ es una función holomorfa, el teorema de Cauchy afirma que la integral de f a lo largo de un arco cerrado es nula. Ello se debe esencialmente a que los arcos cerrados son homotópicos a un punto y las integrales no se alteran al transformar homotópicamente los arcos. Como consecuencia, fijado $P \in U$, la integral

$$\int_P^z f(\zeta)\, d\zeta \tag{10.1}$$

no depende del arco sobre el que se calcula y determina una función holomorfa en U (una primitiva de f, de hecho).

Si f es una función meromorfa, entonces ya no podemos aplicar el teorema de Cauchy, sino que en su lugar tenemos el teorema de los residuos, que dice que la integral a lo largo de un arco cerrado será una combinación lineal entera de los residuos de f multiplicados por $2\pi i$. Pese a ello podemos hablar aún de la integral (10.1), si bien ahora se trata de una integral multiforme meromorfa, en el sentido de que en un entorno de cada punto que no sea un polo de f podemos determinar ramas uniformes meromorfas de la integral. Un caso típico es la integral

$$\int_1^z \frac{d\zeta}{\zeta},$$

que determina la función logaritmo en $\mathbb{C} \setminus \{0\}$.

Para acercarnos a la situación que encontraremos al tratar con superficies, podemos definir los periodos polares de una función meromorfa f como los números complejos $2\pi i \operatorname{Res}_z f$, donde z recorre los polos de U, y así podemos decir que (10.1) está definida módulo los periodos polares de f. No obstante, observemos que si f tiene todos sus residuos nulos, entonces la integral (10.1) define todavía una función uniforme en U.

Si pasamos a considerar integrales de formas diferenciales en una superficie de Riemann, en primer lugar nos encontramos con que, salvo en el caso trivial de la esfera, ya no estamos en un espacio simplemente conexo, por lo que el

[1] Para más detalles, ver mi libro de *Topología algebraica.*

teorema de Cauchy no es válido ni siquiera para integrales de formas holomorfas. Por ejemplo, si integramos una forma holomorfa en un toro a lo largo de un arco que una dos puntos, el resultado dependerá del número de vueltas que demos al toro. De hecho hay dos clases de vueltas distintas: las que damos transversalmente, alrededor del "tubo" y las que damos longitudinalmente, a lo largo del "tubo". Los valores que toma la integral sobre dos arcos cerrados que den una única vuelta transversal y longitudinal respectivamente se llaman periodos de la integral, y de nuevo sucede que la integral entre dos puntos está bien definida módulo estos dos periodos.

Si el integrando es una forma meromorfa, además de los periodos en el sentido anterior tenemos también periodos polares, como en el caso plano (salvo que la forma tenga residuos nulos, es decir, salvo que sea de segunda clase).

A partir de aquí S será una superficie arbitraria, es decir, una variedad diferencial de dimensión 2, no necesariamente conexa o compacta, ni dotada en principio de una estructura analítica. Así mismo $\mathbb{A}$ será un anillo (que en la práctica será siempre $\mathbb{Z}$, $\mathbb{R}$ o $\mathbb{C}$).

Homología singular Definimos los *símplices canónicos* como

$$\Delta_0 = \{0\}, \quad \Delta_1 = [0,1], \quad \Delta_2 = \{(x,y) \in \mathbb{R}^2 \mid x \geq 0,\ y \geq 0,\ x+y \leq 1\}.$$

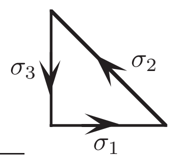
Para $p = 0, 1, 2$, un *p-símplice singular* en una superficie S es una aplicación diferenciable $\sigma : \Delta_p \longrightarrow S$. Para $p = 0$ la diferenciabilidad no significa nada (de modo que los 0-símplices de S pueden identificarse con sus puntos), mientras que para $p \geq 1$ la diferenciabilidad ha de entenderse como que σ se extiende a una aplicación diferenciable[2] de un entorno abierto de Δ_p en $\mathbb{R}^p$ a S. Así, los 1-símplices son los arcos diferenciables en S y los 2-símplices son los triángulos diferenciables (si bien no exigimos que σ sea inyectiva, por lo que la imagen de σ no tiene por qué ser homeomorfa a un segmento o a un triángulo).

Definimos $C_p(S)$ como el $\mathbb{A}$-módulo libre generado por el conjunto de todos los p-símplices en S. A sus elementos los llamaremos *p-cadenas singulares* de S. Definimos los *operadores frontera*

$$C_2(V) \xrightarrow{\partial_2} C_1(V) \xrightarrow{\partial_1} C_0(V)$$

como los homomorfismos dados por $\partial_1(\sigma) = \sigma(1) - \sigma(0)$ y $\partial_2(\sigma) = \sigma_1 + \sigma_2 + \sigma_3$, donde

$$\sigma_1(t) = \sigma(t,0), \qquad \sigma_2(t) = \sigma(1-t,t), \qquad \sigma_3(t) = \sigma(0,1-t).$$



[2]Aquí "diferenciable" significará siempre "de clase C^∞".

Llamaremos *ciclos* a los elementos del submódulo

$$Z_1(S) = \{c \in C_1(S) \mid \partial_1 c = 0\} \subset C_1(S)$$

y *fronteras* a los elementos de

$$F_1(S) = \partial_2[C_2(S)].$$

Se cumple que $\partial_2 \circ \partial_1 = 0$, por lo que $F_1(S) \subset Z_1(S)$, lo cual permite definir el *grupo de homología singular* de S como

$$H_1(S) = Z_1(S)/F_1(S).$$

Cuando dos cadenas se diferencian en una frontera se dice que son *homólogas*, por lo que los elementos de $H_1(S)$ se llaman *clases de homología* de S.

Es claro que si $\phi : S \longrightarrow T$ es una aplicación diferenciable entre dos superficies, podemos definir

$$\phi_\sharp : C_p(S) \longrightarrow C_p(T)$$

como el homomorfismo de módulos que sobre cada símplice actúa en la forma $\phi_\sharp(\sigma) = \sigma \circ \phi$. Se cumple la relación $\phi_\sharp \circ \partial_p = \partial_p \circ \phi_\sharp$, con lo que, en particular, $\phi_\sharp$ transforma ciclos en ciclos y fronteras en fronteras. A su vez, esto implica que $\phi_\sharp$ induce un homomorfismo

$$\phi_* : H_1(S) \longrightarrow H_1(T).$$

Cohomología de De Rham Para $p = 0,\ 1,\ 2$, definimos $\Lambda^p(S)$ como el espacio vectorial de las p-formas diferenciales en S (de clase C^∞). Se entiende que $\Lambda^0(S) = C^\infty(S)$ es el espacio de todas las funciones diferenciables en S.

Para $p = 0,\ 1$ tenemos definida la diferencial $d : \Lambda^p(S) \longrightarrow \Lambda^{p+1}(S)$. Llamaremos *formas diferenciales cerradas* a los elementos del subespacio

$$Z^1(S) = \{\omega \in \Lambda^p(S) \mid d\omega = 0\},$$

mientras que las *formas diferenciales exactas* serán los elementos del subespacio

$$F^1(S) = d[\Lambda^0(S)].$$

Teniendo en cuenta que $d_0 \circ d_1 = 0$ resulta que $F^1(S) \subset Z^1(S)$, por lo que podemos definir el *grupo de cohomología de De Rham* como

$$H^1(S) = Z^1(S)/F^1(S).$$

Si $\omega \in \Lambda^p(S)$ y σ es un p-símplice en S, podemos definir

$$\int_\sigma \omega = \int_{\Delta_p} \sigma^\sharp(\omega),$$

donde la integral de la derecha es una integral de Lebesgue y $\sigma^\sharp(\omega)$ es la p-forma en $\mathbb{R}^p$ dada por

$$\sigma^\sharp(\omega)_a(v_1,\ldots,v_p) = \omega_{\sigma(a)}(d\sigma_a(v_1),\ldots,d\sigma_a(v_p)).$$

Para $p = 0$ ha de entenderse que

$$\int_\sigma \omega = \omega(p).$$

Para una cadena $c = \sum\limits_{i=1}^{n} \alpha_i\sigma_i$ (con $\alpha_i \in \mathbb{R}$), definimos

$$\int_c \omega = \sum_{i=1}^{n} \alpha_i \int_{\sigma_i} \omega.$$

De este modo, la integral es una forma bilineal

$$\int : C_p(S) \times \Lambda^p(S) \longrightarrow \mathbb{R}.$$

El *teorema de Stokes* afirma que, para toda cadena $c \in C_2(S)$ y toda forma $\omega \in \Lambda^1(S)$, se cumple la relación

$$\int_{\partial c} \omega = \int_c d\omega.$$

En particular, la integral de una forma cerrada sobre una frontera o de una forma exacta sobre un ciclo es nula, por lo que la integral induce una forma bilineal

$$\int^* : H_1(S) \times H^1(S) \longrightarrow \mathbb{R}.$$

Si $\phi : S \longrightarrow T$ es una aplicación diferenciable entre superficies, podemos definir la aplicación lineal $\phi^\sharp : \Lambda^p(T) \longrightarrow \Lambda^p(S)$ mediante

$$\phi^\sharp(\omega)_x(v_1,\ldots,v_p) = \omega_{\phi(x)}(d\phi_x(v_1),\ldots,d\phi_x(v_p)).$$

Se comprueba que $\phi^\sharp \circ d = d \circ \phi^\sharp$, por lo que $\phi^\sharp$ transforma formas cerradas en formas cerradas y formas exactas en formas exactas, luego induce una aplicación lineal

$$\phi^* : H^1(T) \longrightarrow H^1(S).$$

El *teorema de cambio de variable* afirma que si $\phi : S \longrightarrow T$ es diferenciable entonces

$$\int_{\phi_\sharp(c)} \omega = \int_c \phi^\sharp(\omega). \tag{10.2}$$

En particular

$$\int^*_{\phi_*([c])} [\omega] = \int^*_{[c]} \phi^*([\omega]). \tag{10.3}$$

Para calcular $\phi^\sharp$ es útil la relación $\phi^\sharp(f\omega) = \phi^\sharp(f)\phi^\sharp(\omega) = (\phi \circ f)\phi^\sharp(\omega)$.

Variedades analíticas Veamos ahora cómo traducir los resultados precedentes a sus análogos complejos sobre variedades analíticas. Suponemos, pues, que S tiene una estructura analítica. Definimos

$$\Lambda^p(S,\mathbb{C}) = \mathbb{C}\otimes_{\mathbb{R}} \Lambda^p(S,\mathbb{R}) = \{\omega_1 + i\omega_2 \mid \omega_1,\omega_2 \in \Lambda^p(S,\mathbb{R})\},$$

de modo que $\Lambda^0(S,\mathbb{C})$ es el conjunto de las funciones diferenciables de S en $\mathbb{C}$. Similarmente, si $\omega \in \Lambda^1(S,\mathbb{C})$ y $x \in S$, entonces ω_p puede verse como un elemento de $T_x(S,\mathbb{C})^*$, según vimos en el capítulo I. Esto nos permite definir puntualmente el producto de una función $f \in \Lambda^0(S,\mathbb{C})$ por una forma $\omega \in \Lambda^1(S,\mathbb{C})$.

Definimos $d : \Lambda^p(S,\mathbb{C}) \longrightarrow \Lambda^{p+1}(S,\mathbb{C})$ mediante $d(\omega_1 + i\omega_2) = d\omega_1 + id\omega_2$. Notemos que si $f \in \Lambda^0(S,\mathbb{C})$ entonces $df|_p$ coincide con la diferencial definida en el capítulo I. En particular, si S es el dominio de una carta z, entonces toda $\omega \in \Lambda^1(S,\mathbb{C})$ es de la forma $\omega = f\,dz + g\,d\bar{z}$, donde f, $g \in \Lambda^0(S,\mathbb{C})$ y si $f \in \Lambda^0(S,\mathbb{C})$ entonces

$$df = \frac{\partial f}{\partial z}\,dz + \frac{\partial f}{\partial \bar{z}}\,d\bar{z}.$$

Este operador d permite definir un grupo de cohomología $H^1(S,\mathbb{C})$ análogamente al caso real, y es claro que la asignación $[\omega_1] + i[\omega_2] \mapsto [\omega_1 + i\omega_2]$ determina un isomorfismo $\mathbb{C}\otimes_{\mathbb{R}} H^1(S,\mathbb{R}) \cong H^1(S,\mathbb{C})$. Así mismo es fácil ver que $H_1(S,\mathbb{C}) \cong \mathbb{C}\otimes_{\mathbb{R}} H_1(S,\mathbb{R})$.

Definimos la integral de una forma $\omega = \omega_1 + i\omega_2 \in \Lambda^p(S,\mathbb{C})$ sobre un símplice $\sigma \in C_p(S,\mathbb{C})$ mediante

$$\int_\sigma \omega = \int_\sigma \omega_1 + i\int_\sigma \omega_2.$$

Por linealidad, la integral se extiende a una forma bilineal

$$\int : C_p(S,\mathbb{C}) \times \Lambda^p(S,\mathbb{C}) \longrightarrow \mathbb{C}.$$

La versión compleja del teorema de Stokes se sigue inmediatamente de la versión real, lo cual nos permite definir una forma bilineal

$$\int^* : H_1(S,\mathbb{C}) \times H^1(S,\mathbb{C}) \longrightarrow \mathbb{C}.$$

Si $\phi : S \longrightarrow T$ es una aplicación diferenciable, definimos la aplicación lineal $\phi^\sharp : \Lambda^p(T,\mathbb{C}) \longrightarrow \Lambda^p(S,\mathbb{C})$ mediante $\phi^\sharp(\omega_1 + i\omega_2) = \phi^\sharp(\omega_1) + i\phi^\sharp(\omega_2)$. Se comprueba inmediatamente que $\phi^\sharp \circ d = d \circ \phi^\sharp$, por lo que $\phi^\sharp$ induce una aplicación lineal $\phi^* : H^1(T,\mathbb{C}) \longrightarrow H^1(S,\mathbb{C})$ y las fórmulas (10.2) y (10.3) se generalizan trivialmente al caso complejo. Así mismo es fácil probar las relaciones

$$\phi^\sharp(f\omega) = (\phi\circ f)\phi^\sharp(\omega), \qquad \phi^\sharp(\omega)_x(v) = \omega_{\phi(x)}(d\phi_x(v)), \quad \omega \in \Lambda^1(S,\mathbb{C}).$$

Formas holomorfas En el capítulo anterior hemos definido las formas diferenciales holomorfas en una superficie S como las aplicaciones que a cada punto $x \in S$ le hacen corresponder un $\omega_x \in T_xS^*$, de modo que localmente $\omega = f\,dz$, donde z es una función coordenada y f una función holomorfa.

En el capítulo I vimos que $T_x(S, \mathbb{C}) = T_x(S) \oplus T_x^a(S)$, donde el segundo sumando es el espacio tangente antiholomorfo, por lo que las cada forma holomorfa puede identificarse con un elemento de $\Lambda^1(S, \mathbb{C})$ que se anula sobre los vectores tangentes antiholomorfos. Más concretamente, una forma $\omega \in \Lambda^1(S, \mathbb{C})$ es holomorfa si y sólo si su restricción a cualquier abierto coordenado (U, z) es de la forma $\omega|_U = f\,dz$, donde f es una función holomorfa en U. Llamaremos $\Lambda^1(S)$ al espacio de todas las formas diferenciales holomorfas en S.

Todas las formas holomorfas son cerradas. En efecto, si $\omega \in \Lambda^1(S, \mathbb{C})$ es holomorfa y $x \in S$, tomamos una carta z en un entorno U de x, de modo que

$$\omega|_U = f\,dz = \operatorname{Re} f\,dx - \operatorname{Im} f\,dy + i(\operatorname{Im} f\,dx + \operatorname{Re} f\,dy),$$

para una cierta función homomorfa f. Teniendo en cuenta que la diferencial es un operador local, vemos que

$$d\omega|_U = \left(-\frac{\partial \operatorname{Re} f}{\partial y} - \frac{\partial \operatorname{Im} f}{\partial x}\right) dx \wedge dy + i\left(-\frac{\partial \operatorname{Im} f}{\partial y} + \frac{\partial \operatorname{Re} f}{\partial x}\right) dx \wedge dy.$$

Como f satisface las ecuaciones de Cauchy-Riemann, concluimos que $d\omega = 0$.

Por otra parte, si una forma holomorfa ω cumple $\omega = dg$, para cierta función $g \in \Lambda^0(S, \mathbb{C})$, de hecho ha de ser $g \in \mathcal{H}(S)$. En efecto, en un entorno coordenado U de un punto arbitrario tenemos que

$$\omega|_U = dg|_U = \frac{\partial \operatorname{Re} g}{\partial x}\,dx + \frac{\partial \operatorname{Re} g}{\partial y}\,dy + i\frac{\partial \operatorname{Im} g}{\partial x}\,dx + i\frac{\partial \operatorname{Im} g}{\partial y}\,dy$$

y, por otra parte,

$$\omega|_U = f\,dz = \operatorname{Re} f\,dx - \operatorname{Im} f\,dy + i(\operatorname{Im} f\,dx + \operatorname{Re} f\,dy),$$

para una cierta función holomorfa f. Comparando ambas expresiones concluimos que g cumple las ecuaciones de Cauchy-Riemann, luego es una función holomorfa.

Esto implica que si definimos $\mathcal{H}^1(S)$ como el cociente del espacio $\Lambda^1(S)$ de las formas holomorfas en S sobre el subespacio de las diferenciales de funciones holomorfas, la aplicación $[\omega] \mapsto [\omega]$ es un monomorfismo de $\mathcal{H}^1(S)$ en $H^1(S, \mathbb{C})$. En general no es un isomorfismo.

Notemos que estos hechos generalizan el teorema de Cauchy sobre integrales curvilíneas. En efecto, si c es una 2-cadena en una superficie analítica S y ω es una forma diferencial holomorfa en S, entonces

$$\int_{\partial c} \omega = \int_c d\omega = \int_c 0 = 0.$$

El teorema de Cauchy clásico se sigue de aquí porque, como es sabido, si S es simplemente conexa entonces $H_1(S,\mathbb{C})=0$, es decir, todo ciclo es una frontera.

Se comprueba fácilmente que si $\phi : S \longrightarrow T$ es una aplicación holomorfa entre variedades analíticas, entonces $\phi^\sharp$ se restringe a una aplicación lineal

$$\phi^\sharp : \Lambda^1(T) \longrightarrow \Lambda^1(S),$$

que a su vez induce $\phi^* : \mathcal{H}^1(T) \longrightarrow \mathcal{H}^1(S)$.

Observemos ahora que si $\sigma : [0,1] \longrightarrow U \subset \mathbb{C}$ es un 1-símplice en un abierto de $\mathbb{C}$, entonces la integral $\int_\sigma f\,dz$ coincide con la integral curvilínea usual en variable compleja. En efecto,

$$\int_\sigma f\,dz = \int_0^1 \sigma^\sharp(f\,dz) = \int_0^1 \sigma^\sharp(f\,dz)(\partial_t)\,dt = \int_0^1 f(\sigma(t))d\sigma_t(\partial_t)(z)\,dt$$

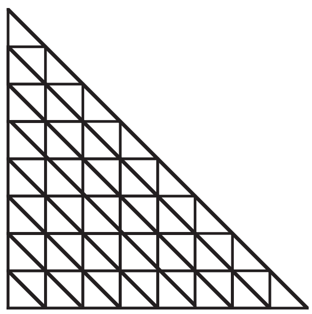
$$= \int_0^1 f(\sigma(t))\frac{\partial \sigma \circ z}{\partial t}\,dt = \int_0^1 f(\sigma(t))\sigma'(t)\,dt.$$

Por otro lado, supongamos ahora que S puede cubrirse por una carta z y que $\omega = f\,dz$ es una forma diferencial meromorfa en en S (que, por consiguiente, es una forma holomorfa en S menos un número finito de puntos). Sea $\tilde{f} = z^{-1}\circ f$ la lectura de f en la carta. Es claro entonces que $\omega = z^\sharp(\tilde{f}\,dz)$, donde en el segundo miembro z es la identidad en $\mathbb{C}$. Para cada $x \in S$, el desarrollo de f en potencias de $z - z(x)$ es el mismo que el de $\tilde{f}$, luego, en particular, $\operatorname{Res}_x \omega = \operatorname{Res}_{z(x)} \tilde{f}$. Esto nos permite traducir el teorema de los residuos a integrales en variedades:

Supongamos que $\sigma : \Delta_2 \longrightarrow S$ es un 2-símplice positivamente orientado que se extienda a un difeomorfismo y cuya frontera no contenga polos de ω. Entonces

$$\int_{\partial\sigma} \omega = \int_{\partial\sigma} z^\sharp(\tilde{f}\,dz) = \int_{z_\sharp(\partial\sigma)} \tilde{f}\,dz = \int_{\partial(\sigma\circ z)} \tilde{f}\,dz = 2\pi i \sum_x \operatorname{Res}_x \omega,$$

donde x recorre los polos de ω contenidos en la imagen de σ (que se corresponden con los polos de $\tilde{f}$ contenidos en la imagen de $\sigma \circ z$).



Un poco más laxamente: si $\sigma : \Delta_2 \longrightarrow S$ es un 2-símplice arbitrario y ω es una forma meromorfa que no tenga polos en la imagen de c, podemos subdividir Δ_2 en triángulos suficientemente pequeños como para que sus imágenes por σ estén contenidas en el dominio de una carta de S. Además podemos retocar levemente la subdivisión para que ningún polo de ω se encuentre sobre los lados de los triángulos obtenidos. Entonces la integral de ω sobre $\partial\sigma$ es igual a la suma de las integrales de ω sobre las fronteras de todos los triángulos pequeños, pues las integrales sobre los lados interiores se cancelan dos a dos y las de los lados exteriores se suman hasta formar $\partial\sigma$.

Al igual que hemos visto antes (aunque sin suponer que los triángulos sean biyectivos) la integral de ω sobre cada uno de estos triángulos equivale a la integral de otra función $\tilde{f}$ sobre un ciclo en un abierto de $\mathbb{C}$, cuyos residuos se corresponden con (algunos de) los de ω. El teorema de los residuos nos da que la integral

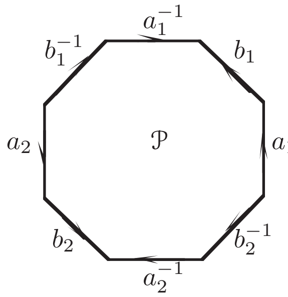
$$\int_{\partial\sigma} \omega$$

es combinación lineal entera de los *periodos polares* $2\pi i \operatorname{Res}_P \omega$ de ω. Por linealidad lo mismo vale para integrales sobre fronteras arbitrarias.

Superficies de Riemann Supongamos ahora que S es una superficie de Riemann (compacta). El teorema de clasificación de superficies compactas afirma que toda superficie (topológica) compacta orientable de género $g \geq 1$ puede obtenerse como cociente de un polígono regular $\mathcal{P}$ de $4g$ lados identificándolos dos a dos en la forma

$$a_1 b_1 a_1^{-1} b_1^{-1} a_2 b_2 a_2^{-1} b_2^{-1} \cdots a_g b_g a_g^{-1} b_g^{-1}.$$

Sea $\phi : \mathcal{P} \longrightarrow S$ la aplicación continua y suprayectiva (inyectiva en el interior de $\mathcal{P}$) que identifica los lados de $\mathcal{P}$ en la forma indicada. Por ejemplo, la figura muestra el polígono cuyo cociente es la superficie de género 2:



Cada arco a_k (recorrido en el sentido de la flecha) se corresponde en S con el mismo arco que a_k^{-1}, e igualmente con los b_k. En general, todos los vértices de $\mathcal{P}$ se identifican con un mismo punto de S, y así, en S tenemos $2g$ arcos cerrados $a_1, b_1, \ldots, a_g, b_g$.

En la prueba del teorema de clasificación se ve que el polígono $\mathcal{P}$ se construye a partir de una triangulación de S. En el capítulo IV hemos visto que las superficies de Riemann se pueden triangular, y la prueba muestra que los triángulos se pueden tomar diferenciables, es decir, podemos tomarla formada por triángulos $\sigma : \Delta_2 \longrightarrow S$ que se extienden a difeomorfismos de un entorno simplemente conexo de Δ_2 en un entorno de la imagen.

Añadiendo este hecho a la prueba del teorema de clasificación se ve que la aplicación $\phi : \mathcal{P} \longrightarrow S$ se puede tomar diferenciable a trozos, es decir, que se puede triangular $\mathcal{P}$ de modo que ϕ coincida con un difeomorfismo en cada triángulo.

Si además elegimos los triángulos de $\mathcal{P}$ de forma que conserven la orientación, tenemos que los lados interiores (compartidos por dos triángulos contiguos) se recorren necesariamente en sentidos opuestos, por lo que constituyen 1-cadenas homólogas en $\mathcal{P}$. Esto nos permite ver a la triangulación de $\mathcal{P}$ como una cadena $\zeta_{\mathcal{P}} \in C_2(\mathcal{P}, \mathbb{Z})$ cuya frontera es homóloga al ciclo

$$a_1 + b_1 - a_1^{-1} - b_1^{-1} + a_2 + \cdots$$

El hecho de que ϕ sea diferenciable a trozos hace que $\zeta_S = \phi_\sharp(\zeta_{\mathcal{P}})$ (que no es sino la triangulación de S) sea también una cadena en S, cuya frontera es ahora

$$a_1 + b_1 - a_1 - b_1 + \cdots = 0.$$

Se demuestra que las clases de los ciclos $a_1, b_1, \ldots, a_g, b_g$ forman una base de $H_1(S, \mathbb{Z})$. En lo sucesivo, salvo que indiquemos lo contrario, cuando hablemos de una base de $H_1(S)$ se entenderá que es una base obtenida de esta forma a partir de un polígono.

La cohomología de las formas holomorfas es especialmente simple: observemos que las únicas funciones holomorfas en S son las constantes, luego no existen formas diferenciales holomorfas exactas (salvo la forma nula). Esto significa que $\mathcal{H}^1(S) = \Lambda^1(S)$ (sin ninguna identificación).

10.2 Integración de formas meromorfas

En 9.24 hemos distinguido tres clases de diferenciales en un cuerpo de funciones algebraicas K. En particular, si K es el cuerpo de funciones meromorfas de una superficie de Riemann S, entonces los divisores primos de K se identifican con los puntos de S y las formas diferenciales de K son las formas diferenciales meromorfas en S. Las diferenciales que hemos llamado de primera clase son simplemente las diferenciales holomorfas, mientras que las diferenciales de segunda clase son las que tienen integral nula sobre las fronteras en S pues, según hemos visto en la sección anterior, la integral de una forma meromorfa ω sobre una frontera es una combinación lineal de sus periodos polares, es decir, de los números $2\pi i \operatorname{Res}_P \omega$.

Sea ω una forma diferencial en una superficie de Riemann S y sea $a_1, \ldots, a_g$, $b_1, \ldots, b_g$ una base de $H_1(S)$ en las condiciones de la sección anterior, es decir, obtenida a partir de una identificación $\phi : \mathcal{P} \longrightarrow S$, donde $\mathcal{P}$ es un polígono de $4g$ lados. Podemos suponer que los ciclos a_k, b_k no pasan por polos de ω (por ejemplo, porque existe un difeomorfismo de S en sí misma que transforma cualquier conjunto finito de puntos prefijado en cualquier otro).

Llamaremos *periodos cíclicos* (o simplemente periodos) de ω (respecto a la base fijada) a los números complejos

$$A_k = \int_{a_k} \omega, \qquad B_k = \int_{b_k} \omega, \qquad k = 1, \ldots, g.$$

Si z es un ciclo en S, tenemos que su clase de homología se expresa como

$$[z] = \sum_{k=1}^{g} (m_k[a_k] + n_k[b_k]), \tag{10.4}$$

para ciertos $m_k, n_k \in \mathbb{Z}$, luego

$$z = \sum_{k=1}^{g} (m_k a_k + n_k b_k) + \partial c,$$

para cierta 2-cadena c en S. Consecuentemente,

$$\int_z \omega = \sum_{k=1}^{g} (m_k A_k + n_k B_k) + \int_{\partial c} \omega.$$

Por el teorema de los residuos, la última integral es combinación lineal entera de los residuos polares de ω. En resumen:

Teorema 10.1 *Si S es una superficie de Riemann de género $g \geq 1$ y ω es una forma diferencial meromorfa en S, entonces las integrales de ω sobre ciclos en S recorren el grupo generado por los periodos (polares y cíclicos) de ω.*

Notemos que ciertamente se recorre todo el grupo porque integrando sobre una pequeña circunferencia alrededor de un polo obtenemos el correspondiente periodo polar. Este teorema muestra que, aunque los periodos de ω dependen de la elección de la base de homología respecto a la que se calculan, el grupo de periodos es independiente de ella.

Fijado un punto $O \in S$, la integral

$$\int_O^P \omega$$

define una función holomorfa multiforme en S menos los polos de ω. Dos valores de la integral en un mismo punto P (calculados con arcos distintos de extremos O y P) se diferencian en un elemento del grupo de periodos de ω.

En el estudio de las integrales abelianas será fundamental una fórmula que vamos a deducir a continuación. Fijemos una forma diferencial ω de primera clase y una forma η arbitraria. Tomamos una base de homología a_k, b_k construida a partir de una identificación $\phi : \mathcal{P} \longrightarrow S$, donde $\mathcal{P}$ es un polígono en forma canónica. Podemos exigir que los ciclos no pasen por polos de η. Llamemos

$$A_k = \int_{a_k} \omega, \quad B_k = \int_{B_k} \omega, \quad A_k' = \int_{a_k} \eta, \quad B_k' = \int_{b_k} \eta.$$

Sea $D \subset S$ la imagen por ϕ del interior de $\mathcal{P}$, que es un abierto simplemente conexo en S. Si P_1 y P_2 son puntos de D, podemos definir

$$\int_{P_1}^{P_2} \omega$$

como la integral sobre cualquier arco en D que una P_1 con P_2. Fijado un punto $O \in D$, la función $g : D \longrightarrow \mathbb{C}$ dada por

$$g(P) = \int_O^P \omega$$

es holomorfa (uniforme) en D.

Sea ζ_S una triangulación (orientada) de S diferenciable a trozos (vista como 2-cadena en S). Podemos suponer que los lados de los triángulos no pasan por polos de η. Sabemos que $\partial\zeta_S = 0$, lo cual significa que cada arista es compartida por dos triángulos pero recorrida en sentidos opuestos. Observemos ahora que si $\sigma : \Delta_2 \longrightarrow S$ es uno de los triángulos, entonces la restricción de g al interior de su imagen se extiende a una función holomorfa en un entorno de $\sigma[\Delta_2]$. En efecto, basta considerar un abierto simplemente conexo U que contenga a $\sigma[\Delta_2]$. Fijado un punto P_1 en el interior de $\sigma[\Delta_2]$, tenemos que, para cualquier otro punto P en dicho interior,

$$g(P) = \int_O^{P_1} \omega + \int_{P_1}^{P} \omega,$$

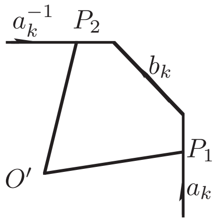
donde la segunda integral se calcula respecto de cualquier arco contenido en U que una P_1 con P, pero esta integral define una función holomorfa en U, que nos permite definir la extensión holomorfa que buscábamos. Obviamente esta extensión es única.

La construcción muestra que si $P \in \sigma[\Delta_2]$, entonces

$$g(P) = \int_O^{P} \omega,$$

donde la integral se calcula sobre cualquier arco que una O con P y que esté contenido en D salvo a lo sumo en su extremo final.

Consideremos ahora un punto P situado sobre la arista común de dos triángulos σ_1 y σ_2 y vamos a calcular la relación entre los valores $g_1(P)$ y $g_2(P)$. Si $P \in D$ tenemos $g_1(P) = g_2(P) = g(P)$. En caso contrario P es la imagen por ϕ de dos puntos P_1 y P_2 situados en la frontera de $\mathcal{P}$, tal y como muestra la figura.



(En realidad la figura ilustra una posibilidad. La otra es que P_1 y P_2 estén sobre dos lados b_k y b_k^{-1}, en cuyo caso la flecha del lado intermedio tendría sentido opuesto.) Llamamos O' al punto de $\mathcal{P}$ que se corresponde con O.

La poligonal γ que va de O' a P_1, de P_1 a P_2 sobre la frontera de $\mathcal{P}$ y de P_2 a O' es un ciclo en $\mathcal{P}$, y como éste es simplemente conexo, γ es una frontera. Por consiguiente, su imagen $\phi_\sharp(\gamma)$ es una frontera en S, luego

$$0 = \int_{\phi_\sharp(\gamma)} \omega = g_1(P) + B_k - g_2(P),$$

donde hemos usado que las integrales sobre los dos fragmentos de a_k y a_k^{-1} se cancelan porque, en S, son integrales de la misma forma ω sobre el mismo arco recorrido en sentidos opuestos. Así pues, $g_1(P) - g_2(P) = -B_k$.

Similarmente, si P_1 está en b_k y P_2 en b_k^{-1}, resulta $g_1(P) - g_2(P) = A_k$.

Sea $\zeta_S = \sigma_1 + \cdots + \sigma_r$ la triangulación que hemos tomado. Definimos

$$\Sigma = \sum_{j=1}^{r} \int_{\partial\sigma_j} g_j \eta, \tag{10.5}$$

donde g_j es la extensión de g al triángulo σ_j.

Cada lado interior a D es recorrido dos veces en sentidos opuestos y, sobre ellos, la función g_j es la misma en ambos casos (pues coincide con la función g definida sobre D), luego las integrales se cancelan, y sólo quedan los términos correspondientes a lados contenidos en los arcos a_k y b_k. Éstos no se cancelan, porque para cada punto $P = \phi(P_1) = \phi(P_2)$ situado sobre uno de estos lados, con P_1 sobre a_k (o b_k) y P_2 sobre a_k^{-1} (o b_k^{-1}), la función g_j toma valores diferentes, digamos $g^+(P)$ cuando recorremos a_k o b_k positivamente y $g^-(P)$ cuando lo hacemos negativamente. El resultado es

$$\begin{aligned} S &= \sum_{k=1}^{g} \left(\int_{a_k} g^+\eta + \int_{b_k} g^+\eta - \int_{a_k} g^-\eta - \int_{b_k} g^-\eta \right) \\ &= \sum_{k=1}^{g} \left(\int_{b_k} (g^+ - g^-)\eta + \int_{a_k} (g^+ - g^-)\eta \right). \end{aligned}$$

Pero hemos visto que $g^+(P) - g^-(P) = A_k$ sobre b_k y $g^+(P) - g^-(P) = -B_k$ sobre a_k. Por consiguiente,

$$\Sigma = \sum_{k=1}^{g} (A_k B_k' - B_k A_k').$$

Por otra parte, podemos evaluar Σ calculando la integral sobre cada triángulo. Observemos que $g_j\eta$ es una forma diferencial meromorfa en un entorno (simplemente conexo) de cada uno de ellos. Subdividiendo la triangulación si es preciso, no perdemos generalidad si suponemos que dicho entorno es el dominio de una carta. Así, aplicando el teorema de los residuos vemos que

$$\Sigma = 2\pi i \sum_P \operatorname{Res}_P(g\eta),$$

donde P recorre los polos de η y g es ahora la función holomorfa (fija) definida en D. Si suponemos que η es una diferencial de tercera clase, entonces se cumple $\operatorname{Res}_P(g\eta) = g(P) \operatorname{Res}_P \eta$, pues si $g(P) = 0$ entonces $g\eta$ es holomorfa en P y su residuo es nulo.

En resumen, si ω es una diferencial de primera clase y η de tercera clase, sus periodos cíclicos A_k, B_k, A_k', B_k' y los periodos polares de η (es decir, los números $2\pi i \operatorname{Res}_P \eta$) satisfacen la relación:

$$\sum_{k=1}^{g} (A_k B_k' - B_k A_k') = 2\pi i \sum_P g(P) \operatorname{Res}_P \eta. \tag{10.6}$$

Si η es también una diferencial de primera clase, el segundo miembro es nulo, con lo que obtenemos el siguiente caso particular:

Teorema 10.2 (Primeras relaciones de Riemann) *Sean ω y η dos diferenciales de primera clase en una superficie de Riemann S de género $g \geq 1$, sean A_k, B_k los periodos de ω y A'_k, B'_k los periodos de η. Entonces*

$$\sum_{k=1}^{g} (A_k B'_k - B_k A'_k) = 0.$$

Más importante es la relación siguiente, pues de ella se deduce que si dos diferenciales de primera clase tienen los mismos A-periodos (o los mismos B-periodos) entonces son iguales:

Teorema 10.3 (Segundas relaciones de Riemann) *Si A_k y B_k son los periodos de una diferencial de primera clase no nula ω en una superficie de Riemann S de género $g \geq 1$, entonces*

$$i \sum_{k=1}^{g} (A_k \bar{B}_k - B_k \bar{A}_k) > 0.$$

Demostración: Consideramos

$$\Sigma' = \sum_{j=1}^{r} \int_{\partial \sigma_j} \bar{g}_j \omega,$$

donde g_j y σ_j son los mismos que en (10.5). El mismo razonamiento que hemos aplicado a Σ nos da ahora que

$$\Sigma' = \sum_{k=1}^{g} (\bar{A}_k B_k - \bar{B}_k A_k),$$

luego basta probar que, para cada j,

$$-i \int_{\partial \sigma_j} \bar{g}_j \omega > 0.$$

Recordemos que, salvo un sumando constante, la función g_j se obtiene integrando ω desde un punto fijo de σ_j, por lo que $\omega|_{\sigma_j[\Delta_2]} = dg_j$. Sin embargo, ahora no podemos decir que la integral sobre $\partial \sigma_j$ es nula porque la forma $\bar{g}_j \omega$ no es holomorfa. Vamos a calcularla explícitamente.

Sea $g_j = u + iv$, de modo que $\omega = dg_j = du + idv$. Aplicamos el teorema de Stokes:

$$-i \int_{\partial \sigma_j} \bar{g}_j \omega = -i \int_{\partial \sigma_j} ((u\,du + v\,dv) + i(u\,dv - v\,du)) = \int_{\sigma_j} du \wedge dv.$$

Podemos suponer que $\sigma_j[\Delta_2]$ está contenido en el dominio de una carta z, con lo que

$$du \wedge dv = \left(\frac{\partial \operatorname{Re} g_j}{\partial x}\, dx + \frac{\partial \operatorname{Re} g_j}{\partial y}\, dy \right) \wedge \left(\frac{\partial \operatorname{Im} g_j}{\partial x}\, dx + \frac{\partial \operatorname{Im} g_j}{\partial y}\, dy \right)$$

$$= \left(\frac{\partial \operatorname{Re} g_j}{\partial x}\frac{\partial \operatorname{Im} g_j}{\partial y} - \frac{\partial \operatorname{Re} g_j}{\partial y}\frac{\partial \operatorname{Im} g_j}{\partial x}\right) dx \wedge dy$$

$$= \left(\left(\frac{\partial \operatorname{Re} g_j}{\partial x}\right)^2 + \left(\frac{\partial \operatorname{Re} g_j}{\partial y}\right)^2\right) dx \wedge dy.$$

Así pues, al transportar la integral mediante la carta, obtenemos

$$\int_{\sigma_j} du \wedge dv = \int_{z_\sharp(\sigma_j)} \left(\left(z^{-1} \circ \frac{\partial \operatorname{Re} g_j}{\partial x}\right)^2 + \left(z^{-1} \circ \frac{\partial \operatorname{Re} g_j}{\partial y}\right)^2\right) dxdy,$$

que es un número real estrictamente positivo, ya que si fuera cero entonces $\operatorname{Re} g_j$ sería constante en un abierto de S, al igual que $\operatorname{Im} g_j$ por las ecuaciones de Cauchy-Riemann, pero entonces g_j sería constante y ω sería nula. ■

Como ya hemos dicho, este teorema implica que si una diferencial de primera clase ω tiene todos sus A-periodos (o todos sus B-periodos) nulos, entonces es la forma nula. Más aún, comparando los dos teoremas anteriores vemos que si ω tiene todos sus periodos reales entonces ha de ser la forma nula.

Las relaciones de Riemann pueden expresarse matricialmente:

Teorema 10.4 (Relaciones de Riemann) *Sea $\Omega = (\omega_1, \ldots, \omega_g)$ una base del espacio de diferenciales de primera clase en una superficie de Riemann de género $g \geq 1$ y sean A_{jk}, B_{jk} los periodos de ω_j, que forman sendas matrices cuadradas A y B. Entonces $AB^t = BA^t$ y la matriz $i(A\bar{B}^t - B\bar{A}^t)$ es definida positiva.*

Demostración: No sólo vamos a probar lo que afirma el teorema, sino, de hecho, que este enunciado es equivalente a los enunciados de los dos teoremas precedentes.

Si $\omega = \alpha\Omega$ y $\eta = \beta\Omega$ son dos diferenciales de primera clase arbitrarias (donde α, $\beta \in \mathbb{C}^g$), los vectores de periodos de ω son αA, αB, y los de η son βA, βB. Las primeras relaciones de Riemann afirman que $\alpha AB^t\beta^t - \alpha BA^t\beta^t = 0$ o, equivalentemente, que $\alpha(AB^t - BA^t)\beta^t = 0$ para todos los α, $\beta \in \mathbb{C}^g$. Esto se reduce a la igualdad $AB^t = BA^t$.

Las segundas relaciones de Riemann afirman que si $\alpha \neq 0$ entonces

$$i(\alpha A\bar{B}^t\bar{\alpha}^t - \alpha B\bar{A}^t\bar{\alpha}^t) > 0$$

o, lo que es lo mismo, que $\alpha(i(A\bar{B}^t - B\bar{A}^t))\bar{\alpha}^t > 0$ para todo $\alpha \in \mathbb{C}^g$ no nulo. Esto es, por definición, que la matriz $i(A\bar{B}^t - B\bar{A}^t)$ es definida positiva. ■

Como consecuencia, la matriz A ha de ser regular, pues en caso contrario existiría un $\alpha \in \mathbb{C}^g$ no nulo tal que $\alpha A = 0$, lo que a su vez implicaría que $\alpha(i(A\bar{B}^t - B\bar{A}^t))\bar{\alpha}^t = 0$, en contradicción con el teorema anterior.

Observemos ahora que si M es una matriz regular y consideramos la base $\Omega' = \Omega M$, entonces $\omega_i' = \sum_k m_{ki}\omega_k$, y el periodo A_j' de ω_i' es $A_j' = \sum_k m_{ki}A_{kj}$, luego la matriz de A-periodos de Ω' es M^tA. En particular, tomando la matriz $M = (A^{-1})^t$, obtenemos una base cuya matriz de A-periodos es la identidad.

Definición 10.5 Sea S una superficie de Riemann de género $g \geq 1$. Una *base canónica* del espacio de diferenciales de primera clase de S (respecto de una base prefijada de $H_1(S)$) es una base tal que su matriz de A-periodos es la identidad.

Acabamos de demostrar que existen bases canónicas. Respecto a tales bases, las relaciones de Riemann se expresan de forma especialmente simple: las primeras relaciones afirman que la matriz B es simétrica, mientras que las segundas se reducen a que la matriz $i(\bar{B} - B) = 2\operatorname{Im} B$ es definida positiva. Puesto que se trata de una matriz real, esto implica que es definida positiva como matriz real, es decir, que $\alpha(\operatorname{Im} B)\alpha^t > 0$ para todo $\alpha \in \mathbb{R}^g$ no nulo.

A partir de una base canónica podemos formar diferenciales de primera clase con cualquier vector de A-periodos prefijado. Como consecuencia podemos dar una condición de unicidad en la descomposición de una forma diferencial:

Teorema 10.6 *Si ω es una forma diferencial en una superficie de Riemann de género $g \geq 1$, entonces ω se descompone de forma única como $\omega = \omega_1 + \omega_2 + \omega_3$, donde los sumandos son, respectivamente, una diferencial de primera clase, una diferencial de segunda clase con A-periodos nulos y una diferencial de tercera clase con A-periodos nulos (respecto de una base de homología prefijada cuyos ciclos no pasen por los polos de ω).*

Demostración: El teorema 9.26 nos da una diferencial de tercera clase ω_3' con los mismos polos de orden 1 que ω y con los mismos residuos, luego $\omega_2' = \omega - \omega_3$ es una diferencial de segunda clase. Sean ω_1' y ω_1'' diferenciales de primera clase con los mismos A-periodos que ω_2' y ω_3' respectivamente. Entonces $\omega_2 = \omega_2' - \omega_1'$ y $\omega_3 = \omega_3' - \omega_1''$ son diferenciales de segunda y tercera clase con A-periodos nulos y, llamando $\omega_1 = \omega_1' + \omega_1''$ tenemos $\omega = \omega_1 + \omega_2 + \omega_3$.

La descomposición es única, pues si $\omega = \omega_1' + \omega_2' + \omega_3'$ es otra descomposición en las mismas condiciones, entonces ω_1 y ω_1' son diferenciales de primera clase con los mismos A-periodos (los de ω), luego $\omega_1 - \omega_1'$ tiene A-periodos nulos y es, por consiguiente, la forma nula.

Similarmente, ω_3 y ω_3' tienen los mismos polos simples que ω con los mismos residuos, luego su diferencia no tiene polos, luego se trata también de una diferencial de primera clase con A-periodos nulos y por lo tanto $\omega_3 = \omega_3'$. Necesariamente entonces $\omega_2 = \omega_2'$. ■

El grupo de periodos de una forma diferencial es en general denso en $\mathbb{C}$, por lo que calcular una integral salvo periodos es hacer poco. La situación es distinta si trabajamos vectorialmente, como vamos a ver a continuación:

Sea $\Omega = (\omega_1, \ldots, \omega_g)$ una base del espacio de diferenciales de primera clase en una superficie de Riemann S. Definimos

$$A_k = \int_{a_k} \Omega = \left(\int_{a_k} \omega_1, \ldots, \int_{a_k} \omega_g \right) \in \mathbb{C}^g,$$

$$B_k = \int_{b_k} \Omega = \left(\int_{b_k} \omega_1, \ldots, \int_{b_k} \omega_g \right) \in \mathbb{C}^g.$$

A estos vectores los llamaremos *periodos* de Ω. Si z es un ciclo en S, la relación (10.4) implica que

$$\int_z \Omega = \left(\int_z \omega_1, \ldots, \int_z \omega_g \right)$$

es una combinación lineal entera de los periodos de Ω, por lo que si P, $Q \in S$, la integral

$$\int_P^Q \Omega = \left(\int_P^Q \omega_1, \ldots, \int_P^Q \omega_g \right),$$

(donde todas las integrales se calculan sobre un mismo arco que una P con Q) está definida salvo combinaciones enteras de los periodos de Ω. La diferencia es que, según se deduce del teorema siguiente, el grupo generado por los periodos es ahora un subespacio discreto de $\mathbb{C}^g$.

Teorema 10.7 *Sea S una superficie de Riemann de género $g \geq 1$ y sea Ω una base de las diferenciales de primera clase. Entonces, los periodos A_k, B_k de Ω (respecto a una base de $H_1(S)$) son linealmente independientes sobre $\mathbb{R}$.*

Demostración: Al construir las bases canónicas hemos visto que los periodos de dos bases distintas se corresponden por un automorfismo de $\mathbb{C}^g$, luego podemos suponer que la base Ω es canónica. Si vemos la matriz de periodos (A, B) como una matriz real de dimensión $2g \times 2g$, es decir, si desdoblamos cada fila en dos filas correspondientes a la parte real y la parte imaginaria, obtenemos una matriz de la forma

$$\left(\begin{array}{c|c} I & \operatorname{Re} B \\ \hline 0 & \operatorname{Im} B \end{array} \right)$$

Sabemos que $\operatorname{Im} B$ es definida positiva, luego en particular es regular, luego la matriz tiene determinante no nulo y sus columnas son linealmente independientes. ■

Por consiguiente, el grupo generado por los periodos de una base Ω es un retículo R_Ω en $\mathbb{C}^g$. Observemos que no depende de la elección de la base de homología, ya que

$$R_\Omega = \left\{ \int_\gamma \Omega \;\middle|\; \gamma \in Z_1(S) \right\}.$$

Por otra parte, los retículos asociados a dos bases del espacio de diferenciales de primera clase se corresponden a través de un automorfismo de $\mathbb{C}^g$, lo que implica que el toro complejo $\mathbb{C}^g/J_\Omega$ está determinado por S salvo un isomorfismo inducido por un automorfismo de $\mathbb{C}^g$, que es claramente una transformación conforme.

Definición 10.8 Si S es una superficie de Riemann de género $g \geq 1$, definimos la *variedad jacobiana* de S como el toro complejo $J(S) = \mathbb{C}^g/J_\Omega$, donde Ω es una base del espacio de diferenciales de primera clase de S y J_Ω es el retículo generado por sus periodos.

En las próximas secciones estudiaremos la relación entre una superficie S y su variedad jacobiana. Ahora vamos a probar que las variedades jacobianas cumplen la hipótesis del teorema de Lefschetz 4.50, por lo que son proyectivas:

Teorema 10.9 *Sea S una superficie de Riemann de género $g \geq 1$, sea Ω una base de las diferenciales de primera clase y sea $R_\Omega \subset \mathbb{C}^g$ el retículo generado por los periodos A_k, B_k de Ω respecto a una base de $H_1(S)$. Entonces existe una forma de Riemann en $\mathbb{C}^g$ respecto de R_Ω. Por consiguiente, la variedad jacobiana $J(S)$ es proyectiva.*

DEMOSTRACIÓN: Como ya hemos observado, no perdemos generalidad si tomamos como Ω una base canónica. Consideremos los periodos A_k, B_k como una $\mathbb{R}$-base de $V = \mathbb{C}^g = \mathbb{R}^{2g}$ y sea x_k, y_k su base dual. Definimos la forma bilineal alternada $E : V \times V \longrightarrow \mathbb{R}$ mediante

$$E(u,v) = \sum_{j=1}^{g} (y_j(u)x_j(v) - x_j(u)y_j(v)).$$

Es obvio que E toma valores enteros sobre R_Ω. Para probar que E es una forma de Riemann sólo falta ver que la forma $S(u,v) = E(iu,v)$ es simétrica y definida positiva.

Dado $u \in V$, sean (α, β) sus coordenadas en la base de periodos, es decir, $u = \alpha + \beta B$. Por otra parte, descompongamos $u = a + ib$, donde a, $b \in \mathbb{R}^g$ y, del mismo modo, $B = P + iQ$, donde las matrices reales P y Q son simétricas y Q es definida positiva. En estos términos, $a + ib = u = \alpha + \beta P + i\beta Q$, luego $a = \alpha + \beta P$, $b = \beta Q$, luego

$$y_j(u) = \beta_j = (bQ^{-1})_j, \qquad x_j(u) = \alpha_j = (a - bQ^{-1}P)_j.$$

Por consiguiente, $y_j(iu) = (aQ^{-1})_j$, $x_j(iu) = -(b + aQ^{-1}P)_j$. Ahora tomamos dos vectores $u = a + ib$, $v = a' + ib'$ y calculamos:

$$\begin{aligned} S(u,v) = E(iu,v) &= \sum_{j=1}^{g} (y_j(iu)x_j(v) - x_j(iu)y_j(v)) \\ &= \sum_{j=1}^{g} ((aQ^{-1})_j(a' - b'Q^{-1}P)_j + (b + aQ^{-1}P)_j(b'Q^{-1})_j) \\ &= (aQ^{-1})(a' - b'Q^{-1}P) + (b + aQ^{-1}P)(b'Q^{-1}) = aQ^{-1}a'^t + bQ^{-1}b'^t, \end{aligned}$$

donde hemos usado que todas las matrices son simétricas. Ahora es inmediato que la forma S es simétrica. Además,

$$S(u,u) = aQ^{-1}a^t + bQ^{-1}b^t.$$

Ahora basta tener en cuenta que si Q es definida positiva Q^{-1} también lo es.[3] ■

[3] Existe una matriz regular H tal que $Q' = HQH^t$ es diagonal (ver el teorema 8.3 de mi libro sobre *Teoría de números.*) Entonces Q' es definida positiva, lo que equivale a que todos los coeficientes de su diagonal sean positivos. Lo mismo le sucede a $Q'^{-1} = H^{-1t}Q^{-1}H^{-1}$, luego Q^{-1} es definida positiva.

10.3 El teorema de Abel

El teorema de Abel nos da una caracterización en términos de integrales de los divisores principales de una superficie de Riemann S. Equivalentemente, nos da una condición necesaria y suficiente para que exista una función meromorfa en S con una distribución dada de ceros y polos. Si Ω es una base del espacio de las diferenciales de primera clase de S, en la sección anterior hemos visto que la integral

$$\int_P^Q \Omega$$

está bien definida módulo los periodos de Ω, es decir, como elemento de la variedad jacobiana $J(S)$, con independencia del arco de extremos P y Q con que la calculemos.

Si identificamos los puntos de S con los divisores primos del cuerpo $\mathcal{M}(S)$ de las funciones meromorfas en S, entonces la integral (con un origen fijo $O \in S$) se extiende por linealidad a un homomorfismo sobre todo el grupo de divisores de S, de modo que

$$\int_O^{\mathfrak{a}} \Omega = \sum_Q v_Q(\mathfrak{a}) \int_O^Q \Omega \in J.$$

La restricción de este homomorfismo al grupo de los divisores de grado 0 es independiente de la elección de O, pues

$$\int_O^{\mathfrak{a}} \Omega - \int_{O'}^{\mathfrak{a}} \Omega = \sum_Q v_Q(\mathfrak{a}) \int_O^{O'} \Omega = 0.$$

Tenemos así un homomorfismo natural del grupo de divisores de grado 0 en la variedad jacobiana J. El teorema de Abel dice esencialmente que el núcleo de este homomorfismo es el subgrupo de los divisores principales. Para probarlo usaremos la versión vectorial de la relación (10.6), que se prueba sin más que aplicar dicha relación componente a componente:

Teorema 10.10 *Sea S una superficie de Riemann de género $g \geq 1$, sea Ω una base del espacio de diferenciales de primera clase en S y η una diferencial de tercera clase. Sea a_k, b_k una base de homología de S sobre la que η no tenga polos, sean A_k, $B_k \in \mathbb{C}^g$ los periodos de Ω y $A'_k, B'_k \in \mathbb{C}$ los periodos de η. Entonces*

$$\sum_{k=1}^{g} (A_k B'_k - B_k A'_k) = 2\pi i \sum_P G(P) \operatorname{Res}_P(\eta),$$

donde, llamando D a la imagen en S del interior del polígono $\mathcal{P}$ que determina la base de homología y $O \in D$ a un punto arbitrario,

$$G(P) = \int_O^P \Omega \in \mathbb{C}^g$$

se calcula mediante un arco contenido en D que una O con P.

El teorema siguiente es la mitad del teorema de Abel:

Teorema 10.11 *Sea S una superficie de Riemann de género $g \geq 1$ y Ω una base del espacio de las diferenciales de primera clase. Sea $O \in S$. Entonces, para cada $\alpha \in \mathcal{M}(S)$ se cumple*

$$\int_O^{(\alpha)} \Omega = 0.$$

Demostración: Puesto que la integral no depende de la base de homología con que se calculan los periodos de Ω, podemos tomar ésta de modo que los arcos a_k y b_k no contengan ceros o polos de α.

Sea D la imagen en S del interior del polígono $\mathcal{P}$ que determina la base, tomemos $O \in S$ y sea

$$G(P) = \int_O^P \Omega \in \mathbb{C}^g,$$

donde las g integrales se calculan sobre un mismo arco contenido en D. Hemos de probar que

$$\sum_P v_P(\alpha) G(P) \in \langle A_k, B_k \mid k = 1, \ldots, g \rangle_{\mathbb{Z}}.$$

Sea $\eta = d\alpha/\alpha$. Se trata de una forma meromorfa en S. Vamos a calcular sus residuos. Para cada punto $Q \in S$ consideramos una función $\pi \in \mathcal{M}(S)$ tal que $v_P(\pi) = 1$ (de modo que π se restringe a una carta alrededor de P). Entonces

$$\eta = \frac{d\alpha}{\alpha} = \frac{1}{\alpha}\frac{d\alpha}{d\pi}\, d\pi,$$

y es fácil ver que $\operatorname{Res}_P \eta = v_P(\alpha)$. Además η es una diferencial de tercera clase, luego podemos aplicar el teorema 10.10, que nos da la relación

$$\sum_{k=1}^{g} (A_k B'_k - B_k A'_k) = 2\pi i \sum_P v_P(\alpha) G(P),$$

donde $A'_k, B'_k \in \mathbb{C}$ son los periodos de η.

Podemos considerar a η como forma holomorfa en el abierto que resulta de quitarle a S los ceros y los polos de α. Así, α también es una función holomorfa con imagen en $\mathbb{C} \setminus \{0\}$ y

$$A'_k = \int_{a_k} \eta = \int_{a_k} \alpha^\sharp(dz/z) = \int_{z_\sharp(a_k)} \frac{dz}{z} = 2m_k\pi i,$$

para cierto $m_k \in \mathbb{Z}$. $B'_k = 2n_k\pi i$, con lo que

$$2\pi i \sum_{k=1}^{g} (n_k A_k - m_k B_k) = 2\pi i \sum_P v_P(\alpha) G(P).$$

Al cancelar los factores $2\pi i$ queda la relación buscada. ■

Para probar el recíproco necesitamos un resultado más:

Teorema 10.12 *Con la notación usual, se cumple*

$$\sum_{k=1}^{g} (\beta_k A_k - \alpha_k B_k) = 0, \qquad \textit{para ciertos } \alpha_k,\ \beta_k \in \mathbb{C},$$

si y sólo si $\beta_k = CB_k$, $\alpha_k = CA_k$, *para cierto* $C \in \mathbb{C}^g$.

Demostración: Sea $\eta = c_1\omega_1 + \cdots + c_g\omega_g$ una diferencial de primera clase. El teorema 10.2 nos da que

$$\sum_{k=1}^{g} (A_k B_k' - B_k A_k') = 0,$$

donde

$$A_k' = \int_{a_k} \eta = (c_1, \ldots, c_g)A_k, \quad B_k' = \int_{b_k} \eta = (c_1, \ldots, c_g)B_k.$$

Esto prueba una implicación. Para probar el recíproco veamos primero que si $X \in \mathbb{C}^g$ cumple $XA_k = XB_k = 0$ para $k = 1, \ldots, g$, entonces $X = 0$.

En efecto, tomemos $\eta = X\Omega$, que es una diferencial de primera clase. Entonces

$$\int_{a_k} \eta = X \int_{a_k} \Omega = XA_k = 0, \qquad \int_{b_k} \eta = X \int_{a_k} \Omega = XB_k = 0.$$

Sabemos que la integral

$$\int_O^Q \eta$$

está bien definida en S salvo múltiplos de los periodos de η, pero éstos son nulos, luego la integral define una función holomorfa en S. Concluimos que es constante, luego $\eta = 0$ y $X = 0$, pues Ω es una base.

Con esto hemos probado que la única solución del sistema de $2g$ ecuaciones lineales con g incógnitas formado con los coeficientes de A_k y B_k es la solución trivial. Esto implica que la matriz de coeficientes tiene rango g, luego los $2g$ vectores A_k, B_k tienen rango g. Por otra parte, estamos buscando el conjunto de las soluciones de un sistema de g ecuaciones lineales con $2g$ incógnitas, con matriz de coeficientes de rango g. El espacio de soluciones ha de tener dimensión g, pero las soluciones que hemos encontrado forman ya un espacio de dimensión g, luego son todas las soluciones. ■

Finalmente podemos probar:

Teorema 10.13 (Abel) *Sea* S *una superficie de Riemann de género* $g \geq 1$, *sea* $O \in S$ *y* Ω *una base del espacio de diferenciales de primera clase. Entonces un divisor* $\mathfrak{a}$ *de grado* 0 *en* S *es principal si y y sólo si*

$$\int_O^{\mathfrak{a}} \Omega = 0.$$

Demostración: Ya hemos probado una implicación. Supongamos que la integral es nula (como elemento de la variedad jacobiana $J(S)$) y veamos que $\mathfrak{a}$ es principal. Con la notación habitual, podemos exigir que los arcos a_k y b_k no contengan puntos P con $v_P(\mathfrak{a}) \neq 0$. Vamos a probar que existe una diferencial de tercera clase η tal que $\operatorname{Res}_P \eta = v_P(\mathfrak{a})$ para todo punto $P \in S$ y además

$$\int_{a_k} \eta = 2\pi i m_k, \qquad \int_{b_k} \eta = 2\pi i n_k, \qquad m_k, n_k \in \mathbb{Z}.$$

Por el teorema 9.26 tenemos una forma η' que cumple la condición sobre los residuos. El teorema 10.10 nos da que

$$\sum_{k=1}^{g} \left(A_k \int_{b_k} \eta' - B_k \int_{a_k} \eta' \right) = 2\pi i \sum_P G(P) v_P(\mathfrak{a}).$$

Por hipótesis $G(P) \in \langle A_k, B_k \rangle_{\mathbb{Z}}$, luego existen enteros m_k y n_k tales que

$$\sum_{k=1}^{g} \left(A_k \int_{b_k} \eta' - B_k \int_{a_k} \eta' \right) = 2\pi i \sum_{k=1}^{g} (A_k n_k - B_k m_k),$$

de donde

$$\sum_{k=1}^{g} \left(\left(\int_{b_k} \eta' - 2\pi i n_k \right) A_k - \left(\int_{a_k} \eta' - 2\pi i m_k \right) B_k \right) = 0.$$

El teorema anterior nos da que

$$\int_{b_k} \eta' - 2\pi i n_k = C B_k, \qquad \int_{a_k} \eta' - 2\pi i m_k = C A_k,$$

para cierto vector $C \in \mathbb{C}^g$.

La forma $\eta = \eta' - C\Omega$ tiene los mismos polos y residuos que η', y además

$$\int_{a_k} \eta = \int_{a_k} \eta' - \int_{a_k} C\Omega = \int_{a_k} \eta' - C A_k = 2\pi i m_k.$$

Con b_k se razona igualmente.

Así, todos los periodos de η son múltiplos enteros de $2\pi i$, luego las integrales

$$\int_O^P \eta$$

están definidas salvo múltiplos enteros de $2\pi i$. Esto nos permite definir

$$\alpha(P) = \exp \int_O^P \eta,$$

que es una función uniforme definida en S salvo en los polos de η. Claramente es holomorfa y no se anula. Vamos a probar que se extiende a una función meromorfa en S de modo que en los polos P de η tiene ceros o polos, y además $v_P(\alpha) = v_P(\mathfrak{a})$.

En efecto, tomemos una función $z \in \mathcal{M}(S)$ tal que $v_P(z) = 1$, con lo que z se restringe a una carta en un entorno (simplemente conexo) U de P. Podemos exigir que U no contenga otros polos de η. Fijemos $R \in U$, de modo que, para puntos $Q \in U$ se cumple

$$\alpha(Q) = \exp \int_O^R \eta \, \exp \int_R^Q \eta = K \exp \int_R^Q \eta.$$

Si $\eta = f\,dz$, entonces $\eta|_U = z^\sharp(\tilde{f}(z)\,dz)$, donde $\tilde{f}$ es una función meromorfa en un entorno de 0 en $\mathbb{C}$ con un polo simple en 0 y $\operatorname{Res}_0 \tilde{f} = \operatorname{Res}_P \eta = v_P(\mathfrak{a})$. Por consiguiente,

$$\tilde{f}(z) = \frac{v_P(\mathfrak{a})}{z} + h(z),$$

donde h es una función holomorfa en 0. Según el teorema de cambio de variable,

$$\int_R^Q \eta = v_P(\mathfrak{a}) \int_{z(R)}^{z(Q)} \frac{dz}{z} + \int_{z(R)}^{z(Q)} h(z)\,dz = v_P(\mathfrak{a})(\log z(Q) - \log z(R)) + H(Q),$$

donde H es una función holomorfa en U y el logaritmo que aparece en el primer sumando depende del arco por el que se integra, pero la elección se vuelve irrelevante al calcular

$$\exp \int_R^Q \eta = \exp(v_P(\mathfrak{a})(\log z(Q) - \log z(R)) \exp H(Q) = z(Q)^{v_P(\mathfrak{a})} K' e^{H(Q)}.$$

En definitiva, $\alpha|_U = KK' z^{v_P(\mathfrak{a})} H$, luego α es meromorfa en P y además $v_P(\alpha) = v_P(\mathfrak{a})$. ■

Veamos un enunciado equivalente del teorema de Abel. Para ello observemos en primer lugar que si $\mathfrak{a} = P_1 \cdots P_n Q_1^{-1} \cdots Q_n^{-1}$ (donde los puntos P_k y Q_k pueden repetirse) entonces

$$\int_O^{\mathfrak{a}} \Omega = \sum_{k=1}^n \int_O^{P_k} \Omega - \sum_{k=1}^n \int_O^{Q_k} \Omega = \sum_{k=1}^n \int_{Q_k}^{P_k} \Omega = \sum_{k=1}^n \int_{\gamma_k} \Omega = \int_\gamma \Omega,$$

donde γ_k es un arco que une Q_k con P_k y $\gamma = \gamma_1 + \cdots + \gamma_n$.

Ahora observemos que las 0-cadenas de S son lo mismo que sus divisores, pues ambos son combinaciones enteras de puntos (salvando el hecho de que para cadenas usamos notación aditiva y para divisores multiplicativa). Teniendo esto en cuenta, podemos afirmar que

$$\partial\gamma = \partial\gamma_1 + \cdots + \partial\gamma_n = P_1 - Q_1 + \cdots + P_2 - Q_2 = P_1 Q_1^{-1} \cdots P_n Q_n^{-1} = \mathfrak{a}.$$

Así pues, la condición del teorema de Abel para que $\mathfrak{a}$ sea principal es que

$$\int_\gamma \Omega \in \langle A_k, B_k \mid k = 1, \ldots, g \rangle$$

para una cadena γ tal que $\partial\gamma = \mathfrak{a}$. Notemos que no importa cuál, pues dos de ellas se diferencian en un ciclo y la integral de Ω sobre un ciclo está también en el grupo de periodos. Por otro lado, cualquier elemento del grupo de periodos puede obtenerse como la integral de Ω sobre un ciclo adecuado. Por consiguiente, si $\mathfrak{a}$ es principal, será

$$\int_\gamma \Omega = \int_z \Omega,$$

para cierto ciclo z, y sustituyendo γ por $\gamma - z$ tenemos otra cadena con la misma frontera y tal que

$$\int_\gamma \Omega = 0.$$

Más aún, esto significa que todas las formas $\omega_1, \ldots, \omega_g$ tienen integral nula sobre γ, y cualquier otra forma de primera clase es combinación lineal de éstas, luego llegamos a que todas tienen integral nula sobre γ. En resumen:

Teorema 10.14 (Abel) *Sea S una superficie de Riemann de género $g \geq 1$ y $\mathfrak{a}$ un divisor de grado 0 en S. Entonces $\mathfrak{a}$ es principal si y y sólo si existe una 1-cadena γ en S tal que $\partial\gamma = \mathfrak{a}$ y*

$$\int_\gamma \omega = 0$$

para toda diferencial de primera clase ω en S.

En realidad Abel sólo probó que la condición del teorema anterior es necesaria para que el divisor $\mathfrak{a}$ sea principal. De hecho, su enunciado no hablaba para nada de divisores, fronteras etc. y, en realidad, era mucho más general que la mitad correspondiente del teorema anterior. La versión moderna del teorema de Abel fue formulado por Clebsch varias décadas después de la muerte de Abel. Después veremos que la implicación del teorema de Abel probada por Abel es suficiente para demostrar las relaciones de aditividad de integrales abelianas descubiertas por Euler.

10.4 El teorema de inversión de Jacobi

El teorema de Abel nos da que la integración de una base Ω de las diferenciales de primera clase desde un punto arbitrario O induce un homomorfismo del grupo de divisores de grado 0 de una superficie de Riemann S en su variedad jacobiana $J(S)$. Ahora probaremos el teorema de Jacobi, que afirma que este homomorfismo es en realidad un isomorfismo, lo que por una parte nos da una representación del grupo de clases de S y por otra nos aporta mucha información sobre $J(S)$ y los periodos de Ω.

Definición 10.15 Un divisor $\mathfrak{a}$ en una superficie de Riemann S es *normal* si $\dim(W/[\mathfrak{a}]) = 0$, donde W es la clase canónica de S.

Puesto que $\operatorname{grad} W = 2g-2$, todo divisor de grado $> 2g-2$ es normal. Recordemos que $\dim(W/[\mathfrak{a}])$ es la dimensión del espacio de las formas diferenciales ω tales que $\mathfrak{a} \mid (\omega)$. En particular, un divisor entero $\mathfrak{a} = P_1 \cdots P_r$ es normal si y sólo si la única diferencial de primera clase que se anula en los puntos $P_1, \ldots, P_r$ es la forma nula.

Teorema 10.16 *Si S es una superficie de Riemann de género $g \geq 1$, existen g puntos distintos $M_1, \ldots, M_g \in S$ tales que el divisor $M_1 \cdots M_g$ es normal, es decir, la única diferencial de primera clase que se anula en $M_1, \ldots, M_g$ es la forma nula.*

DEMOSTRACIÓN: Llamemos W a la clase canónica de S. Sea ω_1 una diferencial de primera clase y M_1 un punto donde ω_1 no se anule. Sabemos que $\dim(W/(M_1))$ es la dimensión del espacio de las diferenciales de primera clase que se anulan en M_1. Por el teorema de Riemann-Roch,

$$\dim(M_1) = 1 + 1 - g + \dim(W/(M_1)),$$

y, por otra parte, $\dim(M_1) = 1$, pues si α tiene a lo sumo un polo simple en M_1, entonces α no tiene polos (porque la suma de los residuos de $\alpha\omega_1$ ha de ser nula) y en consecuencia es constante. Así pues, el espacio de diferenciales de primera clase que se anulan en M_1 tiene dimensión $g-1$. Tomamos una forma ω_2 que se anule en M_1 y un punto $M_2 \in S$ donde no se anule ω_2.

En general, supongamos que hemos encontrado $r < g$ puntos distintos $M_1, \ldots, M_r$ y r diferenciales de primera clase $\omega_1, \ldots, \omega_r$ tales que cada ω_k se anule en $M_1, \ldots, M_{k-1}$ pero no en M_k.

Ahora, el espacio de las diferenciales de primera clase que se anulan en $M_1, \ldots, M_r$ tiene dimensión $\dim(W/(M_1 \cdots M_r))$. El teorema de Riemann-Roch es

$$\dim(W/(M_1 \cdots M_r)) = g - k - 1 + \dim(M_1 \cdots M_r),$$

y la última dimensión es 1, pues si α tiene a lo sumo polos simples en los puntos $M_1, \ldots, M_r$, entonces $\alpha\omega_r$ tendría a lo sumo un polo en M_r, luego no tiene polos, luego α tampoco tiene un polo en M_r. Razonando con $\alpha\omega_{r-1}$ llegamos a que α tampoco tiene un polo en M_{r-1} y repitiendo llegamos a que α no tiene polos, luego es constante.

Así pues, podemos tomar una forma ω_{r+1} que se anule en $M_1, \ldots, M_r$ pero no en un nuevo punto M_{r+1}.

El divisor $M_1 \cdots M_g$ cumple lo pedido, pues las formas $\omega_1, \ldots, \omega_g$ forman una base de las diferenciales de primera clase (es claro que ω_k no es combinación lineal de $\omega_{k+1}, \ldots, \omega_g$) y si una diferencial de primera clase ω tuviera ceros en $M_1, \ldots, M_g$, podríamos expresarla como $\omega = a_1\omega_1 + \cdots + a_g\omega_g$, con $a_k \in \mathbb{C}$, y si a_k fuera el mayor coeficiente no nulo, tendríamos que ω_k se anularía en M_k, contradicción. ■

La prueba del teorema de Jacobi se basa en el resultado siguiente:

Teorema 10.17 *Sea S una superficie de género $g \geq 1$ y $M_1, \ldots, M_g$ puntos distintos en S tales que el divisor $(M_1 \cdots M_g)$ es normal. Sea Ω una base de las diferenciales de primera clase. Entonces la aplicación*

$$(P_1, \ldots, P_g) \mapsto \sum_{k=1}^{g} \int_{M_k}^{P_k} \Omega$$

determina una transformación conforme de un producto $V_1 \times \cdots \times V_g$ de entornos de $P_1, \ldots, P_g$ en un entorno de 0 en $\mathbb{C}^g$.

Demostración: Sea $z_k \in \mathcal{M}(S)$ tal que $v_{M_k}(z_k) = 1$. Vamos a probar que

$$\begin{vmatrix} \left.\frac{\omega_1}{dz_1}\right|_{M_1} & \cdots & \left.\frac{\omega_1}{dz_g}\right|_{M_g} \\ \vdots & & \vdots \\ \left.\frac{\omega_g}{dz_1}\right|_{M_1} & \cdots & \left.\frac{\omega_g}{dz_g}\right|_{M_g} \end{vmatrix} \neq 0.$$

Para ello, consideramos el homomorfismo

$$\omega \mapsto \left(\left.\frac{\omega}{dz_1}\right|_{M_1}, \ldots, \left.\frac{\omega}{dz_g}\right|_{M_g} \right)$$

del espacio de diferenciales de primera clase en $\mathbb{C}^g$. Una forma en su núcleo se anula en $M_1, \ldots, M_g$, luego ha de ser la forma nula. Así pues, el homomorfismo es inyectivo y, comparando las dimensiones, ha de ser un isomorfismo. Por lo tanto el determinante es no nulo.

Sea V_k un entorno simplemente conexo de M_k donde ω_j/dz_k, para todo $j = 1, \ldots, g$, sea holomorfa (es decir, no tenga polos). Sea

$$h_{kj}(w) = \int_{M_k}^{z^{-1}(w)} \omega_j = \int_0^w \left.\frac{\omega_j}{dz_k}\right|_{z^{-1}(\zeta)} d\zeta,$$

que es una función holomorfa en $z_k[V_k]$. Tenemos que $z_1 \times \cdots \times z_g$ es una carta en S^g alrededor de $(M_1, \ldots, M_k)$ y la lectura en esta carta de la aplicación del enunciado es

$$(w_1, \ldots, w_g) \mapsto (h_{11}(w_1) + \cdots + h_{1g}(w_1), \ldots, h_{g1}(w_1) + \cdots + h_{gg}(w_g)).$$

Ciertamente es una función holomorfa, y su determinante jacobiano en 0 es el determinante anterior. El teorema de la función inversa nos da la conclusión.

Teorema 10.18 (Jacobi) *Sea S una superficie de Riemann de género $g \geq 1$ y Ω una base del espacio de diferenciales de primera clase. Para cada $X \in \mathbb{C}^g$ existe un divisor $\mathfrak{a}$ de grado 0 en S y una 1-cadena γ tal que $\partial\gamma = \mathfrak{a}$ y*

$$\int_\gamma \Omega = X.$$

Es claro que este teorema está contenido en el resultado siguiente, que incluye también al teorema de Abel (ver las observaciones previas al teorema 10.14).

Teorema 10.19 (Abel-Jacobi) *Sea S una superficie de Riemann de género $g \geq 1$, sea $O \in S$ y Ω una base del espacio de diferenciales de primera clase. Entonces la aplicación*

$$A \mapsto \int_O^A \Omega$$

determina un isomorfismo entre el grupo de clases de grado 0 de S y su variedad jacobiana $J(S)$.

Demostración: Por el teorema de Abel sabemos que la aplicación está bien definida y es un monomorfismo de grupos. Sea $U \subset \mathbb{C}^g$ el entorno de cero dado por el teorema anterior. Si $\alpha \in \mathbb{C}$, tomamos un número natural n tal que $\beta = \alpha/n \in U$. Si probamos que la clase $[\beta] \in J(S)$ tiene una antiimagen A, entonces $[\alpha]$ tendrá antiimagen nA y el teorema estará probado. Ahora bien, por el teorema anterior, existen puntos $P_k \in V_k$ tales que

$$\sum_{k=1}^{g} \int_{M_k}^{P_k} \Omega = \beta.$$

Concluimos que β es la imagen de la clase de $P_1 \cdots P_g / M_1 \cdots M_g$. ■

Así pues, el grupo de clases de grado 0 de una superficie de Riemann S de género $g \geq 1$ es isomorfo a un producto de $2g$ copias de la circunferencia S^1.

Terminamos esta sección con una aplicación, para la que necesitamos el teorema siguiente:

Teorema 10.20 *Si $c_1, \ldots, c_{2g}$ es una base de homología de una superficie de Riemann S de género $g \geq 1$ y $j \in \{1, \ldots, 2g\}$, existe una diferencial de primera clase ω tal que*

$$\operatorname{Re} \int_{c_k} \omega = \delta_{kj}, \qquad k = 1, \ldots, 2g.$$

Demostración: Fijemos una base $\Omega = (\omega_1, \ldots, \omega_g)$ para las diferenciales de primera clase y consideremos su matriz de periodos:

	c_1	$\cdots$	c_{2g}
ω_1	$u_{11} + iv_{11}$	$\cdots$	$u_{1\,2g} + iv_{1\,2g}$
$\vdots$	$\vdots$		$\vdots$
ω_g	$u_{g1} + iv_{g1}$	$\cdots$	$u_{g\,2g} + iv_{g\,2g}$

El teorema 10.7 afirma que sus columnas son linealmente independientes sobre $\mathbb{R}$. La diferencial ω que buscamos será de la forma $z_1\omega_1 + \cdots + z_g\omega_g$, para ciertos números complejos $z_k = x_k + iy_k$. Suponiendo, por simplicidad, $j = 1$, basta exigir que cumplan

$$\begin{array}{rl} x_1u_{11} - y_1v_{11} + \cdots + x_gu_{g1} - y_gv_{g1} & = 1, \\ x_1u_{12} - y_1v_{12} + \cdots + x_gu_{g2} - y_gv_{g2} & = 0, \\ \\ x_1u_{1\,2g} - y_1v_{1\,2g} + \cdots + x_gu_{g\,2g} - y_gv_{g\,2g} & = 0, \end{array}$$

lo cual es posible porque la matriz de coeficientes tiene determinante no nulo (es la matriz de coordenadas de las columnas de la matriz de periodos respecto a la base canónica de $\mathbb{R}^{2g}$). ■

Como consecuencia:

Teorema 10.21 *Sea S una superficie de Riemann de género $g \geq 1$.*

a) Si ω es una forma diferencial de primera clase con integral nula sobre todo ciclo de S, entonces es la forma nula.

b) Si z es un ciclo en S sobre el que todas las diferenciales de primera clase tienen integral nula, entonces z es una frontera.

Demostración: a) está ya probado, pues ω tendría todos sus periodos nulos (ver las observaciones anteriores o posteriores al teorema 10.3).

b) Sea $c_1, \ldots, c_{2g}$ una base de homología de S. Entonces

$$[z] = m_1[c_1] + \cdots + m_{2g}[c_{2g}],$$

para ciertos enteros m_k. Basta probar que son nulos. Ahora bien, si tomamos una diferencial de primera clase ω que cumpla el teorema anterior para un j y la integramos sobre z obtenemos que $0 = m_j + yi$, luego $m_j = 0$. ■

Equivalentemente, hemos probado que la forma bilineal

$$\int^* : H_1(S, \mathbb{C}) \times \Lambda^1(S) \longrightarrow \mathbb{C}$$

induce isomorfismos entre cada espacio y el dual del otro. Esto es la versión holomorfa del teorema de De Rham.

10.5 Integrales elípticas

Si S es una superficie de Riemann de género $g = 1$, nos encontramos con una situación peculiar. El teorema de Abel-Jacobi prueba que el grupo de clases de grado 0 de S es isomorfo a la variedad jacobiana $J(S)$ y, por otra parte, fijado un punto $P \in S$, el teorema 9.18 afirma que la correspondencia $Q \mapsto [Q/P]$ biyecta S con el grupo de clases de grado 0. Tenemos, pues, una biyección entre S y $J(S)$ que, de hecho, es un isomorfismo de grupos cuando consideramos en

S la estructura dada por 9.19. Enseguida veremos que este isomorfismo está en el fondo de las relaciones de adición de integrales que hemos comentado en la introducción de este capítulo, pero antes estudiaremos más de cerca la situación. Para empezar, resulta natural plantearse si dicho isomorfismo es también una transformación conforme, y la respuesta es afirmativa.

En efecto, si ω es una diferencial no nula de primera clase, a un punto Q le corresponde la clase

$$\int_O^{Q/P} \omega = \int_O^Q \omega - \int_O^P \omega = \int_P^Q \omega \in J.$$

La lectura de esta aplicación en cartas de S y J es una función definida como la integral de una función holomorfa, luego es holomorfa. Concluimos que el isomorfismo de Abel-Jacobi es una transformación conforme entre S y $J(S)$. En resumen:

Teorema 10.22 *Sea S una superficie de Riemann de género 1, sea ω una diferencial no nula de primera clase en S y $J(S)$ su variedad jacobiana. Fijado un punto $P \in S$, la aplicación $S \longrightarrow J(S)$ dada por*

$$Q \mapsto \int_P^Q \omega$$

es una transformación conforme y un isomorfismo de grupos, cuando en S consideramos la estructura de grupo que tiene a P por elemento neutro.

Los toros complejos de dimensión 1 son superficies de Riemann. En este caso conocemos explícitamente una base de homología: si $R = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}}$ es un retículo en $\mathbb{C}$ y $T = \mathbb{C}/R$, entonces la restricción de la proyección natural $p : \mathbb{C} \longrightarrow T$ al conjunto

$$\mathcal{P} = \{\alpha\omega_1 + \beta\omega_2 \mid 0 \leq \alpha,\, \beta \leq 1\}$$

es diferenciable, inyectiva en el interior de $\mathcal{P}$ e identifica los lados dos a dos, de modo que una base de homología de T (en las condiciones que venimos exigiendo) está formada por (las imágenes en T de) los arcos $a(t) = t\omega_1$ y $b(t) = t\omega_2$. En realidad, según los convenios de orientación que hemos adoptado, hemos de exigir que al recorrer la frontera de $\mathcal{P}$ en sentido antihorario recorramos los arcos a y b en la forma $aba^{-1}b^{-1}$, y es fácil ver que esto se traduce en que hemos de ordenar ω_1 y ω_2 de forma que $\operatorname{Im} \omega_2/\omega_1 > 0$. Por ejemplo, si no respetamos este convenio, la desigualdad teorema 10.3 se invertiría.

Una carta alrededor de un punto $P \in T$ es de la forma $z = p|_C^{-1}$, donde C es un abierto en C sobre el que la proyección p sea inyectiva. Si z_1 y z_2 corresponden a dos elecciones de C, entonces $z_1 - z_2$ es constante (es un elemento de R), luego $dz_1 = dz_2$. Esto nos permite definir dz como la única forma diferencial en T que en cada abierto $p[C]$ coincide con la diferencial de $p|_C^{-1}$. Se trata de una forma diferencial holomorfa en T, es decir, de primera clase. La proyección

$p : \mathbb{C} \longrightarrow T$ induce el homomorfismo $p^\sharp : \Lambda^1(T) \longrightarrow \Lambda^1(\mathbb{C})$, y es claro que $p^\sharp(dz) = dz$, donde la z del miembro derecho es la identidad en $\mathbb{C}$. De aquí se sigue que los periodos de dz son

$$A = \int_{p_\sharp(a)} dz = \int_a dz = \int_0^1 \omega_1 t\, dt = \omega_1, \qquad B = \omega_2.$$

Por consiguiente, la variedad jacobiana de T es $J(T) = T$. Si $Q \in T$, podemos expresar $Q = [z]$, donde $z \in \mathcal{P}$. Un camino que une $P = [0]$ con Q es $p_\sharp(\gamma)$, donde $\gamma(t) = tz$. Por lo tanto,

$$\int_P^Q dz = \left[\int_{p_\sharp(\gamma)} dz\right] = \left[\int_\gamma dz\right] = \left[\int_0^1 zt\, dt\right] = [z] = Q.$$

Con esto hemos probado el teorema siguiente:

Teorema 10.23 *Sea T un toro complejo, sea $p : \mathbb{C} \longrightarrow T$ la proyección natural, sea dz la diferencial de primera clase que cumple $p^\sharp(dz) = dz$ y sea $P = [0]$. Entonces el isomorfismo de Abel-Jacobi en la versión del teorema* 10.22 *respecto de dz y P es la identidad. En particular, la estructura de grupo en T de neutro P inducida por el grupo de clases de grado* 0 *coincide con la estructura de T como grupo cociente de $\mathbb{C}$.*

Pasemos ya a abordar la cuestión de la aditividad de integrales. Las fórmulas de adición se deducen del hecho de que la aplicación descrita en el teorema anterior es un homomorfismo de grupos (lo cual requiere sólo la implicación del teorema de Abel que probó realmente Abel).

Para obtener la relación de adición de la lemniscata tenemos que considerar la curva $W^2 = 1 - Z^4 = (1 - Z^2)(1 + Z^2)$. Más en general, vamos a trabajar con la curva de ecuación

$$W^2 = (1 - Z^2)(1 - mZ^2), \qquad 0 \neq m < 1.$$

Aunque tiene género 1, no se trata de una curva elíptica porque no es regular (si lo fuera tendría género 3). Esto lo arreglamos con la transformación birracional $(X, Y) = (Z^2, WZ)$, que hace corresponder dicha curva con la cúbica V de ecuación

$$Y^2 = X(1 - X)(1 - mX).$$

En general, las transformaciones birracionales entre curvas se corresponden con cambios de variable entre integrales, en este caso con el cambio $X = Z^2$. En efecto, si $0 < r < 1$, se cumple

$$\int_0^r \frac{dz}{\sqrt{(1-z^2)(1-mz^2)}} = \frac{1}{2}\int_0^r \frac{2z\, dz}{\sqrt{z^2(1-z^2)(1-mz^2)}}$$

$$= \frac{1}{2}\int_0^t \frac{dx}{\sqrt{x(1-x)(1-mx)}} = \frac{1}{2}\int_0^t \frac{dx}{y}, \qquad t = r^2.$$

La última integral es la integral curvilínea en V de la diferencial de primera clase $\omega = dx/y$ (ver el ejemplo de la página 326) sobre el arco dado por

$$\sigma(x) = (x, \sqrt{x(1-x)(1-mx)}).$$

(Recordemos que hemos tomado $0 \neq m < 1$, con lo que el radicando es positivo en el intervalo $[0,1]$.)

Consideramos en V la estructura de grupo que tiene por elemento neutro al punto $(0,0)$. Fijamos dos puntos distintos $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ y vamos a calcular $P_1 + P_2$. De acuerdo con el teorema 9.20, calculamos la recta que pasa por P_1 y P_2, que está determinada por la ecuación

$$Y = y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(X - x_1) = aX + b,$$

donde

$$b = y_1 - x_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) = \frac{x_1y_2 - x_2y_1}{x_1 - x_2} = x_1x_2\,\frac{1 - mx_1x_2}{x_1y_2 + x_2y_1}.$$

Al sustituir $Y = aX + b$ en la ecuación de V obtenemos

$$(aX + b)^2 = X(1-X)(1-mX),$$

ecuación cuyas raíces son x_1, x_2 y la coordenada x_3 del tercer punto $P_3 = (x_3, y_3)$ en que la recta corta a V. El término independiente es b^2 y el coeficiente director es m, luego tenemos la relación $b^2 = mx_1x_2x_3$. Así pues, $x_3 = b^2/(mx_1x_2)$.

La suma será el punto $P' = (x', y')$ donde la recta que pasa por $(0,0)$ y P_3 corta a V. Dicha recta es $Y = (y_3/x_3)X$. Razonando como antes, sustituimos

$$\frac{y_3^2}{x_3^2}X^2 = X(1-X)(1-mX)$$

y concluimos que $x' = 1/(mx_3)$. Así pues,

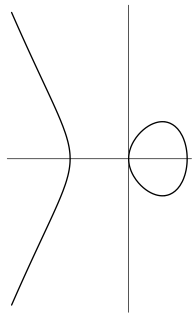
$$x' = \frac{x_1x_2}{b^2} = \frac{1}{x_1x_2}\left(\frac{x_1y_2 + x_2y_1}{1 - mx_1x_2}\right)^2.$$

Todas las operaciones son correctas en el caso que nos va a interesar, a saber, $P_i = \sigma(x_i)$, donde $0 < x_1, x_2 < 1$ (los denominadores no se anulan, etc.). Más aún, la función $\sqrt{x(1-x)(1-mx)}$ es creciente a la derecha de 0, de donde se sigue que si x_1, x_2 están suficientemente cerca de 0, entonces la pendiente de $Y = aX + b$ es positiva, con lo que es fácil ver que $y' > 0$ y, por lo tanto, $P_1 + P_2 = \sigma(x')$.

El hecho de que la integración de $\omega = dx/y$ desde $(0,0)$ sea un homomorfismo de grupos nos da ahora que

$$\int_0^{x_1}\frac{dx}{y} + \int_0^{x_2}\frac{dx}{y} = \int_0^{x'}\frac{dx}{y} + \alpha, \tag{10.7}$$

donde todas las integrales se calculan sobre un segmento del arco σ y α es un elemento del grupo de periodos de ω.



Ahora bien, ω tiene un periodo real y otro imaginario puro. Esto podremos probarlo más fácilmente en el capítulo siguiente (ver la observación tras el teorema 11.16), pero informalmente la razón es ésta: la curva V es un toro y su parte real muestra dos de sus secciones. La figura corresponde al caso $m = -1$, de modo que el "círculo" de la derecha es un corte completo del "tubo" y la rama de la izquierda es otro corte al que le falta el punto del infinito para cerrarse. (Si $0 < m < 1$ la única diferencia es que la rama abierta queda a la derecha de 1.)

Una base de homología la forman, el ciclo que recorre una vez en sentido negativo el "círculo" completo, cuyo periodo es

$$A = 2\int_0^1 \frac{dx}{\sqrt{x(1-x)(1-mx)}} > 0,$$

junto con el ciclo que recorre los puntos $(x, i\sqrt{-x(1-x)(1-mx)})$ desde $x = 1$ a $x = 1/m$ si $m > 0$ o bien desde $x = 1/m$ hasta 0 si $m < 0$ y luego vuelve al punto de partida por los puntos $(x, -i\sqrt{-x(1-x)(1-mx)})$. El periodo correspondiente es imaginario puro.

Así pues, el número α que aparece en (10.7) ha de ser un múltiplo entero del único periodo real A de ω, pues los demás términos de la ecuación son reales. Pero el miembro izquierdo es positivo y menor que A, y la integral del miembro derecho es positiva, luego ha de ser necesariamente $\alpha = 0$. Finalmente deshacemos el cambio $X = Z^2$, con lo que obtenemos que, para $0 < z_1, z_2 < 1$, se cumple

$$\int_0^{z_1} \frac{dz}{\sqrt{(1-z^2)(1-mz^2)}} + \int_0^{z_2} \frac{dz}{\sqrt{(1-z^2)(1-mz^2)}}$$

$$= \int_0^{z'} \frac{dz}{\sqrt{(1-z^2)(1-mz^2)}},$$

donde

$$z'^2 = x' = \frac{1}{x_1x_2}\left(\frac{x_1y_2 + x_2y_1}{1 - mx_1x_2}\right)^2 = \frac{1}{z_1^2z_2^2}\left(\frac{z_1^2z_2w_2 + z_2^2z_1w_1}{1 - mz_1^2z_2^2}\right)^2$$

$$= \left(\frac{z_1w_2 + z_2w_1}{1 - mz_1^2z_2^2}\right)^2,$$

y, en definitiva,

$$z' = \frac{z_1w_2 + z_2w_1}{1 - mz_1^2z_2^2}.$$

Para $m = -1$ tenemos la fórmula de adición para arcos de lemniscata. Si hacemos tender m a 0 obtenemos, mediante oportunos razonamientos de continuidad, la fórmula de adición para el arco seno. Por otra parte, la fórmula general que hemos obtenido está muy cerca de proporcionar una suma de arcos de elipse análoga a la de la lemniscata. En efecto, respecto a un sistema de referencia adecuado, toda elipse admite una ecuación de la forma

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \qquad a \geq b > 0.$$

El número $0 \leq k < 1$ dado por $k^2 = (a^2 - b^2)/a^2$ es la excentricidad de la elipse. Aplicando una homotecia podemos suponer que el semieje mayor es $a = 1$, con lo que la excentricidad es $k = \sqrt{1 - b^2}$. Para calcular el elemento de longitud despejamos $y(x) = b\sqrt{1 - x^2}$, con lo que

$$ds = \sqrt{1 + y'(x)^2}\, dx = \sqrt{\frac{1 - k^2x^2}{1 - x^2}}\, dx = \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}}\, dx$$

Consecuentemente, la longitud del arco de elipse comprendido entre $x = 0$ y $x = x_1 \leq 1$ es

$$s(x) = \int_0^{x_1} \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}}\, dx. \tag{10.8}$$

Si no estuviera el numerador $1 - k^2x^2$ tendríamos una fórmula de adición para esta integral. De hecho, sólo la tenemos para $k = 0$, pero este caso corresponde a una circunferencia, es decir, a la fórmula de adición del seno.

Desde Euler, los matemáticos buscaron una fórmula de adición para los arcos de elipse semejante a la de la lemniscata. Una muestra del interés que suscitó este problema es que las integrales de la forma

$$\int R(x, \sqrt{ax^4 + bx^3 + cx^2 + dx + e})\, dx,$$

donde R es una función racional, se conocen desde entonces como *integrales elípticas,* y de aquí derivan las denominaciones de cuerpos elípticos, curvas elípticas, funciones elípticas, etc.

Sin embargo, no existe tal fórmula de adición, y el motivo es que el integrando de (10.8) es una diferencial de segunda clase. En efecto, si llamamos

$$\omega = \frac{dz}{\sqrt{(1 - z^2)(1 - k^2z^2)}},$$

ya hemos visto que en términos de $x = z^2$, $y = wz$, la diferencial ω se expresa como $\omega = dx/2y$, donde x e y satisfacen una ecuación $y^2 = x(1 - x)(1 - k^2x)$, y el ejemplo de la página 326 muestra que ω es de primera clase.

Por consiguiente (volviendo a llamar x e y a las funciones de partida), el integrando de (10.8) es de la forma $\eta = (1 - k^2x^2)\omega$, donde ω es una diferencial de primera clase de un cuerpo de funciones elípticas. Estas diferenciales no tienen ceros ni polos, luego los polos de $1 - k^2x^2$ son también polos de η. Concretamente, es fácil ver que la función $1 - k^2x^2$ tiene un polo doble en el infinito con residuo nulo, por lo que η es una diferencial de segunda clase.

Si repasamos los argumentos que nos han llevado a concluir que las integrales de formas elípticas de primera clase cumplen teoremas de adición, veremos que ello depende únicamente de que las integrales hasta divisores principales son nulas módulo periodos (la mitad del teorema de Abel), y si nos fijamos en la prueba de este hecho veremos que casi vale para diferenciales de segunda clase, salvo por que si en la fórmula (10.6) la diferencial ω es de segunda clase, la función g puede tener polos, con lo que en lugar de $g(P)\operatorname{Res}_P \eta$ hay que poner $\operatorname{Res}_P(g\eta)$, y el análisis de los residuos de $g\eta$ es más delicado. Aunque no vamos a entrar en ello, afinando los razonamientos es posible tratar este caso y obtener una especie de fórmula de adición para integrales de segunda clase. Concretamente, para la integral del arco de elipse resulta que

$$\int_0^{x_1} \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx + \int_0^{x_2} \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx$$

$$= \int_0^{x'} \frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx + 2k^2x_1x_2x',$$

donde

$$x' = \frac{x_1y_2 + x_2y_1}{1-k^2x_1^2x_2^2},$$

pero la presencia del último término impide que esta relación pueda usarse para sumar arcos de elipse (salvo que la excentricidad sea $k = 0$, con lo que volvemos al caso de la circunferencia).

Para el caso de diferenciales de tercera clase también es posible hacer algo similar, pero el resultado es todavía más complicado. De todos modos, debemos tener presente que, si bien las fórmulas de adición de integrales estuvieron en la base de las investigaciones que llevaron a los teoremas que hemos estudiado en este capítulo, lo cierto es que desde un punto de vista moderno son más bien hechos anecdóticos, pues el valor de estos teoremas reside en sus repercusiones sobre los cuerpos de funciones algebraicas, y ello sólo involucra a las integrales de diferenciales de primera clase.

Capítulo XI

Funciones elípticas

Como consecuencia del teorema de Abel-Jacobi, todo cuerpo de funciones elípticas sobre el cuerpo de los números complejos puede representarse como el cuerpo de las funciones meromorfas de un toro complejo $T = \mathbb{C}/R$, donde R es un retículo en $\mathbb{C}$. Si llamamos $p : \mathbb{C} \longrightarrow T$ a la proyección canónica, vemos que cada función meromorfa f en T se corresponde con una función meromorfa $\bar{f} = p \circ f$ en $\mathbb{C}$ con la propiedad de que $\bar{f}(z + \omega) = \bar{f}(z)$, para todo $\omega \in R$. Esto significa que los elementos de R son periodos de $\bar{f}$. Recíprocamente, toda función con esta propiedad determina una función meromorfa en T.

Esto nos permite tratar a las funciones elípticas como funciones meromorfas en $\mathbb{C}$, con lo que la teoría de funciones de variable compleja se aplica de forma más directa a estas funciones algebraicas. El objeto de este capítulo es mostrar las repercusiones de estas ideas.

11.1 Funciones doblemente periódicas

Las definiciones básicas son las siguientes:

Definición 11.1 Un *periodo* de una función $f : \mathbb{C} \longrightarrow \mathbb{C}^\infty$ es un número complejo $\omega \neq 0$ tal que $f(z + \omega) = f(z)$ para todo $z \in \mathbb{C}$.

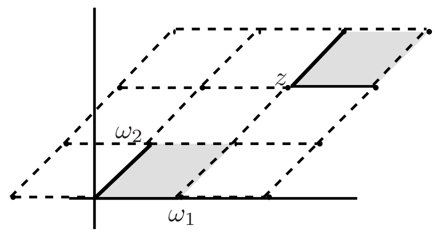
Una *función elíptica* es una función meromorfa $f : \mathbb{C} \longrightarrow \mathbb{C}^\infty$ doblemente periódica, es decir, que admite dos periodos ω_1 y ω_2 linealmente independientes sobre $\mathbb{R}$.

Es claro entonces que todos los puntos del retículo $R = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}}$ son periodos de f, si bien f puede tener todavía más periodos. No es difícil probar que si f no es constante podemos elegir adecuadamente dos periodos ω_1 y ω_2 de modo que el retículo R que generan sea el conjunto de todos los periodos de f, pero no vamos a necesitar este hecho; al contrario, estamos interesados en considerar conjuntamente todas las funciones elípticas cuyos periodos contengan un retículo dado R, sin que importe si tienen más periodos o no. Diremos que tales funciones son *elípticas sobre R*.

El *paralelogramo fundamental* de R asociado a una base ω_1, ω_2 es el conjunto

$$P = \{\alpha\omega_1 + \beta\omega_2 \mid 0 \leq \alpha < 1,\ 0 \leq \beta < 1\}.$$

Es claro que los conjuntos $z + P$, con $z \in R$ forman una partición de $\mathbb{C}$.



La figura muestra algunos puntos del retículo R generado por ω_1, ω_2, el paralelogramo fundamental P correspondiente a esta base y un trasladado $z+P$. Por otra parte, si $z \in \mathbb{C}$ es arbitrario, entonces $z - \frac{\omega_1+\omega_2}{2} + P$ es un entorno de z en $\mathbb{C}$. Así, todo punto está en el interior de un cierto trasladado de P.

La conexión de esta noción de función elíptica con la noción general ya ha sido explicada en la introducción del capítulo: si f es una función meromorfa sobre un toro complejo $T = \mathbb{C}/R$ y $p : \mathbb{C} \longrightarrow T$ es la proyección canónica, entonces $\bar{f} = p \circ f$ es claramente una función elíptica sobre R en el sentido de la definición anterior y, recíprocamente, si $\bar{f}$ es una función elíptica sobre R podemos definir $f : T \longrightarrow \mathbb{C}^\infty$ mediante $f([z]) = \bar{f}(z)$, y es claro que f es meromorfa, pues para cada carta $(p|_C)^{-1}$ de T tenemos que $(p|_C) \circ f = \bar{f}|_C$ es meromorfa.

Vemos así que la aplicación $f \mapsto \bar{f}$ biyecta el conjunto de las funciones elípticas sobre R con el conjunto de las funciones meromorfas sobre T. En lo sucesivo consideraremos indistintamente a las funciones elípticas como funciones meromorfas doblemente periódicas en $\mathbb{C}$ o como funciones meromorfas en un toro $T = \mathbb{C}/R$.

Así podemos traducir fácilmente muchos hechos conocidos sobre funciones elípticas en el sentido general a resultados sobre funciones elípticas como funciones de variable compleja. No obstante, conviene observar que los hechos básicos se demuestran fácilmente a partir de la propia definición de función doblemente periódica.

Por ejemplo, si f y g son funciones elípticas sobre un retículo R, entonces también lo son $f+g$, fg, αf (para todo $\alpha \in \mathbb{C}$) y f/g (si $g \neq 0$). Así pues, las funciones elípticas sobre un retículo R forman un subcuerpo del cuerpo de todas las funciones meromorfas en $\mathbb{C}$ (y la identificación $f \mapsto \bar{f}$ es un isomorfismo de cuerpos). De la definición de derivada se sigue inmediatamente que la derivada de una función elíptica sobre R también es elíptica sobre R.

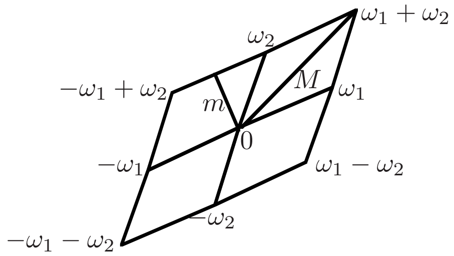
La prueba del teorema 6.29 se basa en un hecho no trivial, a saber, que en toda superficie de Riemann existen funciones meromorfas no constantes. A continuación construiremos ejemplos explícitos de funciones elípticas sobre un retículo dado R que permitirán llevar adelante la prueba del teorema 6.29 para los toros $\mathbb{C}/R$ sin necesidad de apelar al teorema de existencia de funciones meromorfas. Nos basaremos en el teorema siguiente:

Teorema 11.2 *Si R es un retículo en $\mathbb{C}$ y $\alpha \in \mathbb{R}$, entonces la serie*

$$\sum_{\omega \in R\setminus\{0\}} \frac{1}{\omega^\alpha}$$

converge (absolutamente) si y sólo si $\alpha > 2$.

Demostración: Notemos que, puesto que no hemos especificado un orden en los sumandos, sólo tiene sentido hablar de convergencia absoluta. Sea ω_1, ω_2 una base de R y llamemos m y M a las distancias mínima y máxima, respectivamente, de 0 a la frontera del paralelogramo indicado en la figura:



Si $\omega \neq 0$ es cualquiera de los 8 elementos de R representados en la figura, tenemos que $m \leq |\omega| \leq M$. Si dibujamos los 12 paralelogramos que rodean a los 4 que aparecen en la figura, encontraremos 16 nuevos elementos $\omega \in R$ tales que $2m \leq |\omega| \leq 2M$. A continuación encontraremos 24 nuevos elementos tales que $3m \leq |\omega| \leq 3M$, etc.

En general, encontramos $8k$ elementos de R que satisfacen las desigualdades

$$\frac{1}{(kM)^\alpha} \leq \frac{1}{|\omega|^\alpha} \leq \frac{1}{(km)^\alpha}.$$

Si llamamos $S(n) = \sum |\omega|^{-\alpha}$, donde ω recorre los $8(1+2+\cdots+n)$ elementos de R más cercanos a 0, tenemos que

$$\frac{8}{M^\alpha} + \frac{2\cdot 8}{(2M)^\alpha} + \cdots + \frac{n\cdot 8}{(nM)^\alpha} \leq S(n) \leq \frac{8}{m^\alpha} + \frac{2\cdot 8}{(2m)^\alpha} + \cdots + \frac{n\cdot 8}{(nm)^\alpha},$$

lo cual equivale a

$$\frac{8}{M^\alpha}\sum_{k=1}^n \frac{1}{k^{\alpha-1}} \leq S(n) \leq \frac{8}{m^\alpha}\sum_{k=1}^n \frac{1}{k^{\alpha-1}}.$$

Si $\alpha > 2$, la serie de la derecha es convergente, luego $S(n)$ también, mientras que si $\alpha \leq 2$ la serie de la izquierda es divergente, luego $S(n)$ también. La convergencia de $S(n)$ equivale a la convergencia absoluta de la serie del enunciado.

■

De aquí deducimos la convergencia de una serie funcional:

Teorema 11.3 *Si R es un retículo, $\alpha > 2$ y $M > 0$, entonces la serie*

$$\sum_{|\omega|>M} \frac{1}{(z-\omega)^\alpha},$$

donde $\omega \in R$, converge absoluta y uniformemente en el disco $|z| \leq M$.

DEMOSTRACIÓN: Basta encontrar una constante K tal que

$$\frac{1}{|z-\omega|^\alpha} \leq \frac{K}{|\omega|^\alpha}, \tag{11.1}$$

para todo $\omega \in R$ con $|\omega| > M$ y todo z con $|z| \leq M$. La convergencia absoluta de la serie se sigue entonces del criterio de mayoración de Weierstrass y del teorema anterior. A su vez, esta desigualdad equivale a

$$\left|\frac{z-\omega}{\omega}\right|^\alpha \geq \frac{1}{K} = \epsilon.$$

Para encontrar ϵ tomamos un $\omega \in R$ tal que $|\omega| > M$ pero que tenga módulo mínimo $|\omega| = M + \delta$. Entonces, si $|z| \leq M$ se cumple

$$\left|\frac{z-\omega}{\omega}\right| = \left|1 - \frac{z}{\omega}\right| \geq 1 - \frac{|z|}{|\omega|} \geq 1 - \frac{M}{M+\delta} = \epsilon.$$

■

Ahora es fácil mostrar un ejemplo de función elíptica no constante:

Teorema 11.4 *Si R es un retículo, entonces la serie*

$$f(z) = \sum_{\omega \in R} \frac{1}{(z-\omega)^3}$$

define una función elíptica sobre R con polos de orden 3 en cada uno de los puntos de R.

DEMOSTRACIÓN: Por el teorema anterior, la suma para $|\omega| > M$ de la serie del enunciado converge absoluta y uniformemente en el disco $|z| \leq M$, luego define una función holomorfa en el disco abierto. La función f se diferencia de esta suma en un número finito de términos, que constituyen una fracción algebraica con polos triples en cada uno de los puntos de R contenidos en el disco. Como esto vale para todo M, vemos que f es una función meromorfa en $\mathbb{C}$ cuyos únicos polos son los puntos de R.

Si $\omega_0 \in R$, entonces ω_0 es un periodo de f, pues, teniendo en cuenta la convergencia absoluta,

$$f(z+\omega_0) = \sum_{\omega \in R} \frac{1}{(z+\omega_0-\omega)^3} = \sum_{\omega \in R} \frac{1}{(z-\omega)^3},$$

ya que cuando ω recorre R, lo mismo hace $\omega_0 - \omega$. ■

Según comentábamos, esto hace que la prueba del teorema 6.29 para los toros $\mathbb{C}/R$ no dependa del teorema general sobre existencia de funciones meromorfas no constantes. En cualquier caso, lo cierto es que 6.29 nos da que el cuerpo de las funciones elípticas sobre R es un cuerpo de funciones algebraicas de género 1. En particular el teorema 7.7 nos da que una función elíptica no constante tiene el mismo número (no nulo) de ceros y de polos —contados con su multiplicidad— ya sea en el toro $\mathbb{C}/R$ o bien en un paralelogramo fundamental de R.

Definición 11.5 Se llama *orden* de una función elíptica sobre un retículo R al número de ceros (o de polos) que tiene sobre un paralelogramo fundamental de R (contados con su multiplicidad).

El teorema 7.7 implica además que si K es el cuerpo de funciones elípticas sobre un retículo R y $\alpha \in K$ tiene orden n, entonces $|K : \mathbb{C}(\alpha)| = n$. En particular vemos que no puede haber funciones elípticas de orden 1, pues esto implicaría que $K = \mathbb{C}(\alpha)$ y entonces K tendría género 0. La función f que hemos construido tiene orden 3. Vamos a ver que a partir de ella podemos obtener otra de orden 2. La idea es integrar f término a término. Si la parte principal de f alrededor de cada periodo es $(z-\omega)^{-3}$, al integrar quedará $-\frac{1}{2}(\omega - z)^{-2}$, por lo que la multiplicamos por -2 para simplificar el resultado. En lugar de entrar en tecnicismos sobre la determinación de los caminos de integración y de las constantes adecuadas, definimos directamente la que será la integral de f (salvo un factor -2) y luego comprobaremos (derivando) que es efectivamente la función que buscamos.

Definición 11.6 Se llama *función $\wp$ de Weierstrass* asociada a un retículo R de $\mathbb{C}$ a la función dada por

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in R \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Teorema 11.7 *Si R es un retículo en $\mathbb{C}$, entonces la función $\wp$ es una función elíptica sobre R con polos dobles en los puntos de R. Además*

$$\wp'(z) = -2 \sum_{\omega \in R} \frac{1}{(z-\omega)^3}.$$

DEMOSTRACIÓN: Claramente,

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right|.$$

Fijado $M > 0$, hay un número finito de elementos $\omega \in R$ en el disco $|z| \leq M$. Para los restantes tenemos (11.1), con lo que

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \leq \frac{KM(2|\omega| + M)}{|\omega|^4} = \frac{KM(2 + M/|\omega|)}{|\omega|^3} \leq \frac{3KM}{|\omega|^3}.$$

Esto implica que la serie que define a $\wp$ (salvo un número finito de términos) converge absoluta y uniformemente en cada disco $|z| < M$, luego define una función holomorfa. Al sumarle los primeros términos obtenemos una función meromorfa con un polo doble en cada elemento de R. La derivada de $\wp$ puede calcularse término a término, y es claramente la que se indica en el enunciado.

Observemos ahora que $\wp$ es par, es decir, cumple $\wp(z) = \wp(-z)$. En efecto, usamos que

$$(-z-\omega)^2 = (z+\omega)^2 = (z-(-\omega))^2,$$

sumamos sobre ω y usamos que $-\omega$ recorre R cuando ω lo hace.

Sabemos que $\wp'$ es elíptica sobre R, luego si $\omega \in R$ la función $\wp(z+\omega)-\wp(z)$ es constante. Ahora bien, para $z = -\omega/2$ ha de ser

$$\wp(z+\omega) - \wp(z) = \wp(\omega/2) - \wp(-\omega/2) = 0,$$

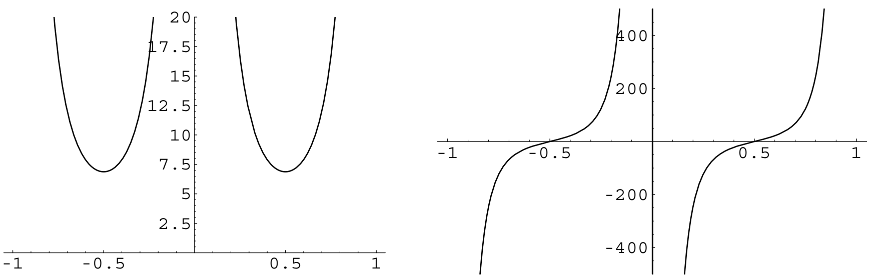
luego $\wp(z+\omega) - \wp(z)$ es la función nula. ■

Las funciones $\wp$ y $\wp'$ se llaman *funciones elípticas de Weierstrass.* Tenemos que $\wp$ es par y $\wp'$ es impar, es decir, se cumplen las ecuaciones funcionales

$$\wp(-z) = \wp(z), \qquad \wp'(-z) = -\wp'(z).$$

La primera ecuación la hemos visto en la prueba del teorema anterior y la segunda se sigue inmediatamente de la serie que define $\wp'$.

Éstas son las gráficas de $\wp$ y $\wp'$ para el retículo $R = \langle 1, i\rangle$:



Como primera muestra de la importancia de estas funciones en la teoría tenemos el teorema siguiente:

Teorema 11.8 *Si R es un retículo en $\mathbb{C}$ y $\wp$ es su función de Weierstrass, entonces $\mathbb{C}(\wp, \wp')$ es el cuerpo de todas las funciones elípticas sobre R.*

Demostración: Basta tener en cuenta el teorema 7.7, según el cual, si K es el cuerpo de las funciones elípticas sobre R, se cumple $|K : \mathbb{C}(\wp)| = 2$ y $|K : \mathbb{C}(\wp')| = 3$. De aquí se sigue que $\wp' \notin \mathbb{C}(\wp)$ y que $\mathbb{C}(\wp, \wp') = K$. ■

Ahora probaremos que $\wp$ y $\wp'$ no son unos generadores cualesquiera del cuerpo de todas las funciones elípticas sobre el retículo correspondiente, sino que además satisfacen una ecuación polinómica en forma normal de Weierstrass. Para ello hemos de calcular la serie de Laurent de $\wp$, para lo cual conviene a su vez definir antes las series de Eisenstein:

Definición 11.9 Sea R un retículo en $\mathbb{C}$. Para cada natural $n \geq 3$, la *serie de Eisenstein* de R de orden n es

$$G_n = \sum_{\omega \in R \setminus \{0\}} \frac{1}{\omega^n}.$$

El teorema 11.2 prueba la convergencia de las series de Eisenstein. En la prueba del teorema siguiente se ve que $G_{2n+1} = 0$ para todo n:

Teorema 11.10 *La serie de Laurent en* 0 *de la función de Weierstrass* $\wp$ *de un retículo* R *es*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}\, z^{2n}.$$

DEMOSTRACIÓN: Usamos el desarrollo de Taylor

$$\frac{1}{(1-z)^2} = \sum_{n=0}^{\infty} (n+1) z^n, \qquad |z| < 1.$$

Sea $m > 0$ el menor módulo de un elemento no nulo de R. Si $0 < |z| < m$ y $\omega \in R$ es no nulo, entonces $|z/\omega| < 1$ y

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2 \left(1 - \frac{z}{\omega}\right)^2} = \frac{1}{\omega^2} \left(1 + \sum_{n=1}^{\infty} (n+1) \left(\frac{z}{\omega}\right)^n\right),$$

luego

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty} \frac{n+1}{\omega^{n+2}} z^n.$$

Sumando sobre ω y teniendo en cuenta que todas las series convergen absolutamente,

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) \sum_{\omega \in R \setminus \{0\}} \frac{1}{\omega^{n+2}}\, z^n = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) G_{n+2}\, z^n.$$

Como $\wp$ es una función par, las series de Eisenstein G_{2k+1} han de ser nulas, con lo que queda la expresión del enunciado. ■

Ahora podemos probar:

Teorema 11.11 *La función* $\wp$ *de un retículo* R *satisface la ecuación diferencial*

$$\wp'^2 = 4\wp^3 - 60 G_4 \wp - 140 G_6.$$

DEMOSTRACIÓN: Derivando la serie de Laurent de $\wp$ obtenemos que (para todo z cercano a 0)

$$\wp'(z) = -\frac{2}{z^3} + 6 G_4 z + 20 G_6 z^3 + \cdots$$

Por lo tanto

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \cdots$$

donde los puntos suspensivos representan una función holomorfa que se anula en 0. Por otra parte,

$$\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + \cdots$$

Por consiguiente

$$\wp'(z)^2 - 4\wp^3 + 60G_4\wp(z) = -140G_6 + \cdots$$

Esta función es elíptica y no tiene polos, luego ha de ser constante, lo que nos da la ecuación diferencial que buscamos. ■

Si llamamos $g_2 = 60G_4$ y $g_3 = 140G_6$ tenemos que las funciones de Weierstrass satisfacen la ecuación diferencial

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

Para que podamos decir que esta ecuación está en forma normal hemos de probar que el polinomio $4X^3 - g_2X - g_3$ no tiene raíces múltiples. Vamos a calcular estas raíces.

Definición 11.12 Si $R = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}}$ es un retículo en $\mathbb{C}$ y $\wp$ es su correspondiente función de Weierstrass, definimos

$$e_1 = \wp\left(\frac{\omega_1}{2}\right), \quad e_2 = \wp\left(\frac{\omega_2}{2}\right), \quad e_3 = \wp\left(\frac{\omega_1 + \omega_2}{2}\right).$$

El teorema siguiente muestra, entre otras cosas, que estos números no dependen (salvo el orden) de la elección de la base de R:

Teorema 11.13 *Si R es un retículo en $\mathbb{C}$, entonces*

$$4\wp^3 - g_2\wp - g_3 = 4(\wp - e_1)(\wp - e_2)(\wp - e_3).$$

Además, las raíces e_1, e_2, e_3 son distintas dos a dos, por lo que el discriminante del polinomio $4X^3 - g_2X - g_3$ cumple $\Delta = g_2^3 - 27g_3^2 \neq 0$.

DEMOSTRACIÓN: Sea α_i uno de los tres números $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$, de modo que $\wp(\alpha_i) = e_i$. Claramente $\alpha_i \notin R$, pero $2\alpha_i \in R$. La función $\wp(z) - e_i$ tiene un cero doble en α_i, pues, usando que $\wp'$ es impar, vemos que

$$-\wp'(\alpha_i) = \wp'(-\alpha_i) = \wp'(-\alpha_i + 2\alpha_i) = \wp'(\alpha_i),$$

luego ha de ser $\wp'(\alpha_i) = 0$ y así α_i es un cero de $\wp - e_i$ de orden al menos dos. Contando los polos vemos que la función tiene orden 2, luego α_i ha de ser su único cero y su orden ha de ser exactamente 2.

Por consiguiente, la función $g(z) = 4(\wp - e_1)(\wp - e_2)(\wp - e_3)$ tiene exactamente tres ceros dobles. Lo mismo podemos decir de la función $\wp'^2$, que tiene orden 6 (sólo tiene polos de orden 6 en los puntos de R) y acabamos de ver que tiene ceros de orden al menos 2 en los mismos puntos que g. Así pues, dichos ceros han de ser exactamente de orden 2 y no puede tener más. El cociente

$$\frac{\wp'(z)^2}{g(z)} = \frac{4\wp(z)^3 - g_2\wp(z) - g_3}{4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)}$$

ha de ser constante y, calculando su límite en 0 (dividiendo entre $\wp^3$), vemos que la constante ha de ser 1, y así tenemos la igualdad del enunciado.

Los e_i han de ser distintos, pues si, por ejemplo, $e_1 = e_2$, entonces $\wp(z) - e_1$ tendría un cero doble en $\omega_1/2$ y otro en $\omega_2/2$, pero ya hemos visto que su orden es 2, luego esto es imposible. ■

Consideremos ahora un toro complejo $T = \mathbb{C}/R$ y la curva proyectiva $V \subset \mathrm{P}^2$ dada por la ecuación $Y^2 = 4X^3 - g_2X - g_3$ (donde g_2 y g_3 son los asociados a las funciones de Weierstrass del retículo R). Definimos $\phi : T \longrightarrow V$ mediante $P \mapsto (\wp(P), \wp'(P))$, con el convenio de que $\phi(0)$ es el único punto infinito de V, de coordenadas homogéneas $(0, 1, 0)$. Si lo llamamos ∞, tenemos que $\phi(0) = \infty$.

Obviamente $\phi|_{T\setminus\{0\}} : T \setminus \{0\} \longrightarrow \mathbb{C}^2$ es holomorfa, luego también lo es como aplicación en V. Así pues, ϕ es holomorfa salvo a lo sumo en 0. Para probar que también aquí lo es, hemos de componerla con una carta de V alrededor de ∞. Sirve la restricción de cualquier función $f \in \mathbb{C}(V)$ tal que $v_\infty(f) = 1$. Por ejemplo, podemos tomar $f = X/Y$. Claramente, $(\phi \circ f)(P) = \wp(P)/\wp'(P)$, que es una función holomorfa en un entorno de 0.

Observemos ahora que ϕ es biyectiva. En efecto, si $\wp(P_1) = \wp(P_2) = \alpha$ y $\wp'(P_1) = \wp'(P_2)$ con $P_1 \neq P_2$, entonces $P_i \neq 0$, pues $\wp$ sólo tiene un polo en 0. Así pues, α es finito y podemos considerar la función $\wp - \alpha$. Vemos que tiene ceros en P_1 y P_2. Como $\wp$ es par, también $-P_2$ es un cero de $\wp - \alpha$.

Distinguimos dos casos: si $P_2 \neq -P_2$, entonces, dado que la función $\wp - \alpha$ tiene orden 2, ha de ser $P_1 = -P_2$, pero entonces $\wp'(P_1) = -\wp'(P_2)$, lo que obliga a que $\wp'(P_1) = \wp'(P_2) = 0$, pero esto es imposible, ya que entonces $\wp - \alpha$ tendría (contando multiplicidades) al menos cuatro ceros.

La otra posibilidad es $P_2 = -P_2$, y entonces $\wp'(P_2) = \wp'(-P_2) = -\wp'(P_2)$, luego ha de ser $\wp'(P_2) = 0$ y así $\wp - \alpha$ tiene un cero en P_1 y dos en P_2, en contradicción nuevamente con que su orden es 2.

La suprayectividad de ϕ es ahora trivial, pues la imagen ha de ser abierta porque ϕ es holomorfa y ha de ser cerrada porque T es compacto. Con esto casi hemos probado el teorema siguiente:

Teorema 11.14 *Sea $T = \mathbb{C}/R$ un toro complejo, sea $\wp$ su función de Weierstrass y sea V la curva elíptica dada por $Y^2 = 4X^3 - g_2X - g_3$. Entonces la aplicación $\phi : T \longrightarrow V$ dada por $\phi(P) = (\wp(P), \wp'(P))$ para $P \neq 0$ y $\phi(0) = \infty$ es una transformación conforme y un isomorfismo de grupos (cuando en V consideramos la estructura de grupo que resulta de tomar como elemento neutro el punto infinito).*

Demostración: Sólo falta probar que ϕ es un homomorfismo de grupos. Ahora bien, $P+Q=S$ equivale a que el divisor $PQ/S0$ sea principal, es decir, a que exista una función elíptica α con ceros en P y Q y polos en S y 0. Entonces $\phi^{-1}\circ\alpha$ es una función meromorfa en V (luego racional) con ceros en $\phi(P)$ y $\phi(Q)$ y polos en $\phi(S)$ e ∞, luego $\phi(P)+\phi(Q)=\phi(S)$. Aquí hemos usado que la estructura de grupo en T coincide con la inducida por su estructura de superficie de Riemann cuando tomamos como elemento neutro el 0 (teorema 10.23). ■

Este teorema nos permite identificar las funciones meromorfas sobre el toro $T=\mathbb{C}/R$ (es decir, las funciones elípticas sobre el retículo R) con las funciones racionales sobre V. Las funciones $\wp$ y $\wp'$ se corresponden con x e y respectivamente.

El isomorfismo hace corresponder la diferencial de primera clase $\omega=dx/y$ en V con $d\wp/\wp'$, y es fácil ver que ésta es simplemente la forma dz en T. A partir de aquí se sigue sin dificultad que el isomorfismo del teorema anterior es el inverso del isomorfismo de Abel-Jacobi de la variedad V determinado por ω.

A cada retículo complejo R le hemos asociado dos invariantes $g_2(R)$ y $g_3(R)$. Conviene considerarlos como funciones de las bases, es decir,

$$g_2(\omega_1,\omega_2)=60\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}\frac{1}{(m\omega_1+n\omega_2)^4},$$

$$g_3(\omega_1,\omega_2)=140\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}\frac{1}{(m\omega_1+n\omega_2)^6}.$$

Estas funciones están definidas cuando ω_1 y ω_2 son linealmente independientes sobre $\mathbb{R}$. Observemos que

$$g_2(\alpha\omega_1,\alpha\omega_2)=\alpha^{-4}g_2(\omega_1,\omega_2),\qquad g_3(\alpha\omega_1,\alpha\omega_2)=\alpha^{-6}g_3(\omega_1,\omega_2),$$

luego en particular

$$g_2(\omega_1,\omega_2)=\omega_1^{-4}g_2(1,\omega_2/\omega_1),\qquad g_3(\omega_1,\omega_2)=\omega_1^{-6}g_3(1,\omega_2/\omega_1).$$

Esto significa que basta estudiar las funciones de una variable

$$g_2(\tau)=60\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}\frac{1}{(m+n\tau)^4},\qquad g_3(\tau)=140\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}\frac{1}{(m+n\tau)^6},$$

definidas para $\operatorname{Im}\tau\neq 0$. Como podemos elegir el orden de ω_1 y ω_2, no perdemos generalidad si las restringimos al semiplano

$$H=\{\tau\in\mathbb{C}\mid \operatorname{Im}\tau>0\}.$$

Similarmente, si definimos $\Delta(\omega_1,\omega_2)=g_2^3(\omega_1,\omega_2)-27g_3^2(\omega_1,\omega_2)$ tenemos $\Delta(\alpha\omega_1,\alpha\omega_2)=\alpha^{-12}\Delta(\omega_1,\omega_2)$ y en particular $\Delta(\omega_1,\omega_2)=\omega_1^{-12}\Delta(1,\omega_2/\omega_1)$. Por lo tanto, basta estudiar la función $\Delta(\tau)=\Delta(1,\tau)=g_2^3(\tau)-27g_3^2(\tau)$.

Por último, consideramos la función

$$J(\omega_1, \omega_2) = \frac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)},$$

que satisface $J(\alpha\omega_1, \alpha\omega_2) = J(\omega_1, \omega_2)$ y cuyo estudio puede reducirse a la función en H dada por

$$J(\tau) = J(1, \tau) = \frac{g_2^3(\tau)}{\Delta(\tau)}.$$

La función $J(\tau)$ se conoce como *función modular de Klein.* Conviene recordar que g_2 y g_3 dependen únicamente del retículo generado por ω_1 y ω_2, luego, dado un retículo R, podemos hablar de $g_2(R)$, $g_3(R)$, $\Delta(R)$ y $J(R)$.

Según el teorema 9.14, el número $J(R)$ depende únicamente del cuerpo de funciones meromorfas de $T = \mathbb{C}/R$ y, por 9.15, sabemos que $J(R)$ determina a dicho cuerpo salvo isomorfismo. Equivalentemente, (ver las observaciones tras la definición 1.82) $J(R)$ determina el toro $\mathbb{C}/R$ salvo transformaciones conformes y el retículo R salvo equivalencia lineal. Además, el teorema 9.17 afirma que existen cuerpos de funciones elípticas cuyo invariante es cualquier número complejo prefijado y, como cualquiera de estos cuerpos puede representarse como el cuerpo de las funciones meromorfas de un toro complejo, concluimos que la función modular $J(\tau)$ toma en H todos los valores complejos. Todavía podemos precisar más:

Teorema 11.15 *Si c_2 y c_3 son números complejos tales que $c_2^3 - 27c_3^2 \neq 0$, entonces existen números complejos ω_1, ω_2 linealmente independientes sobre $\mathbb{R}$ tales que $g_2(\omega_1, \omega_2) = c_2$ y $g_3(\omega_1, \omega_2) = c_3$.*

DEMOSTRACIÓN: Según las observaciones previas al teorema, sabemos que existe $\tau \in H$ tal que $J(\tau) = J(1, \tau) = c_2^3/(c_2^3 - 27c_3^2)$.

Si $c_2 = 0$ entonces $J(1, \tau) = 0$, luego $g_2(1, \tau) = 0$ y $g_3(1, \tau) \neq 0$. Sea $\alpha \in \mathbb{C}$ tal que $\alpha^{-6} g_3(1, \tau) = c_3$. Tomamos $\omega_1 = \alpha$, $\omega_2 = \alpha\tau$, de modo que $g_2(\omega_1, \omega_2) = \alpha^{-4} g_2(1, \tau) = 0 = c_2$ y $g_3(\omega_1, \omega_2) = \alpha^{-6} g_3(1, \tau) = c_3$.

Si $c_2 \neq 0$ entonces $J(1, \tau) \neq 0$, luego $g_2(1, \tau) \neq 0$. Tomamos $\alpha \in \mathbb{C}$ tal que $\alpha^{-4} g_2(1, \tau) = c_2$ y $\omega_1 = \alpha$, $\omega_2 = \alpha\tau$. Entonces $g_2(\omega_1, \omega_2) = \alpha^{-4} g_2(1, \tau) = c_2$. Por otra parte,

$$\frac{c_2^3}{c_2^3 - 27c_3^2} = J(1, \tau) = J(\omega_1, \omega_2) = \frac{c_2^3}{c_2^3 - 27g_3^2(\omega_1, \omega_2)}.$$

Por lo tanto $g_3^2(\omega_1, \omega_2) = c_3^2$ y $g_3(\omega_1, \omega_2) = \pm c_3$. Cambiando ω_1 y ω_2 por $-\omega_1$, $-\omega_2$ no alteramos g_2 pero cambiamos el signo a g_3, con lo que podemos garantizar la igualdad $g_3(\omega_1, \omega_2) = c_3$. ∎

Este teorema garantiza que cualquier ecuación en forma normal de Weierstrass, $y^2 = 4x^3 - c_2 x - c_3$ puede parametrizarse por las funciones de Weierstrass de un cierto retículo complejo R.

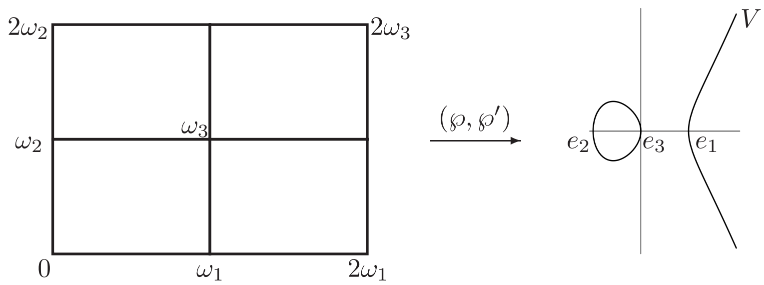
11.2 Curvas elípticas reales

Vamos a analizar con más detalle las curvas elípticas V que admiten una ecuación en forma normal de Weierstrass $Y^2 = 4X^3 - g_2X - g_3$ con invariantes g_2, g_3 reales. Probaremos que estas curvas se corresponden con los retículos complejos generados por un periodo real y otro imaginario puro, o bien por dos periodos imaginarios conjugados.

En esta sección emplearemos la notación clásica de Weierstrass, de modo que $R = \langle 2\omega_1, 2\omega_2\rangle_{\mathbb{Z}}$. Los números ω_1 y ω_2 se llaman *semiperiodos.* También nos va a interesar el semiperiodo $\omega_3 = \omega_1 + \omega_2$ pues, según sabemos, $e_1 = \wp(\omega_1)$, $e_2 = \wp(\omega_2)$ y $e_3 = \wp(\omega_3)$ son los ceros de $4x^3 - g_2x - g_3$, luego ω_1, ω_2 y ω_3 son los ceros de $\wp'(z)$.

Caso ω_1 real y ω_2 imaginario puro No perdemos generalidad si suponemos que $\omega_1 > 0$ y $\omega_2/i > 0$. En este caso, el retículo $R = \langle 2\omega_1, 2\omega_2\rangle_{\mathbb{Z}}$ es estable para la conjugación compleja, es decir, cuando ω recorre R, entonces $\bar{\omega}$ también recorre R. De la definición de $\wp(z)$ se sigue entonces que $\overline{\wp(z)} = \wp(\overline{z})$ y, en particular, $\wp(z)$ es real cuando z es real. Como $\wp(z)$ es par, si $x \in \mathbb{R}$ tenemos también que $\overline{\wp(ix)} = \wp(-ix) = \wp(ix)$, luego $\wp(z)$ también es real sobre el eje imaginario. Por consiguiente, e_1 y e_2 son reales, y lo mismo vale para e_3, pues es la tercera raíz del polinomio $4x^3 - g_2x - g_3$ y, por consiguiente, $e_1 + e_2 + e_3 = 0$. También es claro que los invariantes g_2 y g_3 son reales (por la propia definición).

Sabemos que la aplicación $z \mapsto (\wp(z), \wp'(z))$ hace corresponder los puntos del paralelogramo —rectángulo en este caso— de vértices, 0, $2\omega_1$, $2\omega_2$ y $2\omega_3$ con la curva elíptica V de ecuación $Y^2 = 4X^3 - g_2X - g_3$. Vamos a estudiar más a fondo esta correspondencia. Admitiendo las desigualdades $e_2 < e_3 < e_1$ —que enseguida demostraremos— es claro que el polinomio $4X^3 - g_2X - g_3$ es mayor o igual que 0 en $[e_2, e_3] \cup [e_1, +\infty[$, por lo que la parte real de V tiene la forma que muestra la figura siguiente.



En principio sabemos que los cuatro vértices del rectángulo son polos de $\wp$ y de $\wp'$, por lo que todos ellos se corresponden con el único punto infinito de V. Así mismo tenemos que $\wp'$ se anula en los tres semiperiodos, luego éstos se corresponden con los tres puntos de corte de V con el eje $Y = 0$.

La parte principal de $\wp'(z)$ en 0 es $-2/z^3$. Esto implica que

$$\lim_{x\to 0^+} \wp'(x) = -\infty, \qquad \lim_{x\to 0^-} \wp'(x) = +\infty.$$

Teniendo en cuenta que el único cero de $\wp'(x)$ en $[0, 2\omega_1]$ es ω_1 y la periodicidad, concluimos que $\wp'(x)$ es negativa en $]0, \omega_1[$ y positiva en $]\omega_1, 2\omega_1[$, luego $\wp(x)$ es decreciente en $]0, \omega_1[$ y creciente en $]\omega_1, 2\omega_1[$. Así pues, $\wp(x)$ tiene un mínimo en ω_1, donde toma el valor e_1. En definitiva, su gráfica ha de ser como muestra la figura de la página 380.

Tenemos que $\wp'(x)^2 = 4\wp(x)^3 - g_2\wp(x) - g_3$ no se anula en $]0, \omega_1[$, y cuando x va de 0 a ω_1 la función $\wp(x)$ desciende de $+\infty$ a e_1, luego el polinomio $4x^3 - g_2x - g_3$ no se anula en $]e_1, +\infty[$. Esto significa que, tal y como afirmábamos, e_1 es la mayor de las tres raíces e_1, e_2, e_3.

Ahora es claro que cuando x recorre el intervalo $[0, 2\omega_1]$ el arco $(\wp(x), \wp'(x))$ recorre en sentido horario la rama derecha de la curva V. En particular, la función $\wp'(x)$ es estrictamente creciente en $]0, 2\omega_1[$, tal y como muestra la figura de la página 380.

Una consecuencia de lo que acabamos de obtener es la siguiente: puesto que una integral sobre un arco no depende de la parametrización de éste, tenemos que

$$\int_{e_1}^{+\infty} \frac{dx}{\sqrt{4x^3 - g_2x - g_3}} = \omega_1. \tag{11.2}$$

En efecto, la integral puede verse como la integral de la forma dx/y sobre la mitad superior de la rama derecha de V, la cual se corresponde a su vez con la integral de dz sobre el segmento $[\omega_1, 2\omega_1]$. En otras palabras, basta hacer el cambio de variable $x = \wp(t)$.

Estudiamos ahora el segmento $[0, 2\omega_2]$. Para ello observamos que

$$\wp(iz|\omega_1, \omega_2) = -\wp(z| - i\omega_2, i\omega_1), \qquad \wp'(iz|\omega_1, \omega_2) = i\wp(z| - i\omega_2, i\omega_1).$$

En efecto:

$$\wp(iz|\omega_1, \omega_2) = -\frac{1}{z^2} + \sum_{\omega \in -iR\setminus\{0\}} \left(\frac{1}{(iz - i\omega)^2} - \frac{1}{(i\omega)^2} \right)$$

$$= -\frac{1}{z^2} - \sum_{\omega \in -iR\setminus\{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right) = -\wp(z| - i\omega_1, -i\omega_2) = -\wp(z| - i\omega_2, i\omega_1).$$

La segunda relación se obtiene derivando ésta. Además:

$$e_1(\omega_1, \omega_2) = \wp(i(-i\omega_1)|\omega_1, \omega_2) = -\wp(-i\omega_1| - i\omega_2, i\omega_1) = -e_2(-i\omega_2, i\omega_1).$$

Igualmente, $e_2(\omega_1, \omega_2) = -e_1(-i\omega_2, \omega_1)$ y, como $e_1 + e_2 + e_3 = 0$, ha de ser $e_3(\omega_1, \omega_2) = -e_3(-i\omega_2, i\omega_1)$.

De aquí se sigue que los invariantes de $\wp(z| - i\omega_2, i\omega_1)$ son g_2 y $-g_3$. Aplicando a esta función los resultados anteriores concluimos que e_2 es la menor raíz entre e_1, e_2 y e_3, luego tenemos, en efecto, las desigualdades $e_2 < e_3 < e_1$.

Cuando z varía entre 0 y ω_2, sabemos que $\wp(z|-i\omega_2, i\omega_1)$ decrece de $+\infty$ hasta $-e_2$, luego $\wp(z)$ crece de $-\infty$ hasta e_2. Similarmente, cuando z varía entre ω_2 y $2\omega_2$ la función $\wp(z)$ decrece de e_2 hasta $-\infty$. Así, el segmento $[0, 2\omega_2]$ se corresponde con los puntos de V de la forma $(x, \pm i\sqrt{-4x^3+g_2x+g_3})$, con $x \leq e_2$. Ahora es claro que

$$i\int_{-\infty}^{e_2} \frac{dx}{\sqrt{-4x^3+g_2x+g_3}} = \omega_2. \tag{11.3}$$

Observemos a continuación que si x es un número real, entonces

$$\wp(x+\omega_2) = \wp(x-\omega_2) = \wp(\overline{x+\omega_2}) = \overline{\wp(x+\omega_2)},$$

luego $\wp$ toma valores reales sobre el segmento $[\omega_2, \omega_3]$. Puesto que en los extremos toma los valores $e_2 < e_3$ y $\wp'$ no se anula, concluimos que es estrictamente creciente, luego $\wp'$ es positiva, luego el segmento $[\omega_2, \omega_3]$ se corresponde con la parte positiva de la rama izquierda de la parte real de V. Similarmente concluimos que el segmento $[\omega_3, 2\omega_1+\omega_2]$ se corresponde con la parte negativa de dicha rama. En definitiva, el segmento $[\omega_2, 2\omega_1+\omega_2]$ se corresponde con la rama izquierda de V recorrida en sentido horario. En particular,

$$\int_{e_2}^{e_3} \frac{dx}{\sqrt{4x^3-g_2x-g_3}} = \omega_1.$$

Del mismo modo se comprueba que la función $\wp(z)$ es real sobre el segmento $[\omega_1, \omega_1+2\omega_2]$: primero crece de e_3 a e_1 y luego decrece de e_1 a e_3 (la función $\wp'$ toma valores imaginarios puros). Por consiguiente, este segmento se corresponde con los puntos de V de la forma $(x, \pm i\sqrt{-4x^3+g_2x+g_3})$, con $e_3 \leq x \leq e_1$, luego

$$i\int_{e_3}^{e_1} \frac{dx}{\sqrt{-4x^3+g_2x+g_3}} = \omega_2.$$

Ahora demostraremos que cualquier curva V determinada por una ecuación de la forma $Y^2 = 4X^3 - g_2X - g_3$ con invariantes reales g_2 y g_3 y de modo que el polinomio $4X^3 - g_2X - g_3$ tenga tres raíces reales distintas $e_2 < e_3 < e_1$ está parametrizada por las funciones de Weierstrass de un retículo del tipo que estamos estudiando. Para ello conviene que antes mostremos unas expresiones alternativas para algunas de las integrales que hemos calculado.

Aplicamos a (11.2) el cambio de variable

$$x = e_2 + \frac{e_1-e_2}{t^2},$$

con lo que obtenemos

$$\omega_1 = \int_{e_1}^{+\infty} \frac{dx}{\sqrt{4x^3-g_2x-g_3}} = \int_0^1 \frac{\frac{2(e_1-e_2)}{t^3}}{\frac{2(e_1-e_2)^{3/2}}{t^3}\sqrt{(1-t^2)(1-k^2t^2)}}\,dt$$

$$= \frac{1}{\sqrt{e_1 - e_2}} \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}, \tag{11.4}$$

donde

$$0 < k^2 = \frac{e_3 - e_2}{e_1 - e_2} < 1.$$

En (11.3) cambiamos x por $-x$ y luego hacemos

$$x = \frac{e_1 - e_2}{t^2} - e_1.$$

Tras un cálculo similar al anterior llegamos a

$$\omega_2 = \frac{i}{\sqrt{e_1 - e_2}} \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k'^2t^2)}}, \tag{11.5}$$

donde $k'^2 = 1 - k^2$. Por consiguiente,

$$\frac{i\omega_1}{\omega_2} = \frac{\displaystyle\int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}}{\displaystyle\int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k'^2t^2)}}}. \tag{11.6}$$

Consideremos ahora una cúbica de ecuación $Y^2 = 4X^4 - g_2X - g_3$, donde el miembro derecho tiene tres raíces reales $e_3 < e_2 < e_1$. Equivalentemente, consideremos tres números reales $e_3 < e_2 < e_1$ tales que $e_1 + e_2 + e_3 = 0$ y definamos g_2 y g_3 mediante

$$4X^4 - g_2X - g_3 = 4(X - e_1)(X - e_2)(X - e_3).$$

Vamos a encontrar un retículo $R = \langle 2\omega_1, 2\omega_2\rangle_{\mathbb{Z}}$, con $\omega_1 > 0$, $\omega_2/i > 0$, cuyos invariantes sean los dados. Para ello definimos ω_1 por (11.2) y ω_2 por (11.3). Es fácil ver que las integrales convergen, y claramente $\omega_1 > 0$, $\omega_2/i > 0$. Así tenemos un retículo R que a su vez determina unos invariantes $\bar{g}_2$, $\bar{g}_3$, $\bar{e}_1$, $\bar{e}_2$, $\bar{e}_3$. Nuestro objetivo es probar que coinciden con g_2, g_3, e_1, e_2, e_3.

Veamos en primer lugar que existe un único número real $0 < k^2 < 1$ tal que, tomando $k'^2 = 1 - k^2$, se cumple (11.6). En efecto, notemos que cuando k^2 crece de 0 a 1, el numerador del miembro derecho de (11.6) crece de $\pi/2$ a $+\infty$, mientras que k'^2 decrece de 1 a 0 y el denominador decrece de $+\infty$ a $\pi/2$. Por consiguiente la fracción crece de 0 a $+\infty$ y, ciertamente, hay un único valor de k^2 para el que se cumple (11.6).

La relación (11.4) se cumple ahora para e_1, e_2 y $k^2 = (e_3 - e_2)/(e_1 - e_2)$ como para $\bar{e}_1$, $\bar{e}_2$ y $\bar{k}^2 = (\bar{e}_3 - \bar{e}_2)/(\bar{e}_1 - \bar{e}_2)$. Similarmente ocurre con (11.5), luego concluimos que tanto k^2 como $\bar{k}^2$ cumplen (11.6). Por la unicidad ha de ser $k^2 = \bar{k}^2$. Entonces (11.4) implica que $\sqrt{e_1 - e_2} = \sqrt{\bar{e}_1 - \bar{e}_2}$ o, más sencillamente, $e_1 - e_2 = \bar{e}_2 - \bar{e}_2$. A su vez, $k^2 = \bar{k}^2$ implica entonces que $e_3 - e_2 = \bar{e}_3 - \bar{e}_2$. Uniendo a esto que $e_1 + e_2 + e_3 = \bar{e}_1 + \bar{e}_2 + \bar{e}_3 = 0$, vemos que las dos ternas de invariantes satisfacen un mismo sistema de tres ecuaciones, luego son iguales. Esto implica que también $g_2 = \bar{g}_2$, $g_3 = \bar{g}_3$.

El teorema siguiente resume lo que hemos probado:

Teorema 11.16 *Si V es una curva elíptica de ecuación $Y^2 = 4X^3 - g_2X - g_3$, donde el polinomio de la derecha tiene tres raíces reales distintas, entonces V puede parametrizarse por las funciones de Weierstrass de un retículo complejo generado por un número real ω_1 y un número imaginario puro ω_2. Equivalentemente, el grupo de periodos de V respecto a la diferencial de primera clase dx/y es de esta forma.*

Este resultado se extiende fácilmente al caso en que V satisface una ecuación de la forma $Y^2 = a(X - e_1)(X - e_2)(X - e_3)$, con $a \neq 0$ y e_1, e_2, e_3 números reales distintos. Entonces, el cambio

$$X = \pm X' + \frac{e_1 + e_2 + e_3}{3}, \qquad Y = \frac{\sqrt{|a|}}{2}\,Y',$$

(donde el signo $\pm$ es el de a) determina una transformación proyectiva de P^2 en sí mismo que se restringe a un isomorfismo entre V y una curva V' en las condiciones del teorema. Es fácil ver así que la diferencial de primera clase dx/y de V tiene igualmente un periodo real y otro imaginario puro, el primero de los cuales puede obtenerse integrando sobre cualquiera de las dos ramas reales de V, etc.

Caso ω_1 y ω_2 conjugados Consideremos ahora un retículo R generado por periodos $2\omega_1 = a + bi$ y $2\omega_2 = a - bi$. No perdemos generalidad si suponemos a, $b > 0$. Como en el caso anterior, R es invariante por la conjugación, lo que se traduce en la relación $\overline{\wp(z)} = \wp(\bar{z})$. A su vez, esto implica que $\wp(z)$ es real cuando z es real o imaginario puro. Igualmente, $\wp'(z)$ es real cuando z es real e imaginario puro cuando z es imaginario puro. Los invariantes g_2 y g_3 también son reales. Lo que ya no es cierto es que las raíces e_1, e_2, e_3 sean reales. En efecto,

$$\bar{e}_1 = \overline{\wp(\omega_1)} = \wp(\bar{\omega}_1) = \wp(\omega_2) = e_2,$$

luego e_1 y e_2 son dos números imaginarios conjugados. Por el contrario, e_3 es real, ya que $\omega_3 = \omega_1 + \omega_2 = a$ lo es.

Modificaciones obvias en los razonamientos del caso anterior nos dan que $\wp'(x)$ es estrictamente creciente en $]0, 2\omega_3[$, mientras que $\wp(x)$ tiene un mínimo en ω_3. Así mismo llegamos a que

$$a = \omega_3 = \omega_1 + \omega_2 = \int_{e_3}^{+\infty} \frac{dx}{\sqrt{4x^3 - g_2x - g_3}}.$$

Si consideramos los periodos $2i\omega_1$ y $-2i\omega_2$, entonces ω_3, g_2, g_3 y e_3 pasan a ser $(\omega_1 - \omega_2)/i = b$, g_2, $-g_3$ y $-e_3$, y la igualdad anterior se convierte en

$$bi = \omega_1 - \omega_2 = i\int_{-e_3}^{+\infty} \frac{dx}{\sqrt{4x^3 - g_2x + g_3}} = i\int_{-\infty}^{e_3} \frac{dx}{\sqrt{-4x^3 + g_2x + g_3}}.$$

Recíprocamente, vamos a ver que, dada una ecuación $Y^2 = 4X^3 - g_2X - g_3$, donde el polinomio de la derecha tiene dos raíces complejas conjugadas e_1, e_2 y una raíz real e_3, el retículo R de periodos $2\omega_1 = a+bi$, $2\omega_2 = a-bi$ determinados por las dos integrales anteriores tiene como invariantes los valores dados, es decir, que sus funciones de Weierstrass parametrizan la curva determinada por la ecuación dada.

Como en el caso anterior, empezaremos por transformar las expresiones integrales de los semiperiodos. El cambio $x = e_3 + t^2$ nos da:

$$a = \int_0^{+\infty} \frac{dt}{\sqrt{(t^2 + e_3 - e_1)(t^2 + e_3 - e_2)}}$$

Hagamos $e_3 - e_1 = \rho e^{i\theta}$, $e_3 - e_2 = \rho e^{-i\theta}$, con $0 < \theta < \pi$, donde estamos suponiendo que $\operatorname{Im} e_1 < 0$. En caso contrario haríamos el cambio $e_3 - e_2 = \rho e^{i\theta}$.

$$a = \int_0^{+\infty} \frac{dt}{\sqrt{t^4 + 2\rho t^2 \cos\theta + \rho^2}} = \frac{1}{\sqrt{\rho}} \int_0^{+\infty} \frac{dt}{\sqrt{t^4 + 2t^2 \cos\theta + 1}}, \tag{11.7}$$

donde hemos hecho el cambio $t = \sqrt{\rho}\, t'$.

En la integral que nos da b cambiamos x por $-x$, con lo que tenemos

$$b = \int_{-e_3}^{+\infty} \frac{dx}{\sqrt{4(x + e_1)(x + e_2)(x + e_3)}},$$

Ahora hacemos $t = -e_2 + t^2$ y, similarmente al caso de a, llegamos a que

$$b = \frac{1}{\sqrt{\rho}} \int_0^{+\infty} \frac{dt}{\sqrt{t^4 - 2t^2 \cos\theta + 1}}.$$

Concluimos así que

$$\frac{a}{b} = \frac{\displaystyle\int_0^{+\infty} \frac{dt}{\sqrt{t^4 + 2t^2 \cos\theta + 1}}}{\displaystyle\int_0^{+\infty} \frac{dt}{\sqrt{t^4 - 2t^2 \cos\theta + 1}}}. \tag{11.8}$$

Cuando θ varía entre 0 y π, tenemos que $\cos\theta$ decrece de 1 a -1, con lo que el numerador del miembro derecho crece de $\pi/2$ a $+\infty$, mientras que el denominador decrece de $+\infty$ hasta $\pi/2$. Por consiguiente, la fracción crece de 0 a $+\infty$. Concluimos que, fijados a, $b > 0$, existe un único valor de θ para el que se cumple la igualdad.

Ahora ya podemos razonar exactamente como en el apartado anterior: fijados g_1 y g_2 (o, equivalentemente, e_1, e_2, e_3, definimos ω_1 y ω_2 mediante las expresiones integrales que hemos hallado. Estos semiperiodos determinan un retículo R con invariantes $\bar{g}_1$, $\bar{g}_2$, $\bar{e}_1$, $\bar{e}_2$, $\bar{e}_3$. La ecuación (11.8) se cumple tanto con θ como con $\bar{\theta}$, luego ha de ser $\theta = \bar{\theta}$. De la ecuación (11.7) obtenemos $\rho = \bar{\rho}$, con lo que $e_3 - e_1 = \bar{e}_3 - \bar{e}_1$, $e_3 - e_2 = \bar{e}_3 - \bar{e}_2$, lo cual, unido a que las tres raíces suman 0, nos permite concluir que $e_i = \bar{e}_i$ para $i = 1, 2, 3$. En resumen:

Teorema 11.17 *Si V es una curva elíptica de ecuación $Y^2 = 4X^3 - g_2X - g_3$, donde el polinomio de la derecha tiene una raíz real y dos complejas conjugadas, entonces V puede parametrizarse por las funciones de Weierstrass de un retículo complejo generado por dos números complejos conjugados. Equivalentemente, el grupo de periodos de V respecto a la diferencial de primera clase dx/y es de esta forma.*

Al igual que ocurría con el teorema 11.16, el resultado se extiende fácilmente al caso de una curva de ecuación $Y^2 = a(X - e_1)(X - e_2)(X - e_3)$, donde e_1 y e_2 son números complejos conjugados y e_3 es real.

11.3 Las funciones sigma y dseta

Otra forma de llegar a las funciones de Weierstrass consiste en partir de una función que tenga ceros simples en todos los puntos de un retículo dado R. La forma natural de hacerlo es mediante un producto infinito:

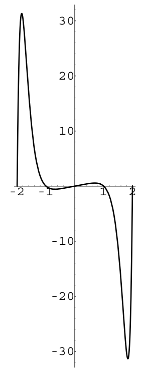
Definición 11.18 La *función sigma de Weierstrass* asociada a un retículo complejo R es la función $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ dada por

$$\sigma(z) = z \prod_{\omega \in R \setminus \{0\}} \left(1 - \tfrac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{z^2}{2\omega^2}}.$$

Según la teoría básica sobre productos infinitos, la convergencia de la serie

$$\sum_{\omega \in R \setminus \{0\}} \tfrac{1}{|\omega|^3}$$

(garantizada por el teorema 11.2) implica la convergencia absoluta y casi uniforme del producto en todo el plano complejo.



Así, la función σ es entera y tiene ceros simples en los puntos de R (y sólo en ellos). Se trata de una función impar, pues $-\omega$ recorre $R \setminus \{0\}$ cuando ω lo hace, y claramente

$$\lim_{z \to 0} \frac{\sigma(z)}{z} = 1.$$

Todos estos hechos determinan una cierta analogía entre las funciones $\sigma(z)$ y $\operatorname{sen} z$. La función sigma no puede ser elíptica sobre R, pues tendría orden 1. La figura muestra la función sigma del retículo $\langle 1, i \rangle_{\mathbb{Z}}$. Presenta oscilaciones cuya amplitud crece muy rápidamente.

Para relacionar la función sigma con las funciones elípticas introducimos la *función dseta de Weierstrass,* definida por

$$\zeta(z) = \frac{\sigma'(z)}{\sigma(z)}.$$

Se trata de una función impar meromorfa en $\mathbb{C}$ con polos simples en los puntos de R. La convergencia absoluta del producto que define la función sigma equivale a la convergencia absoluta y casi uniforme de la serie

$$\log \frac{\sigma(z)}{z} = \sum_{\omega \in R \setminus \{0\}} \left(\log\left(1 - \frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{z^2}{2\omega^2} \right),$$

la cual determina un logaritmo holomorfo de $\sigma(z)/z$ en un entorno de 0. El logaritmo que aparece en la serie es el que toma partes imaginarias en $]-\pi, \pi[$. Derivando queda

$$\frac{\sigma'(z)}{\sigma(z)} - \frac{1}{z} = \sum_{\omega \in R \setminus \{0\}} \left(\frac{-1/\omega}{1 - z/\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right),$$

luego

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \in R \setminus \{0\}} \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right).$$

En principio tenemos probada esta igualdad en un entorno de 0, pero por el principio de prolongación analítica se cumple en todo $\mathbb{C}$, dado que la serie converge uniformemente en todo compacto que no contenga puntos de R. En efecto, el término general es $z^2/(z-\omega)\omega^2$, y basta compararlo con $1/\omega^3$.

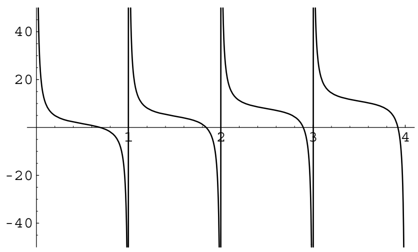
Vemos que ζ tiene residuo 1 en todos sus polos. Volviendo a derivar llegamos a que

$$\zeta'(z) = -\frac{1}{z^2} - \sum_{\omega \in R \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) = -\wp(z).$$

La periodicidad de $\wp$ implica ahora que si $\omega \in R$ la función $\zeta(z+\omega) - \zeta(z)$ tiene derivada nula, luego existe una constante $2\eta_\omega \in \mathbb{C}$ tal que

$$\zeta(z + \omega) = \zeta(z) + 2\eta_\omega.$$

Es inmediato comprobar que $\eta : R \longrightarrow \mathbb{C}$ es un homomorfismo de grupos.

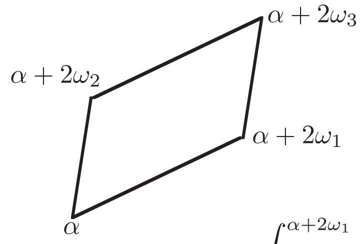


La figura muestra la función dseta del retículo $\langle 1, i \rangle_{\mathbb{Z}}$. Vemos cómo, en efecto, en cada “cuasiperiodo” se incrementa en una cierta cantidad.

Con la notación de Weierstrass, es decir, $R = \langle 2\omega_1, 2\omega_2 \rangle_{\mathbb{Z}}$, $\omega_3 = \omega_1 + \omega_2$, llamaremos $\eta_i = \eta_{2\omega_i}$. Más adelante necesitaremos la fórmula del teorema siguiente, conocida como *relación de Legendre.*

Teorema 11.19 *Sea $R = \langle 2\omega_1, 2\omega_2 \rangle$ un retículo complejo. Entonces*

$$\omega_2\eta_1 - \omega_1\eta_2 = \pm\frac{i\pi}{2}.$$



DEMOSTRACIÓN: Sea $\alpha = -\omega_1 - \omega_2$. Integramos la función ζ sobre la frontera del paralelogramo indicado en la figura. En su interior, la función ζ tiene un único polo en 0 con residuo 1, luego la integral vale $\pm 2\pi i$. Por otra parte,

$$\int_{\alpha}^{\alpha+2\omega_1} \zeta(\xi)\, d\xi + \int_{\alpha+2\omega_3}^{\alpha+2\omega_2} \zeta(\xi)\, d\xi$$

$$= \int_0^1 (\zeta(\alpha + t2\omega_1)2\omega_1 - \zeta(\alpha + 2\omega_2 + t2\omega_1)2\omega_1)\, dt$$

$$= \int_0^1 -2\eta_2 2\omega_1\, dt = -4\eta_2\omega_1;$$

$$\int_{\alpha+2\omega_1}^{\alpha+2\omega_3} \zeta(\xi)\, d\xi + \int_{\alpha+2\omega_2}^{\alpha} \zeta(\xi)\, d\xi$$

$$= \int_0^1 (\zeta(\alpha + 2\omega_1 + t2\omega_2)2\omega_2 - \zeta(\alpha + t2\omega_2)2\omega_2)\, dt$$

$$= \int_0^1 2\eta_1 2\omega_2\, dt = 4\eta_1\omega_2.$$

Por consiguiente, $4\eta_1\omega_2 - 4\eta_2\omega_1 = \pm 2\pi i$. ∎

En términos de la función sigma, la definición de η_ω es

$$\frac{\sigma'(z+\omega)}{\sigma(z+\omega)} - \frac{\sigma'(z)}{\sigma(z)} = 2\eta_\omega.$$

El miembro izquierdo es la derivada de la función $\log \frac{\sigma(z+\omega)}{\sigma(z)}$, luego existe $c_\omega \in \mathbb{C}$ tal que

$$\log \frac{\sigma(z+\omega)}{\sigma(z)} = 2\eta_\omega z + c_\omega,$$

luego

$$\sigma(z+\omega) = \sigma(z)e^{2\eta_\omega z + c_\omega}.$$

Podemos calcular la constante c_ω. Para ello aplicamos la relación anterior a $z = -\omega/2$ y usamos que σ es impar:

$$\sigma(\omega/2) = \sigma(-\omega/2)e^{-\omega\eta_\omega + c_\omega} = -\sigma(\omega/2)e^{-\omega\eta_\omega + c_\omega}.$$

Si suponemos que $\omega/2 \notin R$, llegamos a que $e^{c_\omega} = -e^{\omega\eta_\omega}$, luego

$$\sigma(z+\omega) = -\sigma(z)e^{\eta_\omega(2z+\omega)}.$$

En particular,[1]

$$\sigma(z+2\omega_i) = -\sigma(z)e^{2\eta_i(z+\omega_i)}. \tag{11.9}$$

Esto justifica el comportamiento observado en la gráfica de sigma. Ahora podemos probar un teorema de factorización de funciones elípticas, para lo cual nos apoyaremos en el teorema siguiente:

Teorema 11.20 *Sea f una función elíptica no constante sobre un retículo R y sean $z_1,\ldots,z_r$ los puntos de un paralelogramo fundamental P de R donde f tiene ceros o polos, de multiplicidades $m_1,\ldots,m_r$ respectivamente. Entonces*

$$\sum_{j=1}^{r} m_i z_i \in R.$$

DEMOSTRACIÓN: Teniendo en cuenta que los ceros y polos de f forman un conjunto discreto, es claro que podemos tomar $\zeta\in\mathbb{C}$ tal que el conjunto $\zeta+P$ no tiene ceros o polos de f en su frontera. Cada número complejo es congruente módulo R con un único punto de $\zeta+P$, por lo que los ceros y polos de f en P se corresponden biunívocamente con los ceros y polos de f en $\zeta+P$ con las mismas multiplicidades, y así no perdemos generalidad si suponemos que todos los z_j están en $\zeta+P$.

Ahora consideramos la función zf'/f, que claramente es holomorfa en un entorno de la clausura de P excepto en los puntos z_j, donde tiene polos simples con residuos $\operatorname{Res}_{z_j} f = m_i z_j$. El teorema de los residuos nos da que

$$\int_{\zeta+\partial P} \frac{\xi f'(\xi)}{f(\xi)}\,d\xi = 2\pi i\sum_{j=1}^{r} m_j z_j.$$

Por otra parte, evaluamos la integral en un par de lados opuestos del paralelogramo:

$$\int_{\zeta}^{\zeta+\omega_1} \frac{\xi f'(\xi)}{f(\xi)}\,d\xi + \int_{\zeta+\omega_1+\omega_2}^{\zeta+\omega_2} \frac{\xi f'(\xi)}{f(\xi)}\,d\xi$$

$$= \omega_1\int_0^1 \frac{(\zeta+t\omega_1)f'(\zeta+t\omega_1)}{f(\zeta+t\omega_1)}\,dt - \omega_1\int_0^1 \frac{(\zeta+\omega_2+t\omega_1)f'(\zeta+\omega_2+t\omega_1)}{f(\zeta+\omega_2+t\omega_1)}\,dt$$

$$= -\omega_1\omega_2\int_0^1 \frac{f'(\zeta+t\omega_1)}{f(\zeta+t\omega_1)}\,dt = -\omega_2\int_{\zeta}^{\zeta+\omega_1}\frac{f'(\xi)}{f(\xi)}\,d\xi.$$

Una primitiva del integrando (sobre un entorno del segmento) es una determinación holomorfa $\log f(z)$ del logaritmo de $f(z)$ (que existe porque f no se anula sobre el segmento). Por lo tanto la integral es la diferencia de dos logaritmos de $f(\zeta)=f(\zeta+\omega_1)$. En total obtenemos $-2k\pi i\omega_2$, para cierto $k\in\mathbb{Z}$. Lo mismo es válido para la integral sobre el otro par de lados del paralelogramo, luego

$$2\pi i\sum_{j=1}^{r} m_j z_j = 2\pi i(k_1\omega_1+k_2\omega_2),$$

de donde se sigue el teorema. ■

[1] A partir de esta relación es fácil concluir que σ es una función zeta, en el sentido de 4.37.

Teorema 11.21 *Sea f una función elíptica no nula sobre un retículo R y sean $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n$ los ceros y los polos de f en un paralelogramo fundamental de R (repetidos según su multiplicidad). Entonces existe una constante $c \in \mathbb{C}$ tal que*

$$f(z) = c\,\frac{\sigma(z-\alpha_1)\cdots\sigma(z-\alpha_n)}{\sigma(z-\beta_1)\cdots\sigma(z-\beta_n')},$$

donde $\beta_n' = (\alpha_1+\cdots+\alpha_n) - (\beta_1+\cdots+\beta_{n-1})$.

Demostración: Llamemos $\phi(z)$ al miembro derecho de la igualdad del enunciado (sin la constante c). Por el teorema anterior tenemos que $\beta_n' - \beta_n \in R$, por lo que $\phi(z)$ tiene los mismos ceros y polos que f y f/ϕ es una función holomorfa sin ceros ni polos en $\mathbb{C}$. Si probamos que ϕ es elíptica sobre R, entonces f/ϕ también lo será, y podremos concluir que es constante. Por simplificar la notación llamaremos β_n a β_n'. Si $\omega \in R$ tenemos que

$$\phi(z+\omega) = \phi(z)\exp\sum_i\big(\eta_\omega(2z-2\alpha_i+\omega) - \eta_\omega(2z-2\beta_i+\omega)\big)$$

$$= \phi(z)\exp\left(2\eta_\omega\sum_i(\beta_i-\alpha_i)\right) = \phi(z).$$

■

Un caso particular de interés es el siguiente:

Teorema 11.22 *Sea R un retículo complejo y $\alpha \in \mathbb{C}\setminus R$. Entonces*

$$\wp(z) - \wp(\alpha) = -\frac{\sigma(z+\alpha)\sigma(z-\alpha)}{\sigma^2(z)\sigma^2(\alpha)}.$$

Demostración: La función $\wp(z) - \wp(\alpha)$ tiene un polo doble en 0 y ceros en los puntos $-\alpha$ y α. Notemos que si α y $-\alpha$ son congruentes módulo R se trata del mismo cero, pero el carácter impar de $\wp'$ implica entonces que es un cero doble. La prueba del teorema anterior muestra entonces que la función

$$\phi(z) = \frac{\sigma(z+\alpha)\sigma(z-\alpha)}{\sigma^2(z)}$$

es elíptica sobre R y tiene los mismos ceros y polos de $\wp(z) - \wp(\alpha)$. Por consiguiente $\wp(z) - \wp(\alpha) = c\phi(z)$. Basta probar que $c = -1/\sigma^2(\alpha)$. En efecto,

$$z^2\wp(z) - z^2\wp(\alpha) = c\,\frac{\sigma(z+\alpha)\sigma(z-\alpha)}{\sigma^2(z)/z^2}$$

y, tomando el límite cuando $z \to 0$, queda $1 = c\sigma(\alpha)\sigma(-\alpha) = -c\sigma^2(\alpha)$. ■

En particular

$$\wp(z) - e_i = -\frac{\sigma(z+\omega_i)\sigma(z-\omega_i)}{\sigma^2(z)\sigma^2(\omega_i)}.$$

Ahora bien, $\sigma(z+\omega_i) = \sigma(z-\omega_i+2\omega_i) = -\sigma(z-\omega_i)e^{2\eta_i z}$, luego

$$\wp(z) - e_i = e^{-2\eta_i z}\frac{\sigma(z+\omega_i)^2}{\sigma^2(z)\sigma^2(\omega_i)}.$$

Esto nos permite definir

$$\sqrt{\wp(z) - e_i} = e^{-\eta_i z}\frac{\sigma(z+\omega_i)}{\sigma(z)\sigma(\omega_i)}.$$

Mejor aún, si llamamos

$$\sigma_i(z) = e^{-\eta_i z}\frac{\sigma(z+\omega_i)}{\sigma(\omega_i)},$$

tenemos funciones enteras con ceros simples en los puntos de $\omega_i + R$ y tales que

$$\sqrt{\wp(z) - e_i} = \frac{\sigma_i(z)}{\sigma(z)}. \tag{11.10}$$

La ecuación diferencial de $\wp$ nos da que

$$\wp'(z)^2 = 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3) = 4\,\frac{\sigma_1^2(z)\sigma_2^2(z)\sigma_3^2(z)}{\sigma^6(z)},$$

luego

$$\wp'(z) = \pm 2\,\frac{\sigma_1(z)\sigma_2(z)\sigma_3(z)}{\sigma^3(z)}.$$

Para calcular el signo multiplicamos por z^3 y tomamos límites cuando $z \to 0$. El miembro izquierdo tiende a -2 y el derecho a ± 2, luego el signo es negativo y llegamos a una factorización de $\wp'$:

$$\wp'(z) = -2\,\frac{\sigma_1(z)\sigma_2(z)\sigma_3(z)}{\sigma^3(z)}. \tag{11.11}$$

Conviene observar que las funciones σ_i son pares. En efecto,

$$\sigma_i(-z) = e^{\eta_i z}\frac{\sigma(-z+\omega_i)}{\sigma(\omega_i)} = e^{\eta_i z}\frac{-\sigma(z-\omega_i)}{\sigma(\omega_i)}$$

$$= e^{\eta_i z}\frac{\sigma(z+\omega_i)e^{-z\eta_i}}{\sigma(\omega_i)} = e^{-\eta_i z}\frac{\sigma(z+\omega_i)}{\sigma(\omega_i)} = \sigma_i(z).$$

11.4 Las funciones de Jacobi

Hasta ahora hemos introducido las funciones que definió Weierstrass en su estudio de las funciones elípticas. Jacobi desarrolló independientemente la teoría tomando como base otras funciones. Desde un punto de vista moderno, las funciones de Weierstrass son mucho más cómodas de manejar, pero conviene conocer también el enfoque de Jacobi. Introduciremos sus funciones elípticas a partir de las funciones σ_1, σ_2 y σ_3. Éstas no son elípticas, pero al sumar periodos obtenemos relaciones sencillas. Usando (11.9), vemos que

$$\sigma_i(z+2\omega_j) = e^{-\eta_i(z+2\omega_j)}\frac{\sigma(z+\omega_i+2\omega_j)}{\sigma(\omega_i)}$$

$$= -e^{-\eta_i(z+2\omega_j)+2\eta_j(z+\omega_i+\omega_j)}\frac{\sigma(z+\omega_i)}{\sigma(\omega_i)}$$

$$= -e^{-2\eta_i\omega_j+2\eta_j z+2\eta_j\omega_i+2\eta_j\omega_j}\sigma_i(z) = -e^{2\eta_j(z+\omega_j)+2\eta_j\omega_i-2\eta_i\omega_j}\sigma_i(z).$$

Si $i \neq j$ el teorema 11.19 nos da que $2\eta_j\alpha_i - 2\eta_i\alpha_j = \pm 2\pi i$, por lo que

$$\sigma_i(z+2\omega_j) = e^{2\eta_j(z+\omega_j)}\sigma_i(z).$$

Si $i = j$ queda

$$\sigma_i(z+2\omega_i) = -e^{2\eta_i(z+\omega_i)}\sigma_i(z).$$

Definición 11.23 Con la notación anterior, llamamos

$$\lambda(z) = \frac{\sigma(z)}{\sigma_2(z)}, \qquad \lambda_1(z) = \frac{\sigma_1(z)}{\sigma_2(z)}, \qquad \lambda_3(z) = \frac{\sigma_3(z)}{\sigma_2(z)}.$$

Tenemos así tres funciones meromorfas con polos simples en los puntos de $\omega_2 + R$. Todas ellas tienen ceros simples. Los de λ están en R, los de λ_1 en $\omega_1 + R$ y los de λ_3 en $\omega_3 + R$. Veamos que las tres son elípticas.

$$\lambda(z+2\omega_1) = -\frac{e^{2\eta_1(z+\omega_1)}\sigma(z)}{e^{2\eta_1(z+\omega_1)}\sigma_2(z)} = -\lambda(z),$$

$$\lambda(z+2\omega_2) = -\frac{e^{2\eta_2(z+\omega_2)}\sigma(z)}{e^{2\eta_2(z+\omega_2)}\sigma_2(z)} = \lambda(z).$$

Esto prueba que λ es elíptica sobre $\langle 4\omega_1, 2\omega_2\rangle_{\mathbb{Z}}$. Similarmente se comprueba que

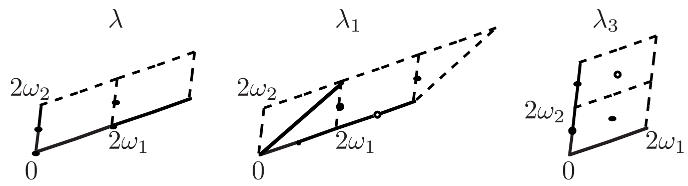
$$\lambda_1(z+2\omega_1) = -\lambda_1(z), \qquad \lambda_1(z+2\omega_2) = -\lambda_1(z),$$

$$\lambda_3(z+2\omega_1) = \lambda_3(z), \qquad \lambda_3(z+2\omega_2) = -\lambda_3(z),$$

de donde concluimos que λ_1 es elíptica sobre el retículo $\langle 4\omega_1, 2\omega_3\rangle_{\mathbb{Z}}$ y λ_3 es elíptica sobre $\langle 2\omega_1, 4\omega_2\rangle_{\mathbb{Z}}$.

Conviene observar que λ^2, λ_1^2 y λ_3^2 son elípticas sobre el retículo original $\langle 2\omega_1, 2\omega_2\rangle_{\mathbb{Z}}$.

La figura muestra los paralelogramos fundamentales de las tres funciones junto con sus ceros (círculos blancos) y sus polos (círculos negros).



Además λ es impar, mientras que λ_1 y λ_3 son pares. Se comprueba inmediatamente que $\lambda(0) = 0$, $\lambda_1(0) = \lambda_3(0) = 1$.

Estas funciones son las funciones elípticas de Jacobi salvo un cambio de variable. Para adecuarnos a su notación, hemos de tener presente que Jacobi representaba a los periodos en la forma $2K$ y $2K'i$. Teniendo en cuenta (11.10) podemos definir

$$\sqrt{e_1 - e_2} = \frac{\sigma_2(\omega_1)}{\sigma(\omega_1)}.$$

Llamamos

$$K = \omega_1\sqrt{e_1 - e_2}, \qquad K'i = \omega_2\sqrt{e_1 - e_2}.$$

Las *funciones elípticas de Jacobi* son las funciones

$$\operatorname{sn} u = \sqrt{e_1 - e_2}\ \lambda\left(\frac{u}{\sqrt{e_1 - e_2}}\right),$$

$$\operatorname{cn} u = \lambda_1\left(\frac{u}{\sqrt{e_1 - e_2}}\right), \quad \operatorname{dn} u = \lambda_3\left(\frac{u}{\sqrt{e_1 - e_2}}\right).$$

Ciertamente, las tres son elípticas de orden 2 con ceros y polos simples. Veamos sus propiedades. Las primeras son meras reformulaciones de las propiedades correspondientes de λ, λ_1 y λ_3.

Periodos Tenemos las relaciones

$$\begin{aligned} \operatorname{sn}(u + 2K) &= -\operatorname{sn} u, & \operatorname{sn}(u + 2K'i) &= \operatorname{sn} u, \\ \operatorname{cn}(u + 2K) &= -\operatorname{cn} u, & \operatorname{cn}(u + 2K'i) &= -\operatorname{cn} u, \\ \operatorname{dn}(u + 2K) &= \operatorname{dn} u, & \operatorname{dn}(u + 2K'i) &= -\operatorname{dn} u. \end{aligned}$$

Por lo tanto la función $\operatorname{sn} u$ es elíptica sobre $\langle 4K, 2K'i\rangle_{\mathbb{Z}}$, mientras que $\operatorname{cn} u$ es elíptica sobre $\langle 4K, 2K + 2K'i\rangle_{\mathbb{Z}}$ (que es un retículo mayor que el obvio $\langle 4K, 4K'i\rangle_{\mathbb{Z}}$) y $\operatorname{dn} u$ es elíptica sobre $\langle 2K, 4K'i\rangle_{\mathbb{Z}}$. Las funciones $\operatorname{sn}^2 u$, $\operatorname{cn}^2 u$ y $\operatorname{dn}^2 u$ son elípticas sobre $\langle 2K, 2K'i\rangle_{\mathbb{Z}}$.

Paridad La función $\operatorname{sn} u$ es impar, y las otras dos son pares:

$$\operatorname{sn}(-u) = -\operatorname{sn} u, \qquad \operatorname{cn}(-u) = \operatorname{cn} u, \qquad \operatorname{dn}(-u) = \operatorname{dn} u.$$

Valores en 0 Se cumple

$$\operatorname{sn} 0 = 0, \qquad \operatorname{cn} 0 = 1, \qquad \operatorname{dn} 0 = 1.$$

Ceros y polos Las tres funciones tienen los mismos polos, todos ellos simples y situados en los puntos $2mK + (2n+1)K'i$. Los ceros también son simples:

Ceros de $\operatorname{sn} u$: $2mK + 2niK'$,

Ceros de $\operatorname{cn} u$: $(2m+1)K + 2niK'$,

Ceros de $\operatorname{dn} u$: $(2m+1)K + (2n+1)iK'$.

Relaciones Las funciones de Jacobi satisfacen muchas relaciones. Por ejemplo, de la ecuación (11.10) se sigue que

$$\operatorname{sn} u = \frac{\sqrt{e_1 - e_2}}{\sqrt{\wp(z) - e_2}}, \quad \operatorname{cn} u = \frac{\sqrt{\wp(z) - e_1}}{\sqrt{\wp(z) - e_2}}, \quad \operatorname{dn} u = \frac{\sqrt{\wp(z) - e_3}}{\sqrt{\wp(z) - e_2}}, \qquad (11.12)$$

donde $z = u/\sqrt{e_1 - e_2}$. De aquí a su vez obtenemos:

$$\operatorname{sn}^2 u + \operatorname{cn}^2 u = 1, \qquad k^2 \operatorname{sn}^2 u + \operatorname{dn}^2 u = 1, \qquad (11.13)$$

donde

$$k = \sqrt{\frac{e_3 - e_2}{e_1 - e_2}} = \frac{\sigma_2(\omega_3)\sigma(\omega_1)}{\sigma_2(\omega_1)\sigma(\omega_3)}$$

se llama *módulo* de las funciones de Jacobi.

Derivadas De (11.12) se sigue que

$$\wp(z) = e_2 + \frac{e_1 - e_2}{\operatorname{sn}^2 u},$$

luego

$$\wp'(z) = -\frac{2(e_1 - e_3)^{3/2}(\operatorname{sn} u)'}{\operatorname{sn}^3 u}.$$

Por otra parte, de (11.11) obtenemos

$$\wp'(z) = -2\,\frac{\sigma_1(z)\sigma_2(z)\sigma_3(z)}{\sigma^3(z)} = -2\,\frac{\sigma_1(z)}{\sigma_2(z)}\frac{\sigma_3(z)}{\sigma_2(z)}\left(\frac{\sigma(z)}{\sigma_2(z)}\right)^{-3}$$

$$= -2 \operatorname{cn} u \operatorname{dn} u\, \frac{(e_1 - e_2)^{3/2}}{\operatorname{sn}^3 u}.$$

Comparando las dos expresiones concluimos que

$$(\operatorname{sn} u)' = \operatorname{cn} u \operatorname{dn} u.$$

Derivando en (11.13) y usando la igualdad anterior obtenemos

$$(\operatorname{cn} u)' = -\operatorname{sn} u \operatorname{dn} u, \qquad (\operatorname{dn} u)' = -k^2 \operatorname{sn} u \operatorname{dn} u.$$

A partir de aquí podemos calcular las series de Taylor en 0 de las tres funciones sn, cn y dn en términos de k^2 únicamente, luego vemos que sólo dependen de k^2.

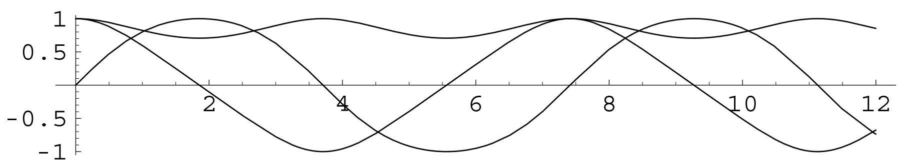
Caso en que ω_1 es real y ω_2 imaginario puro Suponemos sin pérdida de generalidad que ω_1 y ω_2/i son positivos. Entonces $e_2 < e_3 < e_1$ son números reales. Puede probarse que $\sqrt{e_1 - e_2} > 0$, pero podemos suponerlo, pues la definición de las funciones sn, cn y dn no depende de la elección del signo de esta raíz. Así tenemos que K y K' son números reales positivos. Así mismo,

$$0 < k^2 = \frac{e_3 - e_2}{e_1 - e_2} < 1,$$

y podemos tomar $k > 0$ porque las funciones sólo dependen de k^2. Es fácil ver que eligiendo adecuadamente ω_1 y ω_2 podemos conseguir que k tome cualquier valor entre 0 y 1.

Es claro que las series de Taylor en 0 de las tres funciones de Jacobi tienen coeficientes reales, luego, al menos en un entorno de 0, toman valores reales sobre argumentos reales. Ahora bien, no puede haber un $x \in \mathbb{R}$ donde la parte imaginaria deje de ser 0, pues la serie de Taylor calculada en un punto cercano tendría sus coeficientes reales y convergería en x. Concluimos que las tres funciones $\operatorname{sn} x$, $\operatorname{cn} x$ y $\operatorname{dn} x$ toman valores reales en todo $\mathbb{R}$. Las funciones $\operatorname{sn} x$ y $\operatorname{cn} x$ tienen periodo $4K$, mientras que $\operatorname{dn} x$ tiene periodo $2K$.

Las relaciones (11.13) implican que las funciones $\operatorname{sn} x$ y $\operatorname{cn} x$ toman valores entre -1 y 1, mientras que $\operatorname{dn} x$ oscila entre $1 - k^2$ y 1. Los datos que tenemos sobre las derivadas permiten justificar en general las características de la gráfica siguiente, donde se muestran las funciones $\operatorname{sn} x$ y $\operatorname{cn} x$ para $k^2 = 1/2$:



La función $x = \operatorname{sn} t$ es biyectiva en $[0, K]$, luego podemos usarla como cambio de variable en la integral

$$\int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} = \int_0^K \frac{\operatorname{sn} t \operatorname{dn} t\, dt}{\sqrt{(1-\operatorname{sn}^2 t)(1-k^2\operatorname{dn}^2 t)}} = \int_0^K dt = K.$$

Para calcular K' recordamos que el retículo asociado a los semiperiodos $\bar{\omega}_1 = -i\omega_2$, $\bar{\omega}_2 = i\omega_1$ tiene raíces $\bar{e}_1 = -e_2$, $\bar{e}_2 = -e_1$ y $\bar{e}_3 = -e_3$, luego los valores $\bar{K}$ y $\bar{K}'$ para sus funciones de Jacobi resultan ser $\bar{K} = K'$ y $\bar{K}' = K$. El módulo resulta ser

$$\bar{k}^2 = \frac{\bar{e}_3 - \bar{e}_2}{\bar{e}_1 - \bar{e}_2} = \frac{e_1 - e_3}{e_1 - e_2} = 1 - k^2.$$

La notación usual es $k^2 + k'^2 = 1$, y a k' se le llama *módulo complementario* de las funciones de Jacobi (asociadas a ω_1 y ω_2). Aplicando el cálculo anterior a las funciones asociadas a $\bar{\omega}_1$ y $\bar{\omega}_2$ obtenemos que

$$K' = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k'^2x^2)}}.$$

Con esto hemos probado:

Teorema 11.24 *Los valores K e iK' asociados a las funciones de Jacobi de módulo k vienen dados por*

$$K = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} \qquad K' = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k'^2x^2)}},$$

donde k' es el módulo complementario, dado por $k^2 + k'^2 = 1$.

Se suele representar por $K(m)$ la función

$$K(m) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-mx^2)}}, \qquad 0 \leq m < 1,$$

que nos da los periodos de las funciones de Jacobi de parámetro $m = k^2$.

Apéndice A

Divisores en variedades regulares

En este apéndice demostraremos unos resultados adicionales sobre curvas elípticas que requieren más geometría algebraica de la que hemos visto hasta aquí. Concretamente, requieren generalizar la teoría de divisores a variedades regulares de dimensión arbitraria. Sabemos que el grupo de divisores de una curva proyectiva regular es el $\mathbb{Z}$-módulo libre generado por sus puntos. En el caso de una variedad arbitraria, hemos de sustituir los puntos por las subvariedades de codimensión 1 (que en el caso de una curva coinciden con los puntos). Empezaremos, pues, estudiando estas subvariedades.

A.1 Subvariedades de codimensión 1

En esta sección demostraremos una generalización del teorema 3.16 al caso de subvariedades de codimensión 1 en una variedad regular V que no sea necesariamente A^n o P^n. Para ello conviene generalizar como sigue las correspondencias entre conjuntos algebraicos e ideales:

Definición A.1 Sea W una variedad afín sobre un cuerpo de constantes k y sea $S \subset k[W]$. Definimos

$$V_W(S) = \{P \in W \mid f(P) = 0 \text{ para todo } f \in S\}.$$

Así mismo, si $C \subset S$, definimos el ideal

$$I_W(C) = \{f \in k[W] \mid f(P) = 0 \text{ para todo } P \in C\} \subset k[W].$$

Estos conceptos generalizan obviamente a los que introdujimos en el capítulo II para $W = A^n$. Es fácil ver que las propiedades básicas en torno a ellos se generalizan igualmente. Por ejemplo, si $S \subset k[W]$, entonces $V_W(S)$ es un

subconjunto algebraico de W. Para probarlo fijamos un sistema de referencia y tomamos
$$S' = \{F \in k[X_1, \ldots, X_n] \mid [F] \in S\}.$$

Podemos suponer que $0 \in S$, con lo que $I(W) \subset S'$. Claramente
$$V_W(S) = V(S').$$

Por otra parte, si $I \subset k[W]$ es un ideal, tenemos que
$$I_W(V_W(I)) = \operatorname{rad} I.$$

En efecto, como en el argumento anterior, llamamos
$$I' = \{F \in k[X_1, \ldots, X_n] \mid [F] \in I\},$$
que es un ideal del anillo de polinomios, y entonces
$$I_W(V_W(I)) = I_W(V(I')).$$

Si $f = [F] \in I_W(V_W(I))$, tenemos que $F \in I(V(I')) = \operatorname{rad} I'$, luego $F^r \in I'$ para cierto natural r, luego $f^r \in I$, luego $f \in \operatorname{rad} I$. El recíproco es obvio.

También es claro que un conjunto algebraico $C \subset W$ es irreducible si y sólo si el ideal $I_W(C)$ es primo.

En estos términos podemos reformular los teoremas 3.18 y 3.19, según los cuales, si W es una variedad afín y $f \in k[W]$ es una función regular no nula, entonces $V_W(f)$ es el conjunto vacío o bien un conjunto algebraico formado por variedades de codimensión 1.

Definición A.2 Sea V una variedad cuasiproyectiva sobre un cuerpo k y sea $P \in V$. Sea W una subvariedad (cerrada) de V de codimensión 1 tal que $P \in W$. Diremos que una función $\pi \in \mathcal{O}_P(V)$ es una *ecuación local* de W en un entorno de P si existe un entorno afín U de P en V tal que $\pi \in k[U]$ y $I_U(W \cap U) = (\pi)$ (y, por lo tanto, $W \cap U = V_U(\pi)$).

El resultado principal que queremos demostrar es que toda subvariedad de dimensión 1 admite una ecuación local en un entorno de cada uno de sus puntos regulares en V. En primer lugar daremos una caracterización de las ecuaciones locales.

En las condiciones de la definición anterior, llamamos $\mathfrak{m}_P(V/W)$ al ideal de $\mathcal{O}_P(V)$ formado por las funciones que se anulan en un entorno de P en W.

Observemos que $\mathfrak{m}_P(V/W)$ es un ideal primo, pues si $fg \in \mathfrak{m}_P(V/W)$, podemos tomar un entorno U de P tal que $f, g \in k[U]$ y fg se anule en $W_0 = W \cap U$, es decir, $fg \in I_U(W_0)$, que es un ideal primo de $k[U]$, luego uno de los dos factores está en $I_U(W_0) \subset \mathfrak{m}_P(V/W)$.

Si V es una curva y W es un punto $P \in V$, entonces $\mathfrak{m}_P(V/W) = \mathfrak{m}_P$.

Teorema A.3 *Sea V una variedad cuasiproyectiva, $P \in V$ y W una subvariedad de codimensión 1 tal que $P \in W$. Una función $\pi \in \mathcal{O}_P(V)$ es una ecuación local de W en un entorno de P si y sólo si $\mathfrak{m}_P(V/W) = (\pi)$.*

DEMOSTRACIÓN: Si π es una ecuación local de W en un entorno (afín) U de P, entonces $I_U(W \cap U) = (\pi)$. Si $u/v \in \mathfrak{m}_P(V/W)$, donde u, $v \in k[U]$, $v(P) \neq 0$, tenemos que u es regular en $W \cap U$ y se anula en un abierto (denso) de esta variedad, luego u se anula en todo $W \cap U$. Por lo tanto $u \in I_U(W \cap U)$, luego $u = f\pi$, con $f \in k[U]$, luego $u/v = (f/v)\pi$, con $f/v \in \mathcal{O}_P(V)$.

Supongamos ahora que $\mathfrak{m}_P(V/W) = (\pi)$. Sea U_0 un entorno afín de P en V tal que $\pi \in k[U_0]$ y se anule en $W \cap U_0$. Como el anillo $k[U_0]$ es noetheriano, tenemos que $I_{U_0}(W \cap U_0) = (f_1, \ldots, f_r)$, para ciertas funciones $f_i \in \mathfrak{m}_P(V/W)$. Por consiguiente $f_i = g_i\pi$, para ciertas funciones $g_i \in \mathcal{O}_P(V)$.

Las funciones g_i son regulares en un entorno de P, que por 2.39 podemos tomar principal, es decir, de la forma $U = U_0 \setminus V_{U_0}(g)$, con $g \in k[U_0]$. Según el teorema 2.38 se cumple que $k[U] = k[U_0][1/g]$.

Llamemos $W_0 = W \cap U$. Si demostramos que $I_U(W_0) = (f_1, \ldots, f_r)$, tendremos, de hecho, que $(\pi) \subset I_U(W_0) \subset (\pi)$, y el teorema estará probado.

Una inclusión es obvia. Si $v \in I_U(W_0)$, entonces $v = u/g^r$, con $u \in k[U_0]$. La función u se anula en W_0, que es un abierto (denso) en $W \cap U_0$, luego $u \in I_{U_0}(W \cap U_0)$ y $1/g^r \in k[U]$, de donde concluimos que $v \in (f_1, \ldots, f_r)_{k[U]}$. ■

De la prueba del teorema anterior se desprende lo siguiente:

Si π, $\pi' \in \mathcal{O}_P(V)$ son dos ecuaciones locales de W en respectivos entornos U_1 y U_2 de P, entonces existe otro entorno afín $U \subset U_1 \cap U_2$ donde ambas funciones son ecuaciones locales de W.

En efecto, ambas funciones están en $\mathfrak{m}_P(V/W)$, y en la prueba del teorema anterior, el abierto U en el cual π es una ecuación local de W se construye en dos partes: primero se toma un abierto U_0, que puede ser cualquiera suficientemente pequeño (luego podemos tomar el mismo para π y π'), y luego se toma U como un abierto principal en U_0, y también sirve cualquiera suficientemente pequeño, luego también podemos tomar el mismo para π y π'. ■

Otro hecho que se desprende de la prueba de A.3 es que si π es una ecuación local en un entorno de un punto P, entonces dicho entorno puede tomarse arbitrariamente pequeño.

Por último observamos que, para el caso de una curva V, el teorema A.3 afirma que las ecuaciones locales de un punto regular P son simplemente los parámetros locales en P.

Tenemos que las ecuaciones locales de las subvariedades de codimensión 1 que pasan por un punto P son primos en $\mathcal{O}_P(V)$. Recíprocamente, ahora probamos que cada primo de $\mathcal{O}_P(V)$ es la ecuación local de una única subvariedad:

Teorema A.4 *Sea V una variedad cuasiproyectiva, $P \in V$ y π un primo en $\mathcal{O}_P(V)$. Entonces existe una única subvariedad W de codimensión 1 en V tal que $P \in W$ y $(\pi) = \mathfrak{m}_P(V/W)$.*

DEMOSTRACIÓN: Veamos la unicidad: si $\mathfrak{m}_P(V/W) = \mathfrak{m}_P(V/W')$, sea U un entorno de P en V. Si $f \in k[U]$ se anula en $W \cap U$, entonces $f \in \mathfrak{m}_P(V/W)$, luego f se anula en un entorno de P en W', pero por regularidad se anula en $W \cap U'$. Así pues, $I_U(W \cap U) = I_U(W' \cap U)$, luego $W \cap U = W' \cap U$, luego $W = W'$.

Para probar la existencia tomamos un entorno afín U de P tal que $\pi \in k[U]$. El conjunto $V_U(\pi)$ es una unión de subvariedades de U de codimensión 1. Sea W_0 una que contenga a P. Llamemos W' a la unión de las restantes y vamos a probar que $P \notin W'$.

En caso contrario P pertenece a otra variedad $W_1 \subset V_U(\pi)$. Como W_0 y W_1 tienen la misma dimensión, ninguna puede estar contenida en la otra, luego existen funciones h_0, $h_1 \in k[U]$ tales que h_0 es idénticamente nula en W_0 y no en W_1, mientras que h_1 es idénticamente nula en W' y no en W_0. Entonces $h_0h_1 \in I_U(V_U(\pi)) = \operatorname{rad}(\pi)$, luego existe un $r \geq 0$ tal que $(h_0h_1)^r \in (\pi)$, luego $f \mid (h_0h_1)^r$ en $k[U]$ y, por consiguiente, en $\mathcal{O}_P(V)$. Como π es primo en este anillo, divide a un h_i, es decir, $h_i = f\pi$, con $f \in \mathcal{O}_P(V)$. Como f es regular en un entorno de P, concluimos que h_i se anula en un entorno de P en $V_U(\pi)$, luego se anula en W_0 y en W_1, en contradicción con la construcción de las funciones.

Tenemos, pues, que $P \notin W'$, luego restringiendo U a un entorno afín menor, podemos suponer que $V_U(f) = W_0$. Sea W la clausura en V de W_0. Vamos a ver que $\mathfrak{m}_P(V/W) = (\pi)$.

Una inclusión es obvia. Si $u/v \in \mathfrak{m}_P(V/W)$, con u, $v \in k[U]$, $v(P) \neq 0$, tenemos que u se anula en un entorno de P en W_0, pero por regularidad se anula en todo W_0, luego $u \in I_U(V_U(\pi)) = \operatorname{rad}(\pi)$, luego $\pi \mid u^r$ en $k[U]$, luego también en $\mathcal{O}_P(V)$, pero π es primo en este anillo, luego $\pi \mid u$ en $\mathcal{O}_P(V)$, con lo que $u/v \in (\pi)_{\mathcal{O}_P(V)}$. ■

Para terminar de perfilar la correspondencia entre subvariedades de codimensión 1 que pasan por P y los primos de $\mathcal{O}_P(V)$ nos falta demostrar que toda subvariedad tiene una ecuación local. Para ello necesitamos que el punto P sea regular:

Teorema A.5 *Sea V una variedad cuasiproyectiva, sea $P \in V$ un punto regular y sea $W \subset V$ una subvariedad de codimensión 1 tal que $P \in W$. Entonces W admite una ecuación local en un entorno de P.*

DEMOSTRACIÓN: El hecho de que W tenga codimensión 1 en V implica en particular que $I(V) \subsetneq I(W)$, luego podemos tomar una función $f \in I_V(W)$ no nula. En particular $f \in \mathcal{O}_P(V)$ y no es una unidad porque $f(P) = 0$. Según el teorema 3.42 tenemos que $\mathcal{O}_P(V)$ es un dominio de factorización única, luego podemos descomponer f en factores primos $f = \pi_1 \cdots \pi_r$.

Sea U un entorno afín de P donde todos los π_i sean regulares. Los conjuntos $V_{W\cap U}(\pi_i)$ son algebraicos y cubren $W \cap U$, luego por la irreducibilidad de W

ha de ser $W \cap U \subset V_{W\cap U}(\pi_i)$ para algún i, es decir, alguno de los factores π_i se anula sobre todo $W \cap U$. Llamemos $\pi \in k[U]$ a este primo, de modo que $\pi \in \mathfrak{m}_P(V/W)$.

Por el teorema anterior, existe una subvariedad W' de codimensión 1 en V tal que $\mathfrak{m}_P(V/W') = (\pi) \subset \mathfrak{m}_P(V/W)$. De aquí se sigue fácilmente la inclusión $I_U(W' \cap U) \subset I_U(W \cap U)$, luego $W \cap U \subset W' \cap U$ y, como ambas variedades tienen la misma dimensión, se da la igualdad, luego $W' = W$ y π es una ecuación local de W. ■

A.2 Divisores

Introducimos ahora la noción de divisor de una variedad cuasiproyectiva regular de dimensión arbitraria, que generalizará a la que ya tenemos definida para curvas proyectivas regulares. Empezamos por los divisores primos.

Definición A.6 Un *divisor primo* de una variedad cuasiproyectiva regular V es cualquier subvariedad (cerrada) W de codimensión 1 en V.

En particular, si V es una curva, sus divisores primos son sus puntos. Ahora vamos a definir la multiplicidad de un divisor primo en una función racional. La definición se basa en el teorema siguiente:

Teorema A.7 *Sea V una variedad cuasiproyectiva regular, sea W un divisor primo de V y $P \in W$. Sea $\mathfrak{m}_P(V/W) = (\pi)$ y sea U un entorno afín de P donde $I_U(W \cap U) = (\pi)$. Para cada función $f \in k[U]$ no nula y cada natural $r \geq 0$, se cumple que $\pi^r \mid f$ en $\mathcal{O}_P(V)$ si y sólo si $\pi^r \mid f$ en $k[U]$.*

DEMOSTRACIÓN: Una implicación es evidente. Supongamos que $\pi^r \mid f$ en $\mathcal{O}_P(V)$, de modo que $f = \alpha\pi^r$, para cierta función $\alpha \in \mathcal{O}_P(V)$. Podemos tomar un entorno afín U' de P tal que $\alpha \in k[U']$, $U' \subset U$ y π sea una ecuación local de W en U', es decir, $I_{U'}(W \cap U') = (\pi)$.

Si $\pi^r \nmid f$ en $k[U]$, sea $0 \leq s < r$ el máximo natural tal que $\pi^s \mid f$ en $k[U]$. Digamos que $f = \beta\pi^s$, con $\beta \in k[U]$. Entonces $\beta = \alpha\pi^{r-s}$, luego β se anula en $W \cap U'$. Por regularidad se anula en $W \cap U$, luego $\beta \in I_U(W \cap U) = (\pi)$ y $\pi \mid \beta$ en $k[U]$, contradicción. ■

Si P es un punto de una variedad regular V, sabemos que $\mathcal{O}_P(V)$ es un dominio de factorización única, y cada primo $\pi \in \mathcal{O}_P(V)$ induce una valoración v_π en $k(V)$: para cada función $f \in \mathcal{O}_P(V)$ definimos $v_\pi(f)$ como el exponente de π en la descomposición de f en factores primos y para cada $f/g \in k(V)$ (con $f, g \in \mathcal{O}_P(V)$), definimos $v_\pi(f/g) = v_\pi(f) - v_\pi(g)$.

El teorema anterior implica que si W es un divisor primo de V, $P \in W$ y $\mathfrak{m}_P(V/W) = (\pi)$, entonces la valoración v_W^P inducida por π en $k(V)$ no depende de P. En efecto, si $P' \in W$ y $\mathfrak{m}_{P'}(V/W') = (\pi')$ tomamos entornos afines U y U' de P y P' respectivamente, de modo que $I_U(W \cap U) = (\pi)$, $I_{U'}(W \cap U') = (\pi')$, luego tomamos un punto $P'' \in W \cap U \cap U'$.

Entonces $\mathfrak{m}_{P''}(V/W) = (\pi) = (\pi')$ por el teorema A.3 y, por la observación posterior, podemos tomar un entorno afín U'' de P'' donde π y π' son ecuaciones locales de W.

Tomemos $f \in k(V)$ y expresémosla como $f = s/t$, con $s,\ t \in k[U]$. Por el teorema anterior, $v_W^P(s)$ es el máximo r tal que $\pi^r \mid s$ en $\mathcal{O}_P(V)$, o también en $k[U]$, o también en $\mathcal{O}_{P''}(V)$, y éste es $v_W^{P''}(s)$. Lo mismo vale para t, luego $v_W^P(f) = v_W^{P''}(f)$. Igualmente concluimos que $v_W^{P'}(f) = v_W^{P''}(f)$ y, en definitiva, $v_W^P = v_W^{P'}$. Esto justifica la definición siguiente:

Definición A.8 Si W es un divisor primo en una variedad cuasiproyectiva regular V, $P \in W$ y $\mathfrak{m}_P(V/W) = (\pi)$, definimos v_W como la valoración en $k(V)$ inducida por π, de modo que si $f \in \mathcal{O}_P(V)$ entonces $v_W(f)$ es el exponente de π en la descomposición de f en factores primos.

Hemos demostrado que v_W no depende del punto P con el que se calcula. Más aún, el teorema A.7 afirma que si π es una ecuación local de W en un abierto afín U y $f \in k[U]$, entonces $v_W(f)$ es el mayor natural r tal que $\pi^r \mid f$ en $k[U]$.

Si $f \in k(V)$ y $v_W(f) = r > 0$, diremos que f tiene un *cero* de orden r *a lo largo de* W, mientras que si $v_W(f) = -r < 0$ diremos que f tiene un *polo* de orden r *a lo largo de* W.

Notemos que si V es una curva regular y W es un punto $P \in V$, entonces π es un parámetro local de V en P y $v_P(f)$ es el orden de f en P que ya teníamos definido. En particular, las nociones de ceros y polos que acabamos de introducir extienden a las que ya teníamos para curvas.

El teorema siguiente muestra que la definición que hemos dado de cero y polo es razonable:

Teorema A.9 *Sea f una función racional en una variedad regular V*

a) Si f tiene un cero a lo largo de un divisor primo W, entonces f se anula en un abierto de W.

b) Si f tiene un polo a lo largo de un divisor primo W entonces f es singular en todos los puntos de W.

c) Si f se anula en un punto $P \in V$, entonces f tiene un cero W que pasa por P.

d) Si f es singular en un punto $P \in V$, entonces f tiene un polo W que pasa por P.

Demostración: Si f tiene un cero a lo largo de W, sea U un abierto afín donde W tenga una ecuación local π. Expresemos $f = s/t$, con $s,\ t \in k[U]$. Entonces $s = \alpha\pi^r$, $t = \beta\pi^s$ para ciertos $\alpha,\ \beta \in k[U]$, $v_W(\alpha) = v_W(\beta) = 0$ y $v_W(f) = r - s > 0$. Entonces $f = (\alpha/\beta)\pi^{r-s}$ y el hecho de que $v_W(\beta) = 0$

significa que $\beta \notin (\pi) = I_U(W \cap U)$, es decir, que β no se anula en un abierto de $W \cap U$, luego α/β es regular en un abierto de W en el cual se anula f.

Si f tiene un polo a lo largo de W entonces $g = 1/f$ tiene un cero a lo largo de W, luego se anula en un abierto de W en el cual $f = 1/g$ ha de ser singular. Ahora bien, si f fuera regular en algún punto de W, lo sería en todos los puntos de un abierto, lo cual es imposible. Por lo tanto, f es singular en todos los puntos de W.

Si f se anula en un punto $P \in V$ entonces $f \in \mathcal{O}_P(V)$ y no es una unidad, luego es divisible entre un primo π. Por el teorema A.4 existe un divisor primo W tal que $P \in W$ y $\mathfrak{m}_P(V/W) = (\pi)$. Entonces $v_W(f) > 0$ y, por lo tanto, W es un cero de f.

Si f es singular en un punto $P \in V$, entonces $f = g/h$, con g, $h \in \mathcal{O}_P(V)$, pero $g/h \notin \mathcal{O}_P(V)$. Podemos exigir que g y h no tengan factores comunes. Sea π un primo en $\mathcal{O}_P(V)$ tal que $\pi \mid h$, $\pi \nmid g$. Por el teorema A.4 existe un divisor primo W de V tal que $P \in W$ y $\mathfrak{m}_P(V/W) = (\pi)$. Claramente $v_W(f) = v_W(g) - v_W(h) < 0$, luego W es un polo de f. ■

En particular, una función racional es regular si y sólo si no tiene polos. También vemos que el anillo de enteros de la valoración v_W está formada por las funciones que son regulares en algún punto de W (y entonces lo son en un abierto de W).

Ejemplo Sea $V = A^2$ y $f = x/y$. Vamos a ver que V tiene un único cero simple a lo largo de la recta $X = 0$ y un único polo simple a lo largo de la recta $Y = 0$.

Si llamamos W a la recta $X = 0$, entonces una ecuación local de W en todo A^2 es la función x, ya que una función $F \in k[A^2] = k[X,Y] = k[x,y]$ se anula sobre W si y sólo si es un múltiplo de x. Claramente $v_W(x) = 1$ y $v_W(y) = 0$, pues la función y sólo se anula en un punto de W. Por lo tanto $v_W(f) = 1$.

Igualmente razonamos que si W es $Y = 0$ entonces $v_W(f) = -1$. Por el teorema anterior f no puede tener más polos y por esto mismo aplicado a $1/f$, tampoco puede tener más ceros. ■

El teorema siguiente nos permitirá asociar un divisor a cada función racional de una variedad:

Teorema A.10 *Toda función racional no nula sobre una variedad cuasiproyectiva regular tiene a lo sumo un número finito de ceros y polos.*

DEMOSTRACIÓN: Sea $f \in k(V)$ una función racional en una variedad V. Sea C el conjunto de puntos singulares de f, que es cerrado. Por el teorema anterior, si W es un polo de f, entonces $W \subset C$ y, por tener codimensión 1, debe coincidir con una componente irreducible de C, luego f tiene un número finito de polos. Como los ceros de f son los polos de $1/f$, también son un número finito. ■

Definición A.11 Sea V una variedad cuasiproyectiva regular. El *grupo de divisores* de V es el $\mathbb{Z}$-módulo libre $\mathcal{D}_V$ generado por los divisores primos de V. Lo representaremos con notación multiplicativa. Si $\mathfrak{a} \in \mathcal{D}_V$ y W es un divisor primo, representaremos por $v_W(\mathfrak{a}) \in \mathbb{Z}$ al exponente de W en $\mathfrak{a}$.

Para cada función racional $f \in k(V)$ no nula definimos el divisor $(f) \in \mathcal{D}_V$ como el dado por $v_W((f)) = v_W(f)$, para todo divisor primo W. Los divisores de esta forma se llaman *divisores principales* de V.

Claramente $(fg) = (f)(g)$, por lo que los divisores principales forman un subgrupo P del grupo de divisores. El *grupo de clases* de V es el grupo cociente $\mathcal{H}(V) = \mathcal{D}_V/P$.

Observemos que $(f) = 1$ si y sólo si f no tiene ni ceros ni polos en V, es decir, si y sólo si $f \in k[V]$ y no se anula en ningún punto. Si V es una variedad proyectiva regular esto sucede si y sólo si f es una constante no nula. En particular, la igualdad $(f) = (g)$ equivale a que $f = \alpha g$, con $\alpha \in k$. En otras palabras, en una variedad proyectiva regular, el divisor de una función racional determina a ésta salvo una constante.

Ejemplo Veamos que $\mathcal{H}(A^n) = 1$.

En efecto, si W es un divisor primo de A^n, entonces el teorema 3.16 nos da que $W = V(F)$, para cierto polinomio irreducible $F \in k[X_1, \ldots, X_n]$. Es claro entonces que $f = F \in k[A^n]$ es una ecuación local (en este caso "global") de W en A^n, luego $v_W(f) = 1$. Más aún, $W = (f)$, pues f no puede tener polos y todo cero de f ha de ser un polos de $1/f$, luego ha de estar contenido en W, luego ha de ser W. Así pues, todo divisor es principal y el grupo de clases es trivial. ■

Ejemplo Veamos que $\mathcal{H}(\mathrm{P}^n) \cong \mathbb{Z}$.

Como en el ejemplo anterior, tenemos que todo divisor primo de P^n es de la forma $W = V(F)$, donde ahora F es una forma irreducible, digamos, de grado r. No obstante, ahora no es cierto que F determine una función $f \in k[\mathrm{P}^n]$. Lo más que podemos hacer es tomar una forma lineal G distinta de F y definir $f = F/G^r \in k(\mathrm{P}^n)$. Si llamamos $L = V(G)$, tenemos que $(f) = W/L^r$.

En efecto, f es singular en los puntos de L, luego L es su único polo y $1/f$ es singular en los puntos de W, luego W es el único cero de f. Para calcular las multiplicidades tomamos un sistema de referencia en el que la recta infinita sea distinta de W o L. En el abierto afín $U = A^n$ tenemos que $g = [F]/[X_{n+1}^r]$ es una función regular definida por la deshomogeneización de F, que es un polinomio irreducible, luego $I_U(W \cap U) = (g)$. Igualmente, si llamamos $h = [G]/[G']$ tenemos que $I_U(L \cap U) = (h)$. Así pues, $v_W(g) = 1$, $v_L(h) = 1$, $v_W(h) = 0$, $v_L(g) = 0$ (ya que h no puede anularse sobre un abierto de W, o sería $W = L$, y viceversa). Además, $f = g/h^r$, luego $v_W(f) = 1$, $v_L(f) = -r$.

En general, si $f = F/G \in k(\mathrm{P}^n)$, donde F y G son formas del mismo grado, podemos exigir que sean primas entre sí en $k[X_1, \ldots, X_{n+1}]$. Descompongámoslas en factores primos $F = F_1^{m_1} \cdots F_r^{m_r}$, $G = F_{r+1}^{-m_{r+1}} \cdots F_s^{-m_s}$. Tomamos una forma lineal H distinta de todas las formas F_i, de modo que

$$f = f_1^{m_1} \cdots f_s^{m_s},$$

donde $f_i = F_i/H^{\operatorname{grad} F_i}$. Por el caso anterior,

$$(f) = W_1^{m_1} \cdots W_s^{m_s},$$

donde $W_i = V(F_i)$. (Notemos que los divisores $V(H)$ se cancelan porque F y G tienen el mismo grado.)

Observemos ahora que si $W = V(F)$ es un divisor primo, la forma F está determinada por W salvo una constante, luego podemos definir $\operatorname{grad} W = \operatorname{grad} F$ y extender esta aplicación a un epimorfismo de grupos $\operatorname{grad} : \mathcal{D}_{\mathrm{P}^n} \longrightarrow \mathbb{Z}$. Del razonamiento precedente se desprende que todos los divisores principales tienen grado 0 y, recíprocamente, a partir de un divisor $\mathfrak{a}$ de grado 0 podemos construir un cociente de formas del mismo grado que determinen una función racional f tal que $(f) = \mathfrak{a}$. En definitiva, el núcleo de la aplicación grado es precisamente el grupo de los ideales principales, luego tenemos un isomorfismo $\operatorname{grad} : \mathcal{H}(\mathrm{P}^n) \longrightarrow \mathbb{Z}$. ■

Vamos a ver ahora que todo divisor es "localmente principal", lo que nos permitirá definir la antiimagen de un divisor por una aplicación regular.

Definición A.12 Sea V una variedad cuasiproyectiva regular, sea U un abierto en V y sea $\mathfrak{a}$ un divisor en V. Llamaremos $\mathfrak{a}|_U$ al divisor de U dado por $v_W(\mathfrak{a}|_U) = v_{\overline{W}}(\mathfrak{a})$, para cada divisor W de U.

Observemos que al calcular $\mathfrak{a}|_U$ desaparecen los factores correspondientes a divisores de V disjuntos con U, mientras que $\mathfrak{a}|_U$ permite recuperar la multiplicidad en $\mathfrak{a}$ de cualquier divisor de V que corte a U. Es claro entonces que un divisor está completamente determinado por sus restricciones a los miembros de un cubrimiento abierto de V.

Dado un punto $P \in V$ y un divisor $\mathfrak{a}$, de la prueba del teorema A.3 se sigue que podemos encontrar un entorno afín U de P disjunto de los divisores primos de $\mathfrak{a}$ que no pasen por P y en el que cada divisor primo W_i de $\mathfrak{a}$ que pasa por P tiene una ecuación local π_i. Es claro entonces que el divisor de π_i en U es $W_i \cap U$, luego la función $f = \prod\limits_i \pi_i^{v_{W_i}(\mathfrak{a})}$ cumple $(f) = \mathfrak{a}|_U$.

En definitiva, vemos que todo punto de V tiene un entorno donde $\mathfrak{a}$ es principal. Podemos extraer un cubrimiento finito U_i de V tal que $\mathfrak{a}|_{U_i} = (f_i)$, para cierta función $f_i \in k[U_i]$, y entonces es claro que $\mathfrak{a}$ está completamente determinado por los pares (U_i, f_i). Observemos que $(f_i)|_{U_i \cap U_j} = \mathfrak{a}|_{U_i \cap U_j} = (f_j)|_{U_i \cap U_j}$, luego en $U_i \cap U_j$ la función f_i/f_j tiene divisor trivial, es decir, no tiene ni ceros ni polos.

Definición A.13 Un *sistema compatible de funciones* en una variedad cuasiproyectiva regular V es un conjunto finito de pares $\{(U_i, f_i)\}$, donde los conjuntos U_i son un cubrimiento abierto de V y las funciones $f_i \in k[U_i]$ son no nulas y cumplen que, para cada par de índices i, j, el cociente f_i/f_j es regular y no se anula en $U_i \cap U_j$.

Acabamos de ver cómo asignar a cada divisor $\mathfrak{a}$ de V un sistema compatible de funciones en V. Recíprocamente, cada uno de estos sistemas está inducido por un único divisor. En efecto, para cada divisor primo W de V, consideramos un abierto U_i tal que $W \cap U_i \neq \varnothing$ y definimos $v_W(\mathfrak{a}) = v_{W\cap U_i}(f_i)$. La compatibilidad del sistema implica que esto no depende de la elección de i, pues si $W \cap U_j \neq \varnothing$, tomamos $P \in W \cap U_i \cap U_j$ y un entorno afín U de P tal que $U \subset U_i \cap U_j$ y W admita una ecuación local π en U. Entonces $v_{W\cap U_i}(f_i)$ es la multiplicidad de π en f_i en $\mathcal{O}_P(V)$, pero f_i/f_j es una unidad de $\mathcal{O}_P(V)$, luego dicha multiplicidad coincide con la de π en f_j, que es $v_{W\cap U_j}(f_j)$. Es claro que el divisor construido de este modo a partir del sistema de funciones asociado a un divisor $\mathfrak{a}$ es el propio $\mathfrak{a}$.

Por otra parte, un mismo divisor determina distintos sistemas compatibles de funciones porque podemos elegir el cubrimiento abierto. Es fácil ver que dos sistemas $\{(U_i, f_i)\}$, $\{(V_j, g_j)\}$ se corresponden con el mismo divisor si y sólo si las funciones f_i/g_j son regulares y no se anulan en los abiertos $U_i \cap V_j$.

Ahora podemos dar condiciones para que una aplicación $\phi : V \longrightarrow W$ permita asociar a cada divisor $\mathfrak{a}$ de W un divisor $\overline{\phi}(\mathfrak{a})$ en V. En principio sabemos que si ϕ es una aplicación regular densa, entonces induce un monomorfismo de cuerpos $\overline{\phi} : k(W) \longrightarrow k(V)$ dado por $\overline{\phi}(f) = \phi \circ f$. Veremos que la densidad es suficiente para definir $\overline{\phi}(\mathfrak{a})$ para todo divisor $\mathfrak{a}$, pero conviene dar condiciones que garanticen la existencia de $\overline{\phi}(\mathfrak{a})$ para un divisor dado.

Notemos en primer lugar que si $f \in k(W)$ es una función racional no nula, la composición $\phi \circ f$ será también una función racional no nula siempre que exista un punto $P \in \phi[V]$ donde f esté definida y sea no nula. Conviene expresar esta condición en otros términos:

Llamaremos *soporte* de un divisor $\mathfrak{a} = W_1^{m_1} \cdots W_r^{m_r}$ en una variedad V al cerrado $\operatorname{sop} \mathfrak{a} = W_1 \cup \cdots \cup W_r$ (con el convenio $\operatorname{sop} 1 = \varnothing$).

Así, para que $\phi \circ f$ esté definida y sea no nula, basta exigir que $\phi[V] \not\subset \operatorname{sop}(f)$.

Consideremos ahora un divisor $\mathfrak{a}$ en V tal que $\phi[V] \not\subset \operatorname{sop} \mathfrak{a}$. En particular, esto sucede siempre que ϕ es densa. Podemos tomar una familia compatible de funciones (U_i, f_i) tal que $\phi[V] \cap U_i \neq \varnothing$. Vamos a ver que entonces también se cumple $\phi[V] \cap U_i \not\subset \operatorname{sop}(f_i)$.

Supongamos que $\phi[V] \cap U_i \subset \operatorname{sop}(f_i)$. Claramente $\overline{\phi[V]}$ es irreducible, pues en caso contrario V sería reducible. Entonces $\overline{\phi[V]} = \overline{\phi[V] \cap U_i} \subset \operatorname{sop}(f_i)$. Por construcción de f_i tenemos que $\operatorname{sop}(f_i) \cap U_i = \operatorname{sop} \mathfrak{a} \cap U_i$. Así pues,

$$\phi[V] \cap U_i \subset \overline{\phi}[V] \cap U_i \subset \operatorname{sop} \mathfrak{a},$$

luego, tomando clausuras de nuevo,

$$\phi[V] \subset \overline{\phi[V]} = \overline{\phi[V] \cap U_i} \subset \operatorname{sop}\mathfrak{a},$$

contradicción.

De este modo, las funciones $\phi \circ f_i$ son funciones racionales no nulas en $\phi^{-1}[U_i]$, y es inmediato comprobar que los pares $(\phi^{-1}[U_i], \phi \circ f_i)$ forman un sistema compatible de funciones en V. Más aún, si consideramos dos sistemas compatibles de funciones asociados a $\mathfrak{a}$ en W (con la condición $\phi[V] \cap U_i \neq \varnothing$), entonces los sistemas en V definidos según acabamos de ver determinan un mismo divisor, al que podemos llamar $\overline{\phi}(\mathfrak{a})$.

El teorema siguiente resume lo que hemos demostrado:

Teorema A.14 *Sea $\phi : V \longrightarrow W$ una aplicación regular entre dos variedades cuasiproyectivas regulares, sea $\mathfrak{a}$ un divisor en W tal que $\phi[V] \not\subset \operatorname{sop}\mathfrak{a}$ y sea $\{(U_i, f_i)\}$ un sistema compatible de funciones en W asociado a $\mathfrak{a}$ y tal que $\phi[V] \cap U_i \neq \varnothing$ para todo i. Entonces $\{(\phi^{-1}[U_i], \phi \circ f_i)\}$ es un sistema compatible de funciones en V que determina un divisor $\overline{\phi}(\mathfrak{a})$ independiente de la elección del sistema de funciones.*

Si $\mathfrak{a}_1$ y $\mathfrak{a}_2$ son dos divisores de V_2 determinados por los sistemas de funciones $\{(U_i, f_i)\}$ y $\{(V_j, g_j)\}$, es claro que $\mathfrak{a}_1\mathfrak{a}_2$ está determinado por el sistema de funciones $\{(U_i \cap V_j, f_i g_j)\}$, de donde se sigue sin dificultad que si $\overline{\phi}(\mathfrak{a})$ y $\overline{\phi}(\mathfrak{b})$ están definidos, entonces también lo está $\overline{\phi}(\mathfrak{ab})$ y

$$\overline{\phi}(\mathfrak{ab}) = \overline{\phi}(\mathfrak{a})\overline{\phi}(\mathfrak{b}).$$

En particular, si $\phi : V \longrightarrow W$ es una aplicación regular densa entre variedades regulares, tenemos que $\overline{\phi} : \mathcal{D}_W \longrightarrow \mathcal{D}_V$ es un homomorfismo de grupos.

Por otra parte, un divisor principal (f) está determinado por el sistema de funciones (W, f), y es claro entonces que (si está definido) $\overline{\phi}((f)) = (\phi \circ f)$. Como $\overline{\phi}$ transforma divisores principales en divisores principales, vemos que (si ϕ es densa) $\overline{\phi}$ induce un homomorfismo $\overline{\phi} : \mathcal{H}(W) \longrightarrow \mathcal{H}(V)$.

Otra propiedad sencilla de probar es que si $\phi : V \longrightarrow W$ y $\psi : W \longrightarrow X$ son aplicaciones regulares y $\mathfrak{a}$ es un divisor en X tal que están definidos $\overline{\psi}(\mathfrak{a})$ y $\overline{\phi}(\overline{\psi}(\mathfrak{a}))$, entonces

$$\overline{\phi \circ \psi}(\mathfrak{a}) = \overline{\phi}(\overline{\psi}(\mathfrak{a})).$$

Ejercicio: Comprobar que la definición de $\overline{\phi}$ extiende a la que ya teníamos para aplicaciones regulares no constantes entre curvas proyectivas regulares.

A.3 Aplicación a las isogenias

Aunque el interés principal de la teoría de divisores se debe principalmente a su conexión con los números de intersección y el teorema de Bezout, nosotros veremos únicamente una aplicación a la teoría de curvas elípticas. En esta sección supondremos siempre que las curvas consideradas están definidas sobre un cuerpo de constantes de característica distinta de 2 o 3.

Definición A.15 Consideremos dos curvas elípticas E_1 y E_2 consideradas como grupos con la operación definida en 9.19 a partir de sendos puntos O_1 y O_2. Una *isogenia* $\phi : E_1 \longrightarrow E_2$ es una aplicación regular tal que $\phi(O_1) = O_2$.

En realidad las isogenias cumplen más de lo que en principio hemos exigido:

Teorema A.16 *Las isogenias son homomorfismos de grupos.*

DEMOSTRACIÓN: $\phi : E_1 \longrightarrow E_2$ una isogenia entre curvas elípticas. Podemos suponer que es no nula. Consideramos el diagrama siguiente,

$$\begin{tikzcd} E_1 \arrow[r] \arrow[d, "\phi"'] & \mathcal{H}_0(E_1) \arrow[d, "\phi"] \\ E_2 \arrow[r] & \mathcal{H}_0(E_2) \end{tikzcd}$$

donde las flechas horizontales son los isomorfismos $P \mapsto [P/O]$ entre las curvas y sus grupos de clases de grado 0, mientras que la flecha de la derecha es el homomorfismo inducido por la extensión de ϕ al grupo de divisores (es decir, por la norma definida en 7.3, que induce un homomorfismo sobre los grupos de clases en virtud de 7.4). Obviamente el diagrama es conmutativo, luego ϕ es un homomorfismo de grupos. ■

Definición A.17 Si E_1 y E_2 son dos curvas elípticas (con una estructura de grupo prefijada), llamaremos $\operatorname{Hom}(E_1, E_2)$ al conjunto de todas las isogenias de E_1 en E_2, que claramente es un grupo abeliano con la suma definida puntualmente. (Aquí usamos el teorema 9.21.) Llamaremos $\operatorname{End} E$ al grupo de isogenias de una curva elíptica E en sí misma.

En la sección 1.8 hemos estudiado las isogenias de las curvas elípticas complejas a través de su representación como toros complejos (allí las llamábamos homomorfismos analíticos). Los resultados de esta sección generalizan sustancialmente a los vistos allí.

Las isogenias más simples de una curva elíptica E en sí misma son las multiplicaciones enteras $\lambda_m(P) = mP$, para $m \in \mathbb{Z}$. Vamos a investigar sus núcleos, es decir, los subgrupos $E[m]$ formados por los elementos que cumplen $mP = 0$.

En general, el núcleo de una isogenia no nula $\phi : E_1 \longrightarrow E_2$ es un subgrupo finito de E_1, pues cada punto tiene un número finito de antiimágenes por cualquier aplicación regular no constante entre curvas.

Más precisamente, recordemos que el grado de una aplicación regular no constante entre curvas se define como $\operatorname{grad}\phi = |k(E_1) : \overline{\phi}[k(E_2)]|$. Si ϕ es separable, entonces todos los puntos de E_2 salvo a lo sumo un número finito de ellos (los ramificados) tienen $\operatorname{grad}\phi$ antiimágenes, pero si ϕ es una isogenia entonces todos los puntos han de tener el mismo número de antiimágenes (porque es un homomorfismo de grupos), luego, en particular, el núcleo de una isogenia separable ϕ es un grupo de orden $\operatorname{grad}\phi$.

El teorema principal que vamos a demostrar es el siguiente:

Teorema A.18 *Si E es una curva elíptica, existe una aplicación*

$$(\ ,\ ) : \operatorname{End} E \times \operatorname{End} E \longrightarrow \mathbb{Q}$$

que verifica las propiedades

$$(\phi, \psi) = (\psi, \phi), \quad (\phi + \chi, \psi) = (\phi, \psi) + (\chi, \psi)$$

y además $(\phi, \phi) = \operatorname{grad}\phi$, para toda isogenia ϕ (con el convenio de que la isogenia nula tiene grado 0).

Para probar esto basta demostrar que la aplicación $n : \operatorname{End} E \longrightarrow \mathbb{N}$ dada por $n(\phi) = \operatorname{grad}\phi$ satisface la relación

$$n(\phi + \psi) + n(\phi - \psi) = 2(n(\phi) + n(\psi)), \tag{A.1}$$

pues entonces basta definir

$$(\phi, \psi) = \frac{1}{2}(n(\phi + \psi) - n(\phi) - n(\psi)) = \frac{1}{2}(n(\phi) + n(\psi) - n(\phi - \psi)).$$

Obviamente $(\phi, \psi) = (\psi, \phi)$. Veamos que la expresión

$$S(\phi, \chi, \psi) = (\phi + \chi, \psi) - (\phi, \psi) - (\chi, \psi)$$

es idénticamente nula. Aplicando (A.1) con $\phi = \psi = 0$ obtenemos que $n(0) = 0$ y con $\phi = 0$ obtenemos $n(-\psi) = n(\psi)$. De aquí se sigue que $(\phi, -\psi) = -(\phi, \psi)$ y, por simetría, $(-\phi, \psi) = -(\phi, \psi)$. De aquí a su vez obtenemos que

$$S(\phi, \chi, -\psi) = -S(\phi, \chi, \psi), \quad S(-\phi, -\chi, \psi) = -S(\phi, \chi, \psi).$$

Ahora bien, desarrollando la definición de S vemos que

$$2S(\phi, \chi, \psi) = n(\phi+\chi+\psi) - n(\phi+\chi) - n(\phi+\psi) - n(\chi+\psi) + n(\phi) + n(\chi) + n(\psi)$$

es una expresión simétrica en sus tres variables, luego

$$-S(\phi, \chi, \psi) = S(-\phi, -\chi, \psi) = -S(\phi, -\chi, \psi) = S(\phi, \chi, \psi),$$

de donde podemos concluir que $S(\phi, \chi, \psi) = 0$.

La segunda expresión que define a (ϕ, ψ) muestra que $(\phi, \phi) = n(\phi)$. ■

Para demostrar (A.1) necesitamos algunas consideraciones sobre divisores en la superficie $E \times E$. Llamemos

$$\Delta = \{(P,P) \mid P \in E\}, \qquad \Sigma = \{(P,-P) \mid P \in E\}.$$

Se trata de dos curvas isomorfas a E. Aquí usamos que la imagen de la aplicación regular $P \mapsto (P,P)$ (resp. $P \mapsto (P,-P)$) es cerrada y claramente es un isomorfismo, pues su inversa es una proyección. Así pues, Δ y Σ son dos divisores primos de $E \times E$. (Es fácil ver que son distintos.)

Llamemos $S : E \times E \longrightarrow E$ a la aplicación suma $S(P,Q) = P+Q$ y recordemos que $\tau_P : E \longrightarrow E$ representa a la traslación $\tau_P(Q) = P+Q$. Vamos a calcular

$$d_{(P,Q)}S : T_PE \oplus T_QE \longrightarrow T_{P+Q}E.$$

Para ello consideramos la aplicación $i_Q^1 : E \longrightarrow E \times E$ dada por $i_Q^1(R) = (R,Q)$. Como $i_Q^1 \circ S = \tau_Q$, tenemos que $d_P i_Q^1 \circ d_{(P,Q)}S = d_P\tau_Q$. Igualmente sucede con la otra componente, luego

$$d_{(P,Q)}S = d_P\tau_Q + d_Q\tau_P.$$

En particular concluimos que $d_{(P,Q)}S$ es suprayectiva.

Vamos a usar esto para demostrar que $\overline{S}(O) = \Sigma$. En efecto, sea t_O un parámetro local de E en O y sea U un entorno de O donde t_O sea regular y no tenga más ceros. Entonces (U,t_O) forma parte de un sistema compatible de funciones asociado al divisor O. Los puntos no cubiertos por U (un número finito) se cubren con abiertos que no contengan más que un cero o polo de t_O y les asignamos la función constante 1.

Así, $\overline{S}(O)$ es el divisor de $\overline{S}(t_O)$ en $S^{-1}[U]$. Ciertamente, $\overline{S}(t_O)$ es regular en $S^{-1}[U]$, luego $\overline{S}(O)$ no tiene polos. Por otra parte, si $(P,Q) \in S^{-1}[U]$ cumple $\overline{S}(t_O)(P,Q) = t_O(P+Q) = 0$ es porque $P+Q=0$, luego $\overline{S}(t_O)$ se anula únicamente sobre los puntos de $\Sigma \subset S^{-1}[U]$, luego Σ es el único cero de $\overline{S}(O)$. Falta probar que su multiplicidad es 1. Para ello basta probar que $\overline{S}(t_O)$ es una ecuación local de Σ. A su vez, si tomamos $(P,-P) \in \Sigma$, basta ver que $\overline{S}(t_O)$ es primo en $\mathcal{O}_{(P,-P)}(E \times E)$. Este anillo es un dominio de factorización única y el ideal maximal $m_{(P,-P)}$ contiene a todos los primos. Por consiguiente, si $\overline{S}(t_O)$ fuera compuesta, cumpliría $\overline{S}(t_O) \in m^2_{(P,-P)}$.

Ahora bien, como $d_{(P,-P)}S : T_{(P,-P)}(E \times E) \longrightarrow T_OE$ es suprayectiva, su dual $\mathfrak{m}_O/\mathfrak{m}_O^2 \longrightarrow \mathfrak{m}_{(P,-P)}/\mathfrak{m}^2_{(P,-P)}$ es inyectiva, luego $\overline{S}(t_O) \notin \mathfrak{m}^2_{(P,-P)}$.

Similarmente se prueba que si $R : E \times E \longrightarrow E$ es la aplicación dada por $R(P,Q) = P-Q$, entonces $\overline{R}(O) = \Delta$.

Consideremos ahora las proyecciones $p_i : E \times E \longrightarrow E$, para $i = 1,2$, y vamos a demostrar que

$$\overline{p}_1(O) = \{O\} \times E, \qquad \overline{p}_2(O) = E \times \{O\}.$$

Razonando como antes, $\overline{p}_1(O)$ es el divisor de $\overline{p}_1(t_O)$ en $S^{-1}[U]$. De nuevo se trata de un divisor sin polos y con $\{O\}\times E$ como único cero. La multiplicidad es 1 porque $d_{(O,O)}p_1$ es suprayectiva.

El resultado crucial es la siguiente igualdad de clases de divisores en $E\times E$:

$$[\Delta\Sigma] = [\overline{p}_1(O)^2\overline{p}_2(O)^2]. \tag{A.2}$$

Para probarla basta encontrar $f \in k(E\times E)$ con divisor $\Delta\Sigma/\overline{p}_1(O)^2\overline{p}_2(O)^2$.

No perdemos generalidad si suponemos que E es una curva plana definida por una ecuación de Weierstrass cuyo neutro O es su único punto infinito. Entonces, cada recta vertical $X = a$ corta a E en dos puntos finitos P y Q (no necesariamente distintos) y el teorema 9.20 muestra que $P + Q = O$. En otras palabras, dos puntos finitos P y $Q \in E$ cumplen $x(P) = x(Q)$ si y sólo si $P = \pm Q$ en E.

Sean x_1, y_1, x_2, y_2 las funciones coordenadas en $E\times E$ y consideremos la función $f = x_1 - x_2 \in k(E\times E)$.

Tenemos que f se anula sobre los puntos finitos de $\Delta\cup\Sigma$, luego sus ceros son Δ y Σ. Vamos a ver que su multiplicidad es 1.

Sea $P \in E$ un punto finito de E tal que $P \neq -P$. Entonces $x - x(P)$ es un parámetro local en P, luego $x_1 - x_1(P)$, $x_2 - x_2(P)$ son un sistema de parámetros locales en (P,P). Esto implica que $d_{(P,P)}x_1$ y $d_{(P,P)}x_2$ son linealmente independientes, luego $d_{(P,P)}(x_1 - x_2) \neq 0$, luego $x_1 - x_2 \notin \mathfrak{m}^2_{(P,P)}$, luego f es primo en $\mathcal{O}_{(P,P)}(E\times E)$. Según A.4 existe una curva W en $E\times E$ que pasa por (P,P) y de modo que $(f) = \mathfrak{m}_{(P,P)}(E\times E/W)$. Necesariamente $W = \Delta$, luego $v_\Delta(f) = 1$.

También se cumple que $x - x(P) = x - x(-P)$ es un parámetro local en $-P$, luego razonando igualmente con el punto $(P,-P)$ llegamos a que $v_\Sigma(f) = 1$.

Por otra parte, f es singular en los puntos (O,P) y (P,O), donde P es un punto finito de E, luego sus polos son los primos $\overline{p}_1(O)$ y $\overline{p}_2(O)$. Vamos a probar que su multiplicidad en f es 2. Ante todo,

$$f = \left(1 - \frac{x_2}{x_1}\right)x_1,$$

y el primer factor vale 1 en cualquier punto (O,P), luego $v_{\overline{p}_1(O)}(f) = v_{\overline{p}_1(O)}(x_1)$. Un parámetro local de E en O es x/y, luego $t = x_1/y_1$ forma parte de un sistema de parámetros locales de $E\times E$ en (O,P), luego su diferencial es no nula, luego $t \notin \mathfrak{m}^2_{(O,P)}$ y, por consiguiente, es primo en $\mathcal{O}_{(O,P)}(E\times E)$. De aquí se sigue que es una ecuación local de $\overline{p}(O)$ alrededor de (O,P). Como

$$x_1 = \frac{x_1^3}{y_1^2}\,t^{-2}$$

y el primer factor es una unidad de $\mathcal{O}_{(O,P)}(E\times E)$, podemos concluir que $v_{\overline{p}_1(O)}(f) = -2$. Igualmente se razona con el otro polo. ■

Ahora ya podemos demostrar el teorema A.18. Recordemos que basta demostrar la relación (A.1). Consideremos dos isogenias ϕ, $\psi \in \operatorname{End} E$ tales que ϕ, ψ, $\phi+\psi$ y $\phi-\psi$ sean no nulas. Sea $f : E \longrightarrow E \times E$ la aplicación dada por $f(P) = (\phi(P), \psi(P))$. Entonces $f \circ p_1 = \phi$, $f \circ p_2 = \psi$, luego

$$\overline{f}(\overline{p}_1(O)) = \overline{\phi}(O), \qquad \overline{f}(\overline{p}_2(O)) = \overline{\psi}(O).$$

Aquí usamos que $\overline{f}$ está definida porque $\phi \neq 0 \neq \psi$. Similarmente, el hecho de que $\phi+\psi \neq 0$ implica que $\overline{f}$ está definida sobre Σ y como $\phi-\psi \neq 0$ también lo está sobre Δ. Además, $f \circ S = \phi+\psi$, luego $\overline{f}(\Sigma) = \overline{f}(\overline{S}(O)) = (\overline{\phi+\psi})(O)$ e, igualmente, $\overline{f}(\Delta) = \overline{f}(\overline{S}(O)) = (\overline{\phi-\psi})(O)$.

Aplicando $\overline{f}$ a (A.2) obtenemos que

$$[(\overline{\phi+\psi})(O)(\overline{\phi-\psi})(O)] = [\overline{\phi}(O)^2\overline{\psi}(O)^2].$$

Ésta es una igualdad de clases de divisores de la curva E. Teniendo en cuenta que los divisores principales tienen grado 0, vemos que

$$\operatorname{grad}(\overline{\phi+\psi})(O) + \operatorname{grad}(\overline{\phi-\psi})(O) = 2(\operatorname{grad}\overline{\phi}(O) + \operatorname{grad}\overline{\psi}(O)).$$

Por último, es claro que $\operatorname{grad}\overline{\phi}(O) = \operatorname{grad}\phi$, e igualmente con las otras isogenias, luego tenemos (A.1).

Si $\phi = 0$ entonces (A.1) es trivial. Si $\psi = 0$ también, teniendo en cuenta que $\operatorname{grad}\phi = \operatorname{grad}(-\phi)$, dado que $-\phi = \phi \circ \lambda_{-1}$ y λ_{-1} (es decir, la aplicación $P \mapsto -P$) es un isomorfismo, luego tiene grado 1.

Supongamos ahora que $\phi - \psi = 0$. Esto nos impide calcular $\overline{f}(\Delta)$. Sea $t = x/y \in k(E)$, que tiene un cero simple en O. Sea $\mathfrak{a} = O/(t)$, de modo que $[O] = [\mathfrak{a}]$ y $O \notin \operatorname{sop}\mathfrak{a}$. Sea $\Delta' = \overline{S}(\mathfrak{a})$, de modo que $[\Delta'] = [\Delta]$. Por consiguiente, la fórmula (A.2) sigue siendo cierta con Δ' en lugar de Δ, pero ahora Δ no divide a Δ', por lo que $\overline{f}(\Delta')$ sí que está definida. Además

$$\overline{f}(\Delta') = (\overline{\phi-\psi})(\mathfrak{a}) = \overline{0}(\mathfrak{a}) = 1,$$

pues si formamos un sistema compatible de funciones (U_i, f_i) asociado a $\mathfrak{a}$ tal que $0[E] \cap U_i \neq \varnothing$ (es decir, $O \in U_i$), entonces las funciones $0 \circ f_i = f_i(O) \neq 0$ son constantes no nulas, que determinan el divisor trivial.

Así pues, $\operatorname{grad}\overline{f}(\Delta') = 0 = \operatorname{grad}(\phi-\psi)$ y se sigue cumpliendo (A.1). Si $\phi+\psi = 0$ razonamos análogamente. ∎

Ahora podemos calcular el grado de las multiplicaciones λ_m. La relación (A.1) nos da que

$$\operatorname{grad}\lambda_{m+1} + \operatorname{grad}\lambda_{m-1} = 2(\operatorname{grad}\lambda_m + \operatorname{grad}\lambda_1).$$

Puesto que, obviamente, $\operatorname{grad}\lambda_0 = 0$ y $\operatorname{grad}\lambda_1 = 1$, una simple inducción prueba que $\operatorname{grad}\lambda_m = m^2$ para todo $m \geq 0$ y, de aquí, para todo $m \in \mathbb{Z}$ (puesto que $\operatorname{grad}\lambda_{-1} = 1$).

Así, si el cuerpo de constantes k tiene característica 0, entonces λ_m es separable, luego concluimos que el subgrupo $E[m]$ formado por los puntos $P \in E$ tales que $mP = O$ tiene orden m^2. En realidad puede probarse que λ_m es separable incluso si k tiene característica prima p y $p \nmid m$.

Más aún, bajo estas hipótesis podemos determinar la estructura del grupo: necesariamente

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

En efecto, si descomponemos $E[m]$ en producto de grupos cíclicos de orden potencia de primo, cada primo $p \mid m$ no puede aparecer más que en el orden de dos factores, pues de lo contrario $|E[p]| \geq p^3$. Por otra parte, si $m = p^r m'$, con $(m, m') = 1$, entonces $E[m]$ no puede contener un subgrupo de orden p^{2r}, luego ha de haber exactamente dos factores de orden p^r.

En particular, si E es una cúbica regular sobre un cuerpo de característica 0 (o, más en general, de característica distinta de 2 o 3), el grupo $E[3]$ está formado por los puntos $P \in E$ tales que P, P, P estén alineados, y éstos son los puntos de inflexión de E.

Por consiguiente, toda cubica regular E sobre un cuerpo de característica distinta de 2 o 3 tiene exactamente 9 puntos de inflexión. Además, una recta que pase por dos de ellos P y Q corta a E en otro punto de inflexión R, pues $R = -P - Q$, con lo que $3R = 0$.

Bibliografía

[1] Appell, P, y Lacour, E. *Principes de la théorie des fonctions elliptiques et applications.* Gauthier-Villars, Paris, 1897.

[2] Artin, E. *Algebraic Numbers and Algebraic Functions.* Nelson, 1967.

[3] Bliss, G.A. *Algebraic Functions.* Dover, New York, 1966.

[4] Eichler, M. *Introduction to the theory of algebraic numbers and functions.* Academic Press, New York, 1966.

[5] Fulton, W. *Curvas algebraicas. Introducción a la geometría algebraica.* Reverté, Barcelona, 1971.

[6] Iyanaga, S. (Ed.) *The Theory of Numbers.* North Holland, Amsterdam, 1969.

[7] Kendig, K. *Elementary Algebraic Geometry.* Springer, New York, 1977.

[8] Lang, S. *Introduction to algebraic and abelian functions.* Addison-Wesley, Massachusetts, 1972.

[9] Markushevich, A. *Teoría de las funciones analíticas.* Ed. Mir, Moscú, 1978.

[10] Milne, J.S. *Elliptic Curves.* Apuntes, 1996.

[11] Murty, V.K. *Introduction to Abelian Varieties.* AMS, 1993.

[12] Shafarevich, I. R. *Basic Algebraic Geometry.* Springer, New York, 1994.

[13] Siegel, C. L. *Topics in Complex Function Theory.* (3 volúmenes) John Whiley & sons, New York, 1969, 1971, 1973.

[14] Walker, R.J. *Algebraic Curves.* Dover, New York, 1962.

[15] Zariski, O., Samuel, P. *Commutative Algebra.* Springer, New York, 1975.

Índice de Materias