Una Introducción a las Estructuras Algebraicas Básicas

Notas para la asignatura Álgebra 3

Profesora Olga Porras

Departamento de Matemáticas
Facultad de Ciencias
Universidad de los Andes

2 de julio de 2010

Índice general

Introducción histórica

Los problemas planteados en escritura cuneiforme, conservados en tablillas de arcilla escritas en Babilonia, alrededor del año 1600 A.C., constituyen el registro más antiguo que se conoce de esa actividad que hoy llamamos resolución de ecuaciones, y que se vincula naturalmente al desarrollo del Álgebra. Sin duda, la historia de los avances de la Humanidad en la resolución de ecuaciones polinómicas muestra cómo crece lentamente, a través de los siglos, esa "semilla"de la abstracción sembrada en la cultura occidental por los pensadores de la Grecia Antigua, en particular, la abstracción del número como hoy lo concebimos, y que permitió desarrollar toda una simbología al servicio del estudio de la resolución de ecuaciones en su sentido más general, y también al servicio de lo que se conoce como Álgebra Moderna o Álgebra Abstracta, disciplina que ya no tiene, sin embargo, el tema de la resolución de ecuaciones polinómicas como objeto central de su estudio.

La concepción griega del número como asociado a una medida o a una colección de objetos, bien fuesen tangibles como piedras o intangibles como unidades o mónadas sólo accesibles a través del pensamiento, prevaleció por siglos, y marcó toda la visión y el tratamiento de las ecuaciones algebraicas hasta el S.XVI, época en que comienza a concebirse el número como ente abstracto. Es en ese momento, en virtud de esa nueva concepción, desarrollada, entre otros, por el matemático francés François Viète, que éste introduce la simbología que da inicio a una visión general de las ecuaciones algebraicas y permite un tratamiento nuevo de las mismas, así como el desarrollo de la Geometría Analítica por parte de Fermat y Descartes.

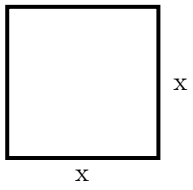
El Álgebra Geométrica de Euclides, llamada así por historiadores modernos, consistió en una sofisticada técnica desarrollada para resolver ecua-

ciones lineales y cuadráticas haciendo uso de representaciones geométricas de los números, sus cuadrados, o productos de números distintos, como longitudes de segmentos, áreas de cuadrados o de rectángulos, respectivamente. A través de ingeniosas construcciones geométricas, se obtenía un segmento de medida conocida, que sería congruente al segmento "incógnita", y se daba por resuelta la ecuación en cuestión. Ha sido cuestionado, por estudiosos del pensamiento griego antiguo [2], el título Álgebra Geométrica dado a esta técnica, puesto que sugiere la presencia de una visión algebraica de la misma, por parte de Euclides, visión que se ha podido constatar ausente en la matemática griega de la época. Veamos un ejemplo del uso de la técnica en cuestión.

Supongamos que se planteaba una ecuación del tipo siguiente:

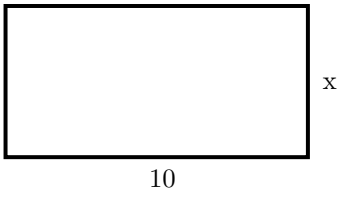
"Si una cantidad se multiplica por sí misma y se le suma diez veces esa cantidad, se obtiene once".

Para resolverla, se interpretaba el producto de la incógnita por sí misma como el área de un cuadrado con lado de longitud igual al número buscado. Si representamos la incógnita por x (como lo hacemos en el lenguaje algebraico moderno, no utilizado por Euclides) tendríamos:



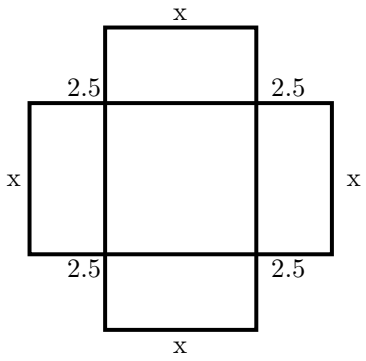
Área: x^2

y el producto del número 10 por esa cantidad, se representaba como el área del rectángulo :



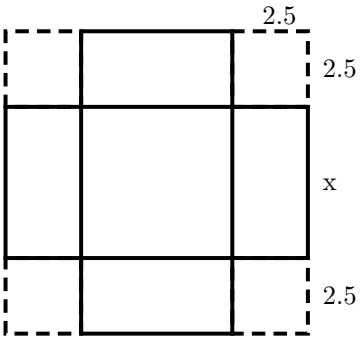
Área: 10x

A continuación, se dividía el rectángulo en 4 rectángulos de área $(2,5)x$ cada uno, y se anexaban estos últimos al cuadrado de la siguiente manera:



Área: $x^2 + 10x$

Lo que plantea la ecuación es que el área de la figura 3 es igual a 11 (aquí se interpreta el número 11 como unidad de área). Luego se procedía a completar esta figura para obtener un cuadrado, adjuntando 4 cuadrados de lado $2,5$ cada uno, de la manera siguiente:



Área: $(x+5)^2$

Como se ha añadido 4 cuadrados de área $(2,5)^2$ cada uno, en total la figura 4 tiene un área igual a $11 + 4(2,5)^2 = 11 + 25 = 36$.

Como el nuevo cuadrado construido tiene lado de longitud igual a $x + 2(2,5) = x + 5$, se obtiene la "nueva" ecuación:

$$(x+5)^2 = 36$$

Esto permite deducir que la cantidad x debe ser igual a 1, puesto que sólo interesa en este caso la solución positiva.

Esta construcción, que podríamos llamar completación geométrica de un cuadrado, constituye el análogo geométrico a la completación algebraica de cuadrados, y es un ejemplo de los más simples utilizados por Euclides para la resolución de ecuaciones cuadráticas. Los más elaborados son un verdadero monumento al ingenio matemático de una cultura que ya había alcanzado un alto grado de madurez, como lo fue la griega, en el S.III a.C.

Más adelante, Diofanto de Alejandría, en el S. III d.C.(según algunos historiadores, vivió en el S. IV), escribió una obra titulada Arithmetica, la cual contiene una importante colección de problemas y sus resoluciones. Debido a la notación utilizada por Diofanto, algunos historiadores modernos lo han considerado el creador del álgebra. Sin embargo, estudios minuciosos han revelado que su tratamiento de las ecuaciones tiene un carácter esencialmente aritmético. Las cantidades o magnitudes que Diofanto denota con símbolos especiales tienen aún el carácter particular que poseía el arithmos (número) de los griegos antiguos señalado arriba.

Durante la Edad Media europea, la cultura árabe penetró las regiones ocupadas por las invasiones en la región del Mediterráneo, y gracias a ello, Europa vio desarrollarse el conocimiento matemático que los árabes habían acumulado al dedicarse a recopilar, traduciendo a su lengua el conocimiento cultivado por siglos en Grecia e India. En particular, el conocimiento antiguo de la resolución de ecuaciones lineales y cuadráticas, así como la introducción del sistema de numeración decimal se hicieron accesibles a Europa, a través de España, gracias a la traducción al latín de la obra del brillante matemático y astrónomo árabe Mohammed Ibn Musa Al-Khwarizmi, llamado por algunos el Padre del Álgebra, quien escribió en el S. IX d.C., entre otros textos importantes, un tratado sobre la resolución de ecuaciones cuyo título fue: Kitab al-jabr wa'l muqäbala. Al-jabr significa restauración (del equilibrio al trasponer términos de una ecuación); muqäbala significa "simplificación"(de la expresión algebraica resultante). Del vocablo Al-jabr se

deriva más tarde el término "álgebra ", adoptado en Occidente, que no sólo se utilizó para la disciplina matemática dedicada a la resolución de ecuaciones, sino también, en España, tuvo un significado asociado a la medicina. El experto en restaurar fracturas o dislocaciones de los huesos era llamado algebrista, como se evidencia en un pasaje de El Quijote y en el Diccionario de la Real Academia Española. Todo esto muestra la gran influencia que tuvo en Europa este tratado, en el cual se hace una clasificación de los diferentes tipos de ecuaciones de grados uno y dos, y se asigna un método particular de resolución para cada uno de estos tipos. Curiosamente, entre los textos antiguos que sirvieron de base a Al-Khwarizmi no se encuentra la Arithmetica de Diofanto.

El poeta y matemático Omar Khayyam, quien vivió en el S. XI d.C., exploró las ecuaciones cúbicas en busca de métodos de resolución para las mismas, basándose en las ideas de Apolonio y otros geómetras griegos. Estas ideas consistían en convertir el problema de hallar una raíz de la ecuación $x^3 - px = q$ en la búsqueda de intersecciones entre una parábola y una hipérbola, obtenidas de la ecuación anterior al dividir entre x ambos miembros: $x^2 - p = \frac{q}{x}$.

Pero no se conoció una solución general para la ecuación cúbica hasta mediados del S. XVI, en la Italia renacentista. Dos matemáticos notables, Scipio del Ferro y Nicolo (Tartaglia) Fontana, trabajando independientemente, encontraron la fórmula que permite encontrar una raíz de la ecuación

$$x^3 + px = q$$

Habían demostrado que la ecuación general

$$ax^3 + bx^2 + cx + d = 0$$

podía reducirse a una del tipo anterior, y que una raíz de aquella está dada por:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

Es curioso el hecho de que la fórmula anterior sea conocida como fórmula de Cardano, matemático, astrólogo y médico, quien no la descubrió, sino que la publicó en su obra Ars Magna en 1545, a pesar de que le costó la amistad de Tartaglia, a quien había jurado no divulgarla. En un momento histórico en que el conocimiento matemático se cultivaba y se guardaba en

celoso secreto como arma para defenderse en los duelos matemáticos públicos, Tartaglia reveló su secreto de la fórmula de la resolución de la ecuación cúbica a Cardano, bajo grave juramento que luego fue incumplido por éste último. Tartaglia nunca pudo perdonarlo, aún cuando, en el Ars Magna, Cardano reconoce la autoría de Tartaglia y Del Ferro en el hallazgo de la fórmula.

Tambien se resuelve en el Ars Magna la ecuación de grado 4, reduciéndola a una de grado 3; el método se debe a Ludovico Ferrari, discípulo y colaborador de Girolamo Cardano.

Este descubrimiento fue alcanzado antes de que François Viète, abogado francés aficionado a las Matemáticas, introdujera la utilización de letras del alfabeto latino en la escritura de las ecuaciones algebraicas: usó vocales para representar las incógnitas y consonantes para representar números dados o parámetros. Este acontecimiento sólo fue posible gracias a la nueva concepción del número que Viète inaugura a plena conciencia, basándose en el estudio minucioso de la obra de Diofanto, Euclides, Eudoxo y Pappus, buscando la unificación de las técnicas utilizadas por éstos para la resolución de problemas geométricos y aritméticos. Antes de este momento, la aritmética consideraba clases de números, de acuerdo a su divisibilidad, pero cada arithmos era considerado al modo de los griegos de la antigüedad: como una característica de una colección de objetos o una medida de tiempo, o una medida de la dimensión de un objeto físico. No se lograba concebir cada arithmos como un objeto en sí mismo, puesto que esto implicaba concebir la multiplicidad como unidad, categorías que se presentaban como opuestas. El trabajo de Tartaglia, Del Ferro, Cardano y Ferrari resulta asombroso al considerar el contexto matemático en el que fue realizado.

Así, la entrada, en el panorama matemático del Renacimiento, de una concepción abstracta del número, desvinculada de la multiplicidad específica a la cual alude cada uno en particular, abre las puertas al pensamiento algebraico propiamente dicho. El acontecimiento provoca un acelerado desarrollo de las Matemáticas en los siglos posteriores, fundado en buena medida en la creación de la Geometría Analítica por parte de René Descartes y Pierre de Fermat.

En particular, la teoría de la resolución de ecuaciones algebraicas comienza su desarrollo en los siglos XVII y XVIII. Uno de los grandes logros de este período es la prueba del Teorema Fundamental del álgebra, por parte de Gauss, quien dio su primera prueba en 1799, en su tesis doctoral. El problema de la posibilidad de factorizar un polinomio de grado arbitrario, con coeficientes reales, como produto de factores lineales y cuadráticos con coeficientes

reales, había creado controversias entre los matemáticos más sobresalientes de la época: Goldbach, Leibniz, Nicholas Bernoulli, Euler, D'Alembert y Lagrange fueron algunos de los que se pronunciaron, unos a favor y otros en contra de la conjetura que afirmaba que sí era posible tal descomposición. Gauss presentó cuatro pruebas diferentes del teorema, a lo largo de su vida, la última de ellas demostrando la versión más general, que incluía polinomios con coeficientes complejos.

La búsqueda de soluciones por radicales para la ecuación de grado 5, es decir, de fórmulas construidas a partir de los coeficientes de la ecuación, por suma, resta, multiplicación, división y radicación, análogas a las obtenidas hasta entonces para las ecuaciones de grado 2, 3, y 4, era entonces un reto para los grandes matemáticos de la época. A fines del siglo XVIII, comienza a sospecharse la imposibilidad de encontrar tal fórmula para la ecuación quíntica. Para esta época, Lagrange había demostrado que las técnicas que condujeron al hallazgo de las fórmulas de resolución de las ecuaciones de grado 2, 3 y 4 dependían de la posibilidad de encontrar funciones de las raíces de la ecuación que fuesen invariantes bajo ciertas permutaciones de esas raíces. (Por ejemplo, la función $f(x, y) = x^2 + y^2$ es invariante bajo la permutación de las variables). Lagrange demostró, además, que no es posible usar esta técnica para la ecuación quíntica.

Ya a principios del s. XIX, en 1813, Ruffini intenta dar una prueba de la imposibilidad de encontrar solución por radicales a la ecuación de grado 5. Publicó sus resultados, pero contenían errores. En 1824, Henryk Abel, joven matemático noruego, tan genial como desafortunado, demostró la imposibilidad de la resolución por radicales de la ecuación de grado 5. Trabajaba en el problema general de poder decidir si una ecuación polinómica de grado arbitrario podría ser o no resuelta por radicales, cuando murió, enfermo, a causa de su extrema pobreza.

En 1832, en Francia, Evariste Galois, un brillante matemático autodidacta de 21 años de edad, quien había sido rechazado tres veces en su solicitud de ingreso a la prestigiosa institución de Educación Superior École Polytechnique, escribió, en la última noche de su breve vida, una carta a su amigo Auguste Chevalier, donde esbozaba sus descubrimientos en torno a la teoría de las ecuaciones polinómicas, particularmente en relación al problema de su solubilidad por radicales. Algún tiempo antes, Galois había intentado hacer conocer esos resultados obtenidos por él, a la Academia de Ciencias, pero sus manuscritos fueron rechazados por Cauchy, quien era jurado evaluador y luego fueron extraviados. En el documento que escribió a su amigo Chevalier,

Galois revelaba la conexión que había encontrado entre los grupos de permutaciones y las ecuaciones polinómicas, además de otros descubrimientos sobre funciones elípticas y la integración de funciones algebraicas. Sabiendo que no sobreviviría al duelo al cual debía enfrentarse al día siguiente, Galois escribió estas notas con desesperación; al margen escribió:"¡No tengo tiempo!". A pesar del rechazo o la indiferencia de que fue víctima durante su vida como matemático, estaba seguro de algo al escribir esas notas precipitadamente: al transcurrir el tiempo, su legado sería valorado. Y no se equivocaba. Once años más tarde, Joseph Liouville se dirigió a la Academia de Ciencias, anunciando que , entre los papeles de Evariste Galois,"había encontrado una solución, tan precisa como profunda, del bello problema de la factibilidad de resolución por radicales de cualquier ecuación polinómica"[4].

El grupo definido por Galois, en 1832, como recurso para el desarrollo de su trabajo en torno a la factibilidad de resolver por radicales un polinomio f, fue el grupo de las permutaciones de las raíces de f. Por muchos años, los únicos grupos considerados por los matemáticos fueron los grupos de permutaciones.

La primera definición de un grupo abstracto fue dada más tarde por Cayley y, sólo en 1870, Kronecker estableció un sistema axiomático satisfactorio para los grupos.

El presente texto ha sido elaborado con la intención de que sirva de apoyo a los estudiantes de un curso introductorio de Álgebra Abstracta, en el cual se estudian las estructuras de grupo, anillo y cuerpo, con especial atención dedicada al grupo simétrico, el anillo de polinomios y el cuerpo de descomposición de un polinomio dado, de manera tal que puedan esbozarse al final las ideas fundamentales de la Teoría de Galois, y el lector adquiera las herramientas necesarias para acceder luego al estudio de esta teoría, que, no sólo tiene un gran interés histórico por marcar el inicio de la llamada "Álgebra Moderna", sino que constituye una verdadera joya de arquitectura matemática.

Otro famoso problema histórico que encontró respuesta entre las aplicaciones de la teoría de cuerpos, es el de la constructibilidad de ciertas figuras geométricas con el uso exclusivo de regla (sin marcas para medir) y compás. Este problema, es decir, la pregunta acerca de cuáles figuras serían constructibles con regla y compás y cuáles no, fue introducido por los matemáticos griegos de la Antigüedad, al constatarse que eran infructuosos todos los intentos por construir con regla y compás la trisección de un ángulo arbitrario, la construcción de un cuadrado con igual área que un círculo dado, conocido como la cuadratura del círculo, y la duplicación del

cubo (construcción de un cubo con volumen igual al doble del volumen de uno dado). Muchas generaciones de matemáticos dedicaron su esfuerzo y su ingenio al intento de realizar estas construcciones, pero la imposibilidad de las mismas sólo pudo demostrarse con la intervención de herramientas algebraicas en el siglo XIX. Mostrar el poder de estas herramientas para la determinación de criterios de constructibilidad, es otro de los objetivos de estas notas.

Capítulo 1

Grupos

1.1. Definiciones básicas

En este primer capítulo haremos una presentación introductoria a la teoría de grupos, utilizando los grupos de permutaciones para ilustrar los aspectos básicos de esta teoría. Una de las razones para valernos del grupo de permutaciones de esta manera, es la dirección que llevaremos en el presente texto, que pretende ubicar al lector, una vez terminada su lectura, en una posición que le permita abordar el estudio de la Teoría de Galois, con las herramientas necesarias para ello. La otra razón, vinculada a la anterior, es la intención de aproximarnos en algún grado al modo histórico en el cual surgieron las ideas que condujeron al desarrollo posterior de la teoría.

Consideremos, entonces, el conjunto $A = \{x_1, x_2, x_3\}$, y definamos el conjunto

$$S_3 = \{f : A \longrightarrow A, \text{tal que } f \text{ es biyectiva}\}$$

La operación de composición de funciones en S_3 será la que dotará a este conjunto de la rica estructura que definiremos como grupo.

En primer lugar, recordemos que, como la composición de funciones biyectivas es biyectiva, la operación está bien definida en S_3, es decir, existe una función

$$\varphi : S_3 \times S_3 \longrightarrow S_3$$

definida por $\varphi(\alpha, \sigma) = \alpha \circ \sigma$.

En lo sucesivo, prescindiremos de la notación $\alpha \circ \sigma$ para denotar por $\alpha\sigma$ al elemento de S_3 que se obtiene de la composición de esas dos permutaciones.

Entre las propiedades básicas de esta operación, podemos observar las siguientes:

1. La composición de funciones es asociativa, en general, y por lo tanto, la operación que hemos definido en S_3 es asociativa.

2. La permutación identidad está en S_3, y constituye el elemento identidad de la operación composición.

3. Dada cualquier permutación α en S_3, dado que α es biyectiva, posee inversa, y además α^{-1} también está en S_3.

Es conveniente utilizar la siguiente notación, para representar una permutación σ en S_3: ya que el conjunto A se puede poner en biyección con $\{1, 2, 3\}$, podemos escribir $\sigma(i)$ en lugar de $\sigma(x_i)$, para $i = 1, 2, 3$, y así, representamos a σ por:

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$$

Ejemplo 1.1 *Si $\sigma \in S_3$ es tal que $\sigma(1) = 3$, $\sigma(2) = 1$ y $\sigma(3) = 2$, entonces representaremos a σ así:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Ejercicio

Utilice la notación sugerida arriba para escribir las 6 permutaciones de S_3. Operando con ellas, explore la conmutatividad de la operación definida en S_3. ¿Existen α y β en S_3 tales que $\alpha\beta \neq \beta\alpha$? ¿Existen α y β tales que $\alpha\beta = \beta\alpha$?

La no conmutatividad de la operación definida en S_3 podría interpretarse como una especie de carencia, y sin embargo, veremos más adelante la riqueza que adquiere la estructura de S_3 con la operación definida (y, en general, la estructura de todo conjunto de permutaciones con la operación de composición), justamente en virtud de la ausencia de conmutatividad.

Como mencionamos en la introducción, el trabajo de Evariste Galois en torno a las permutaciones del conjunto de raíces de un polinomio inició la

exploración de las propiedades de la estructura en cuestión, y varias décadas más tarde, Kronecker propuso la definición de grupo abstracto, a partir de las propiedades observadas en el grupo de permutaciones:

Definición 1.1 *Sea G un conjunto no vacío, dotado de una operación binaria, denotada por $(\cdot)$, se dice que $(G, \cdot)$ es un grupo si se satisfacen las siguientes condiciones:*

1. *Si $a, b, c \in G$ entonces $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
2. *Existe $e \in G$ tal que, para todo $a \in G$, $a \cdot e = e \cdot a = a$*
3. *Para todo $a \in G$, existe $b \in G$ tal que $a \cdot b = b \cdot a = e$*

Ejemplo 1.2 *Un primer ejemplo de grupo a mencionar, porque salta a la vista, es el siguiente:*

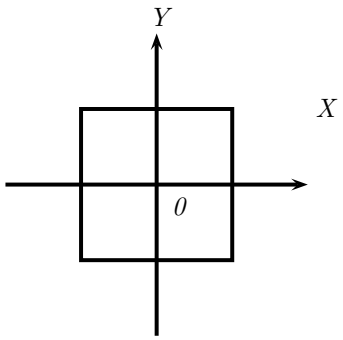
Si A es cualquier conjunto no vacío (no necesariamente finito) y $\mathcal{F}(A)$ es el conjunto de todas las biyecciones de A en A, entonces $(\mathcal{F}(A), \circ)$ es un grupo, donde el símbolo $\circ$ denota la composición de funciones.

Decíamos que salta a la vista, porque generaliza el caso de S_3.

En el caso en que A es un conjunto de n elementos, denotamos al grupo $\mathcal{F}(A)$ por S_n, y lo llamamos el grupo simétrico de grado n.

Ejemplo 1.3 *$(\mathbb{Z}, +)$, es decir, el conjunto de los números enteros, con la operación suma usual, es un grupo. La suma es, además, conmutativa; todos los grupos cuya operación sea conmutativa, son llamados abelianos, en honor a Niels Henrik Abel.*

Ejemplo 1.4 *Consideremos un cuadrado con centro en el origen de coordenadas del plano cartesiano, y sea $\mathcal{D}_4$ el conjunto de todas las isomterías del plano que dejan fijo al cuadrado. Estas son , en total, 8 aplicaciones: la identidad, 3 rotaciones y 4 simetrías.*



El lector puede demostrar, como ejercicio, que $\mathcal{D}_4$ es un grupo con la composición de funciones, determinando con precisión cuáles son los elementos de $\mathcal{D}_4$, y luego comprobando que, en efecto, la composición de funciones es cerrada, asociativa con elemento identidad. Se puede encontrar directamente el inverso de cada uno de los elementos de $\mathcal{D}_4$ para comprobar que la propiedad 3 de la definición dada también se satisface.

Ejemplo 1.5 *Sea $GL(n, \mathbb{R})$ el conjunto de todas las matrices $n \times n$, invertibles, con coeficientes en $\mathbb{R}$. Con el producto de matrices, $GL(n, \mathbb{R})$ es un grupo, llamado el Grupo Lineal General de orden n sobre $\mathbb{R}$. El lector puede probar esto como un ejercicio sencillo.*

En lo que sigue, al considerar un grupo $(G, \cdot)$ arbitrario, escribiremos simplemente G, y omitiremos el signo $(\cdot)$, incluso en la notación de la operación entre dos elementos de G: escribiremos ab en lugar de $a \cdot b$, si a y b son elementos de G.

Proposición 1.2 *Si G es un grupo, entonces se cumple lo siguiente:*

1. *El elemento identidad de G es único.*
2. *Para cada $a \in G$, el inverso de A es único. Se denotará el inverso de a por a^{-1}.*
3. *Para todo $a \in G$, $a = (a^{-1})^{-1}$.*
4. *Para $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

Prueba

1. Sean e_1, e_2 elementos en G tales que, para todo $g \in G$, $e_1 g = g e_1 = g$ y $e_2 g = g e_2 = g$.

   Como $e_1 g = g$ para cualquier $g \in G$, en particular vale para $g = e_2$. Así, $e_1 e_2 = e_2$. Análogamente, se prueba que $e_1 e_2 = e_1$, por lo que obtenemos $e_1 = e_2$.

2. Sea $a \in G$. Supongamos que existen $g_1, g_2 \in G$ tales que $a g_1 = g_1 a = e$ y $a g_2 = g_2 a = e$.

   Entonces, $a g_1 = a g_2$. Por lo tanto, operando con g_1 por la izquierda, en ambos miembros de la igualdad anterior, obtenemos $g_1(a g_1) = g_1(a g_2)$.

   Como la operación de G es asociativa, esta última igualdad equivale a

   $(g_1 a) g_1 = (g_1 a) g_2$, y como $g_1 a = e$, obtenemos $e g_1 = e g_2$, es decir, $g_1 = g_2$, lo que prueba la unicidad del inverso de a, el cual será denotado por a^{-1}.

3. Para ver que $(a^{-1})^{-1} = a$, basta con observar que $a a^{-1} = a^{-1} a = e$. Como, por la parte 2, el inverso de a^{-1} es único, concluimos que a es precisamente el inverso de a^{-1}, lo que buscábamos probar.

4. Sean $a, b \in G$.

   $$(ab)(b^{-1} a^{-1}) = a(b b^{-1}) a^{-1} = a(e a^{-1}) = a a^{-1} = e$$

   De nuevo, por la unicidad del inverso de ab, concluimos que $(ab)^{-1} = b^{-1} a^{-1}$.

■

Utilizaremos la notación a^n para denotar el producto de a por sí mismo, n veces, para $n > 0$. Si $n = 0$, se define $a^0 = e$. Para $n < 0$, se define a^n como $(a^{-1})^{-n}$.

La notación establecida arriba merece una aclaratoria:

Si $a \in G$, y $0 < n \leq 3$, no hay ambigüedad alguna en el significado de a^n, en virtud de la asociatividad de la operación definida en G.

Ejercicio
Para $n > 3$, demuestre que tampoco hay ambigüedad, es decir, que

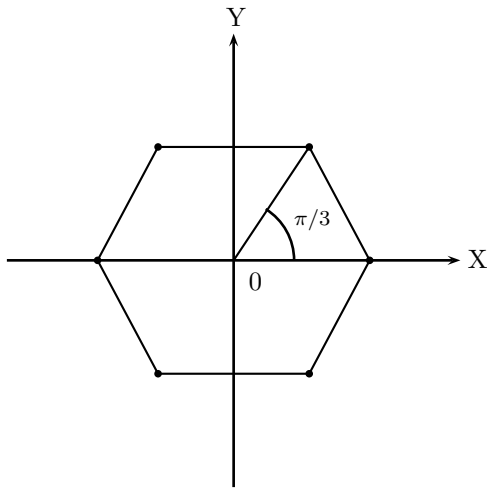
$$a(a^{n-1}) = a^2a^{n-2} = ... = a^{n-1}a$$

Si se trata de un grupo abeliano, con frecuencia se utiliza el signo $(+)$ para denotar la operación del grupo; $-a$ denota el inverso de a y na denota la suma $a+a+...+a$, n veces, para $n > 0$. Para $n < 0$, $na = (-a)+(-a)+...+(-a)$, n veces. Suele denotarse el elemento identidad del grupo por 0, advirtiendo el cuidado que debe tenerse de no confundir a este elemento con el $0 \in \mathbb{Z}$, en expresiones como $0(a) = 0$. Aquí, el 0 del miembro izquierdo de la igualdad es el número entero, mientras que el del miembro derecho es el elemento identidad que está en $(G, +)$.

Ejercicio
Pruebe que si G es un grupo, vale la ley de cancelación por la derecha y por la izquierda en G, es decir, si $a, b, c \in G$ y $ab = ac$, entonces $b = c$; por otra parte, si $ab = cb$, entonces $a = c$.

Examinemos ahora un grupo particular que pertenece a una clase especial, y muy importante, de grupos: los grupos cíclicos.

Consideremos un hexágono regular con centro en el origen de coordenadas del plano cartesiano, y sea α la rotación del plano (en sentido contrario al de las agujas del reloj) de $\frac{\pi}{3}$ radianes.



Sea $G = \{e, \alpha, \alpha^2, ..., \alpha^5\}$.

Aquí, e es la rotación por el ángulo 0, y las potencias de α indican la composición de la rotación α consigo misma, de manera que $\alpha^2 = \frac{2\pi}{3}$, $\alpha^3 = \pi$, etc.

Es claro que G está constituido por rotaciones del plano que preservan el hexágono, en el sentido de que envían vértices a vértices. Más aún, observemos que toda rotación del plano que preserve el hexágono es de un ángulo de la forma $\frac{k\pi}{3}$, y que dos de estas rotaciones, digamos, $\frac{k_1\pi}{3}$ y $\frac{k_2\pi}{3}$ son equivalentes (tienen el mismo efecto sobre las figuras del plano) si $k_1 \equiv k_2 \text{mod } 6$. En virtud de esta observación, concluimos que G contiene a todas las rotaciones no equivalentes que preservan el hexágono.

Dejamos como ejercicio para el lector demostrar que G, con la composición de funciones, es un grupo, si identificamos las rotaciones equivalentes.

La particularidad de G que queremos resaltar en este momento es que todos sus elementos se pueden expresar como potencias de un elemento del grupo. Esta propiedad es la que define a los grupos cíclicos.

Definición 1.3 *Se dice que el grupo $G \neq \{e\}$ es cíclico si existe $a \in G$ tal que $G = \{a^j : j \in \mathbb{Z}\}$. En este caso, se dice que G es generado por a, o que a es un generador de G, y se denota: $G = (a)$.*

Si un grupo G es finito, se denomina orden de G a su cardinalidad, y se denota $o(G)$.

A continuación, mostramos la tabla de multiplicación de un grupo de 4 elementos, denominado el Grupo de Klein, en honor al matemático, eminente geómetra y maestro Felix Klein (1849-1925):

•	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

En la tabla, el elemento que aparece en la fila i, columna j, del arreglo interior de la tabla, corresponde al resultado de multiplicar al elemento de la fila i de la columna exterior y a la izquierda del arreglo, con el elemento de la columna j de la fila exterior y superior al arreglo, en ese orden.

Ejercicios

1. Verificar que el conjunto $G = \{e, a, b, c\}$ con la operación indicada en la tabla, es, en efecto, un grupo, que además es abeliano.

2. Elabore todas las posibles tablas de multiplicación de grupos de orden 2 y 3 respectivamente. Elabore una conclusión acerca de la existencia de grupos cíclicos de orden 2 y 3.

3. Investigue acerca de la existencia de grupos cíclicos de orden 4.

Es importante observar que un grupo cíclico de orden n, para cualquier $n \in \mathbb{N}, n > 2$ puede construirse, sencillamente estableciendo

$$G = \{a^0 = e, a, a^2, ..., a^{n-1}\}$$

y agregando la condición : $a^n = a^0 = e$.

Para construir un grupo cíclico infinito, basta con definir

$$G = \{a^i : i \in \mathbb{Z}\}$$

donde $a^0 = e$, y estableciendo la condición adicional: $a^i \neq a^j$, si $i \neq j$.

Se deja como ejercicio para el lector verificar que, en ambos casos, G es un grupo.

Problemas:

1. Demuestre que, si G es un grupo finito, en cada fila de la tabla de multiplicación de G aparece cada elemento de G una sola vez, e igualmente ocurre con cada columna de la tabla.

2. Pruebe que $(\mathbb{Z}, +)$ es un grupo cíclico.

3. Pruebe que, si G es un grupo y $o(G)$ es par, entonces existe $a \in G$, $a \neq e$, tal que $a^2 = e$.

4. Sea G un conjunto finito, con una operación asociativa $(\cdot)$, respecto a la cual G es cerrado; si las dos leyes de cancelación se verifican en G, pruebe que G es un grupo.

5. Si G es un grupo finito, pruebe que existe un entero positivo N tal que, para todo $a \in G$, $a^N = e$.

6. Sea G un grupo, y $a \in G$. Si existe $n \in \mathbb{N}$ tal que $n = min\{k \geq 1 : a^k = e\}$, entonces se dice que n es el orden de a, y se escribe $o(a) = n$. Pruebe que si $o(G) = n$ y existe $a \in G$ tal que $o(a) = n$, entonces G es cíclico.

7. Pruebe que, si G es un grupo abeliano, entonces para todo $a, b \in G$, y para todo $n \in \mathbb{N}$, se cumple que $(ab)^n = a^n b^n$.

8. Pruebe que, si G es un grupo y para todo $a, b \in G$ se cumple $(ab)^2 = a^2 b^2$ entonces G es abeliano. Dé un ejemplo en S_3 de dos elementos α, β tales que $(\alpha\beta)^2 \neq \alpha^2\beta^2$.

9. Si G es un grupo y para todo $a \in G$ se tiene que $a = a^{-1}$, pruebe que G es abeliano.

10. Pruebe que, si $n > 1$, entonces el conjunto $\mathbb{Z}_n$ de las clases de congruencia de los enteros módulo n es un grupo abeliano con la operación suma definida como:
$$\bar{j} + \bar{k} = \overline{j + k}$$
tomando en cuenta que $\overline{j + k} = \overline{j + k - n}$ siempre que $j + k > n - 1$, donde $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$.

11. Asigne V (verdadero) o F (falso) a cada una de las siguientes afirmaciones:

    a) Si un grupo G es de orden menor o igual que 4, G es abeliano.

    b) Todo grupo cíclico es abeliano.

    c) Todo grupo abeliano es cíclico.

    d) No existe ningún grupo de orden 1.

1.2. Subgrupos

La noción de subgrupo es de fundamental importancia en el desarrollo de la Teoría de Grupos, tal como la de subespacio vectorial lo es en el estudio de los espacios vectoriales en el contexto del Álgebra Lineal. En particular, la noción de subgrupo constituyó una herramienta clave para las construcciones realizadas por Galois en su trabajo sobre la solubilidad por radicales de ecuaciones polinómicas.

Definición 1.4 *Sea G un grupo y $H \subset G$. H es un subgrupo de G (se denotará $H < G$) si H es un grupo con la operación que hace de G un grupo.*

Si G es un grupo, entonces G y $\{e\}$ son, claramente, subgrupos de G, llamados los subgrupos triviales de G.

En cada uno de los ejemplos siguientes, el lector puede verificar que $H < G$.

Ejemplo 1.6 *Si $G = S_3$, definimos $H = \{\sigma \in S_3 : \sigma(2) = 2\}$.*

Ejemplo 1.7 *Para $G = \mathbb{Z}$, con la suma usual, y $n \in \mathbb{N}$, definimos $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.*

Ejemplo 1.8 *Sea G un grupo, y $a \in G$ tal que $o(a) = m > 1$; definamos $H = \{a^j : 0 \leq j \leq m-1\}$. H se denomina el subgrupo cíclico de G generado por a.*

Ejemplo 1.9 *Sea $n \in \mathbb{N}, n > 1$, $G = GL(n, \mathbb{R})$, y*

$$H = SL(n, \mathbb{R}) = \{M \in G : detM = 1\}$$

H se denomina el grupo especial lineal.

Ejemplo 1.10 *Sea $G = S_4$; supongamos que etiquetamos cada vértice del cuadrado centrado en el origen de coordenadas del plano cartesiano con los números $1, 2, 3, 4$. Sea $H = D_4$, el grupo de las isometrías que dejan fijo al cuadrado. Como cada isometría tiene el efecto de una permutación de S_4 sobre los vértices del cuadrado, podemos considerar a H como subconjunto de S_4. Claramente, $H < S_4$.*

Ejemplo 1.11 *Si $G = S_6$, podemos numerar, como en el ejemplo anterior, los vértices de un hexágono con centro en el origen de coordenadas, y considerar el efecto de permutación sobre los vértices que tienen las isometrías del hexágono. Sea J el conjunto de las rotaciones que dejan fijo al hexágono ; si denotamos por I al conjunto de las isometrías que dejan fijo al hexágono, entonces $J < I < S_6$.*

Ejemplo 1.12 *Si V es un espacio vectorial sobre $\mathbb{R}$, entonces V es un grupo abeliano con la operación de la suma de vectores. Si S es un subespacio vectorial de V, entonces S es un subgrupo de V.*

A continuación, veremos ciertos criterios que permiten determinar si un subconjunto de un grupo G es un subgrupo.

Proposición 1.5 *Sea G un grupo; sea $H \subset G$, $H \neq \emptyset$. H es un subgrupo de G si y sólo si H satisface las siguientes condiciones:*

1. *Si $x, y \in H$, entonces $xy \in H$.*
2. *Si $x \in H$, entonces $x^{-1} \in H$.*

Prueba

Está claro que si H es un subgrupo de G, entonces se satisfacen las condiciones 1 y 2. Supongamos ahora que $H \subseteq G$, $H \neq \emptyset$, y que se satisfacen las condiciones 1 y 2.

Basta comprobar que el producto en H es asociativo y que el elemento identidad de G está en H, para concluir que $H < G$.

El producto de G es asociativo, y $H \subseteq G$, por lo que el producto es asociativo en H también.

Finalmente, como $H \neq \emptyset$, podemos seleccionar $x \in H$. En virtud de (2), $x^{-1} \in H$, y por (1), $xx^{-1} = e \in H$. ■

Ejercicio

Pruebe que, si H y K son subgrupos de un grupo G, entonces $H \bigcap K < G$, usando la proposición anterior. Sea I un conjunto de índices arbitrario. Si $K_\lambda, \lambda \in I$ es una familia de subgrupos de G, muestre que $\bigcap_{\lambda \in I} K_\lambda$ es un subgrupo de G.

Si un grupo G es finito, basta con que $H \subseteq G$, $H \neq \emptyset$, cumpla la condición (2) de la proposición anterior, para que se pueda asegurar que $H < G$. Este resultado, bastante asombroso, revela de alguna manera la naturaleza de los grupos finitos, los cuales han sido objeto de investigación extensa durante el S.XX.

Proposición 1.6 *Sea G un grupo finito. Si $H \subseteq G$, $H \neq \emptyset$, y H es cerrado con respecto al producto en G, entonces $H < G$.*

Prueba

Sea G un grupo finito, y H un conjunto que satisface las condiciones de la hipótesis de la Proposición. En virtud de la Proposición 1.5, bastará con verificar que, si $a \in H$, a^{-1} también está en H.

Sea $a \in H$. Consideremos el conjunto

$$S = \{a^i : i \in \mathbb{N}, i \geq 1\}$$

Como H es cerrado respecto al producto en G, $S \subseteq G$; además, S es finito porque H es finito, por lo tanto existen enteros $i, j \in \mathbb{N}$, $i \neq j$, tales que $a^i = a^j$. (De otro modo, S sería infinito). Supongamos que $i > j$. En vista de que $a^i = a^j$, tenemos que $a^{i-j} = e$. Si $i - j = 1$, tendríamos que $a = e$, y en ese caso, $a^{-1} = e$, y por lo tanto $a^{-1} \in H$, que es lo que buscamos probar.

De otro modo, sería $i - j > 1$, ó, equivalentemente, $i - j - 1 > 0$; por definición de S, $a^{i-j-1} \in S$, pero $a^{i-j-1} = ea^{-1} = a^{-1}$, es decir, $a^{-1} \in S$. Así, $a^{-1} \in H$. ■

Dado un subconjunto cualquiera J de un grupo G, es evidente que J no necesariamente será un subgrupo de G. Muchas veces resulta interesante

poder determinar el menor subgrupo de G que contiene a J. La noción de menor subgrupo es la asociada a la contención de conjuntos: H es el menor subgrupo de G que contiene a J si, dado cualquier subgrupo K de G tal que $J \subset K$, se tiene que $H \subset K$. En otras palabras, H se obtiene al agregar a J lo mínimo indispensable para obtener un subgrupo de G. Esta idea es la que subyace a la siguiente definición:

Definición 1.7 *Sea G un grupo , $J \subset G$, $J \neq \emptyset$ y $H < G$. Se dice que H es el subgrupo de G generado por J si $J \subset H$ y para todo subgrupo K de G, tal que $J \subset K$, se cumple que $H \subset K$. Se denotará por $(J) = H$. Si $J = \{a\}$, escribiremos $(a) = H$ en lugar de $(\{a\}) = H$.*

Ahora bien, cabe preguntarse cuáles serían las vías para determinar, en la práctica, el subgrupo generado por un subconjunto J de un grupo G.

Si tomamos, por ejemplo, el subconjunto $J = \{\sigma\}$ de S_3, donde $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Claramente, todas las potencias de σ deben estar en (σ). Como $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ y $\sigma^3 = e$, tenemos que (σ) contiene al conjunto $\{e, \sigma, \sigma^2\}$. El lector puede verificar que, en realidad,
$(\sigma) = \{e, \sigma, \sigma^2\}$. En otras palabras, que el conjunto $\{e, \sigma, \sigma^2\}$ es un subgrupo de S_3, y además es el menor subgrupo que contiene a σ, lo cual hace que la notación introducida en la Definición 1.3 se refiere a un caso particular de la notación presentada en la Definición 1.7.

Supongamos ahora que G es un grupo cualquiera y que $J = \{a, b\}$, donde $a^n \neq b, a \neq b^n, \forall n \in \mathbb{Z}$ y $a \neq e, b \neq e$. Si queremos determinar el subgrupo (J), podemos comenzar por incluir en este subgrupo a todas las potencias de a y de b, además de todos los productos de estas potencias ; en otras palabras,

$$\{a^{i_1} b^{j_1} a^{i_2} b^{j_2} \cdots a^{i_r} b^{j_r} : i_k, j_k \in \mathbb{Z}, k = 1, \ldots, r\} \subseteq (J)$$

El lector puede comprobar que la anterior contención es, en realidad, una igualdad.

Estos preámbulos conducen naturalmente a la siguiente caracterización de la noción de subgrupo generado por un subconjunto cualquiera de un grupo.

Proposición 1.8 *Sea G un grupo y $J \subset G, J \neq \emptyset$. Son equivalentes:*

1. $(J) = H$
2. $H = \bigcap_{K \in \mathcal{S}} K$, *donde* $\mathcal{S} = \{K < G : J \subset K\}$
3. $H = \{a_1^{m_1} a_2^{m_2} ... a_r^{m_r} : r \in \mathbb{N}, a_i \in J, m_i \in \mathbb{Z}, \text{para } 1 \leq i \leq r\}$

Prueba

Veamos que (1) $\Rightarrow$ (2): Supongamos que $H = (J)$. Entonces $H < G$ y $J \subset H$, luego $H \in \mathcal{S}$, y por lo tanto $\bigcap_{K \in \mathcal{S}} K \subset H$. Ahora bien, en un ejercicio anterior se plantea la prueba de que la intersección arbitraria de subgrupos de un grupo G es un subgupo de G. Por lo tanto, $\bigcap_{K \in \mathcal{S}} K$ es un subgrupo de G, ya que la familia $\mathcal{S}$ es no vacía, puesto que $G \in \mathcal{S}$. Denotemos a ese subgrupo, resultado de la intersección mencionada, por $\mathcal{S}_J$. Además, $J \subset \mathcal{S}_J$, y por definición del subgrupo H generado por J, se tiene que $H \subset \mathcal{S}_J$. Así, obtenemos que $H = \bigcap_{K \in \mathcal{S}} K$.

(2) $\Rightarrow$ (1):

Supongamos que $H = \bigcap_{K \in \mathcal{S}} K$. Como vimos antes, esto implica que $H < G$ y, por definición de $\mathcal{S}$, $J \subset H$. Ahora bien, si $M < G$ y $J \subset M$, $M \in \mathcal{S}$, por lo cual necesariamente $H \subset M$, y esto significa que $H = (J)$.

(1) $\Rightarrow$ (3):

Sea $H = (J)$, y sea

$$M = \{a_1^{m_1} a_2^{m_2} ... a_r^{m_r} : r \in \mathbb{N}, a_i \in J, m_i \in \mathbb{Z}, \text{para } 1 \leq i \leq r\}$$

Veamos que $J \subset M$ y $M < G$; como, por definición de $H = (J)$ se deduciría que $H \subset M$, si probamos además que $M \subset H$, quedaría probado que $M = H$.

Si $a \in J$, por definición de M, tenemos que $a = a^1 \in M$; así que $J \subset M$.

Por otra parte, para ver que $M < G$, usaremos la Proposición 1.5. En primer lugar, $M \neq \emptyset$ porque $J \neq \emptyset$ y $J \subset M$. Sean $x, y \in M$, es decir, $x = a_1^{m_1} a_2^{m_2} ... a_r^{m_r}$ y $y = b_1^{n_1} ... b_t^{n_t}$, para ciertos $a_i, b_j \in J$, y ciertos $m_i, n_j \in \mathbb{Z}$. Entonces,

$$xy = a_1^{m_1} a_2^{m_2} ... a_r^{m_r} b_1^{n_1} ... b_t^{n_t}$$

Es decir, xy es un producto finito de potencias enteras de elementos de J, y por definición de M, $xy \in M$.

Finalmente, si $x = a_1^{m_1} a_2^{m_2} ... a_r^{m_r}$, entonces $x^{-1} = a_r^{-m_r} ... a_2^{-m_2} a_1^{-m_1}$ y de nuevo, por definición de M, $x^{-1} \in M$. Así. $M < G$.

Falta ver sólo que $M \subset H$. Sea $x = a_1^{m_1} a_2^{m_2} ... a_r^{m_r} \in M$. Como $J \subset H$ y $a_i \in J$, $\forall i$, tenemos que $a_i^{m_i} \in H$, $\forall i$, puesto que $H < G$. Más aún, siendo $H < G$, el producto de todas estas potencias de elementos de J, está en H, es decir, $x \in H$.

Podemos, entonces, concluir que $M = H$.

(3) $\Rightarrow$ (1):

Ya vimos que, si

$$H = \{a_1^{m_1} a_2^{m_2} ... a_r^{m_r} : r \in \mathbb{N}, a_i \in J, m_i \in \mathbb{Z}, \text{para } 1 \leq i \leq r\}$$

entonces $H < G$. Además, $J \subset H$. Por definición de (J), se obtiene que $(J) \subset H$. Por otra parte, todo subgrupo de G que contiene a J, contiene a H, y por lo tanto, $H \subset \bigcap_{K \in \mathcal{S}} K = (J)$. Así, $H = (J)$ ■

Ejercicio

Suponga que se considera a $(\mathbb{R}^2, +)$ como grupo abeliano, sin la multiplicación por escalares en $\mathbb{R}$ que le da la estructura de espacio vectorial. Determine el subgrupo generado por el conjunto de vectores $J = \{(1, 0), (0, 1)\}$.

Consideremos ahora el grupo abeliano $(\mathbb{Z}, +)$ y el subgrupo $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$. Asociado a $3\mathbb{Z}$ está el grupo $\mathbb{Z}_3$ constituido por las clases de congruencia módulo 3:

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

Sabemos que $\bar{0}$ representa la clase de todos los enteros múltiplos de 3, es decir, el subgrupo $3\mathbb{Z}$; por otra parte, $\bar{1}$ representa la clase de todos los enteros cuyo resto al dividirse entre 3 es igual a 1, lo cual podría expresarse como

$$3\mathbb{Z} + 1 = \{3k + 1 : k \in \mathbb{Z}\}$$

y , análogamente, $\bar{2}$ representa el siguiente subconjunto de $\mathbb{Z}$:

$$3\mathbb{Z} + 2 = \{3k + 2 : k \in \mathbb{Z}\}$$

Otra manera de asociar a estas clases de congruencia con $3\mathbb{Z}$, la obtenemos de la siguiente observación (que por lo general se establece como definición de la relación de congruencia módulo 3):

Dos enteros m, n son congruentes módulo 3 (y por lo tanto están en la misma clase de congruencia) si, y sólo si, $m - n \in 3\mathbb{Z}$.

Esta construcción de una relación de equivalencia en el grupo $\mathbb{Z}$, y de sus correspondientes clases de equivalencia, asociadas a un subgrupo de $\mathbb{Z}$ (construcción que vale para cualquier subgrupo de $\mathbb{Z}$) se generaliza a un grupo arbitrario G, a partir de cualquier subgrupo H , no trivial, de G:

Definición 1.9 *Sea $H < G$, H no trivial, y definamos la siguiente relación en G: dados $x, y \in G$, decimos que x está relacionado con y módulo H, y escribimos $x \sim_H y$, si, y sólo si, $xy^{-1} \in H$.*

Proposición 1.10 *Sea G un grupo, $H < G$. La relación módulo H sobre G es una relación de equivalencia y las clases de equivalencia correspondientes son de la forma $\bar{x} = Hx$.*

Prueba

Veamos que la relación módulo H definida sobre G es de equivalencia.

1. Reflexividad:

   Sea $x \in G$. Como $xx^{-1} = e \in H$, por ser $H < G$, tenemos que $x \sim_H x$.

2. Simetría

   Supongamos que $x, y \in G$ son tales que $x \sim_H y$, y por lo tanto, $xy^{-1} \in H$. Como $H < G$, $(xy^{-1})^{-1} \in H$, es decir, $(y^{-1})^{-1}x^{-1} = yx^{-1} \in H$; esto significa que $y \sim_H x$.

3. Transitividad

   Supongamos que $x, y, z \in G$, que $x \sim_H y$ y $y \sim_H z$. Así, $xy^{-1}, yz^{-1} \in H$, y por ser $H < G$, tenemos que $(xy^{-1})(yz^{-1}) = xz^{-1} \in H$; luego $x \sim_H z$.

Para comprobar que las clases de equivalencia de esta relación son de la forma Hx, observemos que

$$x \sim_H y \iff xy^{-1} \in H \iff xy^{-1} = h$$

para algún $h \in H$. Luego, $x = hy$ lo que significa que $x \in Hy = \{gy : g \in H\}$. Es decir,

$$Hy = \{v \in G : v \sim_H y\} = \bar{y}$$

Las clases Hy, con $y \in G$, son llamadas clases laterales derechas de H en G.

Esto fue lo que obtuvimos en el caso de las clases de congruencia módulo 3 en $\mathbb{Z}$: para cada $n \in \mathbb{Z}$, existe $i \in \mathbb{Z}$ tal que $0 \leq i \leq 2$, y n es congruente con i módulo 3. Por lo tanto, $\bar{n} = \bar{i} = 3\mathbb{Z} + i$

■

Veamos ahora un ejemplo en el caso no abeliano:

Sea $G = S_3$ y sea $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Sea $H = (\alpha) = \{e, \alpha, \alpha^2\}$.

Veamos cuáles son las clases de equivalencia módulo H. Como estas son de la forma Hx con $x \in S_3$, tenemos que, para $x = e, Hx = He = H$, y además, para todo $h \in H$, $Hh = H$. De modo que el mismo subgrupo H es siempre una de las clases de equivalencia.

Tomemos ahora un elemento $\beta \notin H$. Por ejemplo, sea $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

La clase de β es

$$H\beta = \{h\beta : h \in H\} = \{\beta, \alpha\beta, \alpha^2\beta\}$$

El lector puede comprobar con facilidad que $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, y que $\alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Así, las dos clases laterales derechas de H en S_3 son:

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

y

$$H\beta = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

La relación de congruencia módulo H se pudo haber definido sobre el grupo G de la manera siguiente:

$$\forall x, y \in G, x \sim_H y \iff x^{-1}y \in H$$

Es fácil ver que esta relación produce clases laterales izquierdas de la forma $\bar{x} = xH, \forall x \in G$.

Ejercicio

Calcule las clases laterales izquierdas de H en S_3, donde $H = (\alpha)$ y $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Acabamos de ver, en el ejemplo anterior, que, tanto H como $H\beta$ tienen 3 elementos. Esto (la igualdad entre las cardinalidades de las distintas clases laterales derechas) es un fenómeno general que no depende del grupo particular considerado.

Lema 1.11 *Sea G un grupo y $H < G$. Si Ha y Hb son dos clases laterales derechas de H en G, entonces existe una biyección*
$\varphi : Ha \longrightarrow Hb$.

Prueba

Sea $\varphi : Ha \longrightarrow Hb$, definida por $\varphi(ha) = hb$, para todo $h \in H$.

φ es inyectiva, porque si $h, g \in H$ son tales que $\varphi(ha) = \varphi(ga)$, entonces $hb = gb$ y por la ley de cancelación, obtenemos $h = g$.

φ es sobreyectiva porque si $hb \in Hb$, como $h \in H$, se tiene que $ha \in Ha$ y $\varphi(ha) = hb$ ■

El lema anterior tiene consecuencias muy importantes, especialmente cuando el grupo G es finito.

Una de ellas es el famoso Teorema de Lagrange, el cual fue obtenido por este matemático francés, a fines del siglo XVIII, cuando exploraba los grupos de permutaciones de las raíces de un polinomio, en la búsqueda de un método general para encontrar la fórmula que resolviese la ecuación polinómica de grado 5.

Teorema 1.12 *(Teorema de Lagrange)*

Si G es un grupo finito y $H < G$, entonces $o(H)|o(G)$.

Prueba

Supongamos que $o(G) = n$ y $o(H) = k$. Como $G = \bigcup_{a \in G} Ha$, y las clases Ha constituyen una partición de G, tenemos que $o(G) = n = \sum_{a \in G} |Ha|$, donde la suma se toma contando cada clase Ha una sola vez.

Pero por el lema anterior, $|Ha| = o(H)$, $\forall a \in G$; así
$o(G) = n = j(o(H))$, donde j es el número de clases de congruencia módulo H distintas que hay en G.

■

Cuando G es finito y $H < G$, llamamos índice de H en G, y lo denotamos por $i_G(H)$, al número de clases laterales derechas distintas de H que hay en G . Por el Teorema de Lagrange, tenemos que $i_G(H) = \frac{o(G)}{o(H)}$.

Hemos visto ejemplos de elementos en los grupos de permutaciones y los de las isometrías, que tienen la propiedad de que , al elevarse a una cierta potencia, se obtiene el elemento identidad del grupo.

Es el caso de la rotación por el ángulo $\frac{\pi}{3}$ en el grupo $\mathcal{D}_6$ de las isometrías que fijan al hexágono. Sabemos que, si llamamos α a esta rotación, α^6 es la rotación por el ángulo $6\frac{\pi}{3} = 2\pi$, que es la identidad del grupo.

Ahora bien, $\alpha^6 = e$ implica que $\alpha^{6k} = (\alpha^6)^k = e^k = e$, $\forall k \in \mathbb{Z}$, y así, todos los exponentes que sean múltiplos de 6 tienen el mismo efecto sobre α. Además, la menor potencia de α que es igual a la identidad es 6. Esta situación motiva la siguiente definición:

Definición 1.13 *Sea G un grupo y $a \in G$, $a \neq e$. El menor entero positivo n tal que $a^n = e$ es llamado el orden de a. Si no existe $n > 0$ tal que $a^n = e$, se dice que el orden de a es infinito.*

Ejemplo 1.13 *Si $\beta \in \mathcal{D}_6$ es la rotación por el ángulo $\frac{2\pi}{3}$, entonces el orden de β es 3, pues $\beta^3 = e$, y si $0 < k < 3$, $\beta^k \neq e$.*

Ejemplo 1.14 *Si $n \in \mathbb{Z}$, $n \neq 0$, entonces el orden de n es infinito, pues para todo $k > 0$, $kn \neq 0$.*

Ejemplo 1.15 *En $\mathbb{Z}_5$, el orden de $\bar{2}$ es igual a 5, pues $5(\bar{2}) = \bar{10} = \bar{0}$ y si $0 < k < 5$, $k(\bar{2}) \neq \bar{0}$.*

En la siguiente proposición se establece la igualdad entre el orden de un elemento a de un grupo G y el orden del subgrupo cíclico (a) generado por a. Esto justificará el uso de la notación $o(a)$, tanto para referirnos al orden del elemento a, como al orden del subgrupo (a).

Proposición 1.14 *Si G es un grupo finito, y $a \in G$, $a \neq e$, entonces el orden de a es finito y coincide con $o(a)$, el orden del subgrupo de G generado por a.*

Prueba

Si $a \in G$, $a \neq e$, y tiene orden infinito, entonces $\forall n > 0$, $a^n \neq e$; esto implica que si $i, j \in \mathbb{Z}$, $i \neq j$, entonces $a^i \neq a^j$, pues si $a^i = a^j$, y, digamos, $j > i$, entonces $a^{j-i} = e$, y siendo $j - i > 0$ estaríamos contradiciendo el hecho de que a tiene orden infinito.

Así, el subgrupo generado por a, que es $(a) = \{a^i : i \in \mathbb{Z}\}$, resulta ser infinito, lo cual es imposible, siendo G finito y $(a) < G$.

Por lo tanto, a tiene orden finito. Supongamos que el orden de a es $r > 0$.

Veremos ahora que, si el orden del subgrupo (a) es igual a n, entonces $n = r$.

En primer lugar, observemos que, si $j, k \in \{0, ..., r-1\}$, y $j \neq k$, digamos, $j > k$, entonces $a^j \neq a^k$, pues de lo contrario tendríamos $a^{j-k} = e$ con $0 < j - k < r$, lo cual contradice el hecho de ser r el orden de a. Luego, el conjunto $P = \{e, a, a^2, ..., a^{r-1}\}$ tiene exactamente r elementos. Ahora veremos que $P = (a)$, con lo cual habremos concluido que $n = r$.

Por un lado, $P \subseteq (a)$ por definición de (a), y, para ver que $(a) \subset P$, consideremos un elemento $g \in (a)$. Por definición de (a), sabemos que existe $i \in \mathbb{Z}$ tal que $g = a^i$.

Tenemos dos posibilidades:

1. $0 \leq i < r$:

   En este caso, $a^i \in P$ por definición de P.

2. $i < 0$ ó $i \geq r$:

   En cualquiera de estos casos, por el algoritmo de la división , tenemos que $i = kr + j$ para ciertos $k, j \in \mathbb{Z}$, con $0 \leq j < r$, y así,

   $$a^i = a^{kr+j} = a^{kr}a^j = (a^r)^k a^j = e^k a^j = a^j$$

   Es decir, existe j tal que $0 \leq j < r$ y $j \equiv i$ módulo r, y tal que $a^i = a^j$. Por lo tanto, $a^i \in P$. Esto implica que $(a) \subseteq P$. Concluimos así que $P = (a)$ y por lo tanto, $n = r$.

■

Corolario 1.15 *Si G es un grupo finito y $a \in G$, $a \neq e$, entonces el orden de a divide a $o(G)$.*

Prueba

Como el orden de a es igual a $o(a)$, y por el teorema de Lagrange sabemos que $o(a) \mid o(G)$, se deduce de inmediato el corolario ■

Corolario 1.16 *Si G es un grupo finito y $a \in G$, entonces $a^{o(G)} = e$.*

Prueba

Como $o(G) = o(a)k$ para algún $k \in \mathbb{N}$, tenemos que $a^{o(G)} = (a^{o(a)})^k = e^k = e$ ■

Corolario 1.17 *Si G es un grupo finito y $o(G) = p$, p primo, entonces G es cíclico.*

La prueba se deja como ejercicio para el lector.

Problemas

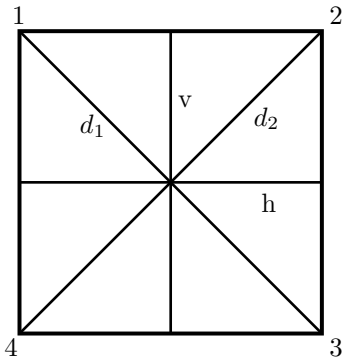
1. Pruebe que si $H \subset \mathbb{Z}$, entonces $H < \mathbb{Z} \iff H = n\mathbb{Z}$ para algún $n \in \mathbb{Z}$.

2. Sea $n \in \mathbb{Z}$. Determine el subgrupo de $\mathbb{Z}$ generado por n.

3. Pruebe que si G es un grupo, $H \subset G$, $H \neq \emptyset$ y se cumple que $\forall x, y \in H$, $xy^{-1} \in H$, entonces $H < G$.

4. Considere el grupo $\mathcal{D}_4$ de las isometrías que dejan fijo al cuadrado. Colocando etiquetas a los vértices del cuadrado con los números del 1 al 4, identifique, como en un ejercicio previo, cada isometría α de $\mathcal{D}_4$ con la permutación de S_4 que corresponde a la acción de α sobre el conjunto $\{1, 2, 3, 4\}$.

   Denotemos las 4 reflexiones sobre los ejes de la siguiente manera: horizontal (h), vertical (v) y diagonales (d_1 y d_2), como en la figura siguiente:



A continuación, presentamos la tabla de multiplicación de $\mathcal{D}_4$, para facilitar los cálculos.

$\bullet$	e	$\pi/2$	π	$3\pi/2$	d_1	d_2	v	h
e	e	$\pi/2$	π	$3\pi/2$	d_1	d_2	v	h
$\pi/2$	$\pi/2$	π	$3\pi/2$	e	h	v	d_1	d_2
π	π	$3\pi/2$	e	$\pi/2$	d_2	d_1	h	v
$3\pi/2$	$3\pi/2$	e	$\pi/2$	π	v	h	d_2	d_1
d_1	d_1	v	d_2	h	e	π	$\pi/2$	$3\pi/2$
d_2	d_2	h	d_1	v	π	e	$3\pi/2$	$\pi/2$
v	v	d_2	h	d_1	$3\pi/2$	$\pi/2$	e	π
h	h	d_1	v	d_2	$\pi/2$	$3\pi/2$	π	e

Tabla de multiplicación para D_4

a) Determine el subgrupo $H = (d_1, d_2)$, generado por las reflexiones sobre las diagonales.

b) Encuentre las clases laterales derechas de H en $\mathcal{D}_4$.

5. Pruebe que, si p es primo y $a \in \mathbb{Z}_p$ entonces $o(a) = p$.

6. Sea H subgrupo de un grupo G. Pruebe que hay una correspondencia biyectiva entre el conjunto de las clases laterales derechas de H en G y el de las clases laterales izquierdas de H en G.

7. Pruebe que si un grupo G no tiene subgrupos distintos de los triviales, entonces G debe tener orden primo.

8. Sean $n, m \in \mathbb{Z}$, $n \neq m$. Determine $n\mathbb{Z} \bigcap m\mathbb{Z}$.

9. Si G es un grupo, se define el centro de G por

$$Z(G) = \{z \in G : xz = zx, \text{para todo } x \in G\}$$

Pruebe que $Z(G) < G$.

10. Sea G un grupo cíclico. Pruebe que si $H < G$ entonces H es cíclico.

11. Sea G un grupo cíclico de orden n. Determine el conjunto $\{g \in G : (g) = G\}$.

12. Sea G un grupo y $a \in G$ tal que $a^m = e$. Pruebe que $o(a) \mid m$.

1.3. Subgrupos Normales y Grupo Cociente

Hemos visto que, dado un grupo G y $H < G$, se establece una biyección entre el conjunto de las clases laterales derechas de H en G y el de las clases laterales izquierdas de H en G. Sin embargo, en general, no es cierto que $\forall a \in G$, $aH = Ha$.

Por ejemplo, si $G = \mathcal{D}_4$, usando la notación del problema 4 de la sección anterior, observamos que $H = \{e, v\}$ no satisface que
$aH = Ha$, $\forall a \in \mathcal{D}_4$. El lector puede verificar que, por ejemplo, $\frac{\pi}{2}H \neq H\frac{\pi}{2}$, y $\frac{3\pi}{2}H \neq H\frac{3\pi}{2}$.

Igualmente, el lector puede comprobar que el subgrupo
$K = \{e, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ de $\mathcal{D}_4$ sí satisface que $gK = Kg$, $\forall g \in \mathcal{D}_4$.

Obsérvese que esto no significa que $gk = kg$, $\forall k \in K$, sino que $\forall k \in K, \exists k' \in K$ tal que $gk = k'g$.

El ejemplo anterior muestra que, en grupos no abelianos, hay algunos subgrupos que se comportan de esta manera especial.

Galois fue el primero en notar la existencia de esta propiedad en ciertos subgrupos de grupos de permutaciones; al observar el fenómeno, detectó su importancia crucial para el desarrollo de su teoría.

Definición 1.18 *Sea G un grupo, $H < G$. Se dice que H es normal en G y se denotará $H \lhd G$, si $\forall g \in G$, $gH = Hg$.*

A continuación, veremos que para probar que un subgrupo es normal en un grupo, basta con probar una de las dos contenciones que definen la igualdad de los conjuntos gH y Hg.

Proposición 1.19 *Sea G un grupo. Si $H < G$, entonces*

$$H \lhd G \Longleftrightarrow \forall g \in G, gHg^{-1} \subset H$$

Prueba

Supongamos que $H \lhd G$. Si $g \in G$, por definición, $gH = Hg$, luego $gHg^{-1} = H$.

Recíprocamente, supongamos que $\forall g \in G, gHg^{-1} \subset H$. Sea $r \in G$; tomando $g = r^{-1}$ en la hipótesis, obtenemos $r^{-1}Hr \subset H$; luego $H \subset rHr^{-1}$. Como además $rHr^{-1} \subset H$ por hipótesis, resulta que $rHr^{-1} = H$ y por lo tanto $rH = Hr$. Como r es un elemento arbitrario de G, obtenemos que $H \lhd G$ ■

1.3.1. Grupo Cociente

Consideremos de nuevo el caso del grupo $(\mathbb{Z}, +)$ y un subgrupo cualquiera $n\mathbb{Z}$, con $n > 1$.

Ya vimos que la relación de congruencia módulo n corresponde a la relación de equivalencia asociada al subgrupo $n\mathbb{Z}$ ya definida, y el conjunto $\mathbb{Z}_n$ de las clases de equivalencia de esta relación, es también un grupo con la suma definida de la manera siguiente:

$$\bar{j} + \bar{k} = \overline{j + k}$$

Como $\bar{j}$ corresponde a la clase lateral $n\mathbb{Z}+j$, se podría escribir lo anterior así:

$$(n\mathbb{Z} + j) + (n\mathbb{Z} + k) = n\mathbb{Z} + (j + k)$$

El hecho de ser $(\mathbb{Z}, +)$ un grupo abeliano, permite definir la suma de esta manera. Si un grupo cualquiera G no es abeliano y $H < G$, podemos definir una operación sobre el conjunto de las clases laterales derechas (o izquierdas)

de H en G, de manera análoga a la definida en $\mathbb{Z}_n$, y estará bien definida siempre que para $a, b \in G$ se cumpla $HaHb = Hab$, donde

$$HaHb = \{hah'b : h, h' \in G\}$$

En otras palabras, se requiere que el producto de dos clases laterales derechas dé como resultado otra clase lateral derecha, y que, además, el resultado de ese producto no dependa de los representantes elegidos en las respectivas clases laterales.

En lo que sigue, mostraremos que esto es lo que ocurre cuando el subgrupo H es normal en G.

Lema 1.20 *Sea G un grupo, y $H < G$. Se verifica que*

$$H \lhd G \Longleftrightarrow HaHb = Hab, \forall a, b \in G$$

Prueba

Supongamos que $H \lhd G$ y que $a, b \in G$. Como $Ha = aH$, tenemos que , si $h_1ah_2b \in HaHb$, entonces existe $h_3 \in H$ tal que $h_1(ah_2)b = h_1(h_3a)b$. Como $h_1h_3 \in H$, tenemos que $h_1h_3ab \in Hab$; por lo tanto, $HaHb \subset Hab$.

Por otra parte, si $hab \in Hab$, podemos escribir $hab = haeb$, donde e es la identidad de G. Así, $haeb \in HaHb$, y obtenemos $Hab \subset HaHb$, y por consiguiente, $HaHb = Hab$.

Recíprocamente, supongamos que $HaHb = Hab, \forall a, b \in G$. En particular, para $a \in G$,

$$HaHa^{-1} = Haa^{-1} = He = H$$

por lo tanto, si $h_1ah_2a^{-1} \in HaHa^{-1}$, existe $h_3 \in H$ tal que $h_1ah_2a^{-1} = h_3$, y así, $ah_2a^{-1} = h_1^{-1}h_3 \in H$.

Luego, $aHa^{-1} \subset H$, y como esto vale para todo $a \in G$, tenemos que $H \lhd G$ ■

Teorema 1.21 *Si G es un grupo y $H \lhd G$, entonces el producto $HaHb = Hab$ definido en el conjunto de las clases laterales derechas de H en G está bien definido y dota a este conjunto de una estructura de grupo.*

Prueba

Veamos que el producto definido arriba está bien definido, es decir, no depende de los representantes de las respectivas clases laterales derechas. En otras palabras, veremos que si $a, a', b, b' \in G$ son tales que $Ha = Ha'$ y

$Hb = Hb'$, entonces $Hab = Ha'b'$. Para verificar que esta última igualdad se cumple para a, b en las condiciones dadas, basta ver que $ab(a'b')^{-1} \in H$. Pero $ab(a'b')^{-1} = ab(b')^{-1}(a')^{-1}$ y como $b \sim_H b'$, tenemos que $b(b')^{-1} = h_1 \in H$. Así, $ab(a'b')^{-1} = ah_1(a')^{-1}$. Como $H \lhd G, aH = Ha$, luego, existe $h_2 \in H$ tal que $ah_1 = h_2a$. Por lo tanto, $ah_1(a')^{-1} = h_2a(a')^{-1}$. Como $a \sim_H a'$, resulta que $a(a')^{-1} = h_3 \in H$. Entonces $h_2a(a')^{-1} = h_2h_3 \in H$, lo que nos permite concluir que $ab(a'b')^{-1} \in H$. Así, $Hab = Ha'b'$, y el producto está bien definido.

Se deja como ejercicio para el lector, verificar que el producto así definido dota al conjunto de las clases laterales derechas de H en G , al que denotaremos G/H, de una estructura de grupo, el cual será llamado el grupo cociente de G por H ■

Cuando un grupo G es finito y $H \lhd G$, el orden del grupo cociente G/H es igual a $i_G(H) = \frac{o(G)}{o(H)}$. Puede también ocurrir que, siendo G infinito, y $H \lhd G$, el orden de G/H sea finito. Un ejemplo de esto es el caso de $\mathbb{Z}$, donde, para cualquier $n > 1$, el grupo cociente $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ tiene orden n.

Consideremos ahora el ejemplo del grupo $G = \mathcal{D}_4$ y el subgrupo $K = \{e, \pi\}$. Para ver que $K \lhd \mathcal{D}_4$, debemos comprobar que $\alpha K = K\alpha$, para todo $\alpha \in \mathcal{D}_4$.

En primer lugar, si α es una rotación, α conmuta con e y con π, así que se verifica la condición.

Por otra parte, si $\alpha = v$, la reflexión sobre el eje vertical del cuadrado, entonces

$vK = \{ve = v, v\pi = h\}$ y $Kv = \{ev = v, \pi v = h\}$.

Dejamos como ejercicio para el lector, comprobar que $\alpha K = K\alpha$ para los elementos α restantes de $\mathcal{D}_4$ y que $\mathcal{D}_4/K = \{K, Kv, Kd_1, Kd_2\}$.

Problemas:

1. Elabore la tabla de multiplicación del grupo cociente $\mathcal{D}_4/K$.
2. Sea G un grupo y $H < G$ tal que $i_G(H) = 2$. Pruebe que $H \lhd G$.
3. Pruebe que si $H < G$ y $N \lhd G$, entonces $H \bigcap N \lhd G$.
4. Pruebe que si $T \lhd G$ y T es cíclico, entonces todo subgrupo de T es normal en G.

5. Sea G un grupo finito y $a \in G$. Pruebe que $o(a) = o(a^{-1})$.

6. Pruebe que si un grupo G es cíclico, y $H < G$, entonces $H \lhd G$.

7. Considere la siguiente conjetura: " Sea $H < G$, G un grupo finito. Si H es abeliano, entonces $H \lhd G$". Si es verdadera, demuéstrela. En caso contrario, exhiba un contraejemplo.

8. Sea $K = \{e, v, h, \pi\} \subset \mathcal{D}_4$. Demuestre que $K \lhd \mathcal{D}_4$ y que $V = \{e, v\} \lhd K$, pero V no es normal en $\mathcal{D}_4$.

1.4. Homomorfismos de Grupos

El papel fundamental que juegan las funciones continuas entre espacios topológicos, y las transformaciones lineales entre espacios vectoriales, lo juegan los homomorfismos entre los grupos. Siendo funciones que preservan lo esencial de la estructura de los conjuntos involucrados, constituyen una herramienta esencial en el desarrollo de la teoría de grupos.

Definición 1.22 *Un homomorfismo del grupo G_1 al grupo G_2 es una función $f : G_1 \longrightarrow G_2$ tal que $f(r_1r_2) = f(r_1)f(r_2), \forall r_1, r_2 \in G_1$.*

Notemos que el producto r_1r_2 se refiere a la operación definida en G_1, mientras que el producto $f(r_1)f(r_2)$ es el definido en G_2.

Ejemplo 1.16 *Si $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ es una transformación lineal, entonces T es un homomorfismo entre los grupos $(\mathbb{R}^3, +)$ y $(\mathbb{R}^2, +)$.*

Ejemplo 1.17 *Sea $G_1 = (\mathbb{R}, +)$ y $G_2 = (\mathbb{R}^*, \cdot)$.*
Sea $\varphi : G_1 \longrightarrow G_2$, definida por $\varphi(x) = 2^x, \forall x \in G_1$. Como

$$\varphi(x + y) = 2^{x+y} = 2^x 2^y = \varphi(x)\varphi(y)$$

se verifica que φ es un homomorfismo.

Ejemplo 1.18 *Sea $\phi : S_3 \longrightarrow S_4$ la función definida por $\phi(\sigma) = \sigma'$, donde $\sigma'(i) = \sigma(i)$ si $1 \leq i \leq 3$ y $\sigma'(4) = 4$.*
Se deja como ejercicio para el lector, verificar que ϕ es un homomorfismo.

Ejemplo 1.19 *Si G_1 y G_2 son grupos cualesquiera, con e_1, e_2 los elementos identidad en G_1 y G_2 respectivamente, la función $\psi : G_1 \longrightarrow G_2$, definida por $\psi(g) = e_2$, $\forall g \in G_1$ y la función identidad de G_1 en sí mismo, son ambas homomorfismos.*

Ejemplo 1.20 *Sea*

$$G = \{T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3 : T \text{ es biyectiva}\}$$

Sabemos que G es un grupo con la composición de funciones. Consideremos la función
$f : S_3 \longrightarrow G$ definida por $f(\sigma) = T_\sigma$, donde

$$T_\sigma(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

para todo $(x_1, x_2, x_3) \in \mathbb{R}^3$.

Se deja como ejercicio para el lector probar que f *es un homomorfismo.*

Ejemplo 1.21 *Sea* G *un grupo y* $H \lhd G$. *Definamos* $\pi : G \longrightarrow G/H$ *de la manera siguiente:*

Si $g \in G$, $\pi(g) = Hg$.

Por lo visto antes, sabemos que si $g_1, g_2 \in G$, *entonces* $Hg_1g_2 = Hg_1Hg_2$, *de manera que se cumple lo requerido para que* π *sea un homomorfismo:* $\pi(g_1g_2) = \pi(g_1)\pi(g_2)$.

π *es llamdo el homomorfismo canónico o proyección de* G *sobre el grupo cociente* G/H.

Un homomorfismo de grupos, como hemos visto, preserva la operación de grupo, lo cual tiene implicaciones importantes en cuanto a la preservación de aspectos relevantes de la estructura de los grupos involucrados. Tal como las transformaciones lineales entre espacios vectoriales transforman subespacios en subespacios, los homomorfismos envían subgrupos en subgrupos; esta y otras propiedades básicas de los homomorfismos se enuncian a continuación.

Proposición 1.23 *Si* G_1, G_2 *son grupos,* e_1 *y* e_2 *son sus respectivos elementos identidad y* $\phi : G_1 \longrightarrow G_2$ *es un homomorfismo, entonces:*

1. $\phi(e_1) = e_2$.
2. $\phi(x^{-1}) = (\phi(x))^{-1}$, *para todo* $x \in G_1$.
3. *Si* $H < G_1$, *entonces* $\phi(H) < G_2$.
4. *Si* $K < G_2$, *entonces* $\phi^{-1}(K) < G_1$.
5. *Si* $H = \{x \in G_1 : \phi(x) = e_2\}$, *entonces* $H \lhd G_1$.

Prueba

1. Para ver que $\phi(e_1) = e_2$, tomemos $x \in G_1$, y observemos que $\phi(x)e_2 = \phi(x)$. Pero por otra parte, $\phi(x) = \phi(xe_1) = \phi(x)\phi(e_1)$, por ser ϕ un homomorfismo. Así, $\phi(x)e_2 = \phi(x)\phi(e_1)$. Por la ley de la cancelación en G_2, obtenemos que $e_2 = \phi(e_1)$.

2. Sea $x \in G_1$. Como $e_1 = xx^{-1}$, tenemos que

$$\phi(e_1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

   por ser ϕ un homomorfismo. Por la parte 1, tenemos que $\phi(x)\phi(x^{-1}) = e_2$. Por un razonamiento análogo, obtenemos que $\phi(x^{-1})\phi(x) = e_2$. Por la unicidad del inverso de un elemento de un grupo, se deduce que $\phi(x^{-1}) = (\phi(x))^{-1}$.

3. Sea $H < G_1$; como $H \neq \emptyset$, podemos elegir $x_1, x_2 \in H$, y eso garantiza que $\phi(H) \neq \emptyset$. Además, $\phi(x_1)(\phi(x_2))^{-1} = \phi(x_1)\phi((x_2)^{-1})$, por la parte 2. Como ϕ es un homomorfismo, tenemos que $\phi(x_1)(\phi(x_2))^{-1} = \phi(x_1(x_2)^{-1})$. Como $H < G_1$, se tiene que $x_1(x_2)^{-1} \in H$, y así,

$$\phi(x_1)(\phi(x_2))^{-1} \in \phi(H)$$

   y por lo tanto, $\phi(H) < G_2$.

4. Sea $K < G_2$. Como $e_2 \in K$, tenemos que $e_1 \in \phi^{-1}(K)$ y así $\phi^{-1}(K) \neq \emptyset$. Si $x_1, x_2 \in G_1$ son tales que $\phi(x_1), \phi(x_2) \in K$, entonces

$$\phi(x_1(x_2)^{-1}) = \phi(x_1)(\phi(x_2))^{-1}$$

   por ser ϕ un homomorfismo y por la parte 2. Como $\phi(x_1), \phi(x_2) \in K$ y $K < G_2$, obtenemos que $\phi(x_1)(\phi(x_2))^{-1} \in K$, y por lo tanto, $x_1(x_2)^{-1} \in \phi^{-1}(K)$, con lo que queda probado que $\phi^{-1}(K) < G_1$.

5. Sea $H = \{x \in G_1 : \phi(x) = e_2\}$. En primer lugar, $H \neq \emptyset$ pues $\phi(e_1) = e_2$. Sean $x_1, x_2 \in H$. Entonces,

$$\phi(x_1(x_2)^{-1}) = \phi(x_1)(\phi(x_2))^{-1} = e_2(e_2)^{-1} = e_2$$

   Por lo tanto, $x_1(x_2)^{-1} \in H$, y obtenemos que $H < G_1$.

Para ver que $H \lhd G_1$, sea $g \in G_1$ y sea $h \in H$.

$$\phi(ghg^{-1}) = \phi(g)\phi(h)(\phi(g))^{-1} = \phi(g)e_2(\phi(g))^{-1} = \phi(g)(\phi(g))^{-1} = e_2$$

Por lo tanto, $gHg^{-1} \subset H$ y entonces obtenemos $H \lhd G_1$.

■

Si $\phi : G_1 \longrightarrow G_2$ es un homomorfismo y $K = \{x \in G_1 : \phi(x) = e_2\}$, entonces K es llamado el núcleo de ϕ y se denota $Ker\phi$.

El hecho de ser $Ker\phi \lhd G_1$ nos permite considerar el grupo cociente $G_1/Ker\phi$. Este grupo está constituido, como sabemos, por las clases laterales Kx, con $x \in G_1$, donde $K = Ker\phi$.

El siguiente lema revela la vinculación entre cada clase Kx y el homomorfismo ϕ; en esencia, nos dice que , si $\phi(x) = v \in G_2$, entonces la clase lateral Kx coincide con el conjunto preimagen por ϕ de v:

$\phi^{-1}(v) = \{g \in G_1 : \phi(g) = v\}$.

Lema 1.24 *Si $\phi : G_1 \longrightarrow G_2$ es un homomorfismo y $K = Ker\phi$, entonces para todo $x \in G_1$,*

$$Kx = \{g \in G_1 : \phi(g) = \phi(x)\}$$

Prueba

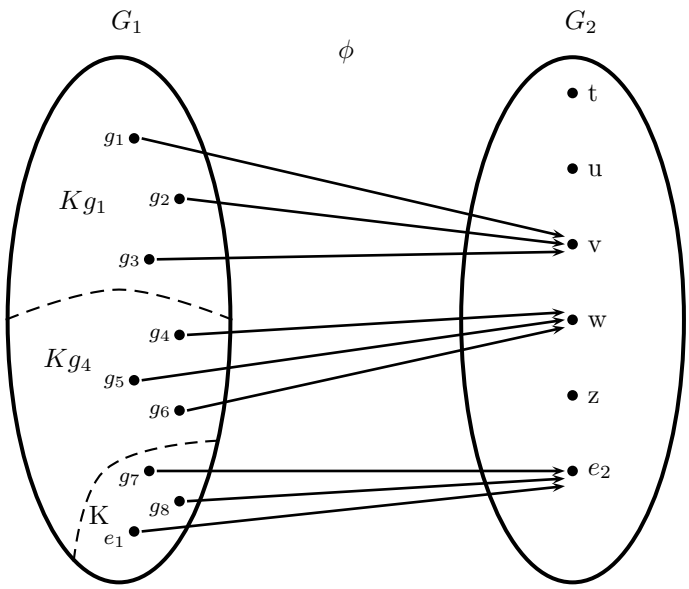
Supongamos que K está definido como en las condiciones del lema. Sea $x \in G_1$ y $g = kx \in Kx$.

Entonces $\phi(g) = \phi(kx) = \phi(k)\phi(x)$. Como $k \in K$, $\phi(k) = e_2$, luego, $\phi(g) = e_2\phi(x) = \phi(x)$. Así, $Kx \subset \{g \in G_1 : \phi(g) = \phi(x)\}$.

Por otra parte, si $g \in G_1$ es tal que $\phi(g) = \phi(x)$, tenemos que $\phi(g)(\phi(x))^{-1} = e_2$, luego $\phi(g)\phi(x^{-1}) = \phi(gx^{-1}) = e_2$, lo que significa que $gx^{-1} \in K$, es decir, $g \in Kx$.

■

El lema anterior muestra cómo las clases laterales de K en G_1 particionan a G_1 en la familia de subconjuntos que corresponden a las imágenes inversas, por ϕ, de cada elemento de $Im\phi$. La figura siguiente ilustra la situación en un caso particular:



Si ϕ es inyectiva, cada clase lateral está constituida por un único elemento, pues $Kx = \phi^{-1}(\phi(x)) = \{x\}$, y, en particular, $K = \{e_1\}$.

Recíprocamente, si $K = \{e_1\}$, como la cardinalidad de cada clase lateral debe ser igual a la de K, tendremos que $Kx = \{x\}$, para todo $x \in G_1$, y, por lo tanto, ϕ es inyectiva.

Hemos probado lo siguiente:

Proposición 1.25 *Si $\phi : G_1 \longrightarrow G_2$ es un homomorfismo, se cumple que $Ker\phi = \{e_1\}$ si, y sólo si ϕ es inyectiva.*

Recordemos que, en la teoría de la resolución de sistemas de ecuaciones lineales se establece que un sistema no homogéneo compatible tiene como solución el conjunto $S + v$, donde S es el subespacio solución del sistema homogéneo asociado y v es una solución particular del no homogéneo. Esto puede verse como un caso particular de lo que afirma el lema anterior:

El sistema no homogéneo de ecuaciones lineales plantea la pregunta siguiente: Si T es la transformación lineal asociada a la matriz $m \times n$ de coeficientes del sistema y $\vec{z} = (z_1, ..., z_m)$ es el vector de términos independientes, ¿ cuál es el conjunto de vectores $\vec{v}$ en $\mathbb{R}^n$ tales que $T(\vec{v}) = \vec{z}$?

Como sabemos, la transformación lineal T es un homomofismo de grupos, y el lema 1.24 nos dice que , si $S = KerT$, y $\vec{u}$ es una solución particular del sistema no homogéneo, es decir, $T(\vec{u}) = \vec{z}$, entonces $T^{-1}(\vec{z}) = S + \vec{u}$.

Ahora bien , volviendo al caso general de un homomorfismo ϕ de grupos cualesquiera, si ϕ no es inyectivo y $Ker\phi = K$, ya vimos que cada clase lateral derecha Kg de K en G_1, tiene la propiedad siguiente:

$$x \in Kg \Longleftrightarrow \phi(x) = \phi(g)$$

Como además las clases laterales derechas son disjuntas dos a dos, podemos definir

$$\bar{\phi} : G_1/K \longrightarrow G_2$$

por $\bar{\phi}(Kg) = \phi(g)$.

El lector puede probar que $\bar{\phi}$ está bien definida, es un homomorfismo, y además es inyectivo. $\bar{\phi}$ constituye, por así decirlo, el homomorfismo inyectivo más cercano a ϕ, y que conserva la información esencial sobre ϕ. Dada $\bar{\phi}$ solamente, podemos reconstruir a ϕ de manera única.

Es oportuno el momento para introducir cierta terminología útil para el tratamiento de los homomorfismos.

Definición 1.26 *Sean G_1 y G_2 grupos. Un monomorfismo de G_1 en G_2 es un homomorfismo inyectivo. Un epimorfismo de G_1 en G_2 es un homomorfismo sobreyectivo, y un isomorfismo es un homomorfismo biyectivo. Cuando existe un isomorfismo entre los grupos G_1 y G_2 se dice que estos grupos son isomorfos, y se denota: $G_1 \cong G_2$.*

Como ocurre con los isomorfismos entre espacios vectoriales, la existencia de un isomorfismo entre dos grupos, indica que éstos son, por así decirlo, una copia el uno del otro. Toda la estructura de cada grupo se reproduce exactamente en el otro.

Problemas:

1. Sea $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_5$ la proyección canónica, es decir, $\pi(n) = \bar{n}(mod 5)$.

   Determine $Ker\pi$ y muestre que $\bar{\pi}$ es un isomorfismo.

2. Construya una función inyectiva λ, definida como una restricción de π (se toma como dominio un subconjunto propio del dominio de π, y se conserva la ley de correspondencia). Muestre que λ no es un homomorfismo.

3. Describa todos los homomorfismos de $\mathbb{Z}$ en $\mathbb{Z}$.

1.4.1. Teoremas de Isomorfismos

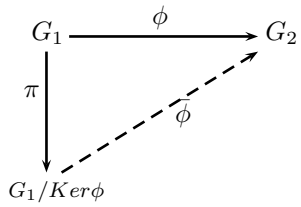
Las consideraciones anteriores sobre un homomorfismo cualquiera $\phi : G_1 \longrightarrow G_2$, pueden ser resumidas del modo siguiente: Si ϕ es un monomorfismo, entonces G_1 es isomorfo al subgrupo $Im\phi$ de G_2. Si ϕ no es un monomorfismo, y $K = Ker\phi$, definimos $\bar{\phi} : G_1/K \longrightarrow G_2$ como lo hicimos antes, y resulta que $\bar{\phi}$ es un monomorfismo y por lo tanto $G_1/K \cong Im\bar{\phi} < G_2$.

Este último resultado se expresa de modo general en el siguiente teorema, el primero de los llamados Teoremas de Isomorfismos.

Teorema 1.27 *(Primer Teorema de Isomorfismos)*

Si $\phi : G_1 \longrightarrow G_2$ es un homomorfismo de grupos, y $K = Ker\phi$, entonces existe un monomorfismo $\bar{\phi} : G_1/K \longrightarrow G_2$ tal que, si $\pi : G_1 \longrightarrow G_1/K$ es la proyección canónica, entonces $\phi = \bar{\phi} \circ \pi$.

Esto equivale a decir que el siguiente diagrama es conmutativo:



Además, resulta del hecho de ser $\bar{\phi}$ un monomorfismo, que

$$G_1/Ker\phi \cong Im\phi$$

Los otros dos Teoremas de Isomorfismos son, en esencia, consecuencias del Primer Teorema de Isomorfismos, consecuencias muy importantes, como veremos.

Teorema 1.28 *(Segundo Teorema de Isomorfismos)*
Sea G un grupo, y sean $N \lhd G$, $M \lhd G$, $NM = \{nm : n \in N, m \in M\}$. Entonces

1. *$NM \lhd G$, $M \lhd NM$ y $N \bigcap M \lhd N$*
2. *$NM/M \cong N/(N \bigcap M)$.*

Prueba

1. En primer lugar, $NM < G$, pues si $n_1m_1, n_2m_2 \in NM$, se tiene que

$$n_1m_1(n_2m_2)^{-1} = n_1(m_1m_2)^{-1}n_2^{-1} = n_1m_3n_2^{-1}$$

para algún $m_3 \in M$.

Como $M \lhd G$, existe $m_4 \in M$ tal que $m_3n_2^{-1} = n_2^{-1}m_4$, y así, resulta que $n_1m_3n_2^{-1} = n_1n_2^{-1}m_4 \in NM$, es decir, $n_1m_1(n_2m_2)^{-1} \in NM$.

Como además $e \in NM$, se tiene que $NM \neq \emptyset$ y así $NM < G$.

Para ver que $NM \lhd G$, basta tomar $g \in G$ y comprobar que $gNM = NMg$. Pero como $N \lhd G$ y $M \lhd G$ sabemos que $gN = Ng$ y $gM = Mg$, luego $gNM = NgM = NMg$.

Por otra parte, siendo $M \lhd G$ y $NM \subset G$, se cumple que $M \lhd NM$. Además, dado que $M \lhd G$ y $N \lhd G$, tenemos que, si $g \in G$ y $u \in N \bigcap M$, entonces existen $n \in N, m \in M$ tales que $gu = ng = mg$, lo cual implica que $n = m \in N \bigcap M$ y por lo tanto, también es cierto que $N \bigcap M \lhd G$. Como $N \subset G$, se cumple que $N \bigcap M \lhd N$.

2. Sea $\varphi : N \longrightarrow NM/M$ definida por $\varphi(n) = Mn$, para cada $n \in N$. Veamos que $Ker\varphi = M \bigcap N$:

Para cualquier $n \in N$, tenemos que

$$n \in Ker\varphi \Longleftrightarrow Mn = M \Longleftrightarrow n \in M \Longleftrightarrow n \in N \bigcap M$$

Luego, por el Primer Teorema de Isomorfismos, obtenemos que

$$N/(N \bigcap M) \cong Im\varphi$$

Ahora veremos que $Im\varphi = NM/M$.

Sea $Mx \in NM/M$, es decir, $x = nm$, con $n \in N, m \in M$. Como $M \lhd G$, sabemos que $nM = Mn$, y por lo tanto, existe $m' \in M$ tal que $nm = m'n$ y así $Mx = Mnm = Mm'n = Mn$. De manera que $Mx = Mn = \varphi(n)$ con $n \in N$, y por lo tanto, $Mx \in Im\varphi$. Concluimos, entonces, que $N/(N \bigcap M) \cong NM/M$.

■

El resultado de este teorema tiene aplicaciones y consecuencias diversas, una de ellas es la que surge cuando G es finito, y $M \bigcap N = \{e\}$. En ese caso, como $o(N/N \bigcap M) = o(N)/1 = o(N)$, obtenemos que $o(N) = o(NM)/o(M)$, es decir, $o(N)o(M) = o(NM)$.

Si $M \bigcap N \neq \{e\}$, resulta que $o(NM) = o(N)o(M)/o(N \bigcap M)$.

Teorema 1.29 *(Tercer Teorema de Isomorfismos)*

Sea $\phi : G_1 \longrightarrow G_2$ un epimorfismo de núcleo K, y sea $N_2 \lhd G_2$, $N_1 = \phi^{-1}(N_2)$. Entonces $K \subset N_1$, $N_1 \lhd G_1$ y $G_1/N_1 \cong G_2/N_2$; equivalentemente, $G_1/N_1 \cong (G_1/K)/(N_1/K)$.

Prueba

Sea $\phi : G_1 \longrightarrow G_2$ un epimorfismo de núcleo K y sea $N_2 \lhd G_2$. Sabemos que $N_1 = \phi^{-1}(N_2) < G_1$. Veamos que $N_1 \lhd G_1$. Sea $g \in G_1$ y $n \in N_1$. Como $N_2 \lhd G_2$, se tiene que $\phi(g)\phi(n)(\phi(g))^{-1} \in N_2$, y como ϕ es un homomorfismo, esto significa que $\phi(gng^{-1}) \in N_2$, por lo que $gng^{-1} \in N_1$. Así, resulta que $N_1 \lhd G_1$.

Por otra parte, como $e_2 \in N_2$, resulta que $K = \phi^{-1}(e_2) \subset N_1$.

Sea $\pi_2 : G_2 \longrightarrow G_2/N_2$ la proyección canónica, i.e., $\pi_2(x) = N_2x$, para todo $x \in G_2$.

Definamos ahora $\psi : G_1 \longrightarrow G_2/N_2$ como la composición $\pi_2 \circ \phi$.

Dejamos como ejercicio para el lector, probar que ψ es un epimorfismo.

Veamos que $Ker\psi = N_1$:

$$g \in Ker\psi \Longleftrightarrow \psi(g) = N_2 \Longleftrightarrow N_2\phi(g) = N_2 \Longleftrightarrow \phi(g) \in N_2 \Longleftrightarrow$$

$$g \in \phi^{-1}(N_2) = N_1$$

Por el Primer Teorema de Isomorfismos, obtenemos que $G_1/N_1 \cong G_2/N_2$. Por el mismo teorema, $G_1/K \cong G_2$ y $N_1/K \cong N_2$ (considerando en este caso la restricción de ϕ a N_1). El lector puede probar, como ejercicio, que

$$G_2/N_2 \cong (G_1/K)/(N_1/K)$$

y usando el hecho de que el isomorfismo entre grupos es una relación transitiva, finalmente concluimos que

$$G_1/N_1 \cong (G_1/K)/(N_1/K)$$

■

Teorema 1.30 *(Teorema de Correspondencia)*
Sea $\phi : G_1 \longrightarrow G_2$ un epimorfismo tal que $Ker\phi = K$. Existe una correspondencia biyectiva entre los conjuntos $\mathcal{S}_1$ y $\mathcal{S}_2$, donde
$\mathcal{S}_1 = \{H < G_1 : K \subset H\}$ *y* $\mathcal{S}_2 = \{T \subset G_2 : T < G_2\}$.

Prueba

Sea $\lambda : \mathcal{S}_1 \longrightarrow \mathcal{S}_2$, la función definida por $\lambda(H) = \phi(H)$, para todo $H \in \mathcal{S}_1$.

λ está bien definida, pues si $H < G_1$, se tiene que $\phi(H) < G_2$.

Veamos que ϕ es biyectiva:

Sean $H_1, H_2 \in \mathcal{S}_1$ tales que $\lambda(H_1) = \lambda(H_2)$, es decir, $\phi(H_1) = \phi(H_2)$.

Probaremos que $H_1 \subset H_2$:

Sea $g \in H_1$. Como $\phi(g) \in \phi(H_1) = \phi(H_2)$, existe $g' \in H_2$ tal que $\phi(g') = \phi(g)$ y por lo tanto $\phi(g'g^{-1}) = e_2$. Luego, $g'g^{-1} \in K \subset H_2$. Como $v = g'g^{-1} \in H_2$, se tiene que $(g')^{-1}v = (g')^{-1}g'g^{-1} \in H_2$, es decir, $g^{-1} \in H_2$ y por lo tanto $g \in H_2$. De manera análoga, se prueba que $H_2 \subset H_1$, y así se obtiene que λ es inyectiva.

Por otra parte, λ es sobreyectiva pues si $T < G_2$, sabemos que $\phi^{-1}(T) < G_1$, $K \subset \phi^{-1}(T)$ y $\lambda(\phi^{-1}(T)) = \phi(\phi^{-1}(T)) = T$, por ser ϕ sobreyectiva. Es decir, si $J = \phi^{-1}(T)$ entonces $J \in \mathcal{S}_1$ y $\lambda(J) = T$ ■

Este último teorema muestra explícitamente cómo un homomorfismo ϕ cualquiera entre los grupos G_1 y G_2 envía subgrupos de G_1 que contiene al núcleo de ϕ , a subgrupos de G_2 contenidos en la imagen de ϕ.

En el caso en que ϕ sea un isomorfismo, resulta que a todo subgrupo de G_1 le corresponde, de manera biunívoca, un subgrupo de G_2, y esto nos da una visión más precisa de lo que significa que $G_1 \cong G_2$.

Problemas

1. Demuestre que si $\varphi : G_1 \longrightarrow G_2$ es un epimorfismo, entonces $H_1 \lhd G_1 \Longrightarrow \varphi(H_1) \lhd G_2$.

2. Sea G un grupo, $g \in G$ y $\phi : G \longrightarrow G$ definida por $\phi(x) = gxg^{-1}, \forall x \in G$. Pruebe que ϕ es un isomorfismo.

3. Sean $a, b \in \mathbb{R}, a \neq 0$, y sea $\mu_{ab} : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $\mu_{ab}(x) = ax + b$. Sea $G = \{\mu_{ab} : a, b \in \mathbb{R}, a \neq 0\}$, y sea $N = \{\mu_{1b} : b \in \mathbb{R}\}$. Pruebe que G es un grupo con la composición de funciones, $N \lhd G$ y $G/N \cong (\mathbb{R}^*, \cdot)$, donde $(\mathbb{R}^*, \cdot)$ es el grupo de los números reales no nulos, con el producto usual en $\mathbb{R}$.

4. Pruebe que todos los grupos de orden 2 son isomorfos.

5. Sea $n \in \mathbb{N}$ y G el grupo generado por los símbolos x, y, bajo las siguientes condiciones:

   a) $x^2 = e$, $y^n = e$.

   b) $xy = y^{-1}x$

   G es el llamado grupo dihédrico de orden $2n$, denotado por $\mathcal{D}_n$, el cual es una generalización del grupo de las isometrías del cuadrado, $\mathcal{D}_4$. ¿A qué isometrías de $\mathcal{D}_4$ corresponden, respectivamente, x y y?

   Pruebe que:

   a) Si $N = (y)$, entonces $N \lhd G$.

   b) $G/N \cong \mathcal{S}$, donde $\mathcal{S}$ es un grupo de orden 2. (Dado el resultado del ejercicio anterior, resulta que G/N es isomorfo a todos los grupos de orden 2).

6. Si G es un grupo no abeliano de orden 6, pruebe que $G \cong S_3$.

1.5. El Teorema de Cayley

El matemático inglés Arthur Cayley (1821 - 1895) dedicó buena parte de su trabajo a temas del Álgebra Lineal vinculados con la Geometría, específicamente en el área de la Teoría de Invariantes, la cual ocupó a muchos matemáticos brillantes de la segunda mitad del siglo XIX. También se debe a Cayley un resultado muy importante de la teoría de grupos, conocido con el título que lleva esta sección. Ya hemos mencionado que, históricamente, los primeros grupos estudiados fueron los grupos de permutaciones. El asombroso Teorema de Cayley afirma que, en esencia, ésos son todos los grupos que existen. Más formalmente hablando, que todo grupo es isomorfo a un subgrupo de algún grupo de permutaciones. Es ese el resultado principal de esta sección.

Comencemos con algunas definiciones previas.

Definición 1.31 *Si G es un grupo, un automorfismo de G es un isomorfismo de G sobre sí mismo.*

Si denotamos por $Aut(G)$ al conjunto de todos los automorfismos de G, tenemos que $Aut(G) \neq \emptyset$, para todo grupo G, pues la función I_G, la función identidad de G en G, es un automorfismo de G.

Además, si $\mathcal{A}(G) = \{f : G \longrightarrow G \text{ tal que } f \text{ es biyectiva}\}$ sabemos que $\mathcal{A}(G)$ es un grupo con la composición de funciones, y por lo tanto en $Aut(G)$ también podemos considerar la misma operación, puesto que
$Aut(G) \subset \mathcal{A}(G)$.

Como $Aut(G) \neq \emptyset$, podemos probar que, de hecho, $(Aut(G), \cdot)$ es un grupo, verificando que, si $\varphi, \phi \in Aut(G)$, entonces

1. $\phi\varphi \in Aut(G)$ y
2. $\phi^{-1} \in Aut(G)$.

Ahora bien, $\phi\varphi \in Aut(G)$ si $\phi\varphi$ es un homomorfismo biyectivo de G en G. Sabemos que es una biyección, porque φ y ϕ, ambas, lo son.

Sean g_1, $g_2 \in G$.

$\phi\varphi(g_1g_2) = \phi[\varphi(g_1)\varphi(g_2)]$, por ser φ un homomorfismo. Al serlo ϕ también, obtenemos que

$$\phi\varphi(g_1g_2) = [\phi\varphi(g_1)][\phi\varphi(g_2)].$$

Luego $\phi\varphi$ es un homomorfimo y así, $\phi\varphi \in Aut(G)$, con lo cual hemos probado 1).

Por otra parte, si ϕ es un isomorfismo, ϕ^{-1} es también biyectiva y además es un homomorfismo:

Sean $x, y \in G$. Como ϕ es biyectiva, existen $a, b \in G$ tales que $\phi(a) = x,\ \phi(b) = y$.

Ahora bien, $\phi^{-1}(xy) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab))$ porque ϕ es un homomorfismo, y así, $\phi^{-1}(xy) = ab = \phi^{-1}(x)\phi^{-1}(y)$; por lo tanto, $\phi^{-1} \in Aut(G)$.

De esta manera, hemos probado que $(Aut(G), \cdot)$ es un grupo. Como, además, $Aut(G) \subset \mathcal{A}(G)$, en realidad tenemos que $Aut(G) < \mathcal{A}(G)$.

Examinaremos ahora algunos ejemplos de automorfismos de grupos.

Ejemplo 1.22 *Sea $G = (\mathbb{Z}, +)$ y sea $\lambda : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $\lambda(n) = -n$.*

Es fácil ver que $\lambda \in Aut(\mathbb{Z})$.

Si G es grupo cualquiera, no abeliano, entonces la función análoga a λ, i.e. $\alpha : G \longrightarrow G$, definida por $\alpha(g) = g^{-1},\ \forall\, g \in G$, no es necesariamente un automorfismo. Dejamos como ejercicio para el lector, la verificación de este hecho.

Ejemplo 1.23 *Sea G un grupo cualquiera, y $g \in G$. Definamos $T_g : G \longrightarrow G$ por $T_g(a) = gag^{-1},\ \forall\, a \in G$.*

T_g es un homomorfismo, pues si $a, b \in G$, entonces $T_g(ab) = g(ab)g^{-1} = ga(g^{-1}g)bg^{-1} = (gag^{-1})(gbg^{-1}) = T_g(a)T_g(b)$.

T_g es inyectiva: si $a \in G$ y $T_g(a) = e$, entonces $gag^{-1} = e$, luego $ga = g$, y por lo tanto $a = e$.

T_g es sobreyectiva también, pues para $b \in G,\ T_g(g^{-1}bg) = gg^{-1}bgg^{-1} = b$. Tenemos, entonces, que $T_g \in Aut(G)$, y si G es no abeliano, y g no está en el centro de G, T_g es distinto de la identidad I_G.

A T_g se le denomina el automorfismo de conjugación por g, y el conjunto $J(G) = \{T_g : g \in G\}$ se denomina el conjunto de todos los automorfismos de conjugación de G, o de los automorfismos interiores de G.

A continuación estudiaremos el caso de los automorfismos de los grupos cíclicos; necesitaremos el siguiente resultado:

Lema 1.32 *Sea G un grupo y $\alpha \in Aut(G)$. Si $a \in G$ y $\circ(a) = k > 0$, entonces $\circ(\alpha(a)) = k$.*

Prueba Sea $\alpha \in Aut(G)$. Si $a \in G$ y $\circ(a) = k > 0$, tenemos que $a^k = e$ y $a^i \neq e$ si $0 < i < k$. Ahora bien, $[\alpha(a)]^k = \alpha(a^k) = \alpha(e) = e$, lo que significa que $\circ(\alpha(a)) \leq k$. Si $\circ(\alpha(a)) = r < k$, entonces $[\alpha(a)]^r = e$, pero $[\alpha(a)]^r = \alpha(a^r) = e$ implica que $a^r \in Ker\,\alpha$, y como α es un automorfismo, $Ker\,\alpha = \{e\}$, por lo tanto $a^r = e$, con $r < k$, lo cual es absurdo, porque $k = \circ(a)$. Así, $\circ(\alpha(a)) = k$. ■

Sea $C_m = \{i \in \mathbb{N} : 0 < i < m,\ (i, m) = 1\}$. Si se define en C_m la operación producto módulo m, se obtiene un grupo.

El lector puede verificar este hecho. Estos grupos nos interesan en este momento, pues el grupo de automorfismos de un grupo cíclico finito, es isomorfo a C_m, con m igual al orden del grupo.

Este es el resultado que demostraremos a continuación.

Proposición 1.33 *Si G es un grupo cíclico finito, entonces $Aut(G) \cong C_m$, donde $m = \circ(G)$. Si G es un grupo cíclico infinito, entonces $Aut(G)$ es isomorfo a un grupo cíclico de orden 2.*

Prueba Consideremos primero el caso en que G es cíclico de orden $m > 1$. Si $\phi \in Aut(G)$, y $G = (a)$, tenemos que ϕ está completamente determinado cuando conocemos $\phi(a)$, pues si $x \in G$, $x = a^j$ para algún $j \in \mathbb{N}$, y por lo tanto, $\phi(x) = \phi(a^j) = [\phi(a)]^j$. De modo que existen tantos automorfismos distintos de G, como valores distintos pueda tomar $\phi(a) \in G$.

Por otra parte, en principio, $\phi(a)$ podría tomar cualquiera de los valores a^i, con $0 < i < m$; veremos que, en realidad, por ser $\phi \in Aut(G)$, los valores que puede tomar i son sólo aquellos para los cuales $(i, m) = 1$.

En efecto, tenemos que $\circ(\phi(a)) = \circ(a)$, por el lema anterior. Es decir, si $\phi(a) = a^i$, tendría que cumplirse que $\circ(a^i) = m$.

Si $(i, m) \neq 1$, entonces existe $r > 1$ tal que $r|i$, $r|m$. Por lo tanto, $[\phi(a)]^{m/r} = (a^i)^{m/r} = (a^m)^{i/r} = e$ y entonces $\circ(\phi(a)) \leq m/r < m$, lo cual contradice que $\circ(\phi(a)) = m$. Así, tenemos que si $\phi \in Aut(G)$ y $\phi(a) = a^i$, entonces $(i, m) = 1$.

Recíprocamente, si $f : G \longrightarrow G$ se define por $f(a^k) = a^{ki}$, donde $0 < i < m$ y además $(i, m) = 1$, veamos que $f \in Aut(G)$.

1. f es un homomorfismo: $f(a^k a^j) = f(a^{k+j}) = a^{(k+j)i} = a^{ki}a^{ji} = f(a^k)f(a^j)$

2. f es biyectiva: Si $f(a^k) = e$, entonces $a^{ki} = e$, luego $ki = sm$ para algún $s \geq 1$; como $(i, m) = 1$, esto implica que $m|k$ y por lo tanto $a^k = e$. Así, $Ker\, f = \{e\}$ y f es inyectiva.

3. f es un epimorfismo: Sea $0 < t < m$; veremos que $a^t \in Im f$. Como $(i, m) = 1$, existen $r, s \in \mathbb{Z}$ tales que $ri + sm = 1$; luego $tri + tsm = t$ y por lo tanto, $a^t = a^{tri+tsm}$; luego
$a^t \cdot a^{-tri} = (a^m)^{ts} = e$. Así, $a^t = a^{rti} = f(a^{rt})$.

De modo que existe una biyección entre $Aut(G)$ y el grupo
$C_m = \{i \,:\, 0 < i < m,\ (i, m) = 1\}$.

Si definimos $\lambda : Aut(G) \longrightarrow C_m$ por $\lambda(\phi) = i$, donde $\phi(a) = a^i$, es fácil ver que λ es un isomorfismo, con lo que queda demostrado que $Aut(G) \cong C_m$.

Supongamos ahora que G es un grupo cíclico infinito. Existe, entonces, $a \in G$ tal que $G = \{a^i \,:\, i \in \mathbb{Z}\}$ y sabemos que $a^i \neq a^j$ si $i \neq j$.

Sea $\phi \in Aut(G)$, y supongamos que $\phi(a) = a^k$, para algún $k \in \mathbb{Z}$. Como ϕ es un epimorfismo, $a \in Im\, \phi$, luego existe $j \in \mathbb{Z}$ tal que $\phi(a^j) = a$, es decir, $(a^j)^k = a^{jk} = a$.

Pero esto sólo es posible si $jk = 1$, lo cual implica necesariamente que $k = \pm 1$.

Así, hay sólo dos automorfismos de G : $\phi_1 = I_G$ (la identidad en G) y
$\phi_2 : G \longrightarrow G$ definida por $\phi_2(a) = a^{-1}$.
En otras palabras, $Aut(G) = \{\phi_1 = e,\ \phi_2\}$ es un grupo cíclico de orden 2 ■

Teorema 1.34 *(Teorema de Cayley)*
Sea G un grupo. Si $A(G) = \{f : G \longrightarrow G$ tal que f es biyectiva$\}$ entonces existe $K < A(G)$ tal que $G \cong K$.

Prueba Para cada $g \in G$, definiremos $\gamma_g : G \longrightarrow G$ por $\gamma_g(a) = ga$, $\forall\, a \in G$.

Veamos que γ_g es biyectiva, $\forall\, g \in G$:

Sean a_1, $a_2 \in G$ tales que $\gamma_g(a_1) = \gamma_g(a_2)$, es decir, $ga_1 = ga_2$. Como G es un grupo, esto implica que $a_1 = a_2$, luego γ_g es inyectiva.

γ_g es sobreyectiva, pues si $b \in G$, entonces $g^{-1} \in G$ y
$\gamma_g(g^{-1}b) = gg^{-1}b = b$.

Definamos ahora un monomorfismo

$$T : \quad G \longrightarrow A(G) \qquad \text{de la siguiente manera:}$$

$$T(g) = \ \gamma_g, \quad \forall\, g \in G.$$

Veamos que, en efecto, T es un monomorfismo:

Sean g_1, $g_2 \in G$. Entonces, $T(g_1g_2) = \gamma_{g_1g_2}$, donde $\gamma_{g_1g_2}(a) = (g_1g_2)a$, $\forall\, a \in G$.

Pero $\gamma_{g_1}(\gamma_{g_2}(a)) = \gamma_{g_1}(g_2a) = g_1(g_2a)$; como el producto en G es asociativo, tenemos que $\gamma_{g_1}\gamma_{g_2}(a) = \gamma_{g_1g_2}(a)$, $\forall\, a \in G$, es decir, $\gamma_{g_1g_2} = \gamma_{g_1}\gamma_{g_2}$ o, equivalentemente, $T(g_1g_2) = T(g_1)T(g_2)$. Además, T es inyectiva, pues si $T(g) = I_G$ (la función identidad en G), entonces $ga = a$, $\forall\, a \in G$, por lo tanto $g = e$, y $Ker\, T = \{e\}$.

Como T es un monomorfismo de grupos, por el 1^{er} teorema de isomorfismos, tenemos que $G \cong Im\, T < A(G)$ ■

1.6. Los Grupos de Permutaciones

Estudiaremos ahora los grupos de permutaciones de conjuntos finitos, sus propiedades básicas, y concluiremos la sección con el tratamiento del grupo alternante A_n y su vinculación con el problema de la irresolubilidad por radicales de las ecuaciones polinómicas de grado mayor o igual que 5.

Una manera muy útil de estudiar una permutación $\sigma \in S_n$ es la que busca determinar el efecto que tiene la aplicación sucesiva de σ sobre cada $i \in \{1, \ldots, n\}$. En otras palabras, se busca determinar los conjuntos $\{\sigma^k(i) : k \in \mathbb{Z}\}$, para cada $i \in \{1, \ldots, n\}$, tomando $\sigma^0(i) = i$.

Por ejemplo, si $\sigma \in S_8$, $\qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 8 & 6 & 5 & 7 \end{pmatrix}$

Para $i = 1$, tenemos $\sigma(1) = 3$, $\sigma^2(1) = 4$, $\sigma^3(1) = 2$, $\sigma^4(1) = 1$. Las potencias subsiguientes de σ, aplicadas a 1, nos remiten al inicio y repetición del ciclo:
$\sigma^5(1) = \sigma(1)$, $\sigma^6(1) = \sigma^2(1)$, etc.

Es decir, $\{\sigma^k(1) : k \in \mathbb{Z}\} = \{1, 3, 4, 2\}$. Este conjunto es llamado la órbita de 1 por σ; (también es la órbita de 3, de 4 y de 2).

La órbita de 5 es $\{5, 8, 7\}$ y la del 6 es $\{6\}$. Si escribimos las órbitas como r - uplas ordenadas: (1,3,4,2), (5,8,7) y (6), estamos determinando con precisión, $\sigma^r(i)$ para cualquier $i \in \{1, \ldots, 8\}$ y cualquier $r \in Z$. En otras palabras, al conocer las órbitas por σ, ordenadas, conocemos cada valor que toma σ, pero además veremos cómo, al determinar esas órbitas obtenemos

información adicional acerca de σ. Más formalmente, podemos definir una relación sobre $\{1, \ldots, 8\}$ dada por $i \sim j \Leftrightarrow j = \sigma^k(i)$ para algún $k \in \mathbb{Z}$.

Se prueba fácilmente que esta es una relación de equivalencia, cuyas clases de equivalencia constituyen precisamente las órbitas por σ.

Llamaremos ciclo a una órbita ordenada: $(i_1, i_2, \ldots, i_k)$; la longitud del ciclo será el número de términos que lo componen. Estas consideraciones valen para cualquier $\sigma \in S_n$, $\forall\, n > 1$; el conjunto $\{1, \ldots, n\}$ queda particionado en órbitas que son las clases de equivalencia de la relación:

$$a \sim b \Leftrightarrow \exists\, k \in \mathbb{Z} \,:\, \sigma^k(a) = b$$

A su vez, cada órbita, al ordenarse según las potencias de σ :
$(\sigma^0(a), \sigma(a), \sigma^2(a), \ldots, \sigma^k(a))$ constituye lo que llamamos un ciclo de la permutación σ.

Por otra parte, dado un ciclo $(i_1, \ldots, i_r) \in S_n$, podemos identificarlo con la permutación $\sigma \in S_n$ tal que:

$$\sigma(i_k) = i_{k+1} \qquad \text{para} \qquad k \in \{1, \ldots, r-1\},$$

$$\sigma(i_r) = i_1$$

$$\sigma(j) = j \qquad \forall\, j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}$$

Un producto de ciclos se interpretará, entonces, como el producto de las permutaciones que representan dichos ciclos. Por ejemplo, si multiplicamos los ciclos (1,3,4) y (2,4,5,7) en S_8, tenemos que

$$(1, 3, 4)(2, 4, 5, 7) = (2, 1, 3, 4, 5, 7)$$

Como los números 6 y 8 quedan fijos en estos dos ciclos, también quedan fijos en el producto, y éste se puede representar así: (2,1,3,4,5,7)(6)(8).

A continuación veremos un resultado que es clave para el estudio y la clasificación de las permutaciones en S_n, para cualquier n dado.

Observemos antes dos hechos importantes:

1. Dos ciclos $(a_1, \ldots, a_r)$ y $(b_1, \ldots, b_s)$ conmutan si son disjuntos, es decir, si $\forall\, i \in \{1, \ldots, r\},\ \forall j \in \{1, \ldots, s\}\ , a_i \neq b_j$.

2. $(a_1, \ldots, a_r) = (a_i,\, a_{i+1}, \ldots, a_r\, a_1, \ldots, a_{i-1})$,
   $\forall\, i \in \{1, \ldots, r\}$.

Teorema 1.35 *Si σ es una permutación, entonces σ es igual a un producto de ciclos disjuntos.*

Prueba Sea $\sigma \in S_n$, y consideremos la relación de equivalencia que define σ sobre $\{1, \ldots, n\}$, cuyas clases de equivalencia son las órbitas de los números $1, \ldots, n$. Como las clases de equivalencia son disjuntas, al ordenar estas órbitas para obtener los respectivos ciclos, obtenemos ciclos disjuntos.

Sean los ciclos de σ los siguientes:

$$(i_1,\, \sigma(i_1), \ldots, \sigma^{k_1}(i_1)), \ldots, (i_s,\, \sigma(i_s), \ldots, \sigma^{k_s}(i_s))$$

Veamos que $\sigma = (i_1,\, \sigma(i_1), \ldots, \sigma^{k_1}(i_1)) \ldots (i_s,\, \sigma(i_s), \ldots, \sigma^{k_s}(i_s))$.

Sea $j \in \{1, \ldots, n\}$. Si $\sigma(j) = j$, entonces la órbita de j es $\{j\}$, y puede omitirse el ciclo (j) entre los ciclos de σ. En este caso, el producto de los ciclos de σ, aplicado a j es, también, igual a j.

Si $\sigma(j) = m \neq j$, entonces m y j pertenecen a la misma órbita, y, en el ciclo correspondiente, j y m son consecutivos. Como los ciclos son disjuntos, ningún otro ciclo "mueve" a j y por lo tanto, el producto de ciclos de σ, aplicado a j, es igual a m.

Queda así probado que $\sigma = (i_1,\, \sigma(i_1), \ldots, \sigma^{k_1}(i_1)) \ldots (i_s,\, \sigma(i_s), \ldots, \sigma^{k_s}(i_s))$.
■

Del modo en que se constituyen los ciclos de σ, se deduce que esta descomposición de σ en producto de ciclos disjuntos, es única. Si σ es un ciclo de longitud k, diremos que es un k - ciclo.

Nuestro próximo objetivo es probar que toda permutación en S_n se puede expresar como el producto de ciclos de longitud 2. En este caso, la descomposición no es única, sin embargo, la paridad del número de ciclos que aparecen en la descomposición dada, sí es invariante. Comenzaremos por denominar a los ciclos de longitud 2, transposiciones.

Lema 1.36 *Si σ es un k - ciclo en S_n, $k > 1$, $n \geq k$, entonces σ es igual a un producto de transposiciones.*

Prueba Sea $\sigma = (i_1, \ldots, i_k) \in S_n$. Si $k = 2$, σ es una transposición y no hay nada que probar.

Si $k > 2$, es fácil ver que, si $\delta = (i_1,\, i_k)(i_1,\, i_{k-1}) \ldots (i_1,\, i_2)$ entonces $\delta = \sigma$, pues $\delta(i_r) = \sigma(i_r)$ para $r \in \{1, \ldots, k\}$ y $\delta(j) = j = \sigma(j)$ para $j \in \{1, \ldots, n\} \backslash \{i_1, \ldots, i_k\}$. ■

La descomposición de un ciclo en producto de transposiciones no es única. Por ejemplo, $(i_1,\, i_2,\, i_3) = (i_1,\, i_3)(i_1,\, i_2) = (i_3,\, i_2)(i_3,\, i_1)$.

Teorema 1.37 *Si σ es una permutación en S_n, entonces σ se puede expresar como un producto de transposiciones. Si $\sigma = \delta_1\,\delta_2 \ldots \delta_k = \alpha_1\,\alpha_2 \ldots \alpha_s$, donde δ_i, α_j son transposiciones, para $i \in \{1, \ldots, k\}$ y $j \in \{1, \ldots, s\}$, entonces $(-1)^k = (-1)^s$.*

Prueba Sea $\sigma \in S_n$. Como $\sigma = \sigma_1 \ldots \sigma_m$, donde σ_i es un ciclo, para $i \in \{1, \ldots, n\}$, y, en virtud del lema anterior, cada σ_i es un producto de trnasposiciones, entonces σ es igual a un producto de transposiciones.

Supongamos que $\sigma = \delta_1\delta_2 \ldots \delta_k = \alpha_1\alpha_2 \ldots \alpha_s$, donde δ_i, α_j son transposiciones, para $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, s\}$.

Sea $\mathbb{Q}[x_1, \ldots, x_n]$ el conjunto de los polinomios en n variables, con coeficientes en $\mathbb{Q}$, y definamos

$$\varphi_\sigma : \quad \mathbb{Q}[x_1, \ldots, x_n] \longrightarrow \mathbb{Q}[x_1, \ldots, x_n] \qquad \text{por}$$

$$\varphi_\sigma(p(x_1, \ldots, x_n)) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

En particular, si $q(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$, entonces

$$\varphi_\sigma(q(x_1, \ldots, x_n)) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}).$$

Por ejemplo, si $\sigma \in S_3$, $\sigma = (3, 1, 2)$, entonces

$\varphi_\sigma(q(x_1, x_2, x_3)) = \varphi_\sigma((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))=$
$(x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = (x_2 - x_3)(-1)(x_1 - x_2)(-1)(x_1 - x_3)=$
$(-1)^2 q(x_1, x_2, x_3) = q(x_1, x_2, x_3)$.

En general, para $\alpha \in S_n$, arbitrario, $\varphi_\alpha(q(x_1, \ldots, x_n)) = \pm q(x_1, \ldots, x_n)$, pues, siendo α una permutación (es una biyección), en el producto $\prod_{i<j}(x_{\alpha(i)} - x_{\alpha(j)})$, todos los factores del polinomio $q(x_1, \ldots, x_n)$ aparecen, sólo que algunos de ellos multiplicados por (-1).

En particular, si β es una transposición, veamos que

$$\varphi_\beta(q(x_1, \ldots, x_n)) = -q(x_1, \ldots, x_n)$$

Supongamos que $\beta = (k, m)$ con $k < m$.

Sabemos que $\varphi_\beta(q(x_1, \ldots, x_n)) = \prod_{i<j}(x_{\beta(i)} - x_{\beta(j)})$.

Ahora bien, $x_{\beta(i)} - x_{\beta(j)} = x_i - x_j$ si $i \neq k$, m, y $j \neq k$, m

Examinemos los casos en que $\{i,j\} \cap \{k,m\} \neq \phi$.

1. Los factores del tipo $(x_i - x_k)$, con $i < k$, no cambiarán de signo al aplicarse β, pues $(x_i - x_{\beta(k)}) = (x_i - x_m)$, y como $i < k < m$, el factor $(x_i - x_m)$ aparece igual en $q(x_1, \ldots, x_n)$.

2. Los factores del tipo $(x_k - x_j)$, con $j < m$, al aplicarles β se transforman en: $(x_{\beta(k)} - x_j) = (x_m - x_j) = -(x_j - x_m)$; como $j < m$, $(x_j - x_m)$ aparece en $q(x_1, \ldots, x_n)$ con signo positivo.

   Así, por cada j tal que $k < j < m$, surge un signo $(-)$ en la expresión de $\varphi_\beta(q(x_1, \ldots, x_n))$. En total, estos son $m - k - 1$ factores.

3. Los factores del tipo $(x_i - x_m)$, con $i < m$, se transforman en $(x_i - x_{\beta(m)}) = (x_i - x_k)$. Cuando $i < k$, no hay cambio de signo, y para i tal que $k \leq i < m$, obtenemos un cambio de signo por cada factor $(x_i - x_m)$. Esto, nos da, en total, $m - k$ cambios de signo.

4. Los factores del tipo $(x_m - x_j)$ no producen ningún cambio de signo, pues $(x_{\beta(m)} - x_j) = (x_k - x_j)$ y este factor está en $q(x_1, \ldots, x_n)$, ya que $k < m < j$.

   En total, tenemos $2(m-k) - 1$ cambios de signo, es decir,

$$q(x_{\beta(1)}, \ldots, x_{\beta(n)}) = (-1)^{2(m-k)-1} q(x_1, \ldots, x_n) = -q(x_1, \ldots, x_n)$$

Volviendo a la permutación $\sigma = \delta_1 \ldots \delta_k = \alpha_1 \ldots \alpha_s$, tenemos que

$$\varphi_\sigma(q(x_1, \ldots, x_n)) = (-1)^k q(x_1, \ldots, x_n) = (-1)^s q(x_1, \ldots, x_n)$$

Por lo tanto, $(-1)^k = (-1)^s$; es decir, en ambas descomposiciones hay un número par de transposiciones, o en ambas hay un número impar de transposiciones. ■

Definición 1.38 *Se dice que una permutación $\sigma \in S_n$ es par, si σ se descompone como producto de un número par de transposiciones. De otro modo, se dice que σ es impar.*

Sea $\mathcal{A}_n \subset S_n$ el conjunto de todas las permutaciones pares de S_n.

Teorema 1.39 *Si $n > 1$, entonces $\mathcal{A}_n$ es un subgrupo normal de S_n y su índice en S_n es 2.*

Prueba Para comenzar, observemos que $A_n \neq \emptyset$, pues $e = (1,2)(1,2) \in A_n$. Como S_n es finito, basta comprobar que $\mathcal{A}_n$ es cerrado respecto al producto, para concluir que $\mathcal{A}_n < S_n$. Pero es claro que el producto de dos permutaciones pares es par; así, $\mathcal{A}_n < S_n$.

Sea $V = \{1, -1\}$ y consideremos el producto usual de los números enteros en V; con esta operación, V es un grupo. Definamos $f : S_n \longrightarrow V$ por:

$$f(\sigma) = \begin{cases} 1 & \text{si} \quad \sigma \text{ es par} \\ \\ -1 & \text{si} \quad \sigma \text{ es impar} \end{cases}$$

f es un homomorfismo de grupos, pues si $\alpha, \sigma \in S_n$ y ambas son pares, $f(\alpha\sigma) = 1$, pues $\alpha\sigma$ es par; además $f(\alpha) \cdot f(\sigma) = 1$. Si α y σ son impares, $\alpha\sigma$ es par, luego $f(\alpha\sigma) = 1 = (-1)(-1) = f(\alpha)f(\sigma)$.

Si α es par y σ es impar, entonces $\alpha\sigma$ es impar y por lo tanto $f(\alpha\sigma) = -1 = f(\alpha)f(\sigma)$. Análogamente, se prueba que, si α es impar y σ es par, $f(\alpha\sigma) = f(\alpha)f(\sigma)$.

Como la identidad en V es 1, tenemos que $Ker\, f = \mathcal{A}_n$. Luego, $\mathcal{A}_n \lhd S_n$ y como $S_n/\mathcal{A}_n \cong Im\, f = V$, tenemos que $\circ(S_n/\mathcal{A}_n) = \frac{\circ(S_n)}{\circ(\mathcal{A}_n)} = 2$, lo cual significa que $i_{S_n}(\mathcal{A}_n) = 2$ ■

Del teorema anterior se desprende que $\circ(\mathcal{A}_n) = \frac{n!}{2}$. $\mathcal{A}_n$ se denomina el grupo alternante de grado n, y juega un papel fundamental en la demostración de que sólo podemos asegurar la resolución por radicales de las ecuaciones polinómicas de grado estrictamente menor que 5.

Veremos que $\mathcal{A}_5$ no contiene ningún subgrupo normal no trivial, y de hecho, lo mismo ocurre para $\mathcal{A}_n$, con $n > 5$. Esta situación amerita la siguiente definición:

Definición 1.40 *Un grupo G es simple si no contiene ningún subgrupo normal no trivial.*

La simplicidad de $\mathcal{A}_n$, para $n \geq 5$ implica que el respectivo grupo de permutaciones S_n tenga una estructura que determina la imposibilidad de resolver por radicales las ecuaciones polinómicas de grado n.

La estructura a la que nos referimos está asociada al concepto de solubilidad de un grupo (el término se debe justamente a su origen en el problema de la resolución por radicales):

Definición 1.41 *Un grupo G es soluble si existen subgrupos de G:*

$$G_0 = \{e\} \subseteq G_1 \subseteq ... \subseteq G_n = G$$

tales que

1. $G_i \lhd G_{i+1}$, *para* $i = 0, ..., n-1$
2. G_{i+1}/G_i *es abeliano, para* $i = 0, ..., n-1$

Se demuestra que S_n es soluble, para $n = 2, 3$ y 4, pero no lo es para $n \geq 5$.

Problemas:

1. Si $(G, +)$ es un grupo abeliano, probar que $T : G \longrightarrow G$ definida por $T(g) = -g$, es un automorfismo de G.
2. Sea G un grupo y Z el centro de G. Se define $\phi : G \longrightarrow Aut(G)$ por $\phi(g) = T_g, \forall\, g \in G$, donde T_g es el automorfismo de conjugación por g. Pruebe que:

   i) ϕ es un homomorfismo de grupos

   ii) $Ker\,\phi = Z$

   iii) $J(G) < Aut(G)$

   iv) $J(G) \cong G/Z$.

3. Sea G un grupo, $N \lhd G$. Pruebe que, si $\phi \in Aut(G)$, entonces $\phi(N) \lhd G$.
4. Si G es un grupo, pruebe que $J(G) \lhd Aut(G)$.
5. Sea G el grupo de Klein. Determine $Aut(G)$.
6. Sea G un grupo y $H < G$. Pruebe que, $\forall\, g \in G,\ gHg^{-1} < G$, y que $V = \bigcap_{g \in G} gHg^{-1} \lhd G$.

7. Sea $\sigma \in S_9$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \\ 4 & 1 & 5 & 3 & 2 & 7 & 9 & 8 & 6 \end{pmatrix}$$

Determine las órbitas y los ciclos de σ. Exprese σ como producto de ciclos disjuntos y como producto de transposiciones.

8. Pruebe que $(1, 2, \ldots, n)^{-1} = (n,\, n-1,\, n-2, \ldots, 2, 1)$. Generalice este resultado:
¿ Cuál es el inverso de un k - ciclo $(i_1,\, i_2, \ldots, i_k)$?

9. Determine la descomposición en ciclos disjuntos de σ^n, para todo $n > 1$, si $\sigma = (1, 2, \ldots, 8)$. ¿ Cuál es el orden de σ? En general, ¿ cuál es el orden de un n - ciclo?

10. Sean $\alpha_1, \ldots, \alpha_k$ ciclos disjuntos en S_n, tales que $\forall\, i \in \{1, \ldots, k\}$, m_i es la longitud de α_i. Determine el orden de $\alpha_1\alpha_2 \ldots \alpha_k$. Si $\sigma \in S_n$, ¿ cómo se determina el orden de σ?

11. Sea σ un k - ciclo. ¿ Qué condición debe satisfacer k para que σ sea una permutación par?

12. Considere las siguientes permutaciones en S_{10} :

$\alpha = (1, 3, 4, 8), \qquad \sigma = (5, 6)(3, 7, 9)$

$\beta = (5, 10, 3), \qquad \delta = (1, 4, 5, 6)$

$\gamma = (1, 7, 9, 4, 2, 5, 6), \qquad \lambda = (1, 7, 5, 6, 10)$

Calcule $\sigma\alpha\sigma^{-1}, \quad \delta\beta\delta^{-1}, \quad \lambda\gamma\lambda^{-1}$.

¿ Podría generalizarse el resultado acerca de la descomposición en ciclos de la permutación $\theta\alpha\theta^{-1}$, cuando α es un k - ciclo y θ una permutación cualquiera?

13. Pruebe que, si α es un k - ciclo y θ es una permutación cualquiera, entonces $\theta\alpha\theta^{-1}$ es un k - ciclo; si $\alpha = (a_1, \ldots, a_k)$, entonces
$\theta\alpha\theta^{-1} = (\theta(a_1), \theta(a_2), \ldots, \theta(a_k))$.

14. Pruebe que, $\forall\, n > 1,\ S_n$ es generado por (1,2) y $(1, 2, \ldots, n)$. Sugerencia:

a) Pruebe que, si $\alpha = (1, 2, \ldots, n)$, entonces $\alpha(1,2)\alpha^{-1} = (2,3)$, $\alpha(2,3)\alpha^{-1} = (3,4)$, etc.

b) Muestre que $(1,2)(2,3)(1,2) = (1,3)$, $\quad (1,3)(3,4)(1,3) = (1,4)$ y, por un proceso recursivo, muestre que (1,2) y $(1, 2, \ldots, n)$ generan a todas las transposiciones de la forma $(1, m)$, con $m \leq n$.

c) Muestre que cualquier transposición (m, k) se expresa como producto de transposiciones del tipo $(1, j)$, y concluya que S_n está generado por (1,2) y $(1, 2, \ldots, n)$.

1.6.1. La ecuación de clase de un grupo

En esta sección nos ocuparemos de definir una nueva relación de equivalencia en un grupo G cualquiera. Se trata de la relación de conjugación. Al considerar las clases de equivalencia de esta relación, obtendremos resultados importantes, los cuales tienen consecuencias particularmente poderosas en el caso de los grupos finitos.

Definición 1.42 *Sea G un grupo, y sean $a, b \in G$. Decimos que b es un conjugado de a en G, si existe $g \in G$ tal que $b = gag^{-1}$.*

Se define la relación de conjugación en G, de la manera siguiente:
$a \sim b \Leftrightarrow b$ es un conjugado de a.

Lema 1.43 *Si G es un grupo, la relación de conjugación en G es una relación de equivalencia.*

Prueba Se deja como ejercicio para el lector.

Es oportuno notar que, si G es abeliano, la relación de conjugación es trivial, puesto que $a \sim b \Leftrightarrow a = b$.

Para $a \in G$, denotaremos por $\mathcal{C}(a)$ a la clase de equivalencia de a respecto a la relación de conjugación, y la llamaremos la clase de conjugados de a en G.

Nos dedicaremos ahora a la tarea de determinar la cardinalidad de $\mathcal{C}(a)$, en el caso en que G es finito. Usaremos la notación $|\mathcal{C}(a)| = C_a$.

Definición 1.44 *Sea G un grupo, y $a \in G$. Definimos el normalizador de a en G como el conjunto*

$$N(a) = \{g \in G \,:\, ga = ag\}$$

$N(a)$ es, entonces, el conjunto de todos los elementos de G que conmutan con a.

Observemos que $N(a) \neq \phi$, $\forall\, a \in G$, pues $(a) \subset N(a)$. El normalizador de a es un conjunto que se asocia naturalmente con $\mathcal{C}(a)$ puesto que, para cada $g \in N(a)$, el conjugado de a dado por gag^{-1} es sencillamente, a : como g conmuta con $a, gag^{-1} = agg^{-1} = ae = a$.

En otras palabras, en $\mathcal{C}(a)$, los conjugados de a que son distintos de a son de la forma cac^{-1}, con $c \notin N(a)$.

Esta situación, aunada al lema que sigue, permitirá obtener una manera precisa de contar los elementos de $\mathcal{C}(a)$, cuando G es un grupo finito.

Lema 1.45 *Si G es un grupo, y $a \in G$ entonces $N(a) < G$.*

Prueba Se deja como ejercicio al lector.

Teorema 1.46 *Si G es un grupo finito, y $a \in G$, entonces $C_a = i_G(N(a)) = \frac{\circ(G)}{\circ(N(a))}$.*

Prueba Consideremos la siguiente función:

$$\varphi : \mathcal{C}(a) \longrightarrow \{gN(a) \,:\, g \in G\}$$

definida, para todo $c \in G$, por $\varphi(cac^{-1}) = cN(a)$.

Veamos que φ está bien definida. Supongamos que $r, s \in G$, y que $rar^{-1} = sas^{-1}$. Entonces, $rar^{-1}s = sa$ y $a(r^{-1}s) = (r^{-1}s)a$. Así, vemos que $r^{-1}s \in N(a)$ y por lo tanto, $rN(a) = sN(a)$.

Verificaremos ahora que φ es biyectiva.

Sean $u, v \in G$ tales que $\varphi(uau^{-1}) = \varphi(vav^{-1})$, es decir, $uN(a) = vN(a)$. Entonces $u^{-1}v \in N(a)$ y tenemos que $(u^{-1}v)a = a(u^{-1}v)$, es decir, $vav^{-1} = uau^{-1}$, luego φ es inyectiva.

Finalmente, si $g \in G,\ \varphi(gag^{-1}) = gN(a)$, y por lo tanto φ es sobreyectiva.

■

Deducimos de este teorema el siguiente colorario, de manera inmediata:

Corolario 1.47 *(Ecuación de Clase del grupo G)*
Si G es un grupo finito, entonces $\circ(G) = \sum \frac{\circ(G)}{\circ(N(a))}$, y en esta suma interviene un solo elemento a por cada clase de conjugación en G.

A continuación, presentamos algunos resultados que se derivan del Teorema 1.46, y que tienen una importancia singular en la teoría de grupos finitos.

Comenzaremos con un teorema que establece una condición suficiente para que el centro de un grupo G sea distinto de $\{e\}$. Recordemos que el centro de G es el subgrupo de G:

$$Z(G) = \{g \in G \,:\, ga = ag,\ \forall\, a \in G\}$$

La ecuación de clase es la herramienta que nos permitirá concluir que $\circ(Z(G)) > 1$.

Teorema 1.48 *Si G es un grupo y $\circ(G) = p^n$, p primo, entonces $Z(G) \neq \{e\}$.*

Prueba Supongamos que p es primo y que $\circ(G) = p^n$. Sea $a \in G$, $a \neq e$; por el teorema de Lagrange, $\circ(N(a))|p^n$, luego $\circ(N(a)) = p^{k_a}$, para algún k_a tal que $1 \leq k_a \leq n$. Por otra parte, k_a alcanza el valor n si y sólo si $a \in Z(G)$.

La ecuación de clase de G es: $p^n = \sum \left(\frac{p^n}{p^{k_a}}\right)$, donde tomamos un elemento a por cada clase de conjugación.

Ahora bien, para cada $v \in Z(G)$, su clase de conjugación es $\{v\}$, de manera que cada $v \in Z(G)$ aporta un término a esta sumatoria, y ese término es $1 = \frac{p^n}{p^{k_v}} = \frac{p^n}{p^n}$.

Así, si $\circ(Z(G)) = m$, se tiene que la ecuación de clase de G se puede expresar así:

$$p^n = m + \sum_{k_a < n} \frac{p^n}{p^{k_a}}$$

Como $p|p^n$ y $p|\sum_{k_a<n} \frac{p^n}{p^{k_a}}$, resulta que $p|m$. Por lo tanto, $m > 1$ y $Z(G) \neq \{e\}$

■

Corolario 1.49 *Si G es un grupo tal que $\circ(G) = p^2$, con p primo, entonces G es abeliano.*

Prueba Probaremos que, si $\circ(G) = p^2$, y p es primo entonces $Z(G) = G$. Por el Teorema anterior y el Teorema de Lagrange, $\circ(Z(G)) = p$ ó $\circ(Z(G)) = p^2$. Mostraremos que esta última es la única opción posible.

Supongamos que $\circ(Z(G)) = p$. Sea $a \in G \backslash Z(G)$; entonces $a \in N(a)$ y $Z(G) \subset N(a)$, luego $\circ(N(a)) > \circ(Z(G))$, lo cual implica que $\circ(N(a)) = p^2$, de nuevo, por el Teorema de Lagrange. Esto significa que $a \in Z(G)$, contra lo supuesto. Así, $\circ(Z(G)) = p^2$ y $Z(G) = G$ ■

Otro importante uso de la conjugación en un grupo viene dado por su efecto sobre las permutaciones en el grupo S_n. Por el teorema 1.35, dada una permutación $\sigma \in S_n$, ésta puede descomponerse de manera única como producto de ciclos disjuntos:

$$\sigma = (i_1, \ldots, i_{r_1})(j_1, \ldots, j_{r_2}) \ldots (k_1, \ldots, k_{r_s}),$$

donde $r_1 + r_2 + \ldots + r_s = n$. Aquí, incluimos en los ciclos de la descomposición, aquellos de longitud 1 que señalan los elementos que quedan fijos por σ. Por ejemplo, si $\sigma \in S_{10}$, y

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \\ 5 & 4 & 3 & 2 & 6 & 1 & 7 & 10 & 8 & 9 \end{pmatrix}$$

entonces $\sigma = (3)(7)(1,5,6)(2,4)(8,10,9)$

Siempre podemos ordenar los ciclos, según su longitud, de menor a mayor:

$$\sigma = (3)(7)(2,4)(1,5,6)(8,10,9)$$

y podemos asociar a σ la sucesión de longitudes de sus ciclos, en orden no decreciente:

$$\{1,\ 1,\ 2,\ 3,\ 3\}$$

Esta sucesión, como observamos antes, constituye una partición del número 10, pues 1+1+2+3+3=10. Esta situación motiva la siguiente definición.

Definición 1.50 *Dada una permutación $\sigma \in S_n$, si la descomposición de σ en ciclos disjuntos es $(i_1, \ldots, i_{r_1})(j_1, \ldots, j_{r_2}) \ldots (k_1, \ldots, k_{r_s})$, con $r_1 \leq r_2 \leq \ldots \leq r_s$, y $r_1 + \ldots + r_s = n$, entonces se llama ciclo de descomposición de σ a la sucesión $\{r_1, r_2, \ldots, r_s\}$.*

La asignación de un determinado ciclo de descomposición a una partición σ dada, no es biunívoca, puesto que es evidente que dos permutaciones distintas pueden tener exactamente el mismo ciclo de descomposición. Ahora bien, el siguiente resultado nos muestra que dos permutaciones con el mismo ciclo de descomposición son conjugadas.

Proposición 1.51 *Dos permutaciones $\sigma, \alpha \in S_n$ son conjugadas si y sólo si σ y α tienen el mismo ciclo de descomposición.*

Prueba Sean $\sigma, \beta \in S_n$, y sea la descomposición de σ en ciclos disjuntos: $\sigma = (i_1, \ldots, i_{r_1})(j_1, \ldots, j_{r_2}) \ldots (k_1, \ldots, k_{r_s})$; sea $\alpha = \beta\sigma\beta^{-1}$.

Veamos que $\alpha(\beta(i_1)) = \beta(i_2)$. En efecto,

$$\alpha(\beta(i_1)) = \beta\sigma\beta^{-1}(\beta(i_1)) = \beta[\sigma(i_1)] = \beta(i_2)$$

De manera análoga, se verifica que, para cualquier $m \in \{1, \ldots, n\}$, si $\sigma(m) = t \neq m$, entonces m y t son números consecutivos en alguno de los ciclos disjuntos que componen a σ, y además $\alpha(\beta(m)) = \beta(t)$.

Si, por otra parte, $\sigma(m) = m$, entonces el ciclo (m) aparece en la descomposición de σ y también ocurre que $\alpha(\beta(m)) = \beta(m)$. En otras palabras, la descomposición de α en ciclos disjuntos es:

$$\alpha = (\beta(i_1), \ldots, \beta(i_{r_1}))(\beta(j_1), \ldots, \beta(j_{r_2})) \ldots (\beta(k_1), \ldots, \beta(k_{r_s}))$$

Recordemos que, al ser β una permutación, los ciclos anteriores resultan ser disjuntos porque los que componen a σ lo son.

Así, el ciclo de descomposición de $\alpha = \beta\sigma\beta^{-1}$ es $\{r_1, r_2, \ldots, r_s\}$, el cual coincide con el de σ.

Ahora, veamos que si dos permutaciones σ y $\alpha \in S_n$ tienen el mismo ciclo de descomposición, entonces son conjugadas. Supongamos que

$$\sigma = (i_1, \ldots, i_{r_1}) \ldots (j_1, \ldots, j_{r_s}), \qquad \text{y} \qquad \alpha = (a_1, \ldots, a_{r_1}) \ldots (b_1, \ldots, b_{r_s}).$$

El ciclo de descomposición de σ es igual al de α, y es $\{r_1, \ldots, r_s\}$. Sea $\beta \in S_n$ definida por $\beta(i_t) = a_t$, para $t \in \{1, \ldots, r\}, \ldots, \beta(j_l) = b_l$, para $l \in \{1, \ldots, r_s\}$.

β está bien definida y es biyectiva por el hecho de ser disjuntos los ciclos de la descomposición de σ y de α.

Por el razonamiento anterior, es claro que $\alpha = \beta\sigma\beta^{-1}$.

Corolario 1.52 *Si $p(n)$ es el número de particiones que tiene el número natural n, entonces el número de clases de conjugación distintas que hay en S_n es igual a $p(n)$.*

Prueba Dada cualquier partición $\{r_1, r_2, \ldots, r_s\}$ de n, podemos definir una permutación $\sigma \in S_n$ de manera tal que su ciclo de descomposición sea $\{r_1, \ldots, r_s\}$. Basta tomar, por ejemplo,

$$\sigma = (1, 2, \ldots, r_1)(r_1 + 1,\, r_1 + 2, \ldots, r_1 + r_2) \ldots \left(\sum_{i=1}^{s-1} r_i + 1, \ldots, \sum_{i=1}^{s} r_i \right).$$

Por la proposición anterior, la clase de conjugación de σ está constituida por todas las permutaciones que tienen el ciclo de descomposición $\{r_1, \ldots, r_s\}$.

Así, obtenemos que hay tantas clases de conjugación distintas en S_n, como particiones de n.

Ahora bien, utilizando la igualdad $C_a = \frac{\circ(G)}{\circ(N(a))}$, podemos calcular el orden del normalizador de una permutación $\sigma \in S_n$, siempre que conozcamos su ciclo de descomposición, y, además, algunas fórmulas de combinatoria que nos permitan contar los elementos de C_σ, la clase de conjugación de σ.

Ejemplo 1.24 *Sea $\sigma = (n-1, n) \in S_n$. Sabiendo que*
$\mathcal{C}(\sigma) = \{\alpha \in S_n : \alpha$ es una transposición$\}$ podemos calcular $C_\sigma = |\mathcal{C}(\sigma)| = \binom{n}{2} = \frac{n(n-1)}{2}$.

Así, $\circ(N(\sigma)) = \frac{\circ(S_n)}{C_\sigma} = \frac{n!}{\frac{n(n-1)}{2}} = 2(n-2)!$

Es decir, el subgrupo de todas las permutaciones de S_n que comutan con $(n-1, n)$, tiene orden $2(n-2)!$

Ejercicio:

Sabiendo que $\circ(N(\sigma)) = 2(n-2)!$, determine todos los elementos que pertenecen a $N(\sigma)$.

Problemas:

1. *a*) Sea G un grupo y $H \lhd G$. Pruebe que, para todo $a \in H$, $\mathcal{C}(a) \subset H$.

   b) Pruebe que $\circ(H) = \sum C_a$, donde intervienen en la suma ciertos elementos $a \in H$.

2. *a*) Sean $m, n \in \mathbb{N}$, $1 < m \leq n$. Pruebe que, en S_n, el m-ciclo $(1, 2, \ldots, m)$ tiene $(\frac{1}{m})(\frac{n!}{(n-m)!})$ conjugados.

   b) Pruebe que si $\alpha \in S_n$ es tal que $\alpha(1, 2, \ldots, m) = (1, 2, \ldots, m)\alpha$, entonces $\alpha = (1, 2, \ldots, m)^i\sigma$, donde $i \in \{0, 1, \ldots, m-1\}$, y $\sigma \in S_n$ es tal que $\sigma(j) = j$, $\forall j \in \{1, \ldots, m\}$.

3. Sea G un grupo finito y $a \in G$. Pruebe que si a tiene sólo 2 conjugados en G, entonces existe $H < G$, H no trivial, tal que $H \lhd G$.

4. Sea $n \geq 4$. Dada la permutación $\sigma = (1, 2)(3, 4) \in S_n$, determine $C_\sigma = |\mathcal{C}(\sigma)|$, y describa los elementos de S_n que conmutan con σ.

5. Sea p un número primo. Encuentre el número de permutaciones $\alpha \in S_p$ tales que $\alpha^p = e$.

6. Determine todas las clases de conjugación en A_5 y calcule la cardinalidad de cada una de ellas. Verifique que se cumple la igualdad del problema 1, parte b), en este caso.

7. Usando los resultados de los problemas 1 y 6, pruebe que A_5 es simple.

   Sugerencia: Observe que $(3, 4, 5)(1, 3, 4) = (1, 4)(3, 5)$ y $[(1, 2)(3, 4)][(1, 2)(3, 5)] = (3, 5, 4)$.

Capítulo 2

Anillos

2.1. Definiciones y propiedades básicas

El concepto de anillo surge como generalización de la estructura que se encuentra en el conjunto $\mathbb{Z}$ de los números enteros y también en el conjunto $\mathbb{R}[x]$, de los polinomios en una indeterminada con coefientes en $\mathbb{R}$. En ambos conjuntos están definidas las operaciones suma y producto, con propiedades algebraicas comunes, de las cuales, las más básicas son las que definen un anillo abstracto.

Definición 2.1 *Sea $\mathcal{A}$ un conjunto no vacío y supongamos que hay operaciones binarias definidas en $\mathcal{A}$, denotadas por "+" y "$\cdot$", llamadas suma y producto respectivamente; decimos que $(\mathcal{A}, +, \cdot)$ es un anillo si se cumple lo siguiente:*

1. *$(\mathcal{A}, +)$ es un grupo abeliano*
2. *El producto en $\mathcal{A}$ es asociativo: $(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad \forall\, a, b, c \in \mathcal{A}$*
3. *Si $a, b, c \in \mathcal{A}$, entonces $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$*

Si, además, ocurre que existe un elemento $1 \in \mathcal{A}$, tal que $1 \cdot a = a \cdot 1 = a, \quad \forall\, a \in \mathcal{A}$, se dice que $\mathcal{A}$ es un anillo con identidad.

Si el producto en $\mathcal{A}$ es conmutativo, se dice que $\mathcal{A}$ es un anillo conmutativo.

Ejemplo 2.1 *$(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con identidad.*

Ejemplo 2.2 $(\mathbb{R}[x], +, \cdot)$ *es un anillo conmutativo, cuyo elemento identidad es el polinomio constante igual a 1.*

Ejemplo 2.3

$(2\mathbb{Z}, +, \cdot)$ *es un anillo conmutativo, sin elemento identidad.*

Ejemplo 2.4 *Sea* $\mathcal{M}_{n\times n}(\mathbb{R})$ *el conjunto de las matrices* $n\times n$ *con coeficientes en* $\mathbb{R}$*. Definiendo la suma y el producto usuales de matrices, obtenemos que* $(\mathcal{M}_{n\times n}(\mathbb{R}), +, \cdot)$ *es un anillo no conmutativo con identidad.*

Ejemplo 2.5 $(\mathbb{Z}_n, +, \cdot)$ *es un anillo conmutativo con identidad, para todo* $n \in \mathbb{N}$*, tomando como suma y producto, los usualmente definidos para las clases de congruencia módulo* n*.*

Si n *es primo, además se cumple que todo elemento no nulo de* $\mathbb{Z}_n$ *tiene un inverso multiplicativo.*

Definición 2.2 *Un anillo conmutativo* $\mathcal{A}$ *con identidad es un cuerpo si todo elemento no nulo de* $\mathcal{A}$ *tiene inverso multiplicativo en* $\mathcal{A}$*.*

Ejemplo 2.6 $(\mathbb{Q}, +, \cdot)$*,* $(\mathbb{R}, +, \cdot)$ *y* $(\mathbb{C}, +, \cdot)$ *son cuerpos, al igual que* $(\mathbb{Z}_n, +, \cdot)$*, con* n *primo.*

Veremos, en lo que sigue, algunas de las propiedades elementales que se deducen de los axiomas que definen a un anillo.

Lema 2.3 *Sea* $(\mathcal{A}, +, \cdot)$ *un anillo, y* 0 *su elemento identidad para la suma. Para cualesquiera* $a, b \in \mathcal{A}$*, se cumple:*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. *Si* $\mathcal{A}$ *es un anillo con identidad igual a 1, entonces también se cumple que*
   $(-1) \cdot a = -a$.

Prueba
1) Sea $a \in \mathcal{A}$. Como $0 + 0 = 0$, tenemos que $a \cdot (0 + 0) = a \cdot 0$ y por la propiedad distributiva, $a \cdot 0 = a \cdot 0 + a \cdot 0$. Siendo $(\mathcal{A}, +)$ un grupo, vale la ley de cancelación y por lo tanto $a \cdot 0 = 0$. Análogamente, se prueba que $0 \cdot a = 0$.
2) Para ver que $a(-b) = -(ab)$, basta con mostrar que $ab + a(-b) = 0$, tomando en cuenta la unicidad del inverso para la suma en $\mathcal{A}$, de ab.

Pero $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$. Análogamente, se prueba que $(-a)b = -(ab)$. La prueba de las partes 3) y 4), se dejan como ejercicio para el lector ■

Las propiedades enunciadas en el lema anterior resultan muy familiares por ser propiedades de los enteros; sin embargo, hay propiedades de los enteros que no son válidas en cualquier anillo $\mathcal{A}$, y una de ellas es la siguiente: si $ab = 0$, entonces $a = 0$ ó $b = 0$.

Un anillo en el que esta propiedad no vale es $\mathbb{Z}_n$, cuando n no es primo. Por ejemplo, en $\mathbb{Z}_6$, tenemos que

$$\overline{3} \cdot \overline{2} = \overline{6} = \overline{0} \qquad \text{y} \qquad \overline{3} \neq \overline{0},\ \overline{2} \neq \overline{0}.$$

Decimos, en este caso, que $\overline{3}$ y $\overline{2}$ son divisores de cero en $\mathbb{Z}_6$. Esta es una definición que se establece de manera general para los anillos conmutativos.

Definición 2.4 *Si $\mathcal{A}$ es un anillo conmutativo y $a \in \mathcal{A},\ a \neq 0$, se dice que a es un divisor de cero si existe $b \in \mathcal{A},\ b \neq 0$, tal que $ab = 0$.*

Definición 2.5 *Un anillo conmutativo es un dominio entero o un dominio de integridad si no tiene divisores de cero.*

A continuación, demostraremos una proposición que explica la diferencia entre $\mathbb{Z}_n$ y $\mathbb{Z}_p$, siendo p primo y n compuesto: el primero no es un cuerpo, mientras que el segundo sí lo es.

Proposición 2.6 *Si $\mathcal{A}$ es un dominio de integridad finito, entonces $\mathcal{A}$ es un cuerpo.*

Prueba
Sea $\mathcal{A} = \{a_1, \ldots, a_n\}$ un dominio de integridad. Para probar que $\mathcal{A}$ es un cuerpo, basta mostrar la existencia de un elemento identidad en $\mathcal{A}$, y de un inverso multiplicativo para cada elemento no nulo de $\mathcal{A}$.

Sea $x \in \mathcal{A},\ x \neq 0$, y consideremos el conjunto $x\mathcal{A} = \{xa_1, xa_2, \ldots, xa_n\}$. $x\mathcal{A} \subset \mathcal{A}$ por ser $\mathcal{A}$ cerrado respecto al producto.

Por otra parte, si $i \neq j$, $xa_i \neq xa_j$, pues si fuese $xa_i = xa_j$, tendríamos que $x(a_i - a_j) = 0$. Por ser $\mathcal{A}$ un dominio de integridad, tendría que ser $x = 0$ ó $a_i - a_j = 0$ y ninguna de las dos igualdades es cierta, por construcción. Así, $xa_i \neq xa_j$ si $i \neq j$, lo que significa que $x\mathcal{A} = \mathcal{A}$, puesto que $x\mathcal{A} \subset \mathcal{A}$ y ambos conjuntos tienen exactamente n elementos. Como $x \in \mathcal{A}$, existe $r \in \{1, \ldots, n\}$ tal que $x = xa_r$. $\mathcal{A}$ es un dominio de integridad, y por lo tanto es conmutativo, y así $x = xa_r = a_r x$. Veremos que $a_r = 1$ (elemento identidad para el producto en $\mathcal{A}$).

Sea $y \in \mathcal{A}$; como $y = xa_k$ para algún $k \in \{1, \ldots, n\}$, tenemos que $ya_r = (xa_k)a_r = a_k x = y$. Así, $a_r = 1$. Como $1 \in \mathcal{A}$, también existe $t \in \{1, \ldots, n\}$ tal que $1 = xa_t$, y esto significa que x tiene un inverso multiplicativo en A. Siendo $x \neq 0$ arbitrario, hemos probado que $\mathcal{A}$ es un cuerpo.

Corolario 2.7 *Si p es primo, entonces $\mathbb{Z}_p$ es un cuerpo.*

Prueba Veamos que $\mathbb{Z}_p$ es un dominio de integridad. Como $\mathbb{Z}_p$ es conmutativo, basta verificar que $\mathbb{Z}_p$ no tiene divisores de cero. Sean $\overline{a}$, $\overline{b} \in \mathbb{Z}_p$ tales que $\overline{a} \cdot \overline{b} = \overline{0}$. Esto significa que $ab \equiv 0 (mod\ p)$; en otras palabras $p|a \cdot b$. Como p es primo, esto implica que $p|a$ ó $p|b$, lo que equivale a decir que $\overline{a} = \overline{0}$ ó $\overline{b} = \overline{0}$. Así, $\mathbb{Z}_p$ es un dominio de integridad, y por la proposición anterior, siendo $\mathbb{Z}_p$ finito, se obtiene que $\mathbb{Z}_p$ es un cuerpo.

Problemas:

1. Pruebe que todo cuerpo es un dominio de integridad.

2. Pruebe que $\mathcal{A}$ es un dominio de integridad si, y sólo si, vale la ley de cancelación para el producto en $\mathcal{A}$.

3. Encuentre un ejemplo de un dominio de integridad infinito que no sea un cuerpo.

4. Sea $\mathcal{A}$ un anillo. Si $a \in \mathcal{A}$ y $n \in \mathbb{Z}$, definimos na como en el Capítulo 1, para cualquier grupo abeliano.

   Pruebe que, para $n, m \in \mathbb{Z}$, $a, b \in \mathcal{A}$ se cumple que $(na)(mb) = (nm)(ab)$.

5. Sea $\mathcal{A}$ un dominio de integridad. Si existe $a \in \mathcal{A},\ a \neq 0$, y $n \in \mathbb{Z},\ n \neq 0$, tal que $na = 0$, se define la característica de $\mathcal{A}$, (y se denotará $Car(\mathcal{A})$) de la manera siguiente:

$$Car(\mathcal{A}) = \text{mín}\{n \in \mathbb{Z},\ n > 0 \,:\, na = 0,\ \text{para algún } a \neq 0 \in \mathcal{A}\}.$$

Si no existe $n > 0$ tal que $na = 0$ para algún $a \neq 0 \in \mathcal{A}$, se dice que $\mathcal{A}$ tiene característica cero.

a) Pruebe que si $\mathcal{A}$ es un dominio de integridad, y $Car(\mathcal{A}) = p$, entonces $pa = 0,\ \forall\, a \in \mathcal{A}$.

b) Si $\mathcal{A}$ es un dominio de integridad y $Car(\mathcal{A}) \neq 0$, entonces $Car(\mathcal{A}) = p$, con p primo.

2.2. Homomorfismos de Anillos, Ideales y Anillos Cocientes

Observemos un homomorfismo del grupo $(\mathbb{Z}, +)$ en sí mismo, por ejemplo:

$$f : \mathbb{Z} \longrightarrow \mathbb{Z} \qquad \text{definida por} \qquad f(n) = 5n$$

Ahora que tenemos la noción de anillo, y que sabemos que $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con identidad, nos podemos preguntar si f también preserva la operación producto en $\mathbb{Z}$, es decir, si $f(m \cdot n) = f(m) \cdot f(n)$, para cualesquiera $m, n \in \mathbb{Z}$. Claramente, la respuesta es negativa, pues para $m = 2,\ n = 3$, tenemos

$$f(2 \cdot 3) = f(6) = 5 \cdot 6 = 30$$

mientras que

$$f(2) \cdot f(3) = (5 \cdot 2)(5 \cdot 3) = 150$$

Sin embargo, resulta natural considerar la necesidad de exigir que los homomorfismos entre anillos preserven ambas operaciones.

Dejamos como ejercicio para el lector, probar que si

$$f : \mathbb{Z} \longrightarrow \mathbb{Z} \qquad \text{satisface :}$$

i) $f(n+m) = f(n) + f(m)$

ii) $f(n \cdot m) = f(n) \cdot f(m)$

iii) f no es idénticamente nula

entonces f es la función identidad de $\mathbb{Z}$. En otras palabras, si definimos el homomorfismo de anillos como aquella función f que satisface i) y ii), entonces el único homomorfismo de anillos, no nulo, de $\mathbb{Z}$ sobre sí mismo, es la identidad.

Este hecho podría inducirnos a pensar que las condiciones i), ii) son demasiado restrictivas, pero lo cierto es que nos permiten explotar la riqueza de la estructura de un anillo, y, por esa razón, establecer elementos fundamentales de la teoría general de anillos.

Definición 2.8 *Sean $\mathcal{A}_1$, $\mathcal{A}_2$ anillos, y $f : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ una función. Se dice que f es un homomorfismo de anillos si se cumplen las dos condiciones siguientes, para cualesquiera $a, b \in \mathcal{A}_1$:*

i) $f(a+b) = f(a) + f(b)$

ii) $f(a \cdot b) = f(a) \cdot f(b)$

Ejemplo 2.7 *1. La proyección canónica sobre el cociente*

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$

es un homomorfismo de anillos, por el modo en que se definen las operaciones de suma y producto módulo n:

$$\pi(m+p) = \overline{m+p} = \overline{m} + \overline{p}$$

$$\pi(m \cdot p) = \overline{m \cdot p} = \overline{m} \cdot \overline{p}$$

2. Sea $\mathcal{A} = \{f : [-1,1] \longrightarrow \mathbb{R} : f \text{ es continua}\}$. Se definen la suma y el producto de funciones de la manera usual, y se obtiene que $(\mathcal{A}, +, \cdot)$ es un anillo conmutativo con identidad.

Sea $\varphi : \mathcal{A} \longrightarrow \mathbb{R}$ definida por $\varphi(f) = f(0)$. Se deja como ejercicio para el lector, probar que φ es un homomorfismo de anillos.

3. *Sea* $f : \mathbb{C} \longrightarrow \mathbb{C}$ *la función definida por* $f(a+bi) = a - bi$. *El lector puede probar como ejercicio, que* f *es un homomorfismo de anillos.*

Dado un homomorfismo de anillos $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$, puesto que φ es un homomorfismo entre los grupos abelianos $\mathcal{A}_1$ y $\mathcal{A}_2$, sabemos que $\varphi(0) = 0$, que $\varphi(-a) = -\varphi(a),\ \forall\, a \in \mathcal{A}_1$, y que el conjunto $I = \{a \in \mathcal{A}_1 : \varphi(a) = 0\}$ es un subgrupo de $(\mathcal{A}_1, +)$, al que llamaremos el núcleo de φ.

Exploramos ahora las propiedades de I como subconjunto del anillo $\mathcal{A}_1$, es decir, tomando en cuenta su comportamiento en relación con el producto en $\mathcal{A}_1$.

En primer lugar, I es cerrado con respecto al producto, pues si $a_1,\ a_2 \in I$, entonces $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2) = 0 \cdot 0 = 0$, y por lo tanto, $a_1 \cdot a_2 \in I$. En otras palabras, I es un subanillo de $\mathcal{A}_1$.

Más aún, al observar las igualdades anteriores, dado que
$x \cdot 0 = 0 \cdot x = 0,\ \forall\, x \in \mathcal{A}_2$, tenemos que bastaría con que sólo a_1 ó sólo a_2 estuviese en I para que $a_1 \cdot a_2 \in I$; en otras palabras, $\forall\, a \in \mathcal{A}_1,\ aI \subset I$ y también $Ia \subset I$: si $a \in \mathcal{A}_1$ y $b \in I$, entonces $\varphi(ab) = \varphi(a)\varphi(b) = \varphi(a) \cdot 0 = 0$, luego $ab \in I$, de modo que resulta $aI \subset I$. Análogamente, se comprueba que $Ia \subset I,\ \forall\, a \in \mathcal{A}_1$.

Esta propiedad que posee I resulta ser muy importante, como era de esperarse, al tratarse del núcleo de un homomorfismo de anillos, y da lugar a la siguiente definición:

Definición 2.9 *Sea* $\mathcal{A}$ *un anillo,* $I \subset \mathcal{A},\ I \neq \emptyset$. *Se dice que* I *es un ideal de* $\mathcal{A}$, *si se cumple:*

1. I *es un subgrupo de* $(\mathcal{A}, +)$
2. $\forall\, a \in I,\ \forall\, r \in \mathcal{A},\ ar \in I$ *y* $ra \in I$.

Cuando se cumple que $rI \subset I,\ \forall\, r \in \mathcal{A}$, pero no necesariamente vale $Ir \subset I,\ \forall\, r \in \mathcal{A}$, se dice que I es ideal izquierdo. Cuando vale $Ir \subset I,\ \forall\, r \in \mathcal{A}$, se dice que I es un ideal derecho.

Hemos visto, entonces, que si $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ es un homomorfismo de anillos, e $I(\varphi)$ es el núcleo de φ entonces $I(\varphi)$ es un ideal de $\mathcal{A}_1$.

Como antes, daremos el nombre de isomorfismo de anillos a un homomorfismo de anillos biyectivo; un monomorfismo y un epimorfismo de anillos corresponden, respectivamente, a un homomorfismo inyectivo y a uno sobreyectivo.

Lema 2.10 *Sea $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ un homomorfismo de anillos. φ es inyectivo si y sólo si el núcleo $I(\varphi) = \{0\}$.*

Prueba Se deja como ejercicio para el lector ■

Ejemplo 2.8 *Veamos un ejemplo de un ideal no trivial en un anillo finito. Sean $n, m \in \mathbb{N}$ tales que $m|n$, y sea $\phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ la función definida por $\phi(\bar{j}(mod\, n)) = \bar{j}(mod\, m)$. Es fácil ver que ϕ es un homomorfismo de anillos, cuyo núcleo $I(\phi)$ es $\{\overline{km} \in \mathbb{Z}_n : 0 \leq k < \frac{n}{m}\}$. $I(\phi)$ es no trivial si $n > m$.*

En lo que sigue, prepararemos el terreno para establecer los teoremas análogos a los teoremas de isomorfismos de grupos. En primer lugar, es fácil ver que la imagen $\varphi(\mathcal{A}_1)$ de un homomorfismo de anillos $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$, es un subanillo de $\mathcal{A}_2$.

Por otra parte, es necesario investigar la estructura del grupo cociente $\mathcal{A}_1/I(\varphi)$, que juega un papel central en los teoremas de isomorfismos de grupos, para determinar si se trata, en este caso, de un anillo al que pudiésemos llamar anillo cociente.

Dado que $(\mathcal{A}_1/I(\varphi), +)$ es un grupo cuyos elementos son las clases laterales $I(\varphi) + a$, con $a \in \mathcal{A}_1$, comenzaremos por determinar si el producto en $\mathcal{A}_1/I(\varphi)$ se puede definir como sigue:

$$(I(\varphi) + a)(I(\varphi) + b) = I(\varphi) + (ab)$$

Para que este producto quede bien definido, es necesario no dependa de los representantes de cada clase elegidos. Veamos que es ese el caso:

Sean a, a', b, $b' \in \mathcal{A}_1$ tales que $I(\varphi)+a = I(\varphi)+a'$, $I(\varphi)+b = I(\varphi)+b'$.

Debe verificarse que $I(\varphi) + (ab) = I(\varphi) + (a'b')$.

Ahora bien, esta última igualdad vale si $ab - a'b' \in I(\varphi)$. Pero

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'$$

Como $(b - b') \in I(\varphi)$ y $(a - a') \in I(\varphi)$ y además $I(\varphi)$ es un ideal de $\mathcal{A}_1$, entonces $a(b - b') \in I(\varphi)$ y $(a - a')b' \in I(\varphi)$, por lo tanto $ab - a'b' \in I(\varphi)$, y el producto está bien definido.

Podemos ahora demostrar que los axiomas que definen a un anillo se verifican en el cociente $\mathcal{A}_1/I(\varphi)$; es la proposición que enunciamos a continuación, donde el ideal por el cual se toma el cociente es cualquiera; no nos

restringiremos al caso del ideal $I(\varphi)$, núcleo de un homomorfismo de anillos φ.

Proposición 2.11 *Sea $\mathcal{A}$ un anillo y $J \subset \mathcal{A}$ un ideal de $\mathcal{A}$. El cociente $\mathcal{A}/J$ es un anillo con las operaciones de suma y producto definidas por:*

$$\begin{aligned} (J+a)+(J+b) &= J+(a+b) \\ (J+a)(J+b) &= J+(ab) \end{aligned}$$

Prueba Ya vimos, en el Capítulo 1, que $(\mathcal{A}/J, +)$ es un grupo; y se deduce que es abeliano del hecho de ser $(\mathcal{A}, +)$ abeliano:

$$\forall\, a, b \in \mathcal{A},\ (J+a)+(J+b) = J+(a+b) = J+(b+a) = (J+b)+(J+a)$$

Falta verificar que el producto es asociativo y que vale la distributatividad del producto respecto a la suma, por la derecha y por la izquierda.

La asociatividad se deduce de la misma propiedad del producto en $\mathcal{A}$:

$$\begin{aligned} [(J+a)(J+b)](J+c) &= (J+ab)(J+c) = J+(ab)c = J+a(bc) = \\ (J+a)(J+bc) &= (J+a)[(J+b)(J+c)] \end{aligned}$$

Se deja como ejercicio para el lector comprobar que la distributividad del producto con respecto a la suma en $(\mathcal{A}/J, +, \cdot)$ se cumple ■

Los teoremas de isomorfismos de grupos tienen sus respectivos teoremas análogos para el caso de los anillos.

Los enunciamos a continuación, dejando su prueba como ejercicio para el lector, ya que los argumentos utilizados son similares en ambos casos.

Teorema 2.12 *Sean $\mathcal{A}_1$, $\mathcal{A}_2$ anillos y $f : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ un homomorfismo de anillos cuyo núcleo es I. Se verifica lo siguiente:*

1. $\mathcal{A}_1/I \cong Im\, f$.

2. *Si J es un ideal de $\mathcal{A}_2$, y f es sobreyectiva, entonces*

$$\mathcal{A}_1/f^{-1}(J) \cong \mathcal{A}_2/J$$

donde $f^{-1}(J) = \{x \in \mathcal{A}_1 \,:\, f(x) \in J\}$ es un ideal que contiene a I.

3. *Hay una correspondencia biyectiva entre los ideales de $\mathcal{A}_2$ y los ideales de $\mathcal{A}_1$ que contienen a I, siempre que f sea sobreyectiva.*

Problemas:

1. Sea $\mathcal{A} = \{f : [-1,1] \longrightarrow \mathbb{R} \,:\, f \text{ es continua}\}$ y sea $\phi : \mathcal{A} \longrightarrow \mathbb{R}$ definida por $\phi(f) = \displaystyle\int_{-1}^{1} f(x)dx$.

   ¿ Es ϕ un homomorfismo de anillos? ¿ Es un homomorfismo de grupos?

2. Sean $\mathcal{A}_1$ y $\mathcal{A}_2$ anillos y sea $f : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ un homomorfismo entre los grupos abelianos $\mathcal{A}_1$ y $\mathcal{A}_2$. ¿ Es f necesariamente un homomorfismo de anillos? Si su respuesta es afirmativa, pruébelo; si es negativa, encuentre un contraejemplo.

3. Sea $\mathcal{A}$ un anillo, $I \subset \mathcal{A}$, I ideal de $\mathcal{A}$. Pruebe que si $\mathcal{A}$ es un anillo con identidad y $1 \in I$, entonces $I = \mathcal{A}$.

4. Pruebe que los únicos ideales en un cuerpo K son $\{0\}$ y K.

5. Pruebe que, si K_1, K_2 son cuerpos y $T : K_1 \longrightarrow K_2$ es un homomorfismo de anillos, entonces, o bien T es un monomorfismo, o $T(x) = 0,\ \forall\, x \in K_1$.

6. Pruebe que, si $\mathcal{A}$ es un anillo y U, V son ideales de $\mathcal{A}$, entonces:

   a) $U \cap V$ es un ideal de $\mathcal{A}$

   b) $U + V = \{u + v \,:\, u \in U,\ v \in V\}$ es un ideal de $\mathcal{A}$

   c) $UV = \{u_1v_1 + \ldots + u_kv_k \,:\, u_i \in U,\ v_i \in V \text{ para } 1 \leq i \leq k\,, k > 1\}$ es un ideal de $\mathcal{A}$.

7. Si $\mathcal{A}_1$ es un anillo con identidad 1, $\mathcal{A}_2$ es un anillo cualquiera y $\phi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ un homomorfismo sobreyectivo, pruebe que $\mathcal{A}_2$ también tiene identidad y ésta es igual a $\phi(1)$.

8. Si $\mathcal{A}_1$ es un anillo con identidad 1, $\mathcal{A}_2$ un dominio de integridad, $\phi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ un homomorfismo no idénticamente nulo, pruebe que $\mathcal{A}_2$ tiene elemento identidad, igual a $\phi(1)$.

9. Si $\mathcal{A}$ es un anillo conmutativo, y $a \in \mathcal{A}$, pruebe que el conjunto $I = \{ra : r \in \mathcal{A}\}$ es un ideal de $\mathcal{A}$. I es llamado el ideal generado por a y se denota por (a).

2.3. Ideales Maximales

Ya hemos visto que, dado un ideal I de un anillo $\mathcal{A}$, el cociente $\mathcal{A}/I$ tiene estructura de anillo. Por otra parte, los cuerpos, siendo una clase especial de anillos que merecen una atención particular, entre otras razones, porque $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos, aparecen en algunas ocasiones como anillos cocientes del tipo $\mathcal{A}/I$, donde $\mathcal{A}$ no es necesariamente un cuerpo.

Es el caso, cuando $\mathcal{A}$ es conmutativo con identidad, e I es un ideal con una propiedad especial, que llamaremos maximalidad, y que definiremos a continuación.

Definición 2.13 *Sea $\mathcal{A}$ un anillo, $I \subsetneq \mathcal{A}$ un ideal. Decimos que I es un ideal maximal de $\mathcal{A}$ si para todo ideal J de $\mathcal{A}$ tal que $I \subset J \subset \mathcal{A}$, se verifica que $I = J$ ó $J = \mathcal{A}$.*

Ejemplo 2.9 *Sea $\mathcal{A} = \mathbb{Z}$, y sea $I = 7\mathbb{Z}$.*

Veamos que I es un ideal maximal de $\mathbb{Z}$. Sea J un ideal de $\mathbb{Z}$ tal que $I \subset J \subset \mathbb{Z}$.

Como todos los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, para algún $n \in \mathbb{N}$, supondremos que $J = n\mathbb{Z}$.

Por otra parte, como $7\mathbb{Z} \subset n\mathbb{Z}$, por hipótesis, necesariamente $n|7$, pues la contención anterior implica que, $\forall\, k \in \mathbb{Z}$, $7k = n \cdot m$, para algún $m \in \mathbb{Z}$. En particular, para $k = 1$, obtenemos que existe $m \in \mathbb{Z}$ tal que $7 = n \cdot m$. Como 7 es primo, resulta que $n = 7$ ó $n = 1$.

Si $n = 7$, entonces $J = 7\mathbb{Z} = I$; si $n = 1$, entonces $J = \mathbb{Z}$. Así, $7\mathbb{Z}$ es maximal en $\mathbb{Z}$.

A continuación, daremos un resultado que caracteriza a los ideales maximales, y que tiene gran importancia en la teoría de anillos.

Teorema 2.14 *Sea $\mathcal{A}$ un anillo conmutativo con identidad, y sea I un ideal de $\mathcal{A}$. I es un ideal maximal de $\mathcal{A}$ si y sólo si $\mathcal{A}/I$ es un cuerpo.*

Es inmediata la verificación de que $\mathcal{A}/I$ es un anillo conmutativo con identidad, siempre que $\mathcal{A}$ lo sea.

Para probar el resultado enunciado en el Teorema, necesitamos el siguiente Lema, que nos da una condición suficiente para que un anillo conmutativo con identidad, sea un cuerpo.

Lema 2.15 *Sea $\mathcal{A}$ un anillo conmutativo con identidad. Si los únicos ideales de $\mathcal{A}$ son $\{0\}$ y $\mathcal{A}$, entonces $\mathcal{A}$ es un cuerpo.*

Prueba Como $\mathcal{A}$ es un anillo conmutativo con identidad, basta probar que cada elemento $a \neq 0$ en $\mathcal{A}$ tiene inverso multiplicativo en $\mathcal{A}$.

Sea $a \in \mathcal{A},\ a \neq 0$. Por el ejercicio 9 de la sección anterior, sabemos que $(a) = \{ra : r \in \mathcal{A}\}$ es un ideal de $\mathcal{A}$. Como por hipótesis, $(a) = 0$ ó $(a) = \mathcal{A}$, y, siendo $a \neq 0$, y por lo tanto, $(a) \neq \{0\}$, concluimos que $(a) = \mathcal{A}$. Esto implica que $1 \in (a)$, es decir, existe $b \in \mathcal{A}$ tal que $1 = ba = ab$. En otras palabras $b = a^{-1}$, y hemos demostrado lo que requeríamos ■

Prueba del Teorema 2.14:

Supongamos, para comenzar, que $\mathcal{A}$ es un anillo conmutativo con identidad, y que I es un ideal maximal en $\mathcal{A}$. Sabemos que $\mathcal{A}/I$ es un anillo conmutativo con identidad. Veamos que los únicos ideales en $\mathcal{A}/I$ son $\{0\}$ y $\mathcal{A}/I$.

Por el teorema 2.12, sabemos que hay una correspondencia biyectiva entre los ideales de $\mathcal{A}$, que contienen a I, y los ideales de $\mathcal{A}/I$, puesto que la proyección canónica $\pi : \mathcal{A} \longrightarrow \mathcal{A}/I$ es un homomorfismo de anillos. Ahora bien, como I es maximal en $\mathcal{A}$, los únicos ideales de $\mathcal{A}$ que contienen a I son I y $\mathcal{A}$.

A estos dos ideales corresponden los ideales $\{\overline{0}\} = \{0+I\}$ y el anillo $\mathcal{A}/I$, pues $\pi(I) = 0 + I$, y $\pi(\mathcal{A}) = \mathcal{A}/I$. Por el lema anterior, el anillo $\mathcal{A}/I$ es un cuerpo.

Supongamos ahora que $\mathcal{A}/I$ es un cuerpo. Por el ejercicio 4 de la sección anterior, los únicos ideales en $\mathcal{A}/I$ son los triviales. Por la correspondencia mencionada antes, estos dos ideales, que son $\overline{0}$ y $\mathcal{A}/I$, correponden a los ideales I y $\mathcal{A}$ en $\mathcal{A}$; éstos son, por lo tanto, los únicos ideales de $\mathcal{A}$ que contienen a I, lo que significa que I es maximal en $\mathcal{A}$ ■

Con este teorema, tenemos la posibilidad de construir un cuerpo a partir de un anillo conmutativo con identidad, a través del cociente por un ideal maximal. Esta construcción es muy útil en la teoría de extensiones de cuerpos y, particularmente, en la aplicación de las herramientas de la Teoría de Galois al problema de la solubilidad de una ecuación polinómica por radicales. Veremos más adelante que, en el anillo de polinomios $\mathbb{Q}[x]$, si $p(x)$ es

un polinomio irreducible (i.e., si $p(x) = q(x) \cdot r(x)$ entonces $q(x)$ ó $r(x)$ es constante) entonces el ideal $I = \{q(x) \cdot p(x) \,:\, q(x) \in \mathbb{Q}[x]\} = (p(x))$ es un ideal maximal en $\mathbb{Q}[x]$ y por lo tanto $\mathbb{Q}[x]/I$ es un cuerpo que contiene a $\mathbb{Q}$, y al menos, una raíz de $p(x)$. Es importante resaltar que $\mathbb{Q}[x]/I$ contiene a $\mathbb{Q}$, mas no contiene al anillo $\mathbb{Q}[x]$.

Existe otra aproximación al problema de la construcción de un cuerpo a partir de un anillo, y es aquella que generaliza lo que ocurre cuando se construye al cuerpo $\mathbb{Q}$ a partir del anillo $\mathbb{Z}$.

En este caso, sí obtenemos $\mathbb{Z} \subset \mathbb{Q}$, y la construcción general que mostraremos a continuación, permite, a partir de un anillo $\mathcal{A}$, que además sea un dominio de integridad, obtener un cuerpo $\overline{\mathcal{A}}$ tal que $\mathcal{A} \subset \overline{\mathcal{A}}$, o, más precisamente, existe un anillo $\mathcal{A}' \subset \overline{\mathcal{A}}$, tal que $\mathcal{A}$ es isomorfo a $\mathcal{A}'$.

Comenzaremos por dar la definición formal de lo que acabamos de mencionar.

Definición 2.16 *Sean $\mathcal{A}$, $\mathcal{A}'$ anillos. Se dice que $\mathcal{A}$ puede sumergirse en $\mathcal{A}'$, si existe un monomorfismo de anillos $f : \mathcal{A} \longrightarrow \mathcal{A}'$. Se dice, en este caso, que f es una inmersión de $\mathcal{A}$ en $\mathcal{A}'$, y que $\mathcal{A}'$ contiene una copia de $\mathcal{A}$. Si $\mathcal{A}$ y $\mathcal{A}'$ tienen identidad, se exige también que f envíe la identidad de $\mathcal{A}$ en la de $\mathcal{A}'$.*

Ejemplo 2.10 *Si definimos $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ por $f(m) = \dfrac{m}{1}$, $\forall\, m \in \mathbb{Z}$, es fácil ver que f es un monomorfismo de anillos; así, $\mathbb{Z}$ puede sumergirse en $\mathbb{Q}$ y además es claro que $\mathbb{Z} \cong Im\, f$, donde $Im\, f$ es un subanillo de $\mathbb{Q}$.*

Teorema 2.17 *Si $\mathcal{A}$ es un dominio de integridad, existe un cuerpo $\overline{\mathcal{A}}$ tal que $\mathcal{A}$ puede sumergirse en $\overline{\mathcal{A}}$, y el cuerpo $\overline{\mathcal{A}}$ es minimal, en el sentido siguiente: si $\mathcal{F}$ es un cuerpo tal que $\mathcal{A}$ puede sumergirse en $\mathcal{F}$, entonces $\overline{\mathcal{A}}$ puede sumergirse en $\mathcal{F}$.*

Prueba Como habíamos anticipado, la construcción del cuerpo $\overline{\mathcal{A}}$, a partir del dominio de integridad $\mathcal{A}$, es una generalización de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$.

Recordemos que $\mathbb{Q}$ se define como el conjunto de las clases de equivalencia de la relación definida sobre $\mathbb{Z} \times \mathbb{Z}^*$, de la siguiente manera: $(a, b) \sim (c, d) \Leftrightarrow ad = bc$, para (a, b), $(c, d) \in \mathbb{Z} \times \mathbb{Z}^*$. Se usa la notación $\dfrac{a}{b}$ con $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, para denotar la clase de equivalencia del par $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, y se definen las operaciones suma y producto de la manera siguiente:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Procedamos, entonces, a realizar la construcción análoga, a partir del dominio de integridad $\mathcal{A}$.

Sea $\mathcal{C} = \{(a,b) : a, b \in \mathcal{A},\ b \neq 0\}$ y definamos la relación siguiente sobre $\mathcal{C}$:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

Dejamos como ejercicio para el lector, verificar que esta relación es de equivalencia, para lo cual deberá utilizarse el hecho de ser $\mathcal{A}$ un dominio de integridad. Denotaremos por $\frac{a}{b}$ a la clase de equivalencia del elemento $(a,b) \in \mathcal{C}$, y sea $\overline{\mathcal{A}} = \left\{\frac{a}{b} : (a,b) \in \mathcal{C}\right\}$.

Mostraremos ahora que $\overline{\mathcal{A}}$ es un cuerpo que satisface las condiciones del teorema.

Definamos, para comenzar, las operaciones de suma y producto del conjunto $\overline{\mathcal{A}}$ que le dan la estructura de cuerpo:

Para $\frac{a}{b}$, $\frac{c}{d}$ en $\overline{\mathcal{A}}$, definiremos su suma así:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

Su producto será definido así:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

(Las operaciones de la derecha de cada una de estas igualdades, corresponden a las del anillo $\mathcal{A}$). Debemos comprobar que estas operaciones están bien definidas. En primer lugar, como $\mathcal{A}$ es un dominio de integridad y $b \neq 0$, $d \neq 0$ tenemos que $bd \neq 0$, y así, $\frac{ad+bc}{bd}$ y $\frac{ac}{bd}$ están en $\overline{\mathcal{A}}$. Por otra parte, como $\frac{a}{b}$ y $\frac{c}{d}$ son clases de equivalencia, debemos probar que el resultado obtenido de su suma no depende de los representantes de las clases elegidos.

Sean $\frac{a'}{b'}$, $\frac{c'}{d'}$ en $\overline{\mathcal{A}}$ tales que $\frac{a'}{b'} = \frac{a}{b}$ y $\frac{c'}{d'} = \frac{c}{d}$; es decir, la clase de (a,b) y la de (a',b') coinciden, así como las de (c',d') y (c,d). Esto significa que $ab' = ba'$ y $c'd = d'c$. Queremos verificar que $\frac{a'd'+b'c'}{b'd'} = \frac{ad+bc}{bd}$, es decir, que

$$(a'd' + b'c')bd \quad = \quad (ad + bc)b'd'$$

ó

$$a'd'bd + b'c'bd \quad = \quad adb'd' + bcb'd'$$

Dado que $ab' = ba'$ y que $c'd = d'c$, el lado izquierdo de la anterior igualdad se puede escribir así: $ab'd'd + d'cbb'$. Como $\mathcal{A}$ es conmutativo, es claro que esta expresión es igual al miembro derecho de la igualdad.

Así, la clase $\frac{ad+bc}{bd}$ coincide en la clase $\frac{a'd'+b'd}{b'd'}$, y la suma está bien definida.

Veamos que el producto también lo está; para ello, basta comprobar que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ si $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$.

Pero $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ si $acb'd' = bda'c'$, y sustituyendo ab' por ba' y cd' por dc' en el miembro izquierdo de la igualdad, obtenemos el miembro derecho, gracias a la conmutatividad del producto en $\mathcal{A}$. Así, el producto queda bien definido.

Es inmediata la comprobación de que $(\overline{\mathcal{A}}, +)$ es un grupo abeliano, con $\dfrac{0}{r}$, $r \neq 0$, como elemento neutro para la suma, y, dado $\dfrac{a}{b} \in \overline{\mathcal{A}}$, $\dfrac{-a}{b}$ es su opuesto.

Veamos ahora que el producto definido en $\overline{\mathcal{A}}$ tiene las propiedades requeridas para hacer de $\overline{\mathcal{A}}$ un cuerpo: $\forall\, \dfrac{a}{b},\ \dfrac{c}{d},\ \dfrac{e}{f} \in \overline{\mathcal{A}}$,

1. Es asociativo: $\left(\dfrac{a}{b} \cdot \dfrac{c}{d}\right)\left(\dfrac{e}{f}\right) = \left(\dfrac{ac}{bd}\right)\left(\dfrac{e}{f}\right) = \dfrac{(ac)e}{(bd)f} = \dfrac{a(ce)}{b(df)} = \dfrac{a}{b}\left(\dfrac{c}{d} \cdot \dfrac{e}{f}\right)$

2. Es conmutativo: $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd} = \dfrac{ca}{db} = \left(\dfrac{c}{d}\right)\left(\dfrac{a}{b}\right)$

3. Si $a \in \mathcal{A},\ a \neq 0$, entonces $\dfrac{a}{a} \cdot \dfrac{c}{d} = \dfrac{ac}{ad}$ y $\dfrac{c}{d} = \dfrac{ac}{ad}$, pues $c(ad) = d(ac)$, por la conmutatividad del producto en $\mathcal{A}$; del mismo modo, se verifica que $\dfrac{c}{d} \cdot \dfrac{a}{a} = \dfrac{c}{d}$; luego, $\dfrac{a}{a}$ es el elemento identidad para el producto en $\overline{\mathcal{A}}$, para cualquier $a \neq 0$ en $\mathcal{A}$. Observemos que $\dfrac{a}{a} = \dfrac{b}{b},\ \forall\, a, b$ en $\mathcal{A},\ a \neq 0,\ b \neq 0$, pues $ab = ab$.

   Denotaremos por 1 al elemento identidad en $\overline{\mathcal{A}}$.

4. El producto es distributivo con respecto a la suma en $\overline{\mathcal{A}}$:

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\left(\frac{cf+ed}{df}\right)=\frac{a(cf+ed)}{bdf}=\frac{acf+aed}{bdf}=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f},$$

pues esta última expresión es igual a $\dfrac{acbf+aebd}{bdbf}$ y como

$$(acf+aed)bdbf=(acbf+aebd)bdf$$

por la conmutatividad y distributividad respecto a la suma, del producto en $\mathcal{A}$, obtenemos que $\dfrac{a}{b}\left(\dfrac{c}{d}+\dfrac{e}{f}\right)=\dfrac{a}{b}\cdot\dfrac{c}{d}+\dfrac{a}{b}\dfrac{e}{f}$

5. Sean $a\neq 0,\ b\neq 0$ en $\mathcal{A}$. Entonces $\dfrac{a}{b}\neq 0$ en $\overline{\mathcal{A}}$ y también $\dfrac{b}{a}\neq 0$.

   $\dfrac{a}{b}\cdot\dfrac{b}{a}=\dfrac{ab}{ba}=\dfrac{ab}{ab}=1\in\overline{\mathcal{A}}$ y también $\dfrac{b}{a}\cdot\dfrac{a}{b}=1$, así que todo elemento no nulo en $\overline{\mathcal{A}}$ tiene inverso multiplicativo en $\overline{\mathcal{A}}$.

   Hemos probado entonces que $\overline{\mathcal{A}}$ es un cuerpo.

Veamos que $\mathcal{A}$ puede sumergirse en $\overline{\mathcal{A}}$, definiendo $\phi:\mathcal{A}\longrightarrow\overline{\mathcal{A}}$ por: $\phi(a)=\dfrac{ab}{b}$, donde $b\in\mathcal{A},\ b\neq 0$. La escogencia de b es irrelevante, pues para cualquier $c\in\mathcal{A},\ c\neq 0$,
$\dfrac{ab}{b}=\dfrac{ac}{c}$, ya que $(ab)c=(ac)b$.

Debemos probar que ϕ es un monomorfismo de anillos.

Sean $a,b\in\mathcal{A}$

$\phi(a+b)=\dfrac{(a+b)x}{x}$, con $x\neq 0,\ x\in\mathcal{A}$. Pero $(a+b)x=ax+bx$, y así $\phi(a+b)=\dfrac{ax+bx}{x}$. Por otro lado, $\phi(a)+\phi(b)=\dfrac{ax}{x}+\dfrac{bx}{x}=\dfrac{ax^2+bx^2}{x^2}$ y $\dfrac{ax+bx}{x}=\dfrac{ax^2+bx^2}{x^2}$, pues $(ax+bx)x^2=(ax^2+bx^2)x$.
Luego $\phi(a+b)=\phi(a)+\phi(b)$.

Además, $\phi(a\cdot b)=\dfrac{(a\cdot b)x}{x}$ y $\phi(a)\cdot\phi(b)=\left(\dfrac{ax}{x}\right)\left(\dfrac{bx}{x}\right)=\dfrac{abx^2}{x^2}$, luego $\phi(a\cdot b)=\phi(a)\cdot\phi(b)$.

Finalmente, ϕ es inyectiva, pues si $\phi(a)=\phi(b)$, tenemos que $\dfrac{ax}{x}=\dfrac{bx}{x}$ y por lo tanto $ax^2=bx^2$. Como $\mathcal{A}$ es un dominio de integridad y $x\neq 0$, vale

la ley de cancelación para el producto en $\mathcal{A}$, y por lo tanto, $a = b$. Así, ϕ es un monomorfismo y concluimos que $\mathcal{A}$ se puede sumergir en $\overline{\mathcal{A}}$.

Para terminar con la demostración del teorema, debemos probar que, si $\mathcal{F}$ es un cuerpo tal que $\mathcal{A}$ puede sumergirse en $\mathcal{F}$, entonces $\overline{\mathcal{A}}$ puede sumergirse en $\mathcal{F}$.

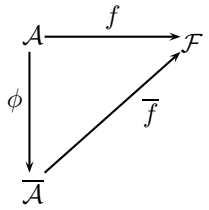
Haremos las construcciones básicas de la prueba, y dejaremos la verificación de los detalles como ejercicio para el lector.

Supongamos, entonces, que existe un monomorfismo de anillos
$f : \mathcal{A} \longrightarrow \mathcal{F}$, donde $\mathcal{F}$ es un cuerpo.

Para ver que $\overline{\mathcal{A}}$ puede sumergirse en $\mathcal{F}$, debemos construir un monomorfismo $\overline{f} : \overline{\mathcal{A}} \longrightarrow \mathcal{F}$, a partir de f.

Lo más natural sería definir $\overline{f}\left(\frac{a}{b}\right) = f(a)[f(b)]^{-1}$, $\forall\, \frac{a}{b} \in \overline{\mathcal{A}}$ puesto que el elemento $\dfrac{a}{b} \in \overline{\mathcal{A}}$ puede interpretarse, en el cuerpo $\overline{\mathcal{A}}$, como el producto de $\phi(a) = \dfrac{ax}{x}$ por $\phi(b^{-1}) = \dfrac{x}{bx}$, donde ϕ es la inmersión de $\mathcal{A}$ en $\overline{\mathcal{A}}$.

En el diagrama siguiente representamos las relaciones entre ϕ, f y $\overline{f}$:



$f = \overline{f} \circ \phi$

Decimos que es "natural" definir a $\overline{f}$ de manera que $f = \overline{f} \circ \phi$ porque la cadena de contenciones $\mathcal{A} \subset \overline{\mathcal{A}} \subset \mathcal{F}$ que queremos probar, sugiere precisamente esa construcción.

Ahora bien, debemos probar que $\overline{f}$ está bien definida y que es un monomorfismo. En primer lugar, si $\dfrac{a}{b} \in \overline{\mathcal{A}}$, tenemos que $b \in \mathcal{A}$ y $b \neq 0$, por lo tanto $f(b) \neq 0$, ya que f es un monomorfismo. Como $\mathcal{F}$ es un cuerpo, $[f(b)]^{-1} \in \mathcal{F}$ y así $f(a)[f(b)]^{-1} \in \mathcal{F}$.

Sean $\dfrac{a}{b}$ y $\dfrac{c}{d} \in \overline{\mathcal{A}}$ tales que $\dfrac{a}{b} = \dfrac{c}{d}$; es decir, $ad = bc$.

Veamos que $\overline{f}\left(\dfrac{a}{b}\right) = \overline{f}\left(\dfrac{c}{d}\right)$.

$$\overline{f}\left(\frac{a}{b}\right) = f(a)[f(b)]^{-1} \qquad \text{y} \qquad \overline{f}\left(\frac{c}{d}\right) = f(c)[f(d)]^{-1}$$

Como $ad = bc$, tenemos que $f(ad) = f(bc)$ y por ser f un homomorfismo de anillos, $f(a)f(d) = f(b)f(c)$. Ahora, $d \neq 0$ y $b \neq 0$ por lo que $f(b) \neq 0$ y $f(d) \neq 0$; estos elementos tienen, por lo tanto, un inverso multiplicativo en $\mathcal{F}$ y así

$$f(a)[f(b)]^{-1} = f(c)[f(d)]^{-1}$$

y hemos probado que

$$\overline{f}\left(\frac{a}{b}\right) = \overline{f}\left(\frac{c}{d}\right).$$

Para ver que $\overline{f}$ es un homomorfismo de anillos, supongamos que $\dfrac{a}{b},\ \dfrac{c}{d} \in \overline{\mathcal{A}}$.

$$\overline{f}\left(\frac{a}{b} + \frac{c}{d}\right) = \overline{f}\left(\frac{ad + bc}{bd}\right) = f(ad + bc)[f(bd)]^{-1} =$$

$$f(a)f(d)[f(b)f(d)]^{-1} + f(b)f(c)[f(b)f(d)]^{-1},$$

por ser f un homomorfismo de anillos, y $\mathcal{F}$ un cuerpo. Luego

$$\begin{aligned}\overline{f}\left(\frac{a}{b} + \frac{c}{d}\right) &= f(a)f(d)[f(b)]^{-1}[f(d)]^{-1} + f(b)f(c)[f(b)]^{-1}[f(d)]^{-1} \\ &= f(a)[f(b)]^{-1} + f(c)[f(d)]^{-1} = \overline{f}\left(\frac{a}{b}\right) + \overline{f}\left(\frac{c}{d}\right).\end{aligned}$$

Dejamos como ejercicio para el lector, ver que $\overline{f}\left(\dfrac{a}{b} \cdot \dfrac{c}{d}\right) = \overline{f}\left(\dfrac{a}{b}\right)\overline{f}\left(\dfrac{c}{d}\right)$

Veamos que $\overline{f}$ es inyectiva:

Sea $\dfrac{a}{b} \in \overline{\mathcal{A}}$ tal que $\overline{f}\left(\dfrac{a}{b}\right) = 0$, es decir, $f(a)[f(b)]^{-1} = 0$. Como $\dfrac{a}{b} \in \overline{\mathcal{A}},\ b \in \mathcal{A}$ y $b \neq 0$; por ser f un monomorfismo, $f(b) \neq 0$ y $[f(b)]^{-1} \neq 0$. Siendo $\mathcal{F}$ un cuerpo, es un dominio de integridad y por ser $f(a)[f(b)]^{-1} = 0$, necesariamente resulta que $f(a) = 0$. De nuevo, usamos el hecho de ser f un monomorfismo para concluir que $a = 0$ y por lo tanto $\dfrac{a}{b} = 0$. ■

El cuerpo $\overline{\mathcal{A}}$ que hemos construido a partir del dominio de integridad $\mathcal{A}$, es llamado el cuerpo de fracciones de $\mathcal{A}$, o cuerpo de cocientes; no debe

confundirse con el cuerpo cociente $\mathcal{A}/I$ que se obtiene cuando I es un ideal maximal de $\mathcal{A}$.

Problemas:

1. Pruebe que $n\mathbb{Z}$ es un ideal maximal en $\mathbb{Z}$ si y sólo si n es primo.

2. Sea $\mathcal{A} = \{f : [0,1] \longrightarrow \mathbb{R},\ f \text{ es continua}\}$.
   Sea $I = \{f \in \mathcal{A} : f(1) = 0\}$.

   a) Pruebe que I es un ideal de $\mathcal{A}$.

   b) Pruebe que, si J es un ideal de $\mathcal{A}$ tal que $I \subsetneq J$, entonces existe $\alpha \in \mathbb{R},\ \alpha \neq 0$, tal que la función constante $h : [0,1] \longrightarrow \mathbb{R}$ tal que $h(x) = \alpha,\ \forall\, x \in [0,1]$, pertenece a J. (Sugerencia: Considere una función $g \in J$ tal que $g \notin I$, y tome $\alpha = g(1)$. Pruebe que $f = g - h \in I$ y por lo tanto, $h = g - f \in J$).

   c) Pruebe que $J = \mathcal{A}$, y, por lo tanto, I es un ideal maximal.

2.4. Anillos de Polinomios

Las construcciones de cuerpos a partir de ciertas clases de anillos que hemos visto en las secciones anteriores, son realizables a partir de $(\mathbb{Z}, +, \cdot)$: para p primo, el anillo cociente $\mathbb{Z}/p\mathbb{Z}$, que hemos denotado por $\mathbb{Z}_p$, es un cuerpo finito; el cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$, el cuerpo de los números racionales.

Estas dos construcciones también se pueden llevar a cabo a partir del anillo de polinomios $K[x]$, donde K es un cuerpo. Además, otras propiedades de $\mathbb{Z}$, como lo son la validez del algoritmo euclidiano de la división y otras derivadas de éste, también se cumplen en $K[x]$. Para enunciar y demostrar con precisión estas propiedades, comenzaremos por construir formalmente el anillo de polinomios $K[x]$, en una indeterminada, con coeficientes en un cuerpo K.

Supongamos, entonces, que K es un cuerpo, y sea

$$\mathcal{L}_K = \{(a_n)_{n\in\mathbb{N}}\,;\, a_n \in K,\, \forall\, n \in \mathbb{N}\}.$$

Consideremos ahora el conjunto $\mathcal{L}_K^*$ de todas las sucesiones en $\mathcal{L}_K$ tales que sólo un número finito de sus términos son distintos de cero (el elemento $0 \in K$); es decir,

$$\mathcal{L}_K^* = \{(a_n)_{n\in\mathbb{N}} \in \mathcal{L}_K \,:\, \exists\, N > 0 \text{ tal que } a_n = 0,\ \forall\, n > N\}$$

Es claro que dos sucesiones a, b en $\mathcal{L}_K^*$ son iguales si y sólo si $a_n = b_n,\ \forall\, n \in \mathbb{N}$.

Se define el grado de $a \in \mathcal{L}_K^*$ como sigue:

Definición 2.18 *Si $a \in \mathcal{L}_K^*$, $a \neq 0$, $a = (a_0, a_1, \ldots, a_n, 0, \ldots, 0, \ldots)$, el grado de a se denota por $gr(a)$ y se define como $gr(a)$=máx $\{n \in \mathbb{N} : a_n \neq 0\}$.*

Definamos una suma y un producto en $\mathcal{L}_K^*$, que dotará a este conjunto de una estructura de anillo conmutativo.

Sean

$$a = (a_0,\, a_1, \ldots, a_k, 0, 0, \ldots, 0, \ldots)$$

y

$$b = (b_0,\, b_1, \ldots, b_m, 0, 0, \ldots, 0, \ldots)$$

elementos de $\mathcal{L}_K^*$.

Definamos $a + b$ de la manera más natural:

Si $m \geq k,\ a+b = (a_0+b_0,\, a_1+b_1, \ldots, a_k+b_k, b_{k+1}, \ldots, b_m, 0, 0, \ldots, 0, \ldots)$

Es fácil ver que la suma así definida le da a $(\mathcal{L}_K^*, +)$ la estructura de un grupo abeliano. Dejamos la verificación de los detalles como ejercicio para el lector, pues las propiedades de la suma definida en $\mathcal{L}_K^*$ dependen de las propiedades de la suma en K.

Definiremos el producto $a \cdot b$, donde a y b son como antes, de la siguiente manera:

$a \cdot b = c = (c_0,\, c_1, \ldots, c_r, 0, 0, \ldots, 0, \ldots)$, donde $r = k + m$ y

$$c_i = \sum_{j+n=i} a_j b_n, \qquad \forall\, i \in \{0, \ldots, k+m\}.$$

El producto así definido es asociativo, conmutativo y distributivo con respecto a la suma definida en $\mathcal{L}_K^*$; además tiene identidad, que es la sucesión

$1 = (1, 0, 0, \ldots, 0, \ldots)$. El lector puede verificar que estas propiedades se cumplen, de nuevo haciendo uso de las propiedades del producto en K.

Así, $(\mathcal{L}_K^*, +, \cdot)$ es un anillo conmutativo con identidad, que se denomina el anillo de polinomios en una indeterminada, con coeficientes en K.

Ahora bien, si denotamos al elemento $(0, 1, 0, 0, \ldots, 0, \ldots)$ de $\mathcal{L}_K^*$ por x, observaremos lo siguiente:

$$\begin{aligned} x^2 = xx &= (0 \cdot 0,\ 0 \cdot 1 + 1 \cdot 0,\ 0 \cdot 0 + 1 \cdot 1,\ 0 + 1 \cdot 0, 0, \ldots) = (0, 0, 1,\ 0, \ldots) \\ x^3 &= (0, 0, 0, 1, 0, 0, \ldots, 0, \ldots) \qquad \text{y en general,} \\ x^n &= (0, 0, 0, \ldots 0, 1, 0, \ldots, 0, \ldots) \qquad \text{donde 1 ocupa el lugar n+1.} \end{aligned}$$

Si se define $x^0 = (1, 0, \ldots, 0, \ldots) = 1 \in \mathcal{L}_K^*$, y se define en $\mathcal{L}_K^*$ un producto por escalares en K del modo natural: para $\alpha \in K$, y $a = (a_0,\ a_1, \ldots, a_k, 0, \ldots, 0, \ldots) \in \mathcal{L}_K^*$, $\alpha a = (\alpha a_0,\ \alpha a_1, \ldots,\ \alpha a_k, 0, \ldots, 0, \ldots)$, resulta que $\mathcal{L}_K^*$ es también un espacio vectorial sobre K, y, como espacio vectorial, está generado por el conjunto $\{x^0,\ x,\ x^2, \ldots x^n, \ldots\}$.

En efecto, si $a = (a_0,\ a_1, \ldots, a_k, 0, 0, \ldots, 0, \ldots)$, entonces

$$\begin{aligned} a &= a_0(1, 0, 0, \ldots, 0, \ldots) + a_1(0,\ 1, 0, \ldots) + \ldots + a_k(0, 0, \ldots, \underbrace{1}_{k+1}, 0, \ldots) \\ &= a_0x^0 + a_1x + \ldots + a_kx^k = \sum_{i=0}^{k} a_ix^i \end{aligned}$$

Este hecho nos da una representación de cada elemento $a \in \mathcal{L}_K^*$, como una combinación lineal de potencias de x, y es esta la notación que usualmente empleamos para operar con estos elementos, llamados polinomios en una indeterminada con coefientes en K.

La construcción precedente podría parecer un tanto rebuscada, sobre todo si se compara con la noción de un polinomio en una "indeterminada" (vocablo éste que tiene un significado matemático bastante indeterminado) asociada a una función polinómica.

El polinomio $p(x) = 3x^3 - 2x + 1$ puede ser "evaluado" en números reales y/o complejos, tal como lo es una función.

Ahora bien, esta noción de los polinomios como "equivalentes" a las funciones polinómicas, adquirida por lo general en los estudios pre-universitarios

de Matemáticas, tiene sentido cuando el cuerpo es infinito, y puesto que en dicho nivel de instrucción no se consideran cuerpos finitos, la equivalencia de estos objetos es, en ese caso, válida. Sin embargo, si el cuerpo de los coeficientes es finito, ya la equivalencia pierde validez.

Más precisamente, si el cuerpo K es infinito, se puede establecer un isomorfismo natural entre el anillo de polinomios $K[x]$ y el anillo de las funciones polinómicas con coeficientes en K; cuando K es finito, ya esa correspondencia deja de ser biyectiva. Veamos:
Sea

$$\mathcal{P}_K = \{f : K \longrightarrow K \,:\, f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i,\ \forall\, \alpha \in K,\ \text{ con } a_i \in K,\ \text{ para } 0 \leq i \leq n,\, n \geq 0\}$$

$\mathcal{P}_K$ tiene estructura de anillo conmutativo con identidad, con la suma y el producto de funciones usualmente definido:

$$(f+g)(\alpha) = f(\alpha) + g(\alpha), \qquad \text{y} \qquad (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha),\ \forall\, \alpha \in K.$$

Además, $\mathcal{P}_K$ es un espacio vectorial sobre el cuerpo K, si se define el producto de una función f por un escalar $\lambda \in K$, como λf, donde
$(\lambda f)(a) = \lambda(f(a)),\ \forall\, a \in K$.

La estructura que poseen $K[x]$ y $\mathcal{P}_K$, que además de ser anillos, son espacios vectoriales sobre el anillo K, se denomina estructura de $K-$álgebra.

Definiremos un homomorfismo de $K-$álgebras, como una función entre $K-$álgebras que es, a la vez, una transformación lineal entre espacios vectoriales y un homomorfismo de anillos.

Un isomorfismo de $K-$álgebras será un homomorfismo biyectivo entre $K-$álgebras.

Para mostrar que, siempre que K sea un cuerpo infinito, $\mathcal{P}_K \cong K[x]$, lo que implica que es válida la identificación de un polinomio con una función polinómica, se requiere del siguiente resultado (Teorema 2.20) cuya prueba se dejará como ejercicio para el lector; al final de esta sección se ofrecen sugerencias para la construcción de la prueba.

Definición 2.19 *Sea* $p(x) = \sum_{i=0}^{r} p_i x^i \in K[x],\ p_i \neq 0$ *para algún* $i \in \{0, \ldots, r\}$ *y sea* $a \in K$. *Se dice que* a *es raíz de* $p(x)$ *si la función* $f_p \in \mathcal{P}_K$ *definida por:* $f_p(t) = \sum_{i=0}^{r} p_i t^i,\ \forall t \in K$, *es tal que* $f_p(a) = 0$.

Teorema 2.20 *Un polinomio en* $K[x]$, *de grado* $n > 0$, *tiene, a lo sumo,* n *raíces en* K.

Teorema 2.21 *Si* K *es un cuerpo infinito, entonces* $K[x] \cong \mathcal{P}_K$.

Prueba Sea $\varphi : K[x] \longrightarrow \mathcal{P}_K$ la función definida por $\varphi(p(x)) = f_p$, donde $f_p : K \longrightarrow K$ es la función tal que

$$f_p(a) = p_0 + p_1 a + p_2 a^2 + \ldots + p_r a^r,\ \forall\, a \in K,$$

siendo

$$p(x) = \sum_{i=0}^{r} p_i x^i.$$

La función φ está bien definida, pues si $p(x) \in K[x],\ p(x) = \sum_{i=0}^{r} p_i x^i$, entonces $p_i \in K,\ \forall\, i \in \{0, \ldots, r\}$, y así $f_p = \varphi(p(x))$ es una función polinómica que está en $\mathcal{P}_K$. Veamos ahora que φ es un homomorfismo de $K-$álgebras:

Sea $\lambda \in K$ y sean $p(x) = \sum_{i=0}^{r} p_i x^i,\ q(x) = \sum_{i=0}^{s} q_i x^i$ polinomios en $K[x]$.

$\varphi(\lambda p(x)) = \varphi(p^*(x))$, donde $p^*(x) = \sum_{i=0}^{r} \lambda p_i x^i$. Así, $\varphi(\lambda p(x)) = f_{p^*}$, donde

$f_{p^*}(a) = \sum_{i=0}^{r} \lambda p_i a^i,\ \forall\, q \in K$. Pero $\sum_{i=0}^{r} \lambda p_i a^i = \lambda(f_p(a)) = \lambda\varphi(p(x))$.

Por otra parte, $\varphi(p(x) + q(x)) = \varphi(g(x)) = f_g$, donde

$$g(x) = (p_0 + q_0) + (p_1 + q_1)x + \ldots + (p_r + q_r)x^r + \ldots + q_s x^s$$

si suponemos que $s > r$.

Así,

$$f_g(a) = (p_0+q_0)+(p_1+q_1)a+(p_2+q_2)a^2+\ldots+(p_r+q_r)a^r+\ldots+q_sa^s,\ \forall\, a \in K.$$

Usando la propiedad distributiva del producto respecto a la suma en K, obtenemos que $f_g(a) = \sum_{i=0}^{r} p_i a^i + \sum_{i=0}^{s} q_i a^i$, y por lo tanto,

$$f_g = f_p + f_q = \varphi(p(x)) + \varphi(q(x)).$$

Dejamos como ejercicio para el lector verificar que, para $p(x)$, $q(x) \in K[x]$, se tiene que $\varphi(p(x) \cdot q(x)) = \varphi(p(x))\varphi(q(x))$.

Veamos ahora que φ es biyectiva.

Para verificar que es inyectiva, probaremos que $Ker\,\varphi = \{0\}$. Sea $p(x) \in K[x]$ tal que $\varphi(p(x)) = 0$ (la función nula en $\mathcal{P}_K$).

Esto significa que, si $p(x) = p_0 + p_1x + \ldots + p_rx^r$, entonces $\forall\, a \in K$ se cumple que $p_0 + p_1a + \ldots + p_ra^r = 0$. Pero por el Teorema 2.19, sabemos que $p(x)$, si es no nulo, tiene, a lo sumo, r raíces en K, y siendo K infinito, tendríamos que $p(x)$ tiene infinitas raíces en K. De modo que $\varphi(p(x)) = 0$ implica necesariamente que $p_i = 0,\ \forall\, i \in \{0, \ldots, r\}$, y por lo tanto $p(x) = 0$.

Así, $Ker\,\varphi = \{0\}$ y φ es inyectiva.

φ es sobreyectiva porque, dada cualquier función polinómica $f : K \longrightarrow K$, definida, digamos, por $f(a) = c_0 + c_1a + \ldots + c_na^n$, es claro que $f = \varphi(c(x))$, donde $c(x) = \sum_{i=0}^{n} c_i x^i$ ■

Hemos visto que la inyectividad de φ depende fuertemente del hecho de ser K infinito. Para constatar que está identificación de un polinomio con la función polinómica asociada no es válida en el caso de ser K finito, examinaremos un ejemplo.

Ejemplo 2.11 *Sea* $K = \mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$

Si definimos $\varphi : \mathbb{Z}_3[x] \longrightarrow \mathcal{P}_{\mathbb{Z}_3}$ *como antes, veremos que* φ *no es inyectiva:*

Sea $p(x) = x^3 + \overline{2}x \neq 0$.

$\varphi(p(x)) = f_p : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$, *es la función definida por* $f(n) = n^3 + \overline{2}n$, $\forall n \in \mathbb{Z}_3$.

Ahora bien,

$f_p(\overline{0}) = \overline{0}^3 + \overline{2} \cdot \overline{0} = \overline{0}$

$f_p(\overline{1}) = (\overline{1})^3 + \overline{2}(\overline{1}) = \overline{1} + \overline{2} = \overline{3} = \overline{0}$

$f_p(\overline{2}) = (\overline{2})^3 + \overline{2}(\overline{2}) = \overline{8} + \overline{4} = \overline{2} + \overline{1} = \overline{3} = \overline{0}$

Como $f_p(a) = 0$, $\forall\, a \in \mathbb{Z}_3$, f_p *es la función idénticamente nula, y sin embargo* $p(x) \neq 0$; *luego* $Ker\,\varphi \neq \{0\}$ *y el homomorfismo no es inyectivo.*

Nos interesa ahora explorar otras propiedades del anillo de polinomios $K[x]$ que comparte con el anillo $\mathbb{Z}$ de los números enteros, y que están asociadas al algoritmo euclidiano de la división.

Recordemos que, si $p(x) \neq 0$, $q(x) \in K[x]$ y $gr(p(x)) = n$, $gr(q(x)) = m$, existen $c(x)$, $r(x) \in K[x]$, con $r(x) = 0$ ó $gr(r(x)) < n$, tales que $q(x) = c(x)p(x) + r(x)$. Este hecho, cuya prueba consiste simplemente en realizar la división del polinomio $q(x)$ entre $p(x)$, generalizando el algoritmo que se aprende en las lecciones de Álgebra de la escuela secundaria, se propondrá como ejercicio para el lector, al final de esta sección.

Las propiedades que comparten $\mathbb{Z}$ y $K[x]$ a las que nos referimos antes, son las que les dan la estructura de lo que se denomina "anillo euclidiano".

Definición 2.22 *Un dominio de integridad* $\mathcal{A}$ *es un anillo euclidiano si se cumplen las siguientes condiciones:*

1. *Existe una función* $d : \mathcal{A}\backslash\{0\} \longrightarrow \mathbb{N}$, *tal que si* $a \neq 0$, $b \neq 0$ *están en* $\mathcal{A}$, *entonces* $d(a) \leq d(ab)$

2. *Para* $a, b \in \mathcal{A}$, $b \neq 0$ *existen* $c, r \in \mathcal{A}$, *tales que* $a = bc + r$, *donde* $r = 0$ *ó* $d(r) < d(b)$.

El elemento $0 \in \mathcal{A}$ *no tiene ningún valor asignado a través de la función* d.

En el caso de $K[x]$, todo parece indicar que la función d de la definición, viene dada por el grado de un polinomio. Veamos que este, en efecto, es el caso.

Teorema 2.23 *Si* K *es un cuerpo, entonces* $K[x]$ *es un anillo euclidiano.*

Prueba Comenzaremos por ver que $K[x]$ es un dominio de integridad; ya hemos visto que es un anillo conmutativo con identidad, y sólo resta ver que, si $f(x)$, $g(x) \in K[x]$ y $f(x) \cdot g(x) = 0$, entonces $f(x) = 0$ ó $g(x) = 0$. De la definición del producto $f(x)g(x)$ se deduce que, si $f(x) \neq 0$ y $g(x) \neq 0$, entonces $gr(f(x)g(x)) = gr(f(x)) + gr(g(x))$. Por lo tanto, si $f(x)$ y $g(x)$ son no nulos, $gr(f(x)g(x)) \geq 0$, lo cual excluye la posibilidad de que $f(x)g(x)$ sea el polinomio nulo. Así, $K[x]$ es un dominio de integridad.

Mencionamos antes que la función

$$d : K[x]\backslash\{0\} \longrightarrow \mathbb{N} \qquad \text{definida por}$$

$$d(f(x)) = gr(f(x))$$

cumple con las condiciones requeridas en la definición 2.21. En efecto, si $f(x) \neq 0$, y $g(x) \neq 0$, se tiene que $gr(f(x)) \geq 0$ y $gr(g(x)) \geq 0$ y en consecuencia, $gr(f(x)g(x)) \geq gr((f(x)))$, puesto que

$$gr(f(x)g(x)) = gr(f(x)) + gr(g(x)).$$

Por otra parte, asumiendo que vale el algoritmo euclidiano de la división en $K[x]$, tenemos que la función d en este caso, hace de $K[x]$ un anillo euclidiano. ■

Habíamos presentado a $\mathbb{Z}$ como un anillo euclidiano también, y para verificarlo debemos definir la función $d : \mathbb{Z}^* \longrightarrow \mathbb{N}$ que posea las características requeridas.

Sabiendo que el algoritmo euclidiano de la división vale en $\mathbb{Z}$, y tomando en cuenta el papel que debe jugar d en ese algoritmo, concluimos que debe definirse

$$d : \mathbb{Z}^* \longrightarrow \mathbb{N}$$

por $d(n) = |n|$; dejamos como ejercicio para el lector verificar que $\mathbb{Z}$ es un anillo euclidiano.

Una de las propiedades fundamentales de los anillos euclidianos es la siguiente: todo ideal de un anillo euclidiano es generado por un elemento del anillo. Esta propiedad ya la hemos observado en $\mathbb{Z}$: todo ideal en $\mathbb{Z}$ es de la forma $n\mathbb{Z} = (n)$, para algún $n \in \mathbb{Z}$.

Definición 2.24 *Un ideal I de un anillo conmutativo es un ideal principal, si existe $a_0 \in \mathcal{A}$ tal que $I = (a_0) = \{ra_0 \ : \ r \in \mathcal{A}\}$. Se dice que un dominio de integridad $\mathcal{A}$, con identidad, es un dominio de ideales principales (D. I. P.) si todo ideal de $\mathcal{A}$ es principal.*

Teorema 2.25 *Todo anillo euclidiano es un D.I.P.*

Prueba Sea $\mathcal{A}$ un anillo euclidiano y sea I un ideal de $\mathcal{A}$. Si $I = \{0\}$, entonces $I = (0) = \{0 \cdot r \,:\, r \in \mathcal{A}\}$.

Supongamos que $I \neq \{0\}$, y en consecuencia, $\exists\, a \in I$ tal que $a \neq 0$. Consideremos el conjunto $d(I) = \{d(a) \,:\, a \in I,\ a \neq 0\} \subset \mathbb{N}$. (Aquí d es la función a valores en $\mathbb{N}$ definida en $\mathcal{A}\backslash\{0\}$, por ser $\mathcal{A}$ un anillo euclidiano).

Como $d(I) \neq \emptyset$, porque existe $a \in I$ tal que $a \neq 0$, tenemos que existe $k \in \mathbb{N}$ tal que $k = \text{mín}\ d(I)$. Sea $a_0 \in I$ tal que $d(a_0) = k$. Sea $a \in I$; como $\mathcal{A}$ es un anillo euclidiano, existen $c, r \in \mathcal{A}$ con $r = 0$ ó $d(r) < d(a_0)$, tales que $a = ca_0 + r$.

Ahora bien, como $a_0 \in I,\ ca_0 \in I$, ya que I es un ideal. Dado que $a \in I$, $a - ca_0 = r \in I$; si $r \neq 0$ tenemos que, $d(a_0) \leq d(r)$, ya que $d(a_0) \leq d(x),\ \forall\, x \in I$, y esto contradice la escogencia de r. De modo que, necesariamente, $r = 0$. Así, $a = ca_0$ y hemos probado que $I \subset (a_0)$. Como $a_0 \in I$, es claro que $(a_0) \subset I$, y así $I = (a_0)$.

Vemos así que todo ideal en $\mathcal{A}$ es generado por un elemento. Resta ver que $\mathcal{A}$ tiene elemento identidad.

Como $\mathcal{A}$ es un ideal en $\mathcal{A}$, por lo que acabamos de probar, sabemos que existe $u \in \mathcal{A}$ tal que $\mathcal{A} = (u)$. En particular, existe $t \in \mathcal{A}$ tal que $u = tu$. Veamos que t es el elemento identidad de $\mathcal{A}$:

Sea $a \in \mathcal{A}$; $ta = tru$, para algún $r \in \mathcal{A}$. Como $\mathcal{A}$ es conmutativo,
$ta = tur = ur = a$; luego t es la identidad de $\mathcal{A}$ ■

Es interesante observar que la prueba anterior nos dice cuáles pueden ser los generadores de un ideal I en un D.I.P.

En el caso en que $\mathcal{A} = K[x]$, si I es un ideal cualquiera en $K[x]$, sabemos que I estará generado por un polinomio de grado mínimo entre los que están en I. En otras palabras, todo ideal I en $K[x]$ está conformado por todos los polinomios que tienen al polinomio generador como factor. Por ejemplo, si $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ y tenemos que $I = (p(x))$, entonces

$$I = \{q(x) \in \mathbb{Q}[x] \,:\, q(x) = (x^3 - 2)g(x),\ g(x) \in \mathbb{Q}[x]\}$$

Una consecuencia de esto es la siguiente: Si α es raíz del polinomio generador de I, entonces α es raíz de todos los polinomios de I. En el ejemplo anterior, $\alpha = \sqrt[3]{2}$ es raíz de todos los polinomios de I.

Por esta razón, un criterio para determinar si un polinomio $g(x)$ está en un ideal I, es determinar si $g(x)$ es divisible entre el polinomio generador.

En el caso $\mathcal{A} = \mathbb{Z}$, ya habíamos probado que todo ideal es de la forma $n\mathbb{Z} = (n)$, y en este ideal el generador, que puede ser n ó $-n$, (se toma $n > 0$ por conveniencia) resulta ser el elemento en I que tiene valor absoluto mínimo, tal como ocurre en la prueba que acabamos de ver.

De hecho, un aspecto fundamental de los anillos euclidianos es el de la divisibilidad, que abordaremos a continuación:

Definición 2.26 *Sea $\mathcal{A}$ un anillo euclidiano, y sean $b, c \in \mathcal{A},\ b \neq 0,\ c \neq 0$. Decimos que b divide a c y escribimos $b|c$, si existe $q \in \mathcal{A}$ tal que $b \cdot q = c$. Si b no divide a c escribimos $b \not| c$.*

Proposición 2.27 *Sea $\mathcal{A}$ un anillo euclidiano; sean $a, b, c \in \mathcal{A}$, todos no nulos. Vale lo siguiente:*

1. *Si $a|b$ y $b|c$, entonces $a|c$*
2. *Si $a|b$ y $a|c$, entonces $a|(b \pm c)$*
3. *Si $a|b$, entonces $a|bx,\ \forall\, x \in \mathcal{A}$.*

La prueba se deja como ejercicio para el lector, ya que no difiere esencialmente de la que se haría para el caso $\mathcal{A} = \mathbb{Z}$.

La idea de máximo común divisor surge naturalmente en este contexto, con una característica que implica diferencias entre el caso general y el de $\mathbb{Z}$.

Cuando se habla del m.c.d.(-15,12), por ejemplo, se hace referencia al número 3, pues, entre los divisores comunes de -15 y 12, que son: -1,1,-3 y 3, éste último es el mayor, según el orden que existe en $\mathbb{Z}$.

Esto hace que, en $\mathbb{Z}$, el m.c.d. de dos o más enteros sea único. La definición de m.c.d., válida para un anillo euclidiano cualquiera, sin que éste tenga un orden definido, no implica la unicidad del m.c.d. de dos elementos del anillo:

Definición 2.28 *Sean $a, b \neq 0 \in \mathcal{A}$, anillo euclidiano. Sea $c \neq 0 \in \mathcal{A}$; decimos que c es un máximo común divisor de a y b, si se cumplen las condiciones siguientes:*

1. *$c|a$ y $c|b$*
2. *Si $x \in \mathcal{A}$ y $x|a,\ x|b$, entonces $x|c$.*

Denotamos, en este caso, el elemento c como (a, b).

Ejemplo 2.12 *En $\mathbb{Z}$, según la definición anterior, tendríamos que* $-4 = (-16, 12)$ *y* $4 = (-16, 12)$. *Lo que ocurre en $\mathbb{Z}$ es que si $c = (a, b)$ y $c' = (a, b)$, entonces $|c| = |c'|$. Dejamos la verificación de este hecho como un ejercicio para el lector.*

Ejemplo 2.13 *Si $\mathcal{A} = \mathbb{Q}[x]$, y $p(x) = x^2 - 4$, $q(x) = x^3 - 2x^2 + 3x - 6$, entonces es fácil ver que $(p(x), q(x)) = x - 2$, pero también se tiene que $(p(x), q(x)) = \lambda(x - 2)$, para cualquier $\lambda \in \mathbb{Q}$, $\lambda \neq 0$.*

Así, hay infinitos polinomios $c(x)$ en $\mathbb{Q}[x]$ tales que $(p(x), q(x)) = c(x)$. Obsérvese que todos estos polinomios $c(x)$ tienen el mismo grado, que es 1 en este caso.

En un ejercicio al final de esta sección, se propone probar la generalización de esta propiedad, para cualquier anillo euclidiano.

Lema 2.29 *Sea $\mathcal{A}$ un anillo euclidiano y $a, b \neq 0 \in \mathcal{A}$. Existe $c \in \mathcal{A}$ tal que $c = (a, b)$ y existen α, $\beta \in \mathcal{A}$ tales que $c = \alpha\, a + \beta\, b$.*

Prueba Sea $I = \{ua + vb : u, v \in \mathcal{A}\}$. Se desprende del ejercicio 1, del final de esta sección, que I es un ideal de $\mathcal{A}$.

Como $\mathcal{A}$ es un D.I.P., existe $c \in \mathcal{A}$ tal que $I = (c)$. Como $c \in I$, existen α, $\beta \in \mathcal{A}$ tales que $c = \alpha\, a + \beta\, b$. Por otra parte, como $a, b \in I$, se tiene que $c|a$ y $c|b$.

Supongamos que $r|a$ y $r|b$ $(r \in \mathcal{A})$. Entonces, por la Proposición 2.27, $r|\alpha\, a$ y $r|\beta\, b$, y por lo tanto, $r|\alpha\, a + \beta\, b = c$. Así, $c = (a, b) = \alpha\, a + \beta\, b$ ■

El lector recordará el algoritmo euclidiano para encontrar el entero $c = (m, n)$, para $m, n \in \mathbb{Z}$, ambos no nulos. Este algoritmo también provee los enteros a, b tales que $c = am + bn$.

Entre los ejercicios propuestos al final de esta sección, está la generalización de este algoritmo para el anillo de polinomios $K[x]$ sobre un cuerpo K, y también el uso de este algoritmo en ciertos casos particulares.

A continuación, definimos los conceptos necesarios para establecer el teorema que generaliza al caso de los anillos euclidianos, lo que se conoce como el Teorema Fundamental de la Aritmética.

Definición 2.30 *Sea $\mathcal{A}$ un anillo conmutativo con identidad. Un elemento $a \in \mathcal{A}$ se denomina una unidad en $\mathcal{A}$, si a es invertible en $\mathcal{A}$, es decir, si existe b en $\mathcal{A}$ tal que $ab = 1$.*

Ejemplo 2.14 *Si $\mathcal{A} = \mathbb{Z}$, las únicas unidades son 1 y -1.*

Ejemplo 2.15 *Si $\mathcal{A} = K[x]$, las unidades son todos los polinomios constantes, $p(x) = c$, donde $c \in K,\ c \neq 0$.*

Teorema 2.31 *Sea $\mathcal{A}$ un dominio de integridad. Sean $a, b \neq 0 \in \mathcal{A}$ tales que $a|b$ y $b|a$. Entonces $a = tb$, donde t es una unidad en $\mathcal{A}$.*

Prueba Se deja como ejercicio para el lector.

Definición 2.32 *Si $a, b \in \mathcal{A}$, donde $\mathcal{A}$ es un dominio de integridad con identidad, y $a = tb$ para alguna unidad $t \in \mathcal{A}$, se dice que a y b son asociados.*

Ejemplo 2.16 *Si $\mathcal{A} = K[x]$, donde K es un cuerpo, dos polinomios $p(x)$ y $q(x)$, son asociados si y sólo si $p(x) = \alpha q(x)$, con $\alpha \in K,\ \alpha \neq 0$.*

Lema 2.33 *Sea $\mathcal{A}$ un anillo euclidiano, $a, b \in \mathcal{A}$ ambos no nulos; si b no es una unidad, entonces $d(a) < d(ab)$. En otras palabras, $d(a) = d(ab)$ implica que b es una unidad.*

Prueba Sea $I = (a) = \{ra : r \in \mathcal{A}\}$. Como a es generador de I, sabemos que $d(a) \leq d(s),\ \forall\, s \in I$. En particular, $ab \in I$ y por lo tanto, $d(a) \leq d(ab)$. Supongamos que $d(a) = d(ab)$. En este caso $d(ab) \leq d(s),\ \forall\, s \in I$; y por lo visto en la prueba del Teorema 2.25, ab es un generador de I. Como $a \in I$, existe $r \in \mathcal{A}$ tal que $a = r(ab) = a(rb)$. Como $\mathcal{A}$ es un dominio de integridad, vale la ley de cancelación para el producto, y resulta que $rb = 1$, lo que significa que b es una unidad. ■

Definición 2.34 *Sea $\mathcal{A}$ un anillo euclidiano, $a \in \mathcal{A}$ tal que a no es una unidad. Se dice que a es un elemento primo en $\mathcal{A}$, si se cumple lo siguiente: Si existen elementos b, $c \in \mathcal{A}$ tales que $a = bc$, entonces b es una unidad o c es una unidad.*

Ejemplo 2.17 *Si $\mathcal{A} = \mathbb{Z}$, entonces -5, 13, 23 son ejemplos de elementos primos; todos los enteros x tales que $|x|$ es un número natural primo, son elementos primos en $\mathbb{Z}$.*

Ejemplo 2.18 *Si* $\mathcal{A} = \mathbb{Q}[x]$, $p(x) = x^2 - 2$ *es un elemento primo en* $\mathbb{Q}[x]$, *ya que sólo puede factorizarse de la forma:* $x^2 - 2 = \lambda(\frac{x^2}{\lambda} - \frac{2}{\lambda})$, *para* $\lambda \in \mathbb{Q}$, $\lambda \neq 0$; *pero no es primo en* $\mathbb{R}[x]$, *pues en este último anillo,* $p(x)$ *puede factorizarse de manera no trivial:*

$p(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. *Se usa el término "irreducible" para los polinomios que son elementos primos.*

Proposición 2.35 *Sea* $\mathcal{A}$ *un anillo euclidiano. Sea* $a \in \mathcal{A}$ *tal que* a *no es una unidad en* $\mathcal{A}$. *Entonces* $a = p_1 p_2 \cdots p_k$ *donde* p_i *es un elemento primo en* $\mathcal{A}$, *para* $i \in \{1, \ldots, k\}$.

Prueba Dado que $\{d(x) : x \in \mathcal{A}\} \subset \mathbb{N}$, usaremos el principio de inducción sobre $d(a)$ para probar lo que afirma la Proposición. Como $\mathcal{A} = (1)$, tenemos que mín$\{d(x) : x \in \mathcal{A}\} = d(1)$. Si $d(a) = d(1)$, entonces a es una unidad en $\mathcal{A}$, y vale la afirmación que buscamos probar.

Supongamos ahora que $d(a) > d(1)$ y que la proposición vale para todo $x \in \mathcal{A}$ tal que $d(x) < d(a)$. Veamos que también vale, entonces, para a.

Si a es un elemento primo, se cumple la conclusión de la Proposición. Si no lo es, existen $r, s \in \mathcal{A}$, ninguno de los cuales es una unidad, tales que $a = rs$. Según el Lema 2.33, $d(r) < d(rs) = d(a)$ y $d(s) < d(rs) = d(a)$, y, por la hipótesis de inducción, existen elementos primos $p_1, \ldots, p_k$ y $p'_1, \ldots, p'_t$ en $\mathcal{A}$, tales que $r = p_1 \ldots p_k$ y $s = p'_1 \ldots p'_t$. Así, $a = p_1 \ldots p_k p'_1 \ldots p'_t$, y hemos probado que a es igual a un producto de elementos primos de $\mathcal{A}$ ■

Esta proposición es uno entre los varios resultados importantes, relativos a la divisibilidad en un anillo euclidiano $\mathcal{A}$, que son análogos a los que se cumplen en $\mathbb{N}$.

En el Lema siguiente, presentamos algunos de estos resultados, cuya prueba es también análoga a la que se obtiene en el caso de $\mathbb{Z}$, y por esta razón, queda como ejercicio para el lector.

Es importante tomar en cuenta que, como consecuencia de las propiedades de los elementos asociados en un anillo euclidiano (ejercicios al final de esta sección), si $(a, b) = t$ y r es asociado a t, entonces $(a, b) = r$.

Lema 2.36 *Sea* $\mathcal{A}$ *un anillo euclidiano,* $a, b, c \in \mathcal{A}$. *Entonces, valen las siguientes afirmaciones:*

1. *Si* $a|bc$ *y* $(a, b) = 1$, *entonces* $a|c$.

2. *Si b es un elemento primo en $\mathcal{A}$, entonces $b|a$ ó $(a,b)=1$.*

3. *Si b es un elemento primo en $\mathcal{A}$, y $b|ac$ entonces $b|a$ ó $b|c$.*

4. *Si b es un elemento primo en $\mathcal{A}$ y $b|a_1 \dots a_n$, con $a_i \in \mathcal{A}$ para $1 \leq i \leq n$, entonces $b|a_i$ para algún $i \in \{1, \dots, n\}$.*

5. *Si r_1, r_2, ..., $r_n \in \mathcal{A}$ y $r_1 r_2 ... r_n = 1$, entonces r_i es una unidad para $i = 1, ..., n$.*

Definición 2.37 *Si $\mathcal{A}$ es un anillo euclidiano y $a, b \in \mathcal{A}$, se dice que a y b son primos relativos si $(a,b) = u$, donde u es una unidad en $\mathcal{A}$.*

Por observaciones anteriores, si a y b son primos relativos, se puede suponer que $(a,b) = 1$.

Para completar la analogía de los anillos euclidianos con el anillo de los enteros, en relación con el Teorema Fundamental de la Aritmética, probaremos la unicidad (salvo unidades) de la descomposición de un elemento no nulo en factores primos.

Teorema 2.38 *Sea $\mathcal{A}$ un anillo euclidiano, $a \in \mathcal{A}$, $a \neq 0$; si a no es una unidad y $a = p_1 \dots p_k = p'_1 \dots p'_j$ con p_i y p'_l elementos primos en $\mathcal{A}$, para $i \in \{1, \dots, k\}$, $l \in \{1, \dots, j\}$, entonces $k = j$, cada p_i es asociado de algún p'_l y cada p'_l es asociado de algún p_i.*

Prueba Como $a = p_1 \dots p_k = p'_1 \dots p'_j$, se tiene que $p_1 | p'_1 \dots p'_j$. Por el lema anterior, $p_1 | p'_r$ para algún $r \in \{1, \dots, j\}$. Como p_1 y p'_r son elementos primos en $\mathcal{A}$, p_1 y p'_r deben ser asociados; es decir, $p'_r = u_1 p_1$, donde u_1 es una unidad en A.

Así, $p_1 \dots p_k = p'_1 \dots p'_{r-1}(u_1 p_1) p'_{r+1} \dots p'_j$ y como $\mathcal{A}$ es un anillo euclidiano, podemos cancelar p_1 en ambos miembros y resulta

$$p_2 \dots p_k = u_1 p'_1 \dots p'_{r-1} p'_{r+1} \dots p'_j$$

Repetimos el proceso con p_2 y así sucesivamente; luego de k pasos, si $k \leq j$, obtendríamos $1 = u_1 u_2 \dots u_k q$ donde q es un producto de $j - k$ elementos primos entre los p'_l. En ese caso, por el Lema 2.35, se obtiene que cada elemento p'_l entre los factores de q, es una unidad, y dado que, por hipótesis, todos los p'_l son elementos primos, se concluye que $j - k = 0$, y por lo tanto, $j = k$ y cada p_i es igual a una unidad por algún p'_l.

Si suponemos que $k > j$, obtenemos, a partir de las operaciones mencionadas arriba: $p_{k-j} \dots p_k = u_1 \cdots u_k$, lo que implicaría que p_i es una unidad para $k - j \leq i \leq k$. De nuevo, esto contradice la hipótesis de ser p_i primo, para $i = 1, \dots, k$. Deducimos, entonces, que es verdadera la conclusión del teorema ■

Hemos probado entonces que para cualquier anillo euclidiano, vale lo que podríamos llamar una generalización del Teorema Fundamental de la Aritmética.

Se han estudiado ejemplos de anillos euclidianos distintos de $\mathbb{Z}$ y $K[x]$, de los cuales no nos ocuparemos en este texto; uno de los más importantes es el anillo de los enteros gaussianos, denotado usualmente por $J[i]$ y definido así:

$$J[i] = \{a + bi \,:\, a, b \in \mathbb{Z},\ i^2 = -1\}.$$

Conocemos ya los cuerpos que se construyen a partir de $\mathbb{Z}$, a saber: los $\mathbb{Z}_p$ obtenidos como el cociente $\mathbb{Z}/p\mathbb{Z}$, con p primo, y el cuerpo de cocientes ó de fracciones de $\mathbb{Z}$, que constituye $\mathbb{Q}$, el cuerpo de los números racionales.

Como $K[x]$ es también un dominio de integridad, y además un D.I.P., tenemos que los anillos cocientes $K[x]/I$, donde I es un ideal en $K[x]$, son de la forma $K[x]/(p(x))$; y por el teorema 2.13, si $(p(x))$ es un ideal maximal, $K[x]/(p(x))$ es un cuerpo.

Por otra parte, el cuerpo de fracciones de $K[x]$ es denotado $K(x)$, y consiste en todas las expresiones racionales $\dfrac{p(x)}{q(x)}$, con $p(x)$, $q(x) \in K[x]$, y $q(x) \neq 0$.

Volviendo a la cuestión de los anillos cocientes $K[x]/(p(x))$, el siguiente teorema nos dice cuáles son los polinomios $p(x) \in K[x]$ que generan un ideal maximal.

En este caso también vale la analogía con el comportamiento de los ideales maximales en $\mathbb{Z}$, donde los números primos son los que generan ideales maximales.

Teorema 2.39 *Si $\mathcal{A}$ es un anillo euclidiano, el ideal $I = (a)$ es maximal si y sólo si a es un elemento primo en $\mathcal{A}$.*

Prueba Supongamos que $I = (a)$ es un ideal maximal en A. Si a no es un elemento primo en $\mathcal{A}$, existen $b, c \in \mathcal{A}$, ninguno de los dos una unidad, tales que $a = bc$.

El ideal $J = (b)$ contiene a I, pues $a = bc$, lo que implica que $a \in J$ y por lo tanto $ra \in J$, $\forall\, r \in \mathcal{A}$; como b no es una unidad, $J \neq A$; además $J \neq I$, pues si $J = I$, existe $r \in \mathcal{A}$ tal que $b = ra$, luego $bc = rac$, y por lo tanto $a = arc$; como A es un dominio de integridad podemos cancelar a en ambos miembros y obtenemos $1 = rc$, lo cual significa que c es una unidad, contra lo supuesto. Así, $J \neq A$, $J \neq I$ y además $I \subset J \subset A$, por lo que I no es un ideal maximal en A. Esta contradicción con lo que suponíamos de entrada, nos hace concluir que a es un elemento primo en A.

Recíprocamente, si a es un elemento primo en $\mathcal{A}$, y se tiene que $I = (a)$, J otro ideal en A tal que $I \subset J \subset A$, tendremos lo siguiente: $J = (r)$ con $r \in A$, por ser A un D.I.P. Como $I = (a) \subset J = (r)$, claramente $a \in J$, luego $a = br$, para algún $b \in A$. Como a es un elemento primo en $\mathcal{A}$, necesariamente se cumple que b es una unidad ó r es una unidad. Si b es una unidad, existe $q \in \mathcal{A}$ tal que $qb = 1$, y así $qa = r$, por lo cual $r \in I = (a)$, y así $I = J$. En el otro caso, si r es una unidad, entonces $J = (r) = A$.

Por lo tanto, I es maximal en $\mathcal{A}$ ■

En el caso del anillo de polinomios $K[x]$, donde K es un cuerpo, $p(x) \neq 0$ es un elemento primo si $p(x)$ es irreducible, es decir, si $p(x)$ es factorizable en $K[x]$ sólo de la forma, $p(x) = cq(x)$, donde c es una constante no nula; como $\mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$, es posible que un polinomio irreducible en $\mathbb{Q}[x]$, no lo sea en $\mathbb{R}[x]$.

Por ejemplo, $p(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$, pero en $\mathbb{R}[x]$ tenemos que $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Así, $\mathbb{Q}[x]/(x^2 - 2)$ es un cuerpo, pero $\mathbb{R}[x]/(x^2 - 2)$ no lo es puesto que el ideal $(x^2 - 2)$ es maximal en $\mathbb{Q}[x]$, y no lo es en $\mathbb{R}[x]$.

Examinamos ahora el cuerpo $\mathbb{Q}[x]/(x^2 - 2)$.

Para comenzar sabemos que, si $(x^2 - 2)$ denota el ideal generado por $x^2 - 2$, entonces

$$\mathbb{Q}[x]/(x^2 - 2) = \{(x^2 - 2) + p(x) \,:\, p(x) \in \mathbb{Q}[x]\}.$$

Si denotamos por I al ideal $(x^2 - 2)$, entonces un elemento cualquiera $p(x) + I \in \mathbb{Q}[x]/I$ se puede expresar como $[q(x)(x^2 - 2) + r(x)] + I$, donde $r(x) = 0$ ó $gr(r(x)) < 2$, usando el algoritmo de la división euclidiana. Luego,

$$p(x) + I = (q(x)(x^2 - 2) + I) + (r(x) + I).$$

Como $q(x)(x^2 - 2) \in I$, tenemos que $p(x) + I = I + (r(x) + I) = r(x) + I$; y dado que $gr(r(x)) < 2$, resulta que $p(x) + I = (ax + b) + I$, para ciertos

$a, b \in \mathbb{Q}$; pero $(ax + b) + I = a(x + I) + (b + I)$. Si denotamos $x + I$ por z, la expresión anterior se escribe $az + b$.

En otras palabras, $\mathbb{Q}[x]/I = \{az + b : a, b \in \mathbb{Q}\}$

Por otra parte,

$$z^2 - 2 = (x + I)^2 - 2 = x^2 + I - 2 = (x^2 - 2) + I = I = 0 \in \mathbb{Q}[x]/I$$

Así, $z = x + I$ es raíz del polinomio $t(x) = x^2 - 2$, y $\mathbb{Q}[x]/I$ resulta ser un cuerpo que contiene una raíz de $t(x)$, raíz que no existe en $\mathbb{Q}$. Veremos más adelante que $\mathbb{Q}[x]/I$ es el menor cuerpo que contiene a $\mathbb{Q}$ y a una raíz de $t(x)$. Esta construcción fue utilizada por Galois en su tratamiento del problema de la resolución por radicales de una ecuación polinómica.

2.4.1. Irreducibilidad de Polinomios en $\mathbb{Q}[x]$

Hemos visto la importancia del papel que juega la irreducibilidad de un polinomio para la construcción de un cuerpo cociente del tipo $\mathbb{Q}[x]/p(x)$.

En esta sección, presentaremos algunos criterios básicos que permiten determinar la irreducibilidad de ciertos polinomios en $\mathbb{Q}[x]$. El problema general de la determinación de irreducibilidad es difícil y permanece abierto.

Probaremos el llamado Lema de Gauss, que reduce el problema de determinar la irreducibilidad de ciertos polinomios en $\mathbb{Q}[x]$, a determinarla en $\mathbb{Z}[x]$. Terminaremos la sección con el llamado criterio de Eisenstein.

Definición 2.40 *Si $p(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$, decimos que $p(x)$ es primitivo si el máximo común divisor de $a_0, a_1, \ldots, a_n$ es igual a 1.*

Lema 2.41 *Si $p(x)$ y $q(x)$ son polinomios primitivos, entonces $p(x)q(x)$ es primitivo.*

Prueba Supongamos que $p(x) = \sum_{i=0}^{n} a_i x^i$ y $q(x) = \sum_{j=0}^{m} b_j x^j$.

Sea $p(x)q(x) = \sum_{k=0}^{n+m} c_k x^k$, es decir, $c_k = \sum_{i+j=k} a_i b_j$, para $k \in \{0, \ldots, n + m\}$.

Suponemos que $p(x)$ y $q(x)$ son primitivos; si $p(x)q(x)$ no lo es, existe $r \in \mathbb{N},\ r > 1$ tal que $r|c_k,\ \forall\, k \in \{0, \ldots, n+m\}$. Por lo tanto, existe un primo p tal que $p|c_k,\ \forall\, k \in \{0, \ldots, n + m\}$.

Como $p \not| a_i$ para algún $i \in \{0, \ldots, n\}$, sabemos que existe $t \in \{0, \ldots, n\}$ tal que $p|a_i$ para $i < t$ y $p \not| a_t$. Análogamente, existe $s \in \{0, \ldots, m\}$ tal que $p|b_j$ para $j < s$ y $p \not| b_s$.

Ahora bien,

$$c_{t+s} = a_t b_s + (a_{t-1}b_{s+1} + \ldots + a_0 b_{s+t}) + (a_{t+1}b_{s-1} + \ldots + a_{s+t}b_0).$$

Como $p|a_i$ para $i < t$, se tiene que $p|(a_{t-1}b_{s-1} + \ldots + a_0 b_{s+t})$ y como $p|b_j$ para $j < s$, resulta que $p|(a_{t+1}b_{s-1} + \ldots + a_{s+t}b_0)$. Dado que hemos supuesto que $p|c_{t+s}$, necesariamente tendríamos que $p|a_t b_s$; pero siendo p primo, eso implicaría que $p|a_t$ ó $p|b_s$, lo cual contradice lo supuesto. Así, podemos concluir que no existe $r > 1$ tal que $r|c_k$, $\forall\, k \in \{0, \ldots, n+m\}$ y por lo tanto $p(x)q(x)$ es primitivo. ■

Si $p(x) \in \mathbb{Z}[x]$ es un polinomio cualquiera y r es el máximo común divisor de sus coeficientes, es claro que podemos expresar a $p(x)$ como $rq(x)$, donde $q(x)$ es primitivo. Llamaremos a r el contenido de $p(x)$.

Teorema 2.42 *(**Lema de Gauss**)*

Sea $p(x)$ un polinomio primitivo. Si $p(x) = f(x)g(x)$, con $f(x), g(x) \in \mathbb{Q}[x]$, entonces existen $q(x), s(x) \in \mathbb{Z}[x]$, tales que $p(x) = q(x)s(x)$.

Prueba Supongamos que $p(x) \in \mathbb{Z}[x]$ es un polinomio primitivo, y que se puede factorizar como $p(x) = f(x) \cdot g(x)$, con $f(x)$, $g(x) \in \mathbb{Q}[x]$. Si

$$f(x) = \frac{a_0}{c_0} + \left(\frac{a_1}{c_1}\right)x + \ldots + \left(\frac{a_k}{c_k}\right)x^k \qquad \text{y} \qquad g(x) = \frac{b_0}{d_0} + \left(\frac{b_1}{d_1}\right)x + \ldots + \left(\frac{b_s}{d_s}\right)x^s,$$

entonces $f(x) \cdot g(x) = \dfrac{m}{n}(a'_0 + a'_1 x + \ldots + a'_k x^k)(b'_0 + b'_1 x + \ldots + b'_s x^k)$ donde

$$n = [\text{m.c.m.}\,(c_0, c_1, \ldots, c_k)][\text{m.c.m}\,(d_0, \ldots, d_s)] \qquad \text{y}$$

$$m = [\text{m.c.d}\,(a_0, \ldots, a_k)][\text{m.c.d}\,(b_0, \ldots, b_s)]$$

Si $h(x) = \displaystyle\sum_{i=0}^{k} a'_i x^i$, $\quad j(x) = \displaystyle\sum_{i=0}^{s} b'_i x^i$ entonces $h(x)$, $j(x) \in \mathbb{Z}[x]$ y son primitivos; además, $p(x) = \dfrac{m}{n}h(x)j(x)$, y por lo tanto, $np(x) = mh(x)j(x)$

Como $p(x)$ es primitivo, el contenido de $np(x)$ es n; como $h(x)$ y $j(x)$ son primitivos, también lo es su producto $h(x)j(x)$, por el Lema 2.41, y entonces el contenido de $mh(x)j(x)$ es m.

Por lo tanto $n = m$ y como $p(x) = \dfrac{m}{n}h(x)j(x)$, resulta que $p(x) = h(x)j(x)$, con $h(x),\ j(x) \in \mathbb{Z}[x]$, y esto es lo que queríamos probar ■

Definición 2.43 *Un polinomio $p(x) \in \mathbb{Z}[x]$ es mónico si $p(x) = a_0 + a_1x + \ldots + a_nx^n$, y $a_n = 1$.*

De las definiciones de polinomio mónico y polinomio primitivo, se deduce que todo polinomio mónico es primitivo.

La prueba del siguiente corolario queda como ejercicio para el lector:

Corolario 2.44 *Sea $p(x)$ un polinomio mónico. Si $p(x) = q(x)r(x)$, donde $q(x)$, $r(x) \in \mathbb{Q}[x]$ y ambos son no constantes, entonces existen polinomios mónicos $f(x)$, $g(x)$ tales que $p(x) = f(x)g(x)$.*

El siguiente es uno de los pocos criterios de irreducibilidad de polinomios en $\mathbb{Q}[x]$ conocidos hasta ahora.

Teorema 2.45 *(***Criterio de Eisenstein***)*

Sea $q(x) = \sum_{i=0}^{n} a_ix^i \in \mathbb{Z}[x]$. Sea p un número primo tal que $p \nmid a_n$, $p^2 \nmid a_0$, y $p|a_i$ para $i \in \{0, \ldots, n-1\}$. Entonces $q(x)$ es irreducible sobre los racionales.

Prueba Sea $q(x) = \sum_{i=0}^{n} a_ix^i \in \mathbb{Z}[x]$ y sea p un número primo que satisface las condiciones del Teorema. Podemos suponer que $q(x)$ es primitivo, pues en caso contrario, dividimos a $q(x)$ entre el m.c.d. de los a_i. Como $p \nmid a_n$, no modificamos las hipótesis.

Supongamos que $q(x)$ se puede factorizar como $q(x) = t(x)r(x)$, con $t(x)$, $r(x) \in \mathbb{Q}[x]$, ambos no constantes. Entonces, por el Lema de Gauss, se puede factorizar también como producto de dos polinomios en $\mathbb{Z}[x]$. Es decir, existen $u(x) = \sum_{i=0}^{k} u_ix^i,\ v(x) = \sum_{j=0}^{m} v_jx^j \in \mathbb{Z}[x]$, con $k > 0,\ m > 0$ tales que $q(x) = u(x)v(x)$. Por lo tanto, $a_0 = u_0v_0$, y por ser p primo y divisor de a_0, tenemos que $p|u_0$ ó $p|v_0$. Pero p no divide a ambos, puesto que $p^2 \nmid a_0$.

Supongamos que $p|u_0$ y $p \not| v_0$. Si $p|u_i$, $\forall\, i \in \{0,\ldots,k\}$, entonces $p|a_i$, $\forall\, i \in \{0,\ldots,n\}$, puesto que $a_i = \sum_{j+l=i} u_j v_l$, para cada i. Como, por hipótesis, $p \not| a_n$, existe $s \in \{0,\ldots,k\}$ tal que $p \not| u_s$. Escogemos s como el mínimo subíndice en $\{0,\ldots,k\}$ con esa propiedad.

Así, $p|u_i$ para $i \in \{0,\ldots,s-1\}$ y $p|a_s$ (pues $k < n$); como $a_s = u_s v_0 + u_{s-1} v_1 + \ldots + u_0 v_s$, necesariamente $p|u_s v_0$. Esto implica una contradicción con lo supuesto, i.e., que $p \not| v_0$ y $p \not| u_s$. Concluimos, entonces, que no es posible factorizar a $q(x)$ como producto de dos polinomios de grado positivo en $\mathbb{Q}[x]$ ■

Con este resultado, cerramos la exploración de las propiedades del anillo euclidiano $K[x]$, donde K es un cuerpo.

En general, si $\mathcal{A}$ es un anillo conmutativo, $A[x]$ resulta ser un anillo conmutativo también, no necesariamente euclidiano. La teoría que se ocupa de las propiedades diversas de los anillos $A[x]$ está comprendida en el área que se ha denominado Álgebra Conmutativa.

Problemas:

1. Probar que, si $\mathcal{A}$ es un anillo conmutativo con identidad, $R = \{r_1, \ldots, r_k\} \subset \mathcal{A}$, el ideal generado por R (el menor ideal de $\mathcal{A}$ que contiene a R) es

$$I = \{a_1 r_1 + a_2 r_2 + \ldots + a_k r_k \,:\, a_1, \ldots, a_k \in A\}$$

2. Pruebe que en $K[x]$, donde K es un cuerpo, vale el algoritmo euclidiano de la división: Dados $p(x)$, $q(x) \in K[x]$, $q(x) \neq 0$, existen $c(x)$ y $r(x)$, con $r(x) = 0$ ó $gr(r(x)) < gr(q(x))$, tales que $p(x) = q(x)c(x) + r(x)$.

3. Asigne V ó F a las siguientes proposiciones, según sean verdaderas o falsas:

   a) La función $d : A[x]\backslash\{0\} \longrightarrow \mathbb{Z}$ definida por $d(p(x)) = gr(p(x))$ es un homomorfismo de anillos.

   b) Todo cuerpo es isomorfo a su cuerpo de fracciones.

   c) $\mathbb{Z}_n$ es un dominio de integridad si y sólo si es un cuerpo.

4. Si $\mathcal{A}$ es un anillo euclidiano, $a, b, r, s \in \mathcal{A}$, ninguno de ellos nulo, $(a, b) = r$ y $(a, b) = s$ entonces $d(r) = d(s)$.

5. Generalice el algoritmo euclidiano para encontrar (a, b) con $a, b \in \mathbb{Z}$, ambos no nulos, al caso de encontrar $(p(x), q(x))$, con $p(x)$, $q(x) \in K[x]$, donde K es un cuerpo.

6. Demuestre el Teorema 2.20.

7. Encuentre $(p(x), q(x)) = c(x) \in \mathbb{Q}[x]$ en cada uno de los casos siguientes, y exprese $c(x)$ como $r(x)p(x) + s(x)q(x)$, utilizando el algoritmo generalizado en el ejercicio anterior:

   a) $p(x) = x^2 + 1, \qquad q(x) = x^2$

   b) $p(x) = x^4 - x^2 - 6, \qquad q(x) = x^3 - x^2 + 2x - 2$

8. Sea $I \subset \mathbb{Q}[x]$ el ideal generado por los polinomios $p(x)$, $q(x)$ en cada uno de los casos siguientes:

a) $p(x) = x^2 + 1, \qquad q(x) = x^2$

b) $p(x) = x^4 - x^2 - 6, \qquad q(x) = x^3 - x^2 + 2x - 2$

Demuestre que, en el caso a), se tiene $I = \mathbb{Q}[x]$, y en el caso b), se cumple $I = (r(x))$, donde $r(x) = x^2 + 2$.

9. Demuestre que el conjunto de todas las unidades de un anillo conmutativo con identidad forman un grupo abeliano bajo el producto de $\mathcal{A}$.

10. Pruebe que si $a \in \mathcal{A}$, $\mathcal{A}$ un anillo euclidiano, se tiene que a es una unidad en $\mathcal{A}$ si y sólo si $d(a) = d(1)$.

11. Sean K_1, K_2 cuerpos tales que $K_1 \subset K_2$, y sean $p(x)$, $q(x) \in K_1[x]$ tales que $(p(x), q(x)) = 1$ en $K_1[x]$. Pruebe que $(p(x), q(x)) = 1$ en $K_2[x]$.

12. Pruebe que $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

13. Sea p un número primo, y $q(x) = x^n - p$, con $n \geq 1$. Pruebe que $q(x)$ es irreducible en $\mathbb{Q}[x]$.

14. Sean $a, b \in \mathbb{Z}$, ambos no nulos, tales que $(a, b) = 1$. Sea $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. Si $\left(x - \frac{a}{b}\right) | p(x)$, pruebe que $a | a_0$ y $b | a_n$.

Capítulo 3

Extensiones de Cuerpos

En la versión general en la que actualmente se presenta la Teoría de Galois, la noción de cuerpo ocupa un lugar central. En particular, la idea de "extender" un cuerpo dado K, i.e., construir un cuerpo K' tal que $K \subset K'$ (y las operaciones en K' "extienden" a las de K) resulta fundamental para la teoría. La razón por la cual estas ideas aparecen naturalmente en la consideración del problema de la resolución de ecuaciones algebraicas por radicales es la siguiente:

Si un polinomio $p(x) \in K[x]$, irreducible en $K[x]$, donde K es un cuerpo, tiene una raíz α tal que $\alpha \notin K$, es posible construir, a partir de K y $p(x)$, un cuerpo K' tal que $K \subset K'$ y $\alpha \in K'$. En el capítulo 2, se muestra un ejemplo de esta construcción en el caso en que $K = \mathbb{Q},\ p(x) = x^2 - 2$ y $K' = \mathbb{Q}[x]/I$, donde I es el ideal generado por $p(x)$. Galois consideró sólo el caso particular de extensiones de $\mathbb{Q}$ y $\mathbb{R}$ contenidas en $\mathbb{C}$.

Antes de estudiar con mayor generalidad los aspectos esenciales involucrados en esta idea, introduciremos algunas definiciones básicas, y propiedades generales de los cuerpos. En lo sucesivo, hablaremos de monomorfismos, epimorfismos e isomorfismos entre cuerpos, al referirnos a los monomorfismos, epimorfismos e isomorfismos de anillos entre ellos.

Definición 3.1 *Sea K un cuerpo, y $F \subset K$. Decimos que F es un subcuerpo de K si F es un cuerpo con las operaciones definidas en K.*

Proposición 3.2 *Si K es un cuerpo, entonces la intersección de todos los subcuerpos contenidos en K, es un subcuerpo de K.*

Prueba Se deja como ejercicio para el lector.

Definición 3.3 *Sea K un cuerpo. El subcuerpo primo (o cuerpo primo) de K es la intersección de todos los subcuerpos de K.*

Intuitivamente hablando, el subcuerpo primo de K es el menor subcuerpo de K.

Cuando un cuerpo K no posee subcuerpos propios, es claro que K es su cuerpo primo. Es el caso de $\mathbb{Z}_p$, con p primo, y también el de $\mathbb{Q}$.

El próximo teorema nos asegura que, en esencia, éstos últimos son los únicos cuerpos primos que existen.

Teorema 3.4 *Sea K un cuerpo y J su cuerpo primo. Entonces $J \cong \mathbb{Q}$ o existe p primo tal que $P \cong \mathbb{Z}_p$.*

Prueba Sea J el cuerpo primo del cuerpo K. Sean 0_k y 1_k, respectivamente, identidades de las operaciones suma y producto en K. Claramente, $0_k \in J$ y $1_k \in J$, por lo tanto, $\forall\, n \in \mathbb{N}$, $1_k + 1_k + \ldots + 1_k = n1_k \in J$ y $-(\underbrace{1_k + 1_k + \ldots + 1_k}_{n}) = n(-1_k) = -n(1_k) \in J$.

Definamos $\lambda : \mathbb{Z} \longrightarrow J$ por $\lambda(n) = n1_k$.

Veamos que λ es un homomorfismo de anillos:

Sean $n, m \in \mathbb{Z}$.

- $\lambda(n+m) = (n+m)1_k = n1_k + m1_k = \lambda(n) + \lambda(m)$
- $\lambda(n \cdot m) = (n \cdot m)1_k = \underbrace{1_k + \ldots + 1_k}_{n \cdot m} = (\underbrace{1_k + \ldots + 1_k}_{n})(\underbrace{1_k + \ldots + 1_k}_{m})$;

está última igualdad se obtiene aplicando la distributividad del producto respecto a la suma en K. Así, $\lambda(n \cdot m) = \lambda(n)\lambda(m)$.

Si λ es un monomorfismo, entonces $Ker(\lambda) = \{0\}$, y

$$S = \{\lambda(m)[\lambda(n)]^{-1} \,:\, m \in \mathbb{Z},\ n \in \mathbb{Z}\backslash\{0\}\} \subset J$$

por ser J un cuerpo. Además, S es un subcuerpo de J, por lo cual $S = J$, ya que J es el subcuerpo primo de K.

Si definimos $f : \mathbb{Q} \longrightarrow S$ por $f\left(\frac{m}{n}\right) = \lambda(m)[\lambda(n)]^{-1}$, entonces f es un isomorfismo, lo cual queda como un ejercicio para el lector. Así, $\mathbb{Q} \cong J$.

Si λ no es un monomorfismo, entonces $Ker\,\lambda \neq \{0\}$. Como $Ker\,\lambda < \mathbb{Z}$, existe $r \in \mathbb{Z},\ r > 0$ tal que $Ker\,\lambda = r\mathbb{Z}$. Afirmamos que r debe ser primo; en efecto, de lo contrario, existirían $t, q \in \mathbb{N},\ t < r,\ q < r,\ r = tq$, lo cual implica que $\lambda(r) = 0 = \lambda(tq) = \lambda(t)\lambda(q)$, y por el hecho de ser J un cuerpo, es un dominio de integridad, de modo que $\lambda(t) = 0$ ó $\lambda(q) = 0$; luego $t \in r\mathbb{Z}$ ó $q \in r\mathbb{Z}$, lo cual es imposible si $0 < t < r$ y $0 < q < r$.

Por lo tanto, $\mathbb{Z}/r\mathbb{Z} = \mathbb{Z}_r$ es un cuerpo isomorfo a $Im\,\lambda$; pero entonces $Im\,\lambda$ es un cuerpo que coincide con J, por ser J el cuerpo primo de K. Así, $\mathbb{Z}_r \cong J$. ■

Proposición 3.5 *Sea K un cuerpo. Si el subcuerpo primo de K es isomorfo a $\mathbb{Z}_p$, entonces $Car(K) = p$. Si el subcuerpo primo de K es isomorfo a $\mathbb{Q}$, entonces $Car(K) = 0$.*

Prueba Se deja como ejercicio para el lector.

Corolario 3.6 *Si K es un subcuerpo de K', entonces $Car(K) = Car(K')$.*

Prueba Como K y K' tienen el mismo subcuerpo primo, se concluye que $Car(K) = Car(K')$ ■

Proposición 3.7 *Sea K un cuerpo y $a \in K,\ a \neq 0$; si $n \in \mathbb{N}$ y $na = 0$, entonces n es múltiplo de $Car(K)$.*

Prueba Supongamos que $a \in K,\ a \neq 0$. Como $na = 0$, por definición de $Car(K)$, tenemos que si $Car(K) = 0$, esto implica que $n = 0$ y en este caso, n es múltiplo de $Car(K)$.

Si $Car(K) = p > 0$, entonces $n \geq p$, por definición de $Car(K)$. Entonces, existen $q,\ r \in \mathbb{N}$ tales que $n = pq + r$, con $0 \leq r < p$, y así,

$$na = (pq + r)a \Rightarrow 0 = pqa + ra = ra = 0$$

Si $0 < r$ esto contradice el hecho de ser $p = Car(K)$. Por lo tanto, $r = 0$ y resulta que $n = pq$ ■

La idea básica de ser K' una extensión de K si $K \subset K'$ requiere de una definición que incluya el caso en que $K \cong L$, con $L \subset K'$, para mayor generalidad.

Por ejemplo, interesa que los casos $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$ sean definidos como extensiones de cuerpos, pero también casos como el siguiente:

Sea A un dominio de integridad, F su cuerpo de fracciones, y K cualquier cuerpo que contenga a A; en este caso, sabemos que existe un monomorfismo $\lambda : F \longrightarrow K$, razón por la cual $F \cong Im(\lambda) \subset K$; aquí es conveniente considerar a K como una extensión de F.

Definición 3.8 *Una extensión de cuerpos es un monomorfismo* $g : K \longrightarrow K'$, *donde* K, K' *son cuerpos.* K *es denominado el cuerpo base y* K' *la extensión de* K.

Ejemplo 3.1 *Las inclusiones* $i_1 : \mathbb{Q} \longrightarrow \mathbb{R}$, $i_2 : \mathbb{Q} \longrightarrow \mathbb{C}$, $i_3 : \mathbb{R} \longrightarrow \mathbb{C}$ *son extensiones de cuerpos.*

Ejemplo 3.2 *Si* K *es un cuerpo y* $K[x]$ *el anillo de polinomios sobre* K, *sabemos que podemos construir el cuerpo de fracciones de* $K[x]$, *llamado el cuerpo de expresiones racionales sobre* K, *y denotado* $K(x)$. *Si definimos* $i : K \longrightarrow K(x)$ *como* $i(\alpha) = \alpha$ *(el polinomio constante igual a* α*), entonces* i *es un monomorfismo y por lo tanto* $K(x)$ *es una extensión de* K.

Ejemplo 3.3 *Si* $p(x) = x^2 - 2 \in \mathbb{Q}[x]$, *tenemos que* $p(x)$ *es irreducible sobre* $\mathbb{Q}$ *y por lo tanto el ideal* $I = (p(x))$ *es maximal en* $\mathbb{Q}[x]$ *y* $\mathbb{Q}[x]/I$ *es un cuerpo. De nuevo, la función* $i : \mathbb{Q} \longrightarrow \mathbb{Q}[x]/I$, *definida por* $i(a) = I + a$, $\forall\, a \in \mathbb{Q}$ *es un monomorfismo, y por lo tanto es una extensión de cuerpos.*

Cuando K, K' son cuerpos y K' es una extensión de K, escribiremos $K' : K$.

En lo que sigue, estudiaremos el caso en que, dada una extensión $K' : K$, y un subconjunto $H \subset K'$, se construye una extensión $F : K$ tal que F es "minimal" entre las extensiones de K que contienen a H, y claramente, $K' : F$ es también una extensión.

Para precisar esa noción de "minimalidad," apelamos a un recurso ya conocido, seguramente, por el lector.

Definición 3.9 *Sea* K *un cuerpo,* $H \neq \phi$, $H \subset K$. *Entonces, el subcuerpo de* K *generado por* H *es la intersección de todos los subcuerpos de* K *que contienen a* H.

Ejemplo 3.4 *Considérese el subcuerpo K de $\mathbb{C}$, generado por $H = \{1, i\}$ ($i = \sqrt{-1}$). Como $\mathbb{Q}$ es el cuerpo primo de $\mathbb{C}$, $\mathbb{Q} \subset K$, y por lo tanto el conjunto $S = \{a + bi : a, b \in \mathbb{Q}\} \subset K$.*

Ahora bien, si se prueba que S es un cuerpo, entonces, por ser K el menor subcuerpo de $\mathbb{C}$ que contiene a H, resultaría que $K = S$.

Queda como ejercicio para el lector, verificar que S es un cuerpo.

Obsérvese que K puede también definirse como el subcuerpo de $\mathbb{C}$ generado por $\mathbb{Q} \cup \{i\}$. En general, hay una notación precisa para representar situaciones análogas a ésta:

Definición 3.10 *Sea $K' : K$ una extensión de cuerpos y sea $H \subset K'$. El subcuerpo de K' generado por $K \cup H$ (o, más precisamente, por $i(K) \cup H$, donde i es el monomorfismo que define la extensión $K' : K$) se denota por $K(H)$, y se dice que es obtenido a partir de K, adjuntando a H.*

Si $H = \{\alpha\}$, se escribe $K(H) = K(\alpha)$ y si $H = \{\alpha_1, \ldots, \alpha_r\}$ entonces $K(H)$ se denota por $K(\alpha_1, \ldots, \alpha_r)$.

Ejemplo 3.5 *Si K es un cuerpo y denotamos por $K(t)$ el cuerpo de expresiones racionales en t sobre K, entonces podría pensarse que hay ambigüedad en la notación, pues en la extensión $K(t) : K$, al subcuerpo de $K(t)$ generado por $K \cup \{t\}$, lo denotamos del mismo modo. Pero, en realidad, no hay ambigüedad, pues el subcuerpo generado por $K \cup \{t\}$ debe contener a todas las expresiones racionales en t sobre K, y además está contenido en ese cuerpo. Así, la notación $K(t)$ está representando a un único objeto.*

Ejemplo 3.6 *En $\mathbb{R} : \mathbb{Q}$, como $\mathbb{Q}(\sqrt{2})$ es el subcuerpo generado por $\mathbb{Q} \cup \{\sqrt{2}\}$, todos los elementos de la forma $p + q\sqrt{2}$, con $p, q \in \mathbb{Q}$ deben estar en $\mathbb{Q}(\sqrt{2})$.*

Queda como ejercicio para el lector probar que el conjunto $S = \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$ es un cuerpo, y por lo tanto, $S = \mathbb{Q}(\sqrt{2})$.

Observe que $\mathbb{Q}(\sqrt{2})$ coincide con el cuerpo $\mathbb{Q}[x]/I$, donde I es el ideal primo generado por $p(x) = x^2 - 2$.

3.1. Extensiones Simples

Definición 3.11 *Una extensión simple es una extensión $K' : K$ tal que $K' = K(a)$ para algún $a \in K'$.*

Ejemplo 3.7 *La extensión $\mathbb{C} : \mathbb{R}$ es simple, pues $\mathbb{R}(i) = \mathbb{C}$, como puede fácilmente comprobar el lector.*

Ejemplo 3.8 $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$, *y* $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ *son extensiones simples. Se puede probar que* $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \ : \ a, b, c \in \mathbb{Q}\}$, *lo cual muestra que los elementos de una extensión simple* $K(\alpha)$ *de un cuerpo* K, *no siempre son de la forma* $a + b\alpha$, *con* $a, b \in K$.

Ejemplo 3.9 $K(t) : K$ *es un extensión simple, si* $K(t)$ *denota el cuerpo de las expresiones racionales en* t *sobre* K.

Los ejemplos 3.7 y 3.8 se diferencian del ejemplo 3.9 en un sentido que explicaremos a continuación.

Definición 3.12 *Sea* $K(a) : K$ *una extensión simple. Si existe un polinomio no nulo* $p(x) \in K[x]$ *tal que* $p(a) = 0$, *entonces* a *es un elemento algebraico sobre* K *y se dice que la extensión es una extensión simple algebraica. De lo contrario, se dice que* a *es trascendente sobre* K *y que* $K(a) : K$ *es una extensión simple trascendente.*

Teorema 3.13 *Si* K *es un cuerpo, entonces el cuerpo de expresiones racionales* $K(t)$ *es una extensión simple trascendente de* K.

Prueba La extensión $K(t) : K$ es simple, por definición. Es trascendente porque si $a_0, a_1, \ldots, a_n \in K$ y $a_0 + a_1 t + \ldots + a_n t^n = 0$, entonces el polinomio $p(t) = \sum_{i=0}^{n} a_i t^i$ es el polinomio nulo en $K(t)$, y por lo tanto es el polinomio nulo en $K[t]$ ■

Veamos ahora cómo se construyen las extensiones simples algebraicas.

Definición 3.14 *Sea* $K' : K$ *una extensión, y sea* $a \in K'$ *algebraico sobre* K. *El polinomio mínimo de* a *sobre* K *es el único polinomio mónico* $m(x) \in K[x]$, *de grado mínimo, tal que* $m(a) = 0$.

El polinomio mínimo de a *sobre* K *es el generador mónico del ideal* $I_a = \{q(x) \in K[x] \ : \ q(a) = 0\} \subseteq K[x]$. *Sabemos que* m *es irreducible.*

Como ejemplos, tenemos que en $\mathbb{C} : \mathbb{R}$, i es algebraico sobre $\mathbb{R}$; también en $\mathbb{R} : \mathbb{Q}$, $\sqrt{2}$ es algebraico sobre $\mathbb{Q}$ y $m(x) = x^2 - 2$ es el polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$.

Veremoa ahora que, dado cualquier cuerpo K, y un polinomio $p(x)$ mónico, irreducible sobre K, se puede construir una extensión simple, algebraica $K(a) : K$, tal que el polinomio mínimo de a sobre K es $p(x)$.

Teorema 3.15 *Si K es un cuerpo y $m(x) \in K[x]$ es un polinomio irreducible sobre K y mónico, entonces existe una extensión simple $K(a) : K$ tal que $m(x)$ es el polinomio mínimo de a sobre K.*

Prueba

Sea $i : K \longrightarrow K[x]$ el monomorfismo natural definido por:

$$i(h) = h, \text{el polinomio constante igual a } h,\ \forall h \in K$$

Sea $K' = K[x]/(m(x))$; como $m(x)$ es irreducible sobre K, el ideal $(m(x))$ es maximal en $K[x]$ y K' es un cuerpo. Si $\pi : K[x] \longrightarrow K'$ es la proyección sobre el cociente, entonces $\pi \circ i : K \longrightarrow K'$ es un homomorfismo entre cuerpos, y como no es idénticamente nulo, pues $\pi \circ i(1) = (m(x)) + 1$ y $1 \notin (m(x))$, entonces $\pi \circ i$ es un monomorfismo.

Así, $K \cong \pi \circ i(K) \subset K'$; si identificamos a K con su imagen, y denotamos por a al elemento $(m(x)) + x \in K'$, entonces $K' = K(a)$, pues el cuerpo generado por $K \bigcup a$ contiene a todos los elementos de la forma $(m(x)) + q(x)$, con $q(x) \in K[x]$.

Por otra parte, como $m(x) \in (m(x))$, se tiene que
$m(a) = (m(x)) = 0 \in K'$. Como $m(x)$ es irreducible sobre K y mónico, entonces $m(x)$ es el polinomio mínimo de a sobre K ■

El siguiente resultado determina la forma que tienen todos los elementos de $K(a)$, cuando $K(a) : K$ es una extensión algebraica.

Proposición 3.16 *Sea $K(a) : K$ una extensión algebraica simple, y sea $m(x)$ el polinomio mínimo de a sobre K, con $gr(m(x)) = s$. Si $\beta \in K(a)$, entonces existen $\lambda_0, \lambda_1, \ldots, \lambda_{s-1} \in K$ tales que $\beta = \lambda_0 + \lambda_1 a + \ldots + \lambda_{s-1} a^{s-1}$, y esta expresión es única.*

Prueba Sea $\beta \in K(a)$; como $K(a)$ es el menor cuerpo que contiene a K y a a, y el conjunto $F = \{\dfrac{f(a)}{g(a)} : f(x), g(x) \in K[x], g(a) \neq 0\}$ es un cuerpo que contiene a K y a a, tenemos que $K(a) \subset F$. Pero, a su vez, toda expresión

del tipo $\dfrac{f(a)}{g(a)} \in F$ está en $K(a)$, por lo cual tenemos que $F = K(a)$. Así, $\beta = \dfrac{f(a)}{g(a)}$ para ciertos polinomios $p(x)$, $g(x) \in K[x]$, con $g(a) \neq 0$. Como $g(a) \neq 0$, $g(x) \notin (m(x))$, es decir, $m(x) \not| g(x)$, y como $m(x)$ es irreducible, resulta que $(m(x), g(x)) = 1$. Luego, existen polinomios $u(x)$, $v(x) \in K[x]$ tales que $1 = u(x)g(x) + v(x)m(x)$.

Pero $v(x)m(x) = 0$ en $K(a)$, por lo que $1 = u(x)g(x)$, ó $\dfrac{1}{g(x)} = u(x)$. Así, $\beta = \dfrac{f(a)}{g(a)} = f(a)u(a) = w(a)$, para un cierto polinomio $w(x) \in K[x]$.

Al dividir $w(x)$ entre $m(x)$, obtenemos $w(x) = q(x)m(x) + r(x)$, donde $r(x) = 0$ ó $gr(r(x)) < s$. Luego, $\beta = w(a) = r(a) = \lambda_0 + \lambda_1 a + \ldots + \lambda_{s-1}a^{s-1}$.

Para probar la unicidad de la expresión encontrada para β, supongamos que existe otro polinomio $t(x) \in K[x]$, con $gr(t(x)) < s$, tal que $t(a) = r(a)$. Sea $p(x) = t(x) - r(x)$. Como $p(a) = 0$, tenemos que $p(x) \in (m(x))$ y esto, junto con el hecho de que $gr(p(x) < s = gr(m(x)))$, implica que $p(x) = 0$; es decir, $t(x) = r(x)$ ■

Problemas:

1. Pruebe que si K es un cuerpo y $H \subset K$, entonces el subcuerpo de K generado por H es el menor subcuerpo de K que contiene a H y está constituido por todos los elementos de K que se obtienen a partir de los elementos de H, por un número finito de las operaciones definidas en K, siempre que $H \neq \emptyset$.

2. Determine los subcuerpos de $\mathbb{C}$ generados por los subconjuntos indicados en cada caso:

   a) $\{0, 1\}$
   b) $\{0, 1, i\}$
   c) $\{i, \sqrt{2}\}$
   d) $\mathbb{R} \bigcup \{i\}$

3. Demuestre que $\mathbb{R}$ no es una extensión simple de $\mathbb{Q}$, mostrando que toda extensión simple de un cuerpo numerable, es numerable.

4. Encuentre el polinomio mínimo sobre el cuerpo base de cada uno de los elementos indicados en las extensiones siguientes:

   a) i en $\mathbb{C} : \mathbb{Q}$

   b) i en $\mathbb{C} : \mathbb{R}$

   c) $\sqrt{2}$ en $\mathbb{R} : \mathbb{Q}$

   d) $(\sqrt{5}+1)/2$ en $\mathbb{C} : \mathbb{Q}$

5. Describa los subcuerpos de $\mathbb{C}$ siguientes:

   a) $\mathbb{Q}(\sqrt[3]{2})$

   b) $\mathbb{Q}(i)$

   c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ Demuestre que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

   d) $\mathbb{Q}(i\sqrt{7})$

6. Construya extensiones $\mathbb{Q}(a) : \mathbb{Q}$, donde a tiene el polinomio mínimo sobre $\mathbb{Q}$ indicado en cada caso:

   a) $p(x) = x^2 - 3$

   b) $p(x) = x^3 + x^2 + x + 1$

3.2. El grado de una extensión

Cuando se observa el resultado de la Proposición 3.16, que da la forma de cada elemento en $K(a)$, donde $K(a) : K$ es una extensión algebraica simple, se puede percibir el comportamiento de las potencias de a como "generadores" de $K(a) = \{\lambda_0 + \lambda_1 a + \ldots + \lambda_s a^{s-1} : \lambda_i \in K\}$, donde s es el grado del polinomio mínimo de a sobre K.

De hecho, toda extensión $K' : K$ le confiere a K' la estructura de espacio vectorial sobre K :

Si $\lambda \in K$ y $v \in K'$, entonces $\lambda v \in K'$ y si u, $v \in K'$, entonces $u + v \in K'$ y es fácil ver que los axiomas de espacio vectorial se satisfacen en este caso.

Al considerar a las extensiones de cuerpos como espacios vectoriales, interesa determinar su dimensión.

Definición 3.17 *Sea $K' : K$ una extensión de cuerpos. Se denomina grado de la extensión a la dimensión de K', como espacio vectorial sobre K, y se denota $[K' : K]$.*

Ejemplo 3.10 $[\mathbb{C} : \mathbb{R}] = 2$ *porque* $\{1, i\}$ *es una base de* $\mathbb{C}$, *como espacio vectorial sobre* $\mathbb{R}$.

Ejemplo 3.11 $[\mathbb{Q}(x) : \mathbb{Q}] = \infty$, *puesto que los elementos* $1,\ x,\ x^2, \ldots, x^n, \ldots$ *son linealmente independientes sobre* $\mathbb{Q}$.

El siguiente teorema permite calcular el grado de una extensión dada, si se conoce el grado de las extensiones intermedias. Por ejemplo, en el caso de las extensiones $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ y $\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}\sqrt{2}$, si se conoce $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ y $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})]$, se puede calcular $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}]$.

Teorema 3.18 *Si K, L, M son cuerpos tales que $K \subseteq L \subseteq M$, entonces* $[M : K] = [M : L][L : K]$.

Prueba Sea $\{\lambda_i : i \in I\}$ una base de L sobre K y sea $\{\mu_j : j \in J\}$ base de M sobre L.

Veremos que $B = \{\lambda_i \mu_j : i \in I,\ j \in J\}$ constituye una base de M sobre K. Una vez probado esto, tendremos la igualdad requerida: si tanto I como J son finitos, resultará inmediata la igualdad. Si alguno de los dos conjuntos de índices es infinito, $[M : K]$ resulta ser infinito también.

En primer lugar, veamos que B es linealmente independiente. Sean $U \subset I$, $V \subset J$, U, V finitos, tales que $\sum_{i \in U, j \in V} a_{ij} \lambda_i \mu_j = 0$, donde $a_{ij} \in K$, para $i \in U,\ j \in V$.

Como $\lambda_i \in K,\ \forall\, i \in U$, y L es un cuerpo que contiene a K, se obtiene que $a_{ij}\lambda_i \in L,\ \forall\, i \in U, \forall\, j \in V$. Si escribimos $a_{ij}\lambda_i = b_{ij}$ entonces se verifica que

$$\sum_{i \in U, j \in V} b_{ij} \mu_j = 0, \text{ es decir, } \sum_{j \in V} \left(\sum_{i \in U} b_{ij} \right) \mu_j = 0.$$

Ahora bien, como los elementos μ_j forman una base de M sobre L, y cada $b_{ij} \in L$, se tiene que la igualdad anterior implica que $\sum_{i \in U} b_{ij} = 0,\ \forall\, j \in V$; es decir, $\forall\, j,\ \sum_{i \in U} a_{ij} \lambda_i = 0$. Como los λ_i forman una base de L sobre K y $a_{ij} \in K,\ \forall\, i \in U,\ j \in V$ tenemos que $a_{ij} = 0$, para todo $i \in U,\ j \in V$.

Así, el conjunto $B = \{\lambda_i \mu_j : i \in I,\ j \in J\}$ es linealmente independiente sobre K. Veamos ahora que B genera a M sobre K.

Si $\alpha \in M$, existen escalares $\alpha_1, \ldots, \alpha_n \in L$ y elementos $\mu_{j_1}, \ldots, \mu_{j_n}$ de la base de M, tales que $\alpha = \sum_{t=1}^{n} \alpha_t \mu_{j_t}$.

A su vez, para cada $t = 1, \ldots, n,\ \alpha_t \in L$ y por lo tanto es combinación lineal de los λ_i, con $i \in I$ y con escalares en K. Así, $\alpha_t = \sum_{k=1}^{s_t} \beta_k^t \lambda_{i_k}$, con $\beta_k^t \in K$ para $k \in \{1, \ldots, s\}$ y $t \in \{1, \ldots, n\}$ y por lo tanto

$$\alpha = \sum_{t=1}^{n} \left(\sum_{k=1}^{s_t} \beta_k^t \lambda_{i_k} \right) \mu_{j_t}$$

de manera que α es combinación lineal de ciertos productos $\lambda_i \mu_j$ con coefientes en K.

Así, hemos probado que B es una base de M sobre K ■

Ejemplo 3.12 *Considere la extensión* $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}]$.

Como $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(i, \sqrt{2})$, *si* $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = r$ *y* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = t$, *entonces, por el teorema anterior,* $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = rt$.

Veamos que una base para $\mathbb{Q}(i, \sqrt{2})$ *sobre* $\mathbb{Q}(\sqrt{2})$ *es* $\{1, i\}$. *Para verificar la independencia lineal, supongamos que* $\alpha_1, \alpha_2 \in \mathbb{Q}(\sqrt{2})$ *son tales que* $\alpha_1 + \alpha_2 i = 0$.

Como $\alpha_1 \in \mathbb{Q}(\sqrt{2})$, *si* $\alpha_1 \neq 0$ *entonces* $\alpha_2 \neq 0$ *y* $\alpha_1 = -\alpha_2 i$. *Pero además,* $-\alpha_2 \in \mathbb{Q}(\sqrt{2})$ *y por lo tanto* $Im(-\alpha_2 i) \neq 0$; *esto significa que* $Im(\alpha_1) \neq 0$, *lo cual es absurdo, ya que* $\alpha_1 \in \mathbb{R}$.

Así, $\alpha_1 = \alpha_2 = 0$.

Por otra parte, veamos que $\{1, i\}$ *genera a* $\mathbb{Q}(i, \sqrt{2})$, *sobre* $\mathbb{Q}(\sqrt{2})$. *En efecto, si* $z \in \mathbb{Q}(i, \sqrt{2})$, *dado que la extensión* $\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})$ *es simple, por la Proposición 3.16, se sabe que* $z = a + bi$ *con* $a, b \in \mathbb{Q}(\sqrt{2})$, *ya que el polinomio mínimo de* i *sobre* $\mathbb{Q}(\sqrt{2})$ *es* $p(x) = x^2 + 1$. *(Esto puede comprobarlo fácilmente el lector). Así,* z *es combinación lineal de* 1 *e* i.

Como $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, *pues una base para* $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$ *es* $\{1, \sqrt{2}\}$ *(lo cual es fácil de probar), entonces* $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. *Más aún, el Teorema 3.18 nos provee de una base para* $\mathbb{Q}(\sqrt{2}, i)$ *sobre* $\mathbb{Q}$, *a saber:*$\{1, \sqrt{2}, i, \sqrt{2}i\}$.

La proposición siguiente muestra la relación entre el grado de una extensión algebraica simple $K(a) : K$ y el grado del polinomio mínimo de a sobre K.

Proposición 3.19 *Sea $K(a) : K$ una extensión algebraica, sea $m(x)$ el polinomio mínimo de a sobre K. Si $gr(m(x)) = r$, entonces $[K(a) : K] = r$.*

Prueba Por la Proposición 3.16, todo elemento de $K(a)$ se expresa de manera única como combinación lineal de los elementos $1, a, a^2, \ldots, a^{r-1}$, donde $r = gr(a)$. Esto significa que $\{1, a, a^2, \ldots, a^{n-1}\}$ es una base para $K(a)$ sobre K ■

Proposición 3.20 *Si $K(a) : K$ es una extensión trascendente simple, entonces $[K(a) : K] = \infty$.*

Prueba Veamos que $\{1, a, a^2, \ldots, a^n, \ldots\}$ es un conjunto linealmente independiente de $K(a)$ sobre K. Sea $t \in \mathbb{N}$ y sean $\alpha_0, \ldots, \alpha_t \in K$ tales que $\alpha_0 + \alpha_1 a + \ldots + \alpha_t a^t = 0$.

Como a es trascendente sobre K, $p(a) \neq 0$, $\forall\, p(x) \neq 0 \in K[x]$; en particular, si $\alpha_0 + \alpha_1(x) + \ldots + \alpha_t x^t = q(x)$, y $q(a) = 0$, necesariamente $q(x) \equiv 0$, luego $\alpha_i = 0$, $\forall\, i$ ■

Definición 3.21 *Una extensión $K' : K$ se dice que es finita si $[K' : K] < \infty$. La extensión $K' : K$ es algebraica si para todo $a \in K'$, a es algebraico sobre K.*

Veremos ahora que toda extensión finita es algebraica; sin embargo, existen extensiones algebraicas que no son finitas.

Proposición 3.22 *La extensión $K' : K$ es finita si y sólo si K' es algebraica sobre K y existe un número finito de elementos $a_1, \ldots, a_r \in K'$ tales que $K' = K(a_1, \ldots, a_r)$.*

Prueba Usemos inducción sobre n para demostrar que si $K(a_1, \ldots, a_n) : K$ es una extensión algebraica, entonces es finita.

Para $n = 1$, la Proposición 3.19 asegura que $[K(a_1) : K] = m$, donde $m = gr(p(x))$, con $p(x)$ el polinomio mínimo de a_1 sobre K. Supongamos que toda extensión algebraica $K(a_1, \ldots, a_r) : K$, con $r \leq n$, es finita, y sea $K(a_1, \ldots, a_{n+1}) : K$ una extensión algebraica.

Si $a_{n+1} \in K(a_1, \ldots, a_n)$, entonces $K(a_1, \ldots, a_{n+1}) = K(a_1, \ldots, a_n)$ y por la hipótesis inductiva, $[K(a_1, \ldots, a_{n+1}) : K] < \infty$.

Si $a_{n+1} \notin K(a_1, \ldots, a_n)$, y $L = K(a_1, \ldots, a_n)$, entonces tenemos que a_{n+1} es algebraico sobre L, puesto que, por hipótesis, es algebraico sobre $K \subset L$.

Entonces, tenemos que, por la hipótesis inductiva, $[L : K] = s < \infty$ y $[K(a_1, \ldots, a_{n+1}) : L] = [L(a_{n+1}) : L] = t < \infty$. Por el Teorema 3.18, tenemos que $[K(a_1, \ldots, a_{n+1}) : K] = st < \infty$.

Recíprocamente, si $K' : K$ es una extensión finita, entonces $\exists\, n \geq 1$ tal que $[K' : K] = n$, es decir, existe una base $\{a_1, \ldots, a_n\}$ de K' como espacio vectorial sobre K. Por lo tanto, $K' \subset K(a_1, \ldots, a_n)$; pero $K(a_1, \ldots, a_n)$ es el menor cuerpo que contiene a $K \cup \{a_1, \ldots, a_n\}$, por lo que resulta $K(a_1, \ldots, a_n) \subset K'$. Así, $K' = K(a_1, \ldots, a_n)$.

Ahora, resta ver que K' es algebraica sobre K. Sea $u \in K'$; como $[K' : K] = n$, el conjunto $\{1, u, u^2, \ldots, u^n\}$ es linealmente dependiente sobre K; en consecuencia existen $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$ tales que $\alpha_i \neq 0$ para algún $i \in \{0, \ldots, n\}$ y $\displaystyle\sum_{i=0}^{n} \alpha_i u^i = 0$. Esto significa que u es raíz del polinomio no nulo $p(x) = \displaystyle\sum_{i=0}^{n} \alpha_i x^i \in K[x]$; en otras palabras, u es algebraico sobre K ■

Las extensiones finitas algebraicas juegan un papel muy importante en la Teoría de Galois, puesto que, asociado a un polinomio $p(x) \in K[x]$, donde K es un cuerpo cualquiera, se define el cuerpo de descomposición del polinomio $p(x)$, al cual, de manera intuitiva, podemos definirlo como la menor extensión de K que contiene a todas las raíces de $p(x)$; se demuestra que el cuerpo de descomposición de $p(x)$ es precisamente la extensión finita algebraica $K(\alpha_1, \cdots, \alpha_r)$, donde $\alpha_1, \cdots, \alpha_r$ son todas las raíces de $p(x)$.

Finalizamos esta sección mencionando un ejemplo muy importante de extensión algebraica:

Si se considera el conjunto $\mathcal{A}(\mathbb{Q}) \subset \mathbb{C}$ de todos los números que son algebraicos sobre $\mathbb{Q}$, se puede probar (problema 5 al final de esta sección) que $\mathcal{A}(\mathbb{Q})$ es un cuerpo, y que $[\mathcal{A}(\mathbb{Q}) : \mathbb{Q}] = \infty$. Este ejemplo muestra que no toda extensión algebraica es finita. $\mathcal{A}(\mathbb{Q})$ es llamado el cuerpo de los números algebraicos.

Problemas:

1. Determine el grado de las siguientes extensiones y encuentre una base para la extensión, sobre el cuerpo base.

   a) $\mathbb{C} : \mathbb{Q}$

   b) $\mathbb{Z}_3(t) : \mathbb{Z}_3$

   c) $\mathbb{R}(\sqrt{7}) : \mathbb{R}$

   d) $\mathbb{Q}(\sqrt{5}, \sqrt{11}, \sqrt{7}) : \mathbb{Q}$

2. Pruebe que si $[K' : K] = p$, con p primo, entonces no existe ningún cuerpo M tal que $M \neq K'$, $M \neq K$ y $K \subset M \subset K'$.

3. Pruebe que $[K' : K] = 1$ si y sólo si $K' = K$.

4. Sean $K_0, K_1, \ldots, K_r$ cuerpos tales que $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$. Pruebe que $[K_r : K_0] = [K_r : K_{r-1}][K_{r-1} : K_{r-2}] \cdots [K_1 : K_0]$.

5. *a*) Sea $\mathcal{A}(\mathbb{Q})$ el conjunto de los números algebraicos. Usando la Proposición 3.22, pruebe que $\mathcal{A}(\mathbb{Q})$ es un cuerpo.

   b) Use el criterio de Eisenstein para probar que $\forall\, N \in \mathbb{N}$ existe un polinomio irreducible sobre $\mathbb{Q}$, de grado m, donde $m > N$. Concluya que $[A(\mathbb{Q}) : \mathbb{Q}] = \infty$.

   c) Un cuerpo K es algebraicamente cerrado si toda extensión algebraica de K coincide con K. Pruebe que $\mathcal{A}(\mathbb{Q})$ es algebraicamente cerrado, asumiendo que $\mathbb{C}$ lo es.

6. Sea $K' : K$ una extensión finita y sea $p(x) \in K[x]$ un polinomio irreducible sobre K. Muestre que si $gr(p(x)) = m$, $[K' : K] = n$ y $(m, n) = 1$, entonces $p(x)$ no tiene raíces en K'.

7. Pruebe que si $[K' : K] = p$ y p es primo, entonces K' es una extensión simple de K.

3.2.1. Construcciones con Regla y Compás

Entre los más famosos problemas planteados por los griegos de la Antigüedad están tres construcciones geométricas, a realizarse usando sólo una regla sin marcas para medir y un compás:

- La duplicación del cubo: a partir de un cubo dado, de volumen V, construir un cubo de volumen $2V$.
- La trisección del ángulo: dado un ángulo cualquiera de medida α, construir otro ángulo de medida $\alpha/3$.
- La cuadratura del círculo: dado un círculo de área A, construir un cuadrado de área A.

El requerimiento de usar sólo la regla y el compás para realizar estas construcciones, está asociado a la visión que tenía Platón de la recta y el círculo: estas dos eran las únicas figuras "perfectas."

Muchas construcciones geométricas son realizables con regla y compás: segmentos de rectas pueden ser divididos en cualquier número de segmentos de igual medida; se pueden trazar paralelas a una recta dada; se puede trazar la bisectriz de un ángulo dado; se puede construir un cuadrado de igual área que la de un polígono cualquiera dado.

En la búsqueda de una construcción con regla y compás que resolviera los tres problemas mencionados arriba, los griegos invirtieron todo su ingenio y esfuerzo, sin alcanzarla nunca, aunque, como suele suceder en estos casos, otros hallazgos se obtuvieron en el camino de esa búsqueda. Por ejemplo, Arquímedes llegó a aproximar a π con un error menor que 10^{-2}, notable logro, para los recursos disponibles en la época.

Por casi 20 siglos, matemáticos profesionales y aficionados intentaron resolver la cuadratura del círculo, la trisección del ángulo y la duplicación del cubo, sin éxito. Sólo en el s. XIX surge la herramienta algebraica que permite obtener la prueba de la imposibilidad de tales construcciones. De hecho, en el año 1837, el excéntrico y hoy poco conocido matemático francés Pierre Wantzel (1814-1848) probó algebraicamente la imposibilidad de la construcción con regla y compás del ángulo $\pi/9$ a partir de $\pi/3$.

La técnica empleada para probar la imposibilidad de las construcciones mencionadas incluye la formulación de las mismas en términos de la Geometría Analítica, y el uso de la teoría de las extensiones de cuerpos.

Comenzaremos por formalizar la idea de la construcción con regla y compás.

Supongamos que un subconjunto M de puntos del plano cartesiano, es dado.

Consideremos los siguientes tipos de trazados en el plano, a partir de los puntos de M :

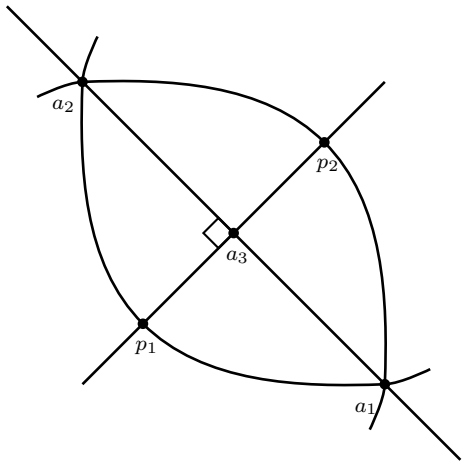
1. El trazado de una línea recta que pase por dos puntos de M.

2. El trazado de una circunferencia, cuyo centro es un punto de M y cuyo radio es igual a la distancia entre algún par de puntos de M.

Definición 3.23 *Un punto P del plano es construible en un paso a partir de M si P es la intersección de cualesquiera dos de las rectas o circunferencias trazadas como en 1 y 2.*

Un punto $P \in \mathbb{R}^2$ es construible a partir de M si existe una sucesión finita $P_1, \ldots, P_n = P$ de puntos en $\mathbb{R}^2$ tal que para cada $i \in \{1, \ldots, n\}$, el punto P_i es construible en un paso a partir del conjunto $M \cup \{P_1, \ldots, P_{i-1}\}$.

Ejemplo 3.13 *Ilustremos la idea anterior, a través de la construcción con regla y compás del punto medio de un segmento p_1p_2, donde p_1, $p_2 \in \mathbb{R}^2$ son puntos dados, como en la figura siguiente.*



Sea $M = \{p_1, p_2\}$
Paso 1: Trazado de la recta que pasa por p_1 y p_2.
Paso 2: Trazado de la circunferencia con centro p_1 y radio $\overline{p_1p_2}$.

Paso 3: Trazado de la circunferencia con centro p_2 y radio $\overline{p_1p_2}$.

Paso 4: Si a_1, a_2 son los puntos de intersección de las circunferencias trazadas en los pasos 2 y 3, se traza ahora la recta que pasa por a_1 y a_2. Sea a_3 el punto de intersección de la rectas trazadas en los pasos 1 y 4.

La existencia de la sucesión a_1, a_2, a_3 nos permite afirmar que el punto a_3 es construible a partir de M, pues a_1 y a_2 son construibles en un paso a partir de M y a_3 es construible en un paso a partir de $M \cup \{a_1, a_2\}$.

Con el fin de utilizar la teoría de extensiones de cuerpos en el contexto de las construcciones con regla y compás, sea $P_0 \subset \mathbb{R}^2$ y consideremos el subcuerpo $K_0 \subseteq \mathbb{R}$ generado por las coordenadas de cada punto en P_0.
Si $P_0 = \{(a_1, b_1), \ldots, (a_s, b_s)\}$, por ejemplo, entonces

$$K_0 = \mathbb{Q}(a_1, \ldots, a_s, b_1, \ldots, b_s).$$

Supongamos que construimos el punto $p_1 = (x_1, y_1)$ en un paso a partir de P_0.

Sea $K_1 = K_0(x_1, y_1)$, es decir, K_1 es el subcuerpo de $\mathbb{R}$ generado por las coordenadas de los puntos de P_0 y por $\{x_1, y_1\}$.

Recursivamente, definimos $K_i = K_{i-1}(x_i, y_i)$, donde $p_i = (x_i, y_i) \in \mathbb{R}^2$ es un punto construido en un paso a partir de $P_0 \cup \{p_1, \ldots, p_{i-1}\}$.

Si $Q = (s, t)$ es construible a partir de P_0, a través de la sucesión de puntos $\{p_1, \ldots, p_m\}$, entonces asociamos a Q el cuerpo $K = K_{m+1} = K_m(x_{m+1}, y_{m+1})$ con $x_{m+1} = s,\ y_{m+1} = t$ y se obtiene una cadena de extensiones de K_0 :

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{m+1} \subseteq \mathbb{R}.$$

La extensión $K_{m+1} : K_0$ corresponde, algebraicamente, a la construcción geométrica de $Q(s, t)$ a partir de P_0.

Veremos a continuación que las extensiones asociadas a construcciones de puntos del plano con regla y compás, son algebraicas, finitas y más aún, de grado igual a una potencia de 2.

Este hecho es el que permite determinar que ciertas construcciones son imposibles de realizar con regla y compás.

Lema 3.24 *Sea $K_0 \subset \mathbb{R}$, K_0 el subcuerpo generado por las coordenadas x, y de los puntos de un subconjunto M de $\mathbb{R}^2$. Si $P_1 \in \mathbb{R}^2$ es un punto construible en un paso a partir de M y $P_1 = (x_1, y_1)$, entonces x_1, y_1 son raíces en $K_0(x_1, y_1)$ de ecuaciones lineales ó cuadráticas con coeficientes en K_0.*

Prueba Si el punto (x_1, y_1) es construible a partir de M, entonces (x_1, y_1) se obtiene de alguna de las siguientes maneras:

1. Como intersección de dos rectas que pasan por puntos de M.

2. Como intersección de una recta que pasa por puntos de M con una circunferencia de centro $c = (q_1, q_2)$ y radio r, donde q_1 y q_2 están en K_0 y $r^2 \in K_0$, pues r es la distancia entre dos puntos de M. (Si (a, b), (c, d) son tales puntos, entonces $r = \sqrt{(a-c)^2 + (c-d)^2}$; como $a, b, c, d \in K_0$, se tiene que $r^2 \in K_0$).

3. Como intersección de dos circunferencias que cumplen las condiciones del caso 2.

   Si (x_1, y_1) se obtiene como en el caso 1, existen puntos $R = (r_1, r_2)$, $S = (s_1, s_2)$, $T = (t_1, t_2)$, $U = (u_1, u_2) \in M$ tales que las rectas de ecuaciones

   $$\frac{y - r_2}{x - r_1} = \frac{s_2 - r_2}{s_1 - r_1} \qquad (1)$$

   y

   $$\frac{y - t_2}{x - t_1} = \frac{u_2 - t_2}{u_1 - t_1} \qquad (2)$$

   respectivamente, se intersectan en (x_1, y_1).

   Es claro que x_1, y_1 se obtienen como soluciones del sistema de ecuaciones lineales (1) y (2), y por lo tanto son soluciones de ecuaciones lineales con coefientes en K_0, puesto que $r_i, s_i, t_i, u_i \in K_0$, para $i = 1, 2$.

   Si (x_1, y_1) se obtiene como en el caso 2, sea $C = (q_1, q_2) \in M$ el centro de la circunferencia de radio r, que intersecta a la recta l en el punto (x_1, y_1), donde l pasa por los puntos (m_1, m_2), $(n_1, n_2) \in M$.

   Dado que la ecuación de la circunferencia es

   $$(x - q_1)^2 + (y - q_2)^2 = r^2$$

   y la de la recta l es

   $$\frac{y - m_2}{x - m_1} = \frac{n_2 - m_2}{n_1 - m_1},$$

obtenemos que x_1 es solución de la ecuación

$$(x-q_1)^2+\left[\left[(x-m_1)\left(\frac{n_2-m_2}{n_1-m_1}\right)+m_2\right]-q_2\right]^2=r^2$$

la cual es una ecuación cuadrática con coefientes en K_0. Análogamente, se obtiene que lo mismo vale para y.

Si (x_1, y_1) se obtiene como en el caso 3), procediendo de manera similar, es fácil ver que x_1 y y_1 son soluciones de ecuaciones cuadráticas con coefientes en K_0. ■

Teorema 3.25 *Si el punto $p=(x,y)$ es construible a partir de un subconjunto M de $\mathbb{R}^2$ y si K_0 es el subcuerpo de $\mathbb{R}$ generado por las coordenadas de los puntos de M, entonces los grados*

$$[K_0(x):K_0] \qquad y \qquad [K_0(y):K_0]$$

son potencias de 2.

Prueba Supongamos que $p=(x,y)$ es construible a partir de M, a través de la sucesión $p_1=(x_1,y_1),\ldots,p_r=(x_r,y_r)=(x,y)$ y que $K_i=K_{i-1}(x_i,y_i)$, para $i=1,\ldots,r$. Por el Lema 3.24, se tiene que, para $i=1,\ldots,r$,

$$[K_{i-1}(x_i):K_{i-1}]=1 \quad \text{ó} \quad 2$$

y

$$[K_{i-1}(y_i):K_{i-1}]=1 \quad \text{ó} \quad 2$$

Por lo tanto, por el Teorema 3.18,

$$[K_{i-1}(x_i,y_i):K_{i-1}]=[K_{i-1}(x_i,y_i):K_{i-1}(x_i)][K_{i-1}(x_i):K_{i-1}]=2^n$$

donde n puede tomar valores en el conjunto $\{0,1,2\}$. Luego, $[K_i:K_{i-1}]$ es una potencia de 2, para $i=1,\ldots,r$.

Usando el resultado del ejercicio 4 de la sección anterior, obtenemos que $[K_r:K_0]$ es una potencia de 2.

Como $[K_r:K_0]=[K_r:K_0(x)][K_0(x):K_0]$ resulta que $[K_0(x):K_0]$ es una potencia de dos. Por un argumento similar, se obtiene que $[K_0(y):K_0]$ es una potencia de 2 ■

Corolario 3.26 *Un cubo dado no puede duplicarse a través de una construcción con regla y compás.*

Prueba Supongamos que un cubo es dado, y sin pérdida de generalidad, podemos suponer que una arista del mismo es el segmento OA, donde $O = (0, 0)$ y $A = (1, 0)$. Si se puede construir con regla y compás, a partir de O y A, un cubo con el doble del volumen que el volumen del cubo dado (que es igual a 1), entonces se puede construir el punto $r = (a, 0)$, donde $a^3 = 2$. El subcuerpo de $\mathbb{R}$ generado por $\{0, 1\}$ es $\mathbb{Q}$, y por el teorema 3.25, $[\mathbb{Q}(a) : \mathbb{Q}]$ debe ser una potencia de 2.

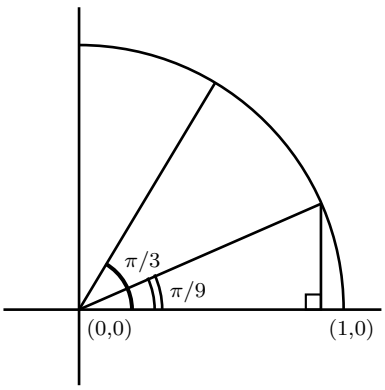
Ahora bien, el polinomio $p(x) = x^3 - 2$ es irreducible sobre $\mathbb{Q}$, por el criterio de Eisenstein; como a es raíz de $p(x)$, se tiene que $p(x)$ es el polinomio mínimo de a sobre $\mathbb{Q}$, y por lo tanto $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.

Esta contradicción implica que el punto $(a, 0)$ no puede construirse con regla y compás a partir de O y A, y por lo tanto el cubo dado no puede duplicarse a través de una construcción con regla y compás. ■

Corolario 3.27 *El ángulo de medida $\frac{\pi}{3}$ no puede ser trisecado a través de construcciones con regla y compás.*

Prueba

Consideremos el ángulo α de medida $\frac{\pi}{3}$, ubicado en el plano cartesiano, como en la figura siguiente:



Sea $a = cos(\frac{\pi}{9})$; la construcción del ángulo $\frac{\pi}{9}$ a partir de α, equivale a la construcción del punto $(a, 0)$ a partir de $(0, 0)$ y $(1, 0)$.

Supongamos que es posible construir $(a, 0)$ con regla y compás. En ese caso, podríamos construir también $(b, 0)$, donde $b = 2cos\frac{\pi}{9}$.

De las identidades trigonométricas relativas al seno y el coseno del ángulo suma y el ángulo doble, se obtiene que , $\forall\beta$,

$$4cos^3\beta - 3cos\beta = cos3\beta$$

Para $\beta = \frac{\pi}{9}$, obtenemos: $\frac{1}{2} = \frac{b^3}{2} - \frac{3b}{2}$, es decir, $b^3 - 3b - 1 = 0$.

En otras palabras, b es raíz del polinomio $q(x) = x^3 - 3x - 1$; pero $q(x)$ es irreducible sobre $\mathbb{Q}$, lo cual se comprueba usando el criterio de Eisenstein para ver que $q(x + 1) = x^3 - 3x - 3$ es irreducible sobre $\mathbb{Q}$. Como $q(x)$ es el polinomio mínimo de b sobre $\mathbb{Q}$, resulta que $[\mathbb{Q}(b) : \mathbb{Q}] = 3$. Hemos llegado a una contradicción, puesto que $[\mathbb{Q}(b) : \mathbb{Q}]$ debería ser una potencia de 2 ■

Corolario 3.28 *La construcción de un cuadrado de igual área a la de un círculo dado, no puede realizarse con regla y compás.*

Prueba

Consideremos la circunferencia de radio 1 y centro en el origen de coordenadas del plano cartesiano; el área del círculo encerrado por dicha circunferencia es igual a π. La construcción, con regla y compás, de un cuadrado de área igual a π equivale a la construcción del punto $(\sqrt{\pi}, 0)$, a partir de los puntos $(0, 0)$ y $(1, 0)$.

Esto último implica que $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] < \infty$ y como $\pi \in \mathbb{Q}(\sqrt{\pi})$, se tiene que $\mathbb{Q}(\pi) \subset \mathbb{Q}(\sqrt{\pi})$ y por lo tanto, $[\mathbb{Q}(\pi) : \mathbb{Q}] < \infty$; pero esto es imposible, puesto que π es trascendente sobre $\mathbb{Q}$.

Así, no es posible la cuadratura del círculo usando construcciones con regla y compás ■

Bibliografía

[1] I. N. Herstein, *Álgebra Moderna*, Editorial Trillas, México, 1974.

[2] J. Klein, *Greek Mathematical Thought and the Origin of Algebra*, MIT Press, Boston, 1976.

[3] J. E. Maxfield and M. W. Maxfield, *Abstract algebra and solution by radicals*, Dover, New York, 1992.

[4] I. Stewart, *Galois Theory*, Chapman and Hall, New York, 1987.