Hernández Magdaleno | Castillo Ramírez

Álgebra moderna

Anillos y campos

EDITORIAL UNIVERSITARIA

Centro Universitario de Ciencias Exactas e Ingenierías

Universidad de Guadalajara

Índice

Índice alfabético 214

Prefacio

Aunque en ocasiones parezca difícil decir con precisión en qué consiste el trabajo de un matemático, no es tan complicado decir en qué *no* consiste. Uno de estos contraejemplos es la solución de ejercicios repetitivos y mecánicos. La capacidad de resolver una tarea con cien integrales no es una característica que define a un buen matemático. Si bien es cierto que es conveniente que el estudiante sepa resolver integrales por distintos métodos y tenga familiaridad en su manipulación algebraica, esto no debe ser el objetivo principal de un curso de cálculo.

Sin importar si se trata de un matemático puro o aplicado, una habilidad mucho más importante que la mencionada es la habilidad de comprender conceptos abstractos y demostrar teoremas. En la licenciatura en matemáticas de la Universidad de Guadalajara, lamentablemente, es común oír a los estudiantes decir que no les gusta o no saben demostrar. Es necesario romper con el prejuicio de que ser un buen demostrador de teoremas está reservado a algún tipo especial de matemático.

Los principales objetos matemáticos que estudia el álgebra moderna son las estructuras algebraicas. En general, una estructura algebraica consiste en un conjunto (no vacío), junto con una o más operaciones definidas sobre él, las cuales deben satisfacer ciertas propiedades. Estas propiedades pueden variar de una estructura algebraica a otra, y pueden referirse a la existencia de elementos especiales o describir el comportamiento cuando se mezclan las mismas operaciones de la estructura. Algunos ejemplos clásicos de estas propiedades son la propiedad asociativa, la propiedad distributiva y la propiedad de la existencia de un elemento identidad. Es muy probable que el lector tenga familiaridad con algunas estructuras algebraicas, como los grupos y los espacios vectoriales.

Este texto está dividido en dos partes principales: anillos y campos. La primera parte, sobre anillos, consta de ocho capítulos. En los primeros dos se definen varios tipos de anillos, como los dominios enteros, y se abordan conceptos básicos relacionados con los anillos. En los capítulos 3, 4 y 5 se desarrolla parte de la teoría elemental de los anillos, tratando temas como los ideales, los anillos cociente y los homomorfismos. En los capítulos 6 y 7 se presenta un anillo de particular importancia: el anillo de polinomios, el cual será fundamental para el desarrollo posterior del texto. Finalmente, en el capítulo 8 se estudian tres tipos de dominios enteros especiales: los dominios de ideales principales, los dominios de factorización única y los dominios euclidianos.

La segunda parte, sobre campos, consta de cinco capítulos. En

los capítulos 9, 10 y 11 se desarrolla la teoría de campos clásica, con enfoque principalmente en las extensiones de campos. Los últimos dos capítulos, el 12 sobre campos finitos y el 13 sobre teoría de Galois, están escritos de tal forma que sean independientes uno del otro y cualquiera de los dos es una buena culminación para un curso de álgebra moderna.

Cada capítulo incluye ejercicios para reafirmar los contenidos estudiados o para introducir nuevos temas. Los ejercicios están diseñados para que cualquier estudiante suficientemente dedicado pueda resolverlos. Al final se incluyen las respuestas de algunos ejercicios. Además, el "Apéndice E" es una guía rápida con algunas de las técnicas de demostración estándar más utilizadas. El lector encontrará útil consultarla antes de resolver los ejercicios de cada capítulo.

Este texto fue realizado para el segundo curso de álgebra de la Universidad de Guadalajara. Aunque está escrito de tal manera que no sean necesarios muchos conceptos preliminares, se asume que el lector conoce la definición y está familiarizado hasta cierto punto, con los siguientes conceptos: relación de equivalencia, clase de equivalencia, partición de un conjunto, función inyectiva, sobreyectiva y biyectiva, y el principio de inducción matemática. Una buena revisión de este material puede encontrarse en el capítulo 0 del libro *Contemporary abstract algebra* de Joseph A. Gallian. Idealmente, el estudiante debió haber llevado un primer curso de álgebra que abarque por lo menos temas como subgrupos normales, grupos cociente, el teorema de Lagrange y homomorfismos de grupos. La ventaja de esto es que el estudiante tendrá mayor familiaridad con conceptos similares que se presentan en la teoría de anillos. Sin embargo, durante este curso prácticamente no se asumirá mayor conocimiento de teoría de grupos fuera de las definiciones elementales, las cuales se abordan en el "Apéndice B". La segunda parte del texto requiere ciertos conocimientos sobre espacios vectoriales, los cuales se estudian en el "Apéndice C". También recomendamos que el lector se familiarice con los conceptos de teoría de números elemental del "Apéndice A" antes de comenzar la primera parte del texto.

Por supuesto, también es necesario que el lector conozca las herramientas lógicas y de teoría de conjuntos básicas. Estas herramientas constituyen no sólo la base del álgebra abstracta, sino la base de toda la matemática moderna. Puede consultarse, por ejemplo, la sección 0 del libro *A first course in abstract algebra* de John B. Fraleigh para un repaso de teoría de conjuntos.

Parte I

Anillos

Si las personas no creen que las matemáticas son simples, es sólo porque no se dan cuenta de lo complicada que es la vida.

John von Neumann, matemático estadounidense

1

Propiedades básicas de los anillos

Las matemáticas puras son, en cierta forma,
la poesía de las ideas lógicas.

Albert Einstein, físico alemán

1.1 Anillos

Antes de comenzar este capítulo es recomendable que el lector esté familiarizado con los conceptos básicos de teoría de números y teoría de grupos, tratados en los apéndices A y B respectivamente.

Un anillo es una estructura algebraica con dos operaciones que satisfacen ciertas propiedades. El concepto surgió para generalizar las propiedades algebraicas de los números enteros. El término "anillo" fue utilizado por primera vez por el matemático alemán David Hilbert en 1892, aunque Richard Dedekind ya había trabajado con este tipo de estructura algebraica algunos años antes.

Definición 1.1 (anillo). Un anillo es una tríada $(R, +, \cdot)$ en la cual R es un conjunto no vacío, $+$ es una operación binaria llamada suma, y $\cdot$ es una operación binaria llamada multiplicación. Además deben satisfacerse las siguientes propiedades para cualquier $a, b, c \in R$:

1) *Conmutatividad de la suma.* $a + b = b + a$.
2) *Asociatividad de la suma.* $(a + b) + c = a + (b + c)$.
3) *Identidad aditiva.* Existe un elemento $0 \in R$ tal que $a + 0 = a$ para toda $a \in R$.
4) *Inversos aditivos.* Para toda $a \in R$ existe un $(-a) \in R$ tal que $a + (-a) = 0$.
5) *Asociatividad de la multiplicación.* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6) *Leyes distributivas.* $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$.

Observación 1.2. Las operaciones suma y multiplicación de un anillo cualquiera $(R, +, \cdot)$ no necesariamente deben ser la suma y multiplicación usual de números, ya que, de hecho, el conjunto R puede no contener números. Así pues, los nombres "suma" y "multiplicación" son nombres formales que se asignan a las operaciones binarias que cumplen las propiedades $1) - 6)$ de la definición 1.1.

Notación 1.3. Escribiremos R en lugar de $(R, +, \cdot)$ para denotar un anillo, siempre que la suma y la multiplicación en R estén claramente definidas. Si $a, b \in R$, escribiremos ab en lugar de $a \cdot b$. También denotaremos como $a - b$ al elemento $a + (-b)$.

En la práctica, para demostrar que un conjunto R es un anillo es necesario verificar también que las funciones $+ : R \times R \longrightarrow R$ y

$\cdot : R \times R \longrightarrow R$ son verdaderamente operaciones binarias (véase definición B.1). Esto implica verificar que se cumplen las propiedades de cerradura; es decir, que $a + b \in R$ y $ab \in R$ para toda $a, b \in R$. Además, debe verificarse que las operaciones están bien definidas en el sentido de que si $a = a'$ y $b = b'$ entonces $a + b = a' + b'$ y $ab = a'b'$. Esta última propiedad surge directamente de la definición de función y comprueba que, aunque se cambie la presentación de los elementos que se están operando, el resultado será el mismo. En la práctica, en casi todos los primeros ejemplos de anillos que estudiemos resultará obvio que las operaciones binarias están bien definidas (excepto el caso de $\mathbb{Z}_n$). Sin embargo, esto no será así cuando se estudie el capítulo 4, "Anillos cociente".

Observación 1.4. El par $(R, +)$ es un grupo abeliano (véase definición B.10).

Debe tenerse presente siempre que si R es un anillo, el conjunto R junto con la multiplicación no necesariamente es un grupo. Es decir, que en un anillo cualquiera, la existencia de la identidad multiplicativa y de los inversos multiplicativos no está garantizada.

Definición 1.5 (anillo con identidad). Un anillo R es un anillo con identidad si se cumple:

7) *Identidad multiplicativa.* Existe un elemento $1 \in R$, $1 \neq 0$, tal que $a1 = 1a = a$ para toda $a \in R$.

También es común llamar a la identidad multiplicativa *elemento unitario*. Sin embargo, llamarlo de esta forma puede causar ciertas confusiones debido a la siguiente definición de *elemento unidad*.

Definición 1.6 (unidad). Si R es un anillo con identidad, decimos que un elemento $a \in R$ es una unidad si existe un elemento $a^{-1} \in R$ tal que $aa^{-1} = a^{-1}a = 1$.

Las siguientes definiciones establecen dos tipos más de anillos.

Definición 1.7 (anillo con división). Un anillo con división R es un anillo con identidad en el cual todos sus elementos distintos de cero son unidades.

Definición 1.8 (anillo conmutativo). Un anillo R es un anillo conmutativo si se cumple:

8) *Conmutatividad de la multiplicación.* $ab = ba$ para toda $a, b \in R$.

Dado un anillo conmutativo R, si $a, b \in R$, $a \neq 0$, decimos que a divide a b, o que a es factor de b, y escribimos $a \mid b$ si existe un elemento $t \in R$ tal que $b = ta$.

Es sencillo verificar que si R es un anillo conmutativo con identidad el conjunto de unidades

$$R^* = \left\{ a \in R : \text{existe } a^{-1} \in R \text{ tal que } aa^{-1} = 1 \right\}$$

es un grupo abeliano con respecto a la multiplicación (*ejercicio 1.6.*). Antes de presentar algunos ejemplos enunciaremos una definición más.

Definición 1.9 (campo). Un campo F es un anillo conmutativo con división.

El campo es una de las estructuras algebraicas que tienen mayor número de propiedades. La parte II de este texto está totalmente dedicada al estudio de los campos.

Los siguientes ejemplos presentan los principales anillos y campos con los que se trabajará posteriormente.

Ejemplo 1.10 ($\mathbb{Z}$). El conjunto de los enteros $\mathbb{Z}$ junto con la suma y la multiplicación usuales forman un anillo conmutativo con identidad $1 \in \mathbb{Z}$. Las unidades de $\mathbb{Z}$ son 1 y -1.

Ejemplo 1.11 ($\mathbb{Z}_n$). Sea $n \in \mathbb{N}$. El conjunto de clases de equivalencia $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ de la relación módulo n (véase definición A.16) es un anillo conmutativo con identidad $[1]$. Si $[m]$ es una clase de $\mathbb{Z}_n$, entonces $[m]$ tiene la forma

$$[m] = \{m, m \pm n, m \pm 2n, \ldots\}$$

La suma y la multiplicación de clases se realizan sumando y multiplicando los respectivos representantes de cada clase; es decir, $[m] + [k] = [m + k]$ y $[m][k] = [mk]$. Para demostrar que estas operaciones están bien definidas, supongamos que $[m] = [m']$ y que $[k] = [k']$. Esto significa que $n \mid (m - m')$ y que $n \mid (k - k')$. Por el lema A.5,

$$n \mid (m - m') + (k - k') = (m + k) - (m' + k')$$

así que $[m + k] = [m' + k']$. De manera similar podemos demostrar que $[mk] = [m'k']$ (*ejercicio 1.1.*).

Ejemplo 1.12 ($\mathbb{Z}_n$). El grupo de unidades de $\mathbb{Z}_n$ es el conjunto de clases cuyo representante es primo relativo con n. Es decir,

$$\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n : mcd\,(a,n) = 1\}$$

Supongamos primero que $mcd\,(a,n) = 1$. Por el teorema A.10, $1 = as + nt$ para algunos $s,t \in \mathbb{Z}$. Luego, $n \mid nt = 1 - as$, así que $[1] = [as] = [a][s]$. Por lo tanto $[a] \in \mathbb{Z}_n^*$. Para demostrar el converso, supongamos que $[a] \in \mathbb{Z}_n^*$. Entonces existe $[b] \in \mathbb{Z}_n^*$ tal que $[ab] = [1]$ y $1 = ab + nk$ para algún $k \in \mathbb{Z}$. Si $d = mcd\,(a,n)$, $d \mid ab + nk = 1$, por el lema A.5. Por lo tanto $d = 1$.

Ejemplo 1.13 ($M_n\,(\mathbb{Z})$). El conjunto de matrices $M_n\,(\mathbb{Z})$ de $n \times n$ con entradas enteras es un anillo no conmutativo con identidad.

Ejemplo 1.14 ($R_1 \oplus R_2$). Sean R_1 y R_2 anillos. El conjunto

$$R = R_1 \oplus R_2 = \{(a_1, a_2) : a_1 \in R_1,\, a_2 \in R_2\}$$

junto con la suma y la multiplicación definidas como

$$\begin{aligned}(a_1,a_2) + (b_1,b_2) &= (a_1 + b_1, a_2 + b_2)\\ (a_1,a_2)\,(b_1,b_2) &= (a_1b_1, a_2b_2)\end{aligned}$$

forman un anillo llamado suma directa de R_1 y R_2.

Ejemplo 1.15 ($\mathbb{Z}\,[i]$). El conjunto de los enteros gaussianos

$$\mathbb{Z}\,[i] = \{a + bi : a,b \in \mathbb{Z}\}$$

es un anillo conmutativo con identidad (*ejercicio 1.2.*).

Ejemplo 1.16 ($\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$). El conjunto de los números complejos $\mathbb{C}$, los números reales $\mathbb{R}$ y los números racionales $\mathbb{Q}$ son todos campos.

Ejemplo 1.17 ($\mathbb{Q}\left(\sqrt{d}\right)$). El conjunto $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a,b \in \mathbb{Q}\right\}$ es un campo. Para comprobar esto primero observemos que $\mathbb{Q}\left(\sqrt{2}\right)$ es cerrado bajo la suma y la multiplicación usual: si $a_i, b_i \in \mathbb{Q}$, $i = 1,2$, entonces

$$\left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$$

$$\begin{aligned}\left(a_1 + b_1\sqrt{2}\right)\left(a_2 + b_2\sqrt{2}\right) &= \\ (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} &\in \mathbb{Q}\left(\sqrt{2}\right)\end{aligned}$$

Es sencillo verificar que se cumplen las demás propiedades de un anillo conmutativo con identidad. El inverso multiplicativo en $\mathbb{R}$ de $a + b\sqrt{2}$, con $a \neq 0$ o $b \neq 0$, es $1/\left(a + b\sqrt{2}\right)$. Para mostrar que $1/\left(a + b\sqrt{2}\right) \in \mathbb{Q}\left(\sqrt{2}\right)$ es necesario racionalizar el denominador:

$$\begin{aligned}\frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}}\frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]\end{aligned}$$

Por lo tanto, $\mathbb{Q}\left(\sqrt{2}\right)$ es un campo (de hecho, un subcampo de $\mathbb{R}$).

Otro ejemplo importante es el anillo de polinomios, pero trataremos este caso hasta el capítulo 6, "Anillos de polinomios". Los siguientes teoremas abordan algunas propiedades importantes de los anillos.

Teorema 1.18. Si R es un anillo, la identidad aditiva 0 es única. Además, los inversos aditivos son únicos.

Demostración. Supongamos que $0'$ es otra identidad aditiva de R, es decir que $a + 0' = a$ para toda $a \in R$. Elijamos $a = 0$. Así $0 + 0' = 0$. Por otro lado, como 0 es identidad aditiva tenemos que $0 + 0' = 0'$ y por lo tanto $0' = 0$.

Sea $a \in R$ y $-a$ su inverso aditivo. Supongamos que b es otro inverso aditivo de a. Entonces

$$-a + a = 0 = b + a$$

Sumando ambos lados en la igualdad anterior $-a$ obtenemos

$$\begin{aligned}-a + (a - a) &= b + (a - a) \\ -a + 0 &= b + 0 \\ -a &= b\end{aligned}$$

■

Teorema 1.19. Si R es un anillo con identidad, la identidad multiplicativa 1 es única. Además, si un elemento tiene inverso multiplicativo éste es único.

Demostración. La demostración es idéntica a la del teorema anterior. ■

Proposición 1.20. Sea R un anillo. Entonces $a0 = 0a = 0$ para toda $a \in R$.

Demostración. Observemos que

$$\begin{aligned} a0 + 0 &= a0 \\ &= a(0 + 0) \\ &= a0 + a0 \end{aligned}$$

Así que cancelando $a0$ obtenemos que $0 = a0$. De manera similar, se demuestra que $0a = 0$. ■

Proposición 1.21. Sea R un anillo. Entonces

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

para toda $a, b \in R$.

Demostración. Observemos que

$$\begin{aligned} a(b - b) &= a0 \\ &= 0 \end{aligned}$$

Entonces

$$\begin{aligned} ab + a(-b) &= 0 \\ a(-b) &= -(ab) \end{aligned}$$

De manera similar se demuestra que $(-a)b = -(ab)$. ■

1.2 Subanillos

Definición 1.22 (subanillo). Sea R un anillo. Decimos que un subconjunto S de R es un subanillo de R si S es en sí mismo un anillo bajo las operaciones de R.

Decimos que un subanillo S de R es propio si S es un subconjunto propio de R. El siguiente teorema proporciona la herramienta principal para demostrar que un subconjunto es un subanillo.

Teorema 1.23 (test del subanillo). Un subconjunto no vacío S de un anillo R es un subanillo si y sólo si para toda $a, b \in S$ se tiene que $a - b \in S$ y $ab \in S$.

Demostración. Obviamente si S es subanillo de R, la propiedad deseada se cumple. Supongamos ahora que para toda $a, b \in S$ se tiene que $a - b \in S$ y $ab \in S$. Debemos verificar que S cumple las propiedades de anillo. Es claro que las propiedades 1), 2), 5) y 6) de la definición de anillo se cumplen porque las operaciones en S son las mismas que en R. Debido a que S es no vacío, sabemos que existe por lo menos un $x \in S$. Debido a que $a - b \in S$ para toda $a, b \in S$, eligiendo $a = b = x$ obtenemos que $x - x = 0 \in S$. Esto verifica la propiedad 3). Ahora eligiendo $a = 0$ y $b = x$ obtenemos que $0 - x = -x \in S$. Esto verifica la propiedad 4). Finalmente, si $y \in S$, podemos elegir $a = y$ y $b = -x$ para obtener que $y - (-x) = y + x \in S$, lo cual verifica la cerradura. Observemos que la cerradura en la multiplicación está dada por hipótesis. ■

Ejemplo 1.24. Los conjuntos $\{0\}$ y R son subanillos de cualquier anillo R. El subanillo $\{0\}$ es llamado el subanillo trivial de R.

Ejemplo 1.25 ($M_n(\mathbb{Z})$). Demostraremos que el conjunto

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{Z} \right\}$$

es un subanillo de $M_2(\mathbb{Z})$. Claramente, S es un subconjunto no vacío. Sean

$$A = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \in S$$

$$B = \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \in S$$

Entonces,

$$\begin{aligned} A - B &= \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{bmatrix} \in S \end{aligned}$$

ya que $a_1 - a_2, b_1 - b_2 \in \mathbb{Z}$. También,

$$\begin{aligned} AB &= \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{bmatrix} \in S \end{aligned}$$

ya que $a_1a_2, b_1b_2 \in \mathbb{Z}$. Por lo tanto, por el test del subanillo, S es un subanillo.

1.3 Ejercicios

1.1. Demuestra que la multiplicación de clases de equivalencia en $\mathbb{Z}_n$ está bien definida.

1.2. Verifica que el conjunto

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

satisface todas las propiedades de un anillo conmutativo con identidad con respecto a la suma y multiplicación de números complejos.

1.3. Encuentra el grupo de unidades $\mathbb{Z}[i]^*$.

1.4. Demuestra que en cualquier anillo R se cumplen las siguientes propiedades para todo $a, b, c \in R$:

a) $(-a)(-b) = ab$.

b) $a(b - c) = ab - ac$.

c) $(-1)a = -a$ siempre que R sea un anillo con identidad.

1.5. Sea R un anillo. Demuestra que si $u \in R$ es una unidad, entonces $u \mid a$ para cualquier $a \in R$.

1.6. Demuestra que el conjunto de unidades de un anillo conmutativo con identidad es un grupo bajo la multiplicación.

1.7. Demuestra que si $n \in \mathbb{N}$, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$ es un subanillo de $\mathbb{Z}$. Además, demuestra que si $n \mid m \in \mathbb{N}$, entonces $m\mathbb{Z} \subseteq n\mathbb{Z}$.

1.8. Demuestra que el conjunto de funciones $R = \{f : \mathbb{R} \to \mathbb{R}\}$ es un anillo junto con las operaciones $(f + g)(x) = f(x) + g(x)$ y $(fg)(x) = f(x)g(x)$, $f, g \in R$. Además demuestra que $S = \{f \in R : f(0) = 0\}$ es un subanillo de R.

1.9. Sea R un anillo. Demuestra que

$$Z(R) = \{x \in R : xa = ax \text{ para toda } a \in R\}$$

es un subanillo de R. El conjunto $Z(R)$ es llamado el centro de R.

1.10. Sea R un anillo con identidad y a un elemento de R tal que $a^2 = 1$. Muestra que el conjunto

$$S = \{x \in R : x = ara \text{ para algún } r \in R\}$$

es un subanillo de R.

1.11. Un anillo R se dice que es un anillo booleano si $a^2 = a$ para toda $a \in R$. Demuestra que todo anillo booleano es conmutativo.

2

Dominios enteros

En la vida real, te aseguro que no hay tales cosas como álgebra.

Fran Lebowitz, escritora estadounidense

2.1 Propiedades

Como se dijo anteriormente, el concepto de anillo surgió para generalizar el concepto de los números enteros. Sin embargo, los enteros poseen una propiedad importante que no está incluida en la definición de anillo. Esta propiedad es la que define a un dominio entero. Se recomienda que al terminar este capítulo el lector profundice en el campo de los números complejos del apéndice D.

Definición 2.1 (dominio entero). Un dominio entero es un anillo conmutativo R con identidad que satisface la siguiente propiedad:

9) *Cancelación.* Para cualesquier $a, b, c \in R$, con $a \neq 0$, si $ab = ac$ entonces $b = c$.

Esta propiedad no implica la existencia de inversos multiplicativos. El converso, por otro lado, sí es verdad; es decir, la existencia de inversos multiplicativos implica la propiedad de cancelación, como lo muestra la siguiente proposición.

Proposición 2.2. Cualquier campo es un dominio entero.

Demostración. Si F es un campo, entonces para $a, b, c \in F$, $a \neq 0$,

$$\begin{aligned} ab &= ac \\ a^{-1}ab &= a^{-1}ac \\ 1b &= 1c \\ b &= c \end{aligned}$$

■

Ejemplo 2.3 ($\mathbb{Z}$). El anillo de los enteros $\mathbb{Z}$ es un dominio entero. Observemos que aunque cualquier entero distinto de 1 y -1 no tiene inverso multiplicativo, la propiedad de cancelación efectivamente se cumple.

Definición 2.4 (divisor de cero). Sea R un anillo. Decimos que $a \in R$, $a \neq 0$, es un divisor izquierdo de cero si existe un elemento $b \in R$, $b \neq 0$, tal que $ab = 0$.

Análogamente definimos los divisores derechos de cero. Si R es conmutativo, los divisores derechos e izquierdos son los mismos.

Ejemplo 2.5 ($\mathbb{Z}_n$). Consideremos el anillo $\mathbb{Z}_6$ de los enteros módulo 6. La clase $[3]$ es un divisor de cero porque $[3] \cdot [2] = [3 \cdot 2] = [6] = [0]$. Por la misma razón, $[2]$ es un divisor de cero.

La característica especial que hace que en los enteros se cumpla la cancelación es que no existen los divisores de cero. De hecho estas dos propiedades son equivalentes.

Teorema 2.6. El anillo conmutativo R con identidad es un dominio entero si y sólo si no tiene divisores de cero.

Demostración. Supongamos primero que R es un dominio entero. Sean $a, b \in R$ tales que $ab = 0$. Demostraremos que $a = 0$ o $b = 0$. La técnica estándar para demostrar una proposición disyuntiva, de la forma P es verdad o Q es verdad, consiste en negar P y demostrar que Q debe ser verdad. Siguiendo esto, supongamos que $a \neq 0$. Entonces $ab = 0 = a0$ y por cancelación obtenemos que $b = 0$. Por lo tanto, R no tiene divisores de cero.

Supongamos ahora que R es un anillo conmutativo con identidad que no tiene divisores de cero. Sean $a, b, c \in R$, $a \neq 0$, tales que $ab = ac$. Demostraremos que $b = c$, lo cual implica que la propiedad de cancelación se cumple. Observemos que

$$\begin{aligned} ab - ac &= 0 \\ a(b - c) &= 0 \end{aligned}$$

Como $a \neq 0$ y R no tiene divisores de cero, debemos concluir que

$$\begin{aligned} b - c &= 0 \\ b &= c \end{aligned}$$

Por lo tanto, R es un dominio entero. ■

En el siguiente ejemplo y el siguiente teorema usaremos varios conceptos del apéndice A: "Teoría de números elemental".

Ejemplo 2.7 ($\mathbb{Z}_p$). El anillo $\mathbb{Z}_p$, donde p es un primo, no tiene divisores de cero. Para comprobar esto, supongamos que $[a][b] = [0]$ para algunos $[a], [b] \in \mathbb{Z}_p$. Entonces $p \mid ab$. Sin embargo, por el lema A.13 de Euclides, tenemos que $p \mid a$ o $p \mid b$. Así $[a] = [0]$ o $[b] = [0]$.

Observación 2.8. Recordemos que para demostrar una proposición de la forma $P \longleftrightarrow Q$ debemos demostrar $P \rightarrow Q$ y $Q \rightarrow P$. En forma equivalente, en lugar de demostrar $P \rightarrow Q$, podemos demostrar que $(\sim Q) \rightarrow (\sim P)$, donde $\sim$ indica la negación del predicado. Utilizaremos esta técnica en la demostración del siguiente teorema.

Teorema 2.9. Sea $n \in \mathbb{N}$. Un elemento $[m] \in \mathbb{Z}_n$, $[m] \neq [0]$ es divisor de cero si y sólo si m no es primo relativo con n, es decir si $mcd\,(m,n) \neq 1$.

Demostración. Supongamos que m y n no son primos relativos y sea $d = mcd\,(m,n) \neq 1$. Por definición, $d \mid m$ y $d \mid n$, lo que implica que

$$m = dq_1 \tag{i}$$

y

$$n = dq_2 \tag{ii}$$

para algunos $q_1, q_2 \in \mathbb{Z}$. Demostraremos primero que $[q_2] \neq [0]$, es decir que $n \nmid q_2$. Observemos que si $n \mid q_2$,

$$q_2 = ns_1 \tag{iii}$$

para algún $s_1 \in \mathbb{Z}$, y sustituyendo la relación (iii) en (ii), obtenemos que $n = dns_1$ y $1 = ds_1$. Esto implica que $d = 1$, lo cual es una contradicción. Por lo tanto $[q_2] \neq [0]$. Ahora, multiplicando (i) por q_2 y sustituyendo (ii) obtenemos

$$\begin{aligned} q_2 m &= q_2 dq_1 \\ &= nq_1 \end{aligned}$$

Por lo tanto, $n \mid q_2 m$ y así $[q_2][m] = 0$. Esto implica que $[m]$ es un divisor de cero en $\mathbb{Z}_n$.

Supongamos ahora que m y n son primos relativos. Por reducción al absurdo, supongamos que $[m]$ es divisor de cero, así que $[m][s] = [0]$ para algún $s \in \mathbb{Z}_n$, $[s] \neq [0]$. Luego, $n \mid ms$. Por el lema A.13 de Euclides (forma alternativa), $n \mid s$, por lo que $[s] = [0]$. Esto es una contradicción, lo que implica que $[m]$ no es un divisor de cero. ■

Ejemplo 2.10. Por el teorema anterior, todos los divisores de cero en $\mathbb{Z}_6$ son $[2]$, $[3]$ y $[4]$.

El siguiente teorema es un resultado importante sobre los dominios enteros finitos.

Teorema 2.11 (dominio entero finito). Todo dominio entero finito es un campo.

Demostración. Sea $D = \{0, 1, a_1, a_2, \ldots, a_n\}$ un domino entero finito y $b \in D$, $b \neq 0$. Demostraremos que b es una unidad. Consideremos el siguiente conjunto de elementos en D:

$$L = \{b1, ba_1, ba_2, \ldots, ba_n\}$$

Es claro que todos los elementos de L son distintos, ya que si $ba_i = ba_j$ para algunos $i, j = 1, \ldots, n$, $i \neq j$, por cancelación tenemos que $a_i = a_j$. Además, ninguno de los elementos de L es 0 porque D no tiene divisores de cero. De esta forma tenemos que $L = D \setminus \{0\}$, lo que implica que $1 = b1$, o $1 = ba_i$ para alguna i. En el primer caso $b = 1$, lo que implica que b es una unidad, y en el segundo a_i es el inverso multiplicativo de b, por lo que b es una unidad. ■

Corolario 2.12. El anillo $\mathbb{Z}_n$ es un campo si y sólo si n es primo.

Demostración. Si $n = p$ es primo, por el *ejemplo 2.7* sabemos que $\mathbb{Z}_p$ no tiene divisores de cero y por lo tanto es un dominio entero. Así que por el teorema 2.11, $\mathbb{Z}_p$ es un campo.

Supongamos ahora que n no es primo. Entonces $n = st$ para algunos $s, t \in \mathbb{Z}$, $0 < s, t < n$. Así $[s][t] = [0]$, con $[s] \neq [0]$ y $[t] \neq [0]$, lo que muestra que s y t son divisores de cero en $\mathbb{Z}_n$. Por lo tanto $\mathbb{Z}_n$ no puede ser un campo. ■

2.2 Elementos irreducibles y primos en un dominio entero

Para el caso de los dominios enteros existen algunas definiciones particulares relacionadas con la divisibilidad de sus elementos.

Definición 2.13 (asociados). Sea D un dominio entero. Dos elementos $a, b \in D$ se llaman asociados si $a = ub$, donde $u \in D$ es una unidad.

Definición 2.14 (irreducible). Sea $a \neq 0$ un elemento de un dominio entero D que no es una unidad. Decimos que a es un elemento irreducible en D si siempre que lo factorizamos de la forma $a = bc$ para algunos $b, c \in D$, tenemos que b o c es una unidad.

Definición 2.15 (elemento primo). Sea $a \neq 0$ un elemento de un dominio entero D que no es una unidad. Decimos que a es un elemento primo en D si siempre que $a \mid bc$ para algunos $b, c \in D$, tenemos que $a \mid b$ o $a \mid c$.

Ejemplo 2.16 ($\mathbb{Z}$). En $\mathbb{Z}$, los números primos son irreducibles por definición. Además, los números primos también son elementos primos por el lema A.13 de Euclides. Observemos también que para cualquier $a \in \mathbb{Z}$, a es asociado de a y de $-a$.

Teorema 2.17. En cualquier dominio entero D, si $a \in D$ es un elemento primo, entonces a es irreducible.

Demostración. Supongamos que $a = bc$, $b, c \in D$. Debemos demostrar que b o c es una unidad. Como $a \mid bc$, por definición de elemento primo sabemos que $a \mid b$ o $a \mid c$. Supongamos que $a \mid b$, es decir, $b = ad$ para algún $d \in D$. Entonces

$$b1 = b = ad = (bc)\, d = b\,(cd)$$

Así que $1 = cd$ por cancelación. Por lo tanto, c es una unidad. En forma análoga demostramos que si $a \mid c$, b es una unidad. ■

A simple vista podría parecer que en cualquier dominio entero los elementos primos e irreducibles siempre coincidirán. Es decir, ¿existen dominios enteros en los cuales haya elementos irreducibles que no sean primos? Sí existen este tipo de dominios enteros; un ejemplo es

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\}$$

donde $d \in \mathbb{Z}$ no es 1 y no es divisible por el cuadrado de un número primo. Para trabajar más cómodamente en este dominio entero, podemos definir una norma; esto es una función $N : \mathbb{Z}\left[\sqrt{d}\right] \longrightarrow \mathbb{N}_0$ de la siguiente forma:

$$N\left(a + b\sqrt{d}\right) = \left|a^2 - db^2\right|$$

Proposición 2.18. La función $N : \mathbb{Z}\left[\sqrt{d}\right] \longrightarrow \mathbb{N}_0$ definida arriba cumple las siguientes propiedades:

1) $N(x) = 0$ si y sólo si $x = 0$.
2) $N(xy) = N(x)\, N(y)$ para toda $x, y \in \mathbb{Z}\left[\sqrt{d}\right]$.
3) $N(x) = 1$ si y sólo si x es una unidad
4) Si $N(x)$ es un número primo entonces x es irreducible en $\mathbb{Z}\left[\sqrt{d}\right]$.

Demostración.

1) Si $x = 0$, claramente $N(x) = 0$. Si $N\left(a + b\sqrt{d}\right) = 0$, entonces $|a^2 - db^2| = 0$ y $a^2 = db^2$. Supongamos que $b \neq 0$. Esto implica que $a \neq 0$ porque $a^2 = db^2$. Luego $d = \frac{a^2}{b^2}$ es un entero distinto de 1. Descompongamos a y b en factores primos $a = p_1 \dots p_n$ y $b = q_1 \dots q_m$. Ahora

$$d = \frac{p_1^2 \dots p_n^2}{q_1^2 \dots q_m^2}$$

Al simplificar la fracción, los q_i^2s deben cancelarse con los p_i^2s porque $d \in \mathbb{Z}$, pero debe quedar al menos un p_k^2 sin cancelarse porque $d \neq 1$. Por lo tanto, $p_k^2 \mid d$, lo cual es una contradicción con la elección de d. Luego, $b = 0$ y $a = 0$.

2) *Ejercicio 2.8.*

3) Si $N\left(a + b\sqrt{d}\right) = 1$, entonces $|a^2 - db^2| = 1$ y $\pm 1 = a^2 - db^2 = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right)$, por lo que $\left(a + b\sqrt{d}\right)$ es una unidad. Si $x \in \mathbb{Z}\left[\sqrt{d}\right]$ es una unidad, $xy = 1$ para algún $y \in \mathbb{Z}\left[\sqrt{d}\right]$. Luego $1 = N(1) = N(xy) = N(x)N(y)$ por la parte 2) de esta proposición. Así $N(x) = 1 = N(y)$.

4) *Ejercicio 2.8.*

■

Ejemplo 2.19 ($\mathbb{Z}\left[\sqrt{d}\right]$). Consideremos el dominio entero $\mathbb{Z}[\sqrt{-3}]$. En este caso, $N(a + b\sqrt{-3}) = |a^2 + 3b^2|$. Demostraremos que el elemento $1 + \sqrt{-3}$ es irreducible pero no es primo. Supongamos que $1 + \sqrt{-3}$ no es irreducible, es decir que $1 + \sqrt{-3} = xy$ donde $x, y \in \mathbb{Z}[\sqrt{-3}]$ no son unidades. Entonces,

$$N(xy) = N(x)N(y) = N\left(1 + \sqrt{-3}\right) = 4$$

Por la propiedad 3) de la proposición anterior, $N(x) \neq 1$ y $N(y) \neq 1$, así que la única alternativa es que $N(x) = N(y) = 2$. Sin embargo esto es una contradicción, porque no existen $a, b \in \mathbb{Z}$ tales que

$$\left|a^2 + 3b^2\right| = 2$$

Así, $1 + \sqrt{-3}$ es irreducible.

Ahora, para mostrar que $1+\sqrt{-3}$ no es primo, observemos que

$$\left(1+\sqrt{-3}\right)\left(1-\sqrt{-3}\right) = 4 = 2 \cdot 2$$

De esta forma, $(1+\sqrt{-3}) \mid 2 \cdot 2$. Supongamos que $(1+\sqrt{-3})$ es primo. Entonces, la relación anterior implica que $(1+\sqrt{-3}) \mid 2$, es decir

$$\left(1+\sqrt{-3}\right)\left(a+b\sqrt{-3}\right) = 2$$

para algunos $a, b \in \mathbb{Z}$. Luego

$$(a-3b) + (a+b)\sqrt{-3} = 2$$

implica que $a-3b=2$ y $a+b=0$, lo cual es una contradicción ya que no hay números enteros que satisfagan ambas ecuaciones. Por lo tanto, $(1+\sqrt{-3})$ no es primo.

2.3 Característica de un anillo

Finalizaremos este capítulo presentando un concepto que no es exclusivo de los dominios enteros, sino que se aplica a cualquier anillo en general. Una aclaración con respecto a la notación: en un anillo R, para $a \in R$, $n \in \mathbb{N}$, $n > 0$, definimos $n \cdot a = a + \ldots + a$, donde hay n sumandos en el lado derecho de la igualdad anterior. Si $n < 0$, $n \cdot a = -a - a - \ldots - a$ donde hay n sumandos.

Definición 2.20 (característica). La característica de un anillo R es el menor entero positivo n tal que $n \cdot x = 0$ para toda $x \in R$. Si no existe tal entero, decimos que R tiene característica cero.

Si la característica de un anillo R es $n \in \mathbb{N}_0$ escribimos

$$char(R) = n.$$

Ejemplo 2.21 ($\mathbb{Z}$). La característica de $\mathbb{Z}$ es 0.

Ejemplo 2.22 ($\mathbb{Z}_n$). La característica de $\mathbb{Z}_n$ es n, ya que $n \cdot [x] = 0$ para toda $[x] \in \mathbb{Z}_n$ y n es el menor entero positivo con tal propiedad.

Teorema 2.23. Sea R un anillo con identidad 1. Si $n \cdot 1 \neq 0$ para toda $n \in \mathbb{N}$, entonces la característica de R es 0. Si $n \cdot 1 = 0$ para algún $n \in \mathbb{N}$ y además n es el menor entero positivo con tal propiedad, entonces la característica de R es n.

Demostración. Si $n \cdot 1 \neq 0$ para toda $n \in \mathbb{N}$, es claro que no existe un entero $m \in \mathbb{N}$ para el cual $m \cdot x = 0$ para toda $x \in R$ (ya que seguramente no se cumplirá con $x = 1$). Por lo tanto, la característica de R es 0.

Supongamos que $n \cdot 1 = 0$ para algún $n \in \mathbb{N}$, donde n es el menor entero positivo con tal propiedad. Entonces para cualquier $x \in R$

$$\begin{aligned} n \cdot x &= x + x + \ldots + x \\ &= 1x + 1x + \ldots + 1x \\ &= (1 + 1 + \ldots + 1)\, x \\ &= (n \cdot 1)\, x \\ &= 0x = 0 \end{aligned}$$

■

Proposición 2.24. Sea R un anillo con identidad tal que $char\,(R) = n \neq 0$. Si $m \cdot 1 = 0$ para algún $m \in \mathbb{N}$ entonces $n \mid m$.

Demostración. Por el algoritmo de la división (teorema A.6), existen $q, r \in \mathbb{Z}$ tales que

$$m = qn + r \text{ con } 0 \leq r < n$$

Si $r \neq 0$, entonces

$$\begin{aligned} 0 &= m \cdot 1 \\ &= (qn + r) \cdot 1 \\ &= q\,(n \cdot 1) + r \cdot 1 \\ &= q0 + r \cdot 1 \\ &= r \cdot 1 \end{aligned}$$

Lo que contradice que n es el menor entero positivo tal que $n \cdot 1 = 0$. Así $r = 0$, por lo que $n \mid m$. ■

Teorema 2.25. La característica de un dominio entero es 0 o un número primo.

Demostración. Sea D un dominio entero. Supongamos que D tiene característica $n \neq 0$, así que $n \cdot 1 = 0$. Supongamos que n no es primo. Entonces $n = st$, donde $1 < s, t < n$. Por el *ejercicio 2.6*,

$$0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)\,(t \cdot 1)$$

Como D es un dominio entero, debemos tener que $s \cdot 1 = 0$ o $t \cdot 1 = 0$. Esto contradice que n es el menor entero positivo con la propiedad $n \cdot 1 = 0$. Por lo tanto n es primo. ■

2.4 Ejercicios

2.1. Determina si los siguientes anillos son dominios enteros. Justifica tu respuesta.

a) El anillo de los enteros gaussianos

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

b) El anillo $M_2(\mathbb{Z})$ de matrices de 2×2 sobre $\mathbb{Z}$.

c) El anillo $\mathbb{Z} \oplus \mathbb{Z}$.

2.2. Sea U el conjunto de todos los anillos. Realiza un diagrama de Venn en el que se muestren los siguientes subconjuntos de U: anillos conmutativos, anillos con identidad, dominios enteros y campos. Da un ejemplo de anillo de cada sección del diagrama.

2.3. Encuentra todas las unidades y todos los divisores de cero de $\mathbb{Z}_7$ y de $\mathbb{Z}_{12}$.

2.4. Sea R un anillo finito conmutativo con identidad. Demuestra que cualquier elemento de R distinto de cero es una unidad o un divisor de cero. Sugerencia: usa un argumento similar al usado en el teorema 2.11 del dominio entero finito.

2.5. Encuentra la característica de los siguientes anillos: $4\mathbb{Z}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_4$, $\mathbb{Z}_3 \oplus 3\mathbb{Z}$ y $\mathbb{Z}_6 \oplus \mathbb{Z}_{15}$.

2.6. Sea R un anillo. Si $m, n \in \mathbb{N}$ y $a, b \in R$, muestra que $m \cdot (ab) = (m \cdot a)\, b = a\,(m \cdot b)$ y que $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$.

2.7. Sea D un dominio entero. Muestra que el conjunto

$$S = \{n \cdot 1 : n \in \mathbb{Z}\}$$

es un subdominio entero de D. Muestra además que S está contenido en cualquier otro subdominio entero de D.

2.8. Demuestra que si $N : \mathbb{Z}\left[\sqrt{d}\right] \longrightarrow \mathbb{N}_0$ es una función definida por $N\left(a + b\sqrt{d}\right) = |a^2 - db^2|$ entonces:

a) $N(xy) = N(x)\,N(y)$ para toda $x, y \in \mathbb{Z}\left[\sqrt{d}\right]$.

b) Si $N(x)$ es un número primo, entonces x es irreducible en $\mathbb{Z}\left[\sqrt{d}\right]$. Sugerencia: usa el hecho de que $N(x) = 1$ si y sólo si x es una unidad.

2.9. Sea D un dominio entero y sean $a, b \in D$. Demuestra que la relación $a \sim b$, que significa "a es asociado de b", es una relación de equivalencia.

2.10. Sea R un anillo (no necesariamente conmutativo) que contiene por lo menos dos elementos. Supongamos que para cada $a \in R$, $a \neq 0$ existe un único $b \in R$ tal que $aba = a$. Demuestra que R no tiene divisores de cero.

2.11. Muestra que la matriz $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ con $a, b \in \mathbb{Z}_3$, forman un campo de nueve elementos, y que el grupo multiplicativo de este campo es cíclico, de orden 8.

3
Ideales

Matemáticas es la única ciencia donde uno nunca sabe de lo que está hablando y menos si lo que dice es cierto.

Bertrand Russell, matemático y filósofo británico

La subestructura más importante de un anillo es un ideal. Además de que permiten la construcción de anillos cociente, los ideales son fundamentales en muchas áreas de las matemáticas modernas como la teoría de números algebraicos y la geometría algebraica. Informalmente, podemos decir que un ideal es un subanillo que "absorbe" la multiplicación.

Definición 3.1 (ideal). Un subanillo I de un anillo R se llama ideal de R si para toda $r \in R$ y $a \in I$ se tiene que $ra, ar \in I$.

Obviamente, si R es un anillo conmutativo, un ideal I sólo debe cumplir que $ra \in I$ para cualquier $a \in I$, $r \in R$. Decimos que I es un ideal propio de R si I es un subconjunto propio de R (es decir, $I \subsetneq R$). El siguiente teorema es una consecuencia directa del test del subanillo (teorema 1.23).

Teorema 3.2 (test del ideal). Un subconjunto no vacío I de un anillo R es un ideal de R si para toda $a, b \in I, r \in R$, tenemos que $a-b \in I$ y $ar, ra \in I$.

Ejemplo 3.3. Para cualquier anillo R, los conjuntos $\{0\}$ y R son ideales de R.

Ejemplo 3.4 ($\mathbb{Z}$). Para cualquier $n \in \mathbb{N}$ el conjunto

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$$

es un ideal de $\mathbb{Z}$. Para verificar que cumple la propiedad de los ideales observemos los elementos de $n\mathbb{Z}$ que tienen la forma nt donde $t \in \mathbb{Z}$. De esta forma, para cualquier $r \in \mathbb{Z}$, $(nt)\, r = n\,(tr) \in n\mathbb{Z}$.

Ejemplo 3.5 ($\mathbb{R}$). $\mathbb{Z}$ no es un ideal de $\mathbb{R}$ ya que por ejemplo $\sqrt{2}a \notin \mathbb{Z}$ para cualquier $a \in \mathbb{Z}$.

Ejemplo 3.6 ($M_2(\mathbb{Z})$). Consideremos el anillo $M_2(\mathbb{Z})$ de las matrices de 2×2 con entradas en $\mathbb{Z}$. Mostraremos que el conjunto

$$I = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} : a_i \in \mathbb{Z} \text{ es par}, \, i = 1, 2, 3, 4 \right\}$$

es un ideal de $M_2(\mathbb{Z})$. Supongamos que $A, B \in I$. Entonces

$$\begin{aligned} A - B &= \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} - \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \\ &= \begin{bmatrix} a_1 - b_1 & a_2 - b_2 \\ a_3 - b_3 & a_4 - b_4 \end{bmatrix} \in I \end{aligned}$$

porque $a_i - b_i$ es un entero par, para toda $i = 1, 2, 3, 4$. Ahora, si $C \in M_2(\mathbb{Z})$

$$\begin{aligned} AC &= \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \\ &= \begin{bmatrix} a_1c_1 + a_2c_3 & a_1c_2 + a_2c_4 \\ a_3c_1 + a_4c_3 & a_3c_2 + a_4c_4 \end{bmatrix} \in I \end{aligned}$$

porque todas las entradas son enteros pares. Esto se desprende del hecho de que al multiplicar un número par por cualquier entero resulta un número par, y de que al sumar o restar números pares resulta un número par. De manera similar $CA \in I$.

El siguiente lema es muy útil para determinar cuándo un ideal de un anillo es igual al anillo mismo.

Lema 3.7. Sea R un anillo con identidad 1 y sea I un ideal de R. Entonces $1 \in I$ si y sólo si $I = R$.

Demostración. Supongamos que $1 \in I$. Por definición $I \subseteq R$. Para mostrar la inclusión opuesta, sea $a \in R$. Entonces $a = a1 \in I$, por la definición de ideal, debido a que $1 \in I$ y $a \in R$. Luego, $R \subseteq I$. Obviamente, si $I = R$ entonces $1 \in I$. ■

A partir de ahora trabajaremos principalmente con anillos conmutativos.

Teorema 3.8. Sea $A = \{a_1, a_2, \ldots, a_n\}$ un subconjunto finito de un anillo conmutativo R. Entonces el conjunto

$$\langle a_1, a_2, \ldots, a_n \rangle = \{x_1a_1 + x_2a_2 + \ldots + x_na_n : x_1, x_2, \ldots, x_n \in R\}$$

es el ideal más pequeño que contiene a A.

Demostración. Primero comprobaremos que $\langle a_1, a_2, \ldots, a_n \rangle$ es un ideal de R. Si $x_1a_1 + x_2a_2 + \ldots + x_na_n$ y $y_1a_1 + y_2a_2 + \ldots + y_na_n$ son elementos de $\langle a_1, a_2, \ldots, a_n \rangle$ entonces

$$\begin{aligned} & (x_1a_1 + x_2a_2 + \ldots + x_na_n) - (y_1a_1 + y_2a_2 + \ldots + y_na_n) \\ = \; & (x_1 - y_1)\, a_1 + (x_2 - y_2)\, a_2 + \ldots + (x_n - y_n)\, a_n \\ \in \; & \langle a_1, a_2, \ldots, a_n \rangle \end{aligned}$$

Además si $r \in R$,

$$\begin{aligned} & r\,(x_1a_1 + x_2a_2 + \ldots + x_na_n) \\ & = (rx_1)\, a_1 + (rx_2)\, a_2 + \ldots + (rx_n)\, a_n \in \langle a_1, a_2, \ldots, a_n \rangle \end{aligned}$$

Sea ahora I un ideal de R tal que $A \subseteq I$. Como $ra_i \in I$ para cualquier $r \in R$, el ideal I debe contener a todos los elementos de la forma $x_1a_1 + x_2a_2 + \ldots + x_na_n$ para $x_i \in R$, $i = 1, \ldots, n$. Así $\langle a_1, a_2, \ldots, a_n \rangle \subseteq I$. Esto demuestra que $\langle a_1, a_2, \ldots, a_n \rangle$ es el ideal más pequeño que contiene al conjunto A. ■

3.1 Algunos tipos especiales de ideales

Los siguientes son algunos tipos especiales de ideales.

Definición 3.9 (ideal generado). Sea R un anillo conmutativo. Decimos que $\langle a_1, a_2, \ldots, a_n \rangle$ es el ideal generado por los elementos $a_1, a_2, \ldots, a_n \in R$.

Definición 3.10 (ideal principal). Sea R un anillo conmutativo. Decimos que I es un ideal principal de R si $I = \langle a \rangle$ para alguna $a \in R$.

Definición 3.11 (anillo de ideales principales). Decimos que un anillo conmutativo R es un anillo de ideales principales si cualquier ideal de R es principal.

Ejemplo 3.12 ($\mathbb{Z}$). El ideal $n\mathbb{Z}$, $n \in \mathbb{N}$, es un ideal principal de $\mathbb{Z}$. En este caso, $n\mathbb{Z} = \langle n \rangle$. De hecho, sostenemos que $\mathbb{Z}$ es un dominio de ideales principales ya que cualquier ideal de $\mathbb{Z}$ debe ser de la forma $\langle n \rangle$. Para demostrar esto podemos analizar a $\mathbb{Z}$ como un grupo cíclico (generado por 1 o -1) bajo la suma (véase definición B.14). Por el teorema B.18 sabemos que cualquier subgrupo de un grupo cíclico es cíclico; en el caso de $\mathbb{Z}$ esto significa que los únicos subgrupos son los múltiplos de algún entero n. Como un ideal es un subgrupo bajo la suma, concluimos que un ideal de $\mathbb{Z}$ debe consistir en los múltiplos de algún entero n, y esto es exactamente lo que significa $\langle n \rangle$.

Ejemplo 3.13 ($\mathbb{Z}_n$). El anillo $\mathbb{Z}_n$ es un anillo de ideales principales por la misma razón que $\mathbb{Z}$ es un dominio de ideales principales.

Lema 3.14 (ideales principales). Sea D un dominio entero. Entonces, para cualquier $a, b \in D \setminus \{0\}$.

1) $\langle a \rangle \subseteq \langle b \rangle$ si y sólo si $b \mid a$.
2) $\langle a \rangle = \langle b \rangle$ si y sólo si a es asociado de b.
3) $\langle a \rangle = D$ si y sólo si a es una unidad.

Demostración.

1) Si $\langle a\rangle \subseteq \langle b\rangle$, tenemos que $a \in \langle b\rangle = \{rb : r \in D\}$, por lo que $a = qb$ para algún $q \in D \setminus \{0\}$. Esto implica que $b \mid a$. Por otro lado, si $b \mid a$, entonces $a = qb$ para algún $q \in D \setminus \{0\}$. De esta forma, si $xa \in \langle a\rangle$, $xa = (xq)\, b \in \langle b\rangle$. Luego $\langle a\rangle \subseteq \langle b\rangle$.

2) *Ejercicio 3.4.*

3) Observemos que $\langle 1\rangle = D$. Por la parte 2) de este lema, $\langle a\rangle = \langle 1\rangle = D$, si y sólo si a es asociado de 1, lo cual ocurre si y sólo si a es una unidad.

■

Ejemplo 3.15 ($\mathbb{Z}$). En $\mathbb{Z}$ sabemos que $\langle 8\rangle \subseteq \langle 4\rangle \subseteq \langle 2\rangle$ porque $2 \mid 4$ y $4 \mid 8$. Además $\langle 2\rangle = \langle -2\rangle$, porque 2 y -2 son asociados en $\mathbb{Z}$.

Si I, J son ideales de un anillo R, podemos definir la suma y el producto de ideales de la siguiente forma:

$$\begin{aligned} I + J &= \{i + j : i \in I, j \in J\} \\ IJ &= \langle ij : i \in I, j \in J\rangle \\ &= \left\{ \sum_{k=1}^{n} i_k j_k : i_k \in I, j_k \in J, n \in \mathbb{N} \right\} \end{aligned}$$

El conjunto IJ es un ideal de R por definición, y se pide en el *ejercicio 3.1* que se demuestre que $I + J$ también es un ideal de R.

Proposición 3.16. Sea R un anillo conmutativo con ideales I, J y K. Entonces $I\,(J + K) = IJ + IK$.

Demostración. Sea $x \in I\,(J + K)$. Por definición, para algunos $i_s \in I$, $j_s \in J$, $k_s \in K$, tenemos que

$$\begin{aligned} x &= \sum_{s=1}^{n} i_s\,(j_s + k_s) \\ &= \sum_{s=1}^{n} (i_s j_s + i_s k_s) \\ &= \sum_{s=1}^{n} i_s j_s + \sum_{s=1}^{n} i_s k_s \in IJ + IK \end{aligned}$$

Esto muestra que $I\,(J + K) \subseteq IJ + IK$. Invirtiendo los pasos anteriores obtenemos que $IJ + IK \subseteq I\,(J + K)$. ■

3.2 Más definiciones de tipos particulares de ideales

Definición 3.17 (ideal primo). Sea R un anillo conmutativo. Decimos que un ideal propio I de R es primo si para toda $a, b \in R$ tales que $ab \in I$, tenemos que $a \in I$ o $b \in I$.

Definición 3.18 (ideal maximal). Sea R un anillo conmutativo. Decimos que un ideal propio I de R es maximal si no existe un ideal A de R tal que $I \subsetneq A \subsetneq R$.

Observación 3.19. Una de las técnicas estándar para demostrar que un ideal I de R es maximal es suponer que existe un ideal A de R tal que $I \subseteq A \subseteq R$, y mostrar que debe tenerse que $I = A$ o $A = R$.

Ejemplo 3.20 ($\mathbb{Z}_n$). Demostraremos que $\langle [2] \rangle$ es un ideal maximal en $\mathbb{Z}_{12}$. Supongamos que existe un ideal A de $\mathbb{Z}_{12}$ tal que $\langle [2] \rangle \subseteq A \subseteq \mathbb{Z}_{12}$. Debido a que $\mathbb{Z}_{12}$ es un anillo de ideales principales, debemos tener que $A = \langle [m] \rangle$ para algún $[m] \in \mathbb{Z}_{12}$. Por el lema 3.14, $\langle [2] \rangle \subseteq \langle [m] \rangle$, implica que $[m] \mid [2]$, así que $[2] = [r][m]$ para algún $[r] \in \mathbb{Z}_{12}$. Por lo tanto, para $k \in \mathbb{Z}$ tenemos que

$$\begin{aligned} 2 &= rm + 12k \\ 2 - 12k &= rm \\ 2(1 - 6k) &= rm \end{aligned}$$

Esto implica que $2 \mid rm$, así que $2 \mid r$ o $2 \mid m$ por el lema A.13 de Euclides. Si $2 \mid m$ tenemos que $\langle [m] \rangle \subseteq \langle [2] \rangle$, así que $\langle [m] \rangle = [\langle 2 \rangle]$. Si $2 \mid r$, $r = 2a$ para algún $a \in \mathbb{Z}$, así que, sustituyendo en la relación de arriba,

$$1 = am + 6k$$

Como $[6] = [2] \cdot [3] \in \langle [2] \rangle \subseteq \langle [m] \rangle$ tenemos que $[1] = [a][m] + [6][k] \in \langle [m] \rangle$ por cerradura. Por el lema 3.7 $\langle [m] \rangle = \mathbb{Z}_{12}$. Esto demuestra que $\langle [2] \rangle$ es un ideal maximal.

Ejemplo 3.21 ($\mathbb{Z}_p$). Si p es un número primo, el ideal $\langle [0] \rangle$ es un ideal maximal en $\mathbb{Z}_p$. Para demostrar esto, supongamos que A es un ideal de $\mathbb{Z}_p$ tal que

$$\langle [0] \rangle \subseteq A \subseteq \mathbb{Z}_p.$$

Por definición de ideal, A es un subanillo de $\mathbb{Z}_p$, lo que implica que A es también un subgrupo bajo la suma. Por el teorema B.27 de Lagrange, $|A|$ divide a $|\mathbb{Z}_p| = p$, así que $|A| = 1$ o $|A| = p$. Si $|A| = 1$, $A = \langle [0] \rangle$, y si $|A| = p$, $A = \mathbb{Z}_p$.

Proposición 3.22. Sea D un dominio entero y $p \in D$, $p \neq 0$. El ideal $\langle p \rangle$ es primo si y sólo si p es un elemento primo en D.

Demostración. Supongamos que p es un elemento primo en D. Si $ab \in \langle p \rangle$, para $a, b \in D$, entonces $p \mid ab$. Por definición de elemento primo, $p \mid a$ o $p \mid b$. De esta forma, $a \in \langle p \rangle$ o $b \in \langle p \rangle$, y $\langle p \rangle$ es un ideal primo.

Supongamos ahora que el ideal $\langle p \rangle$ es primo y que $p \mid ab$ donde $a, b \in D$. Entonces $ab \in \langle p \rangle$, y $a \in \langle p \rangle$ o $b \in \langle p \rangle$ por definición de ideal primo. Luego $p \mid a$ o $p \mid b$, lo que significa que p es un elemento primo. ■

3.3 Lema de Zorn

Esta sección puede omitirse la primera vez que se lee el texto ya que no es esencial para el desarrollo posterior del mismo.

Nuestro objetivo es demostrar que en cualquier anillo conmutativo con identidad, cualquier ideal propio está contenido en un ideal maximal. La demostración de este hecho requiere del conocido lema de Zorn, el cual es equivalente al axioma de elección. Por tal motivo, consideraremos al lema de Zorn como un axioma en lugar de como un lema. Antes de enunciarlo, recordemos que un conjunto parcialmente ordenado es un conjunto S junto con una relación de orden, es decir, una relación reflexiva, antisimétrica y transitiva. En general denotaremos a esta relación de orden como $\leq$.

Una cadena de S es un subconjunto C tal que $a \leq b$ o $b \leq a$ para toda $a, b \in C$. Decimos que $x \in S$ es una cota superior de un subconjunto $A \subseteq S$ si $a \leq x$ para toda $a \in A$. Decimos que $m \in S$ es un elemento maximal si $m \leq s$, $s \in S$, implica que $m = s$.

Ejemplo 3.23. Sea $S = \{\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}, I\}$ donde $I = \mathbb{R} \setminus \mathbb{Q}$. Consideremos la relación de orden $\subseteq$ sobre S. El conjunto $C = \{\mathbb{Q}, \mathbb{Z}, \mathbb{N}\}$ es una cadena de S porque $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$. Observemos que $\mathbb{R} \in S$ es una cota superior de C. Notemos que el subconjunto $B = \{\mathbb{Q}, \mathbb{Z}, I\}$ no es una cadena de S porque ni $I \nsubseteq \mathbb{Q}$ ni $\mathbb{Q} \nsubseteq I$. El elemento $\mathbb{C} \in S$ es el único elemento maximal de S.

Axioma 3.24 (lema de Zorn). Si S es un conjunto parcialmente ordenado en el cual cualquier cadena de S tiene una cota superior en S, entonces S tiene un elemento maximal.

Teorema 3.25. Sea R un anillo conmutativo con identidad e I un ideal propio de R. Entonces existe un ideal maximal M de R tal que $I \subseteq M$.

Demostración. Utilizaremos el lema de Zorn. Consideremos el conjunto

$$S = \{J \text{ ideal propio de } R : I \subseteq J\}$$

Este es un conjunto parcialmente ordenado junto con la relación de orden $\subseteq$. Obviamente, $S \neq \emptyset$ porque $I \in S$. Demostraremos que toda cadena $C = \{J_k\}$ de S tiene una cota superior. Consideremos el conjunto $T = \cup J_k$. Observemos que T es un ideal de R. Sean $x, y \in T$, entonces $x \in J_i$ y $y \in J_j$ para algunos índices i, j. Como C es una cadena, podemos suponer que $J_i \subseteq J_j$. Entonces $x - y \in J_j$ y $rx \in J_j$ para toda r. Esto implica que $x - y \in T$ y $rx \in T$, y T es un ideal de R. Claramente, $I \subseteq T$ porque $I \subseteq J_k$ para toda k. Además, $T \neq R$, ya que de lo contrario $1 \in T$ y $1 \in J_i$ para algún índice i, esto contradice que $J_i \in S$. Por lo tanto, $T \in S$, y T es una cota superior para C. Por el lema de Zorn, existe un elemento maximal M en S. Así, M es un ideal maximal de R tal que $I \subseteq M$. ■

3.4 Ejercicios

3.1. Si A y B son ideales de un anillo R, muestra que

$$A + B = \{a + b : a \in A, b \in B\}$$

es un ideal de R. Además, muestra que $A \cap B$ es un ideal de R.

3.2. Encuentra un subanillo de $\mathbb{Z} \oplus \mathbb{Z}$ que no sea un ideal de $\mathbb{Z} \oplus \mathbb{Z}$.

3.3. Sea R un anillo conmutativo y A un subconjunto de R. Muestra que el aniquilador de A, definido como

$$Ann(A) = \{r \in R, ra = 0 \text{ para toda } a \in A\}$$

es un ideal de R.

3.4. Sea D un dominio entero y $a, b \in D$. Demuestra que $\langle a \rangle = \langle b \rangle$ si y sólo si a es asociado de b.

3.5. Sea R un anillo conmutativo y A un ideal de R. Muestra que $N(A) = \{r \in R : r^n \in A \text{ para algún } n \in \mathbb{N}\}$ es un ideal de R.

3.6. Con la notación del *ejercicio 3.5,* demuestra que si P es un ideal primo de un anillo R, $N(P^n) = P$ para toda $n \in \mathbb{N}$, donde P^n representa la multiplicación del ideal P por sí mismo n veces.

3.7. El ideal $N(\langle 0\rangle)$ es llamado el nilradical de R. Calcula $N(\langle 0\rangle)$ en $\mathbb{Z}_{27}$ y $N(\langle 0\rangle)$ en $\mathbb{Z}_{36}$.

3.8. Demuestra que si $p \in \mathbb{Z}$ es un número primo, $\langle p\rangle$ es un ideal maximal en $\mathbb{Z}$.

3.9. Demuestra que en $\mathbb{Z} \oplus \mathbb{Z}$, $I = \{(a, 0) : a \in \mathbb{Z}\}$ es un ideal primo pero no maximal.

3.10. El conjunto de las matrices triangulares superiores

$$T = \left\{ \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} : a, b, c \in \mathbb{Z} \right\}$$

forman un subanillo en $M_2(\mathbb{Z})$. Convencerse de esto y hacer una descripción de los ideales del anillo T.

4

Anillos cociente

Hay cosas que les parecen increíbles a la mayoría de los hombres que no han estudiado matemáticas.

Aristóteles, filósofo griego

Al igual que en el caso de los grupos, es posible formar clases laterales de subanillos. Estas clases laterales serán los bloques principales para la construcción de un anillo cociente.

Definición 4.1 (clase lateral). Sea R un anillo y A un subanillo de R. Para cualquier $r \in R$, al conjunto

$$r + A = \{r + a : a \in A\}$$

se le llama la clase lateral de A en R que contiene a r.

El siguiente lema ayuda a trabajar con las clases laterales más cómodamente.

Lema 4.2 (de clases laterales). Sea R un anillo y A un subanillo de R. Entonces para cualquier $a, b \in R$,

1) $a \in a + A$.

2) $a + A = A$ si y sólo si $a \in A$.

3) $a + A = b + A$ si y sólo si $b - a \in A$.

4) $a + A = b + A$ o $(a + A) \cap (b + A) = \emptyset$.

Demostración.

1) Como A es un subanillo de R, $0 \in A$. Luego $a = a + 0 \in a + A$.

2) *Ejercicio 4.1.*

3) *Ejercicio 4.1.*

4) Supongamos que $(a + A) \cap (b + A) \neq \emptyset$. Entonces existe un elemento $x \in R$ tal que $x \in a + A$ y $x \in b + A$. Así $x = a + c = b + c'$ para algunos $c, c' \in A$. Luego, $x - a = c \in A$ y $x - b = c' \in A$. Por la parte 3) de este lema, $a + A = x + A$ y $b + A = x + A$. Por lo tanto $a + A = b + A$.

■

La propiedad 4) del lema anterior, junto con la propiedad 1), implica que el conjunto de clases laterales de A en R forma una partición del conjunto R. De hecho es fácil demostrar que los subconjuntos de la partición son todos del mismo tamaño (*ejercicio 4.2.*).

En teoría de grupos, el conjunto de clases laterales de un subgrupo es un grupo en sí mismo si y sólo si el subgrupo es normal. Para el caso de los anillos tenemos el siguiente teorema:

Teorema 4.3 (anillo cociente). Sea R un anillo y A un subanillo de R. El conjunto de clases laterales

$$R/A = \{r + A : r \in R\}$$

es un anillo bajo las operaciones

$$(s + A) + (t + A) = s + t + A$$

y

$$(s + A)(t + A) = st + A$$

si y sólo si A es un ideal de R. Al anillo R/A se le llama anillo cociente de R sobre A.

Demostración. Supongamos primero que A es un ideal. Es necesario verificar que R/A cumple las propiedades de un anillo. En la definición de la suma y la multiplicación observamos que se cumplen las propiedades de cerradura; sin embargo, también es necesario comprobar que estas operaciones estén bien definidas. Para esto, supongamos que $s+A = s'+A$ y que $t+A = t'+A$ con $s, s', t, t' \in R$. Por la parte 1) del lema 4.2 sabemos que $s \in s' + A$ y $t \in t' + A$, así que $s = s' + a$ y $t = t' + b$ para algunos $a, b \in A$. Así,

$$\begin{aligned}(s + A) + (t + A) &= s + t + A \\ &= (s' + a) + (t' + b) + A \\ &= s' + t' + (a + b) + A \\ &= s' + t' + A \\ &= (s' + A) + (t' + A)\end{aligned}$$

usando el hecho de que $(a + b) \in A$ y la parte 2) del lema 4.2. De manera similar,

$$\begin{aligned}(s + A)(t + A) &= st + A \\ &= (s' + a)(t' + b) + A \\ &= s't' + at' + s'b + ab + A \\ &= s't' + A\end{aligned}$$

debido a que A es un ideal y entonces $at', s'b, ab \in A$. Es sencillo verificar que se cumplen las demás propiedades de los anillos (*ejercicio 4.3.*).

Supongamos ahora que R/A es un anillo. Como A ya es subanillo, sólo debemos demostrar que se cumple la propiedad de los

ideales de absorción de la multiplicación. Tomemos cualquier $a \in A$ y $r \in R$. Usando la parte 2) del lema 4.2 tenemos que $a + A = A = 0 + A$. Entonces,

$$(a + A)(r + A) = ar + A$$

$$(0 + A)(r + A) = A$$

por lo que $ar + A = A$ (aquí estamos utilizando el hecho de que R/A es un subanillo y por lo tanto la multiplicación de clases laterales está bien definida). Por la propiedad 2) del lema 4.2, $ar \in A$. De manera similar, podemos demostrar que $ra \in A$. ■

Ejemplo 4.4 ($\mathbb{Z}$). Sabemos que para cualquier $n \in \mathbb{N}$ el conjunto $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$. De esta forma podemos crear el anillo cociente $\mathbb{Z}/n\mathbb{Z}$. Los elementos de este anillo serán las clases laterales $a + n\mathbb{Z}$ para $a \in \mathbb{Z}$. Sin embargo, este anillo contiene sólo n elementos:

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

Observemos que para cualquier $a \geq n$ o $a \leq -1$, el elemento $a + n\mathbb{Z}$ es ya uno de los elementos del conjunto anterior. Por ejemplo, si $a \geq n$, podemos aplicar el algoritmo de la división para obtener $a = qn + r$, $q, r \in \mathbb{Z}$, $0 \leq r < n$. Así

$$\begin{aligned} a + n\mathbb{Z} &= qn + r + n\mathbb{Z} \\ &= r + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

ya que $qn \in n\mathbb{Z}$. Lo mismo ocurre cuando $a \leq -1$.

Ejemplo 4.5 ($\mathbb{Z}$). El anillo $2\mathbb{Z}$ es un ideal de $\mathbb{Z}$. A su vez, $8\mathbb{Z}$ es un ideal contenido en $2\mathbb{Z}$ porque $2 \mid 8$ (véase lema 3.14). Consideremos ahora el anillo cociente $2\mathbb{Z}/8\mathbb{Z}$. Los elementos del cociente son clases laterales de la forma $a + 8\mathbb{Z}$ donde $a \in 2\mathbb{Z}$. Al igual que en ejemplo anterior, si $a \in 2\mathbb{Z}$ con $a \geq 8$ o $a \leq -1$, usando el algoritmo de la división podemos demostrar que la clase lateral $a + 8\mathbb{Z}$ es una de las clases del siguiente conjunto:

$$2\mathbb{Z}/8\mathbb{Z} = \{0 + 8\mathbb{Z}, 2 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 6 + 8\mathbb{Z}\}$$

Lo siguiente ilustra la forma de sumar y multiplicar en este anillo:

$$\begin{aligned} (3 + 8\mathbb{Z}) + (5 + 8\mathbb{Z}) &= (3 + 5) + 8\mathbb{Z} \\ &= 8 + 8\mathbb{Z} \\ &= 0 + 8\mathbb{Z} \end{aligned}$$

$$\begin{aligned}(6+8\mathbb{Z})\,(2+8\mathbb{Z}) &= 6\cdot 2+8\mathbb{Z}\\ &= 12+8\mathbb{Z}\\ &= 4+8+8\mathbb{Z}\\ &= 4+8\mathbb{Z}\end{aligned}$$

Ejemplo 4.6 ($M_2(\mathbb{Z})$). En el *ejemplo 3.6* del capítulo anterior se demostró que el conjunto I de matrices de 2×2 con entradas enteras pares es un ideal de $R = M_2(\mathbb{Z})$. Sabemos que el anillo cociente R/I es de la forma

$$R/I = \{A+I : A \in M_2(\mathbb{Z})\}$$

Para conocer un poco más sobre la forma de los elementos de R/I, observemos que siempre es posible elegir una matriz A representante de la clase lateral $A+I$ con entradas 0 o 1. Si la entrada a_i de A es cualquier otro número, aplicamos el algoritmo de la división para obtener $a = 2q + r$, con $r = 0$ o 1. Sin embargo, como el número $2q$ es par, éste es "absorbido" por I. Por ejemplo, si $A = \begin{bmatrix} 7 & 6 \\ 2 & -3 \end{bmatrix}$, las siguientes clases laterales son iguales:

$$\begin{aligned}\begin{bmatrix} 7 & 6 \\ 2 & -3 \end{bmatrix} + I &= \begin{bmatrix} 6+1 & 6+0 \\ 2+0 & -4+1 \end{bmatrix} + I\\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 6 & 6 \\ 2 & -4 \end{bmatrix} + I\\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + I\end{aligned}$$

porque $\begin{bmatrix} 6 & 6 \\ 2 & -4 \end{bmatrix} \in I$. Es decir, el conjunto de las clases laterales que forman a R/I debe ser

$$R/I = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + I : a_i \in \{0,1\} \right\}$$

Como cada entrada tiene sólo dos posibles valores, conjeturamos que el anillo R/I contiene exactamente $2^4 = 16$ elementos. Para comprobar esto es necesario verificar que todos los elementos de R/I enlistados anteriormente son diferentes. Supongamos que dos de estas clases son iguales,

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + I = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} + I$$

Por la propiedad 3) del lema 4.2,

$$\begin{bmatrix} a_1 - b_1 & a_2 - b_2 \\ a_3 - b_3 & a_4 - b_4 \end{bmatrix} \in I$$

Debido a que a_i y b_i sólo pueden ser 0 o 1, la única forma de que la entrada $a_i - b_i$ sea par es que $a_i - b_i = 0$. Por lo tanto, $a_i = b_i$ para $i = 1, 2, 3, 4$.

Ejemplo 4.7 ($\mathbb{Z}[i]$). Consideremos el anillo cociente

$$\mathbb{Z}[i] / \langle 2 - i \rangle$$

donde $\langle 2 - i \rangle$ es el ideal generado por el elemento $2 - i \in \mathbb{C}$. Trataremos de identificar cómo son los elementos de este anillo cociente. Sea $I = \langle 2 - i \rangle$. Ciertamente

$$\mathbb{Z}[i] / I = \{a + bi + I : a, b \in \mathbb{Z}\}$$

pero esto lamentablemente no ofrece mucha información. Por el lema 4.2 sabemos que

$$2 + I = i + I \qquad (*)$$

ya que $2 - i \in I$. Esto simplifica la presentación de los elementos de $\mathbb{Z}[i] / I$. Por ejemplo,

$$\begin{aligned} 9 - 2i + I &= (9 + I) - (2 + I)(i + I) \\ &= (9 + I) - (2 + I)(2 + I) \\ &= 5 + I \end{aligned}$$

Entonces cualquier clase lateral de la forma $a + bi + I$ es igual a alguna clase lateral de la forma $k + I$, con $k \in \mathbb{Z}$. Además, elevando al cuadrado la relación $(*)$,

$$\begin{aligned} 4 + I &= -1 + I \\ 5 + I &= 0 + I \end{aligned}$$

Así es posible reducir cualquier clase lateral de la forma $k + I$, $k \in \mathbb{Z}$ a una clase de la forma $s + I$ con $s \in \mathbb{Z}$, $0 \leq s < 5$. Por lo tanto, afirmamos que

$$\mathbb{Z}[i] / \langle 2 - i \rangle = \{0 + I, 1 + I, 2 + I, 3 + I, 4 + I\}$$

Para poder asegurar que $|\mathbb{Z}[i] / \langle 2 - i \rangle| = 5$, es necesario verificar que los elementos enlistados anteriormente son distintos. Como

$\mathbb{Z}[i]/I$ es un grupo abeliano bajo la suma, basta con encontrar un elemento de orden aditivo 5 (véase definición B.16). Observemos que

$$\begin{aligned}(1+I)+(1+I)+(1+I)+(1+I)+(1+I) &= 5+I \\ &= 0+I\end{aligned}$$

lo que implica que el orden de $1+I$ es 1 o 5 (esto es una consecuencia de la proposición 2.24, si $m \cdot 1 = 0$, entonces el orden de 1 divide a m). Suponiendo que el orden de $1+I$ es 1, tenemos que

$$1+I = 0+I$$

y $1 \in I = \langle 2-i \rangle$. Luego, para algunos $a, b \in \mathbb{Z}$,

$$\begin{aligned}1 &= (a+bi)(2-i) \\ &= (2a-b)+i(2b-a)\end{aligned}$$

Así, obtenemos las ecuaciones

$$\begin{aligned}2a+b &= 1 \\ 2b-a &= 0 \;\rightarrow\; a = 2b\end{aligned}$$

Resolviéndolas encontramos que $a = {}^2/_5$ y $b = {}^1/_5$, lo cual contradice que $a, b \in \mathbb{Z}$. Por lo tanto el orden de $1+I$ es 5, y $\mathbb{Z}[i]/I$ tiene exactamente cinco elementos. De hecho, en el siguiente capítulo podremos demostrar que este anillo cociente es esencialmente $\mathbb{Z}_5$.

Los siguientes teoremas establecen una fuerte conexión entre los anillos cociente y los ideales primos y maximales estudiados en el capítulo anterior.

Teorema 4.8. Sea R un anillo conmutativo con identidad y A un ideal de R. Entonces R/A es un dominio entero si y sólo si A es un ideal primo de R.

Demostración. Supongamos que R/A es un dominio entero, y sea $ab \in A$, $a, b \in R$. Entonces,

$$\begin{aligned}(a+A)(b+A) &= ab+A \\ &= 0+A\end{aligned}$$

Como R/A no tiene divisores de cero, debe ser cierto que $a+A = 0+A$ o que $b+A = 0+A$. Por el lema 4.2, $a \in A$ o $b \in A$, y por lo tanto A es un ideal primo de R.

Supongamos ahora que A es un ideal primo de R. Por el teorema 4.3, R/A es un anillo, y es fácil verificar que es conmutativo con identidad (*ejercicio 4.3.*). Para demostrar que R/A es un dominio entero, supongamos que

$$(a + A)(b + A) = 0 + A$$

Por el lema 4.2, $ab \in A$. Debido a que A es un ideal primo, debemos tener que $a \in A$ o $b \in A$. Así $a + A = 0 + A$ o $b + A = 0 + A$. Esto demuestra que R/A no tiene divisores de cero, y por lo tanto es un dominio entero. ■

Teorema 4.9. Sea R un anillo conmutativo con identidad y A un ideal de R. Entonces R/A es un campo si y sólo si A es un ideal maximal de R.

Demostración. Supongamos que R/A es un campo. Sea B un ideal de R tal que $A \subsetneq B \subseteq R$, $A \neq B$. Demostraremos que $B = R$. Tomemos $b \in B$ tal que $b \notin A$. Así, la clase $b + A$ es distinta de $0 + A$, por lo que tiene un inverso multiplicativo en R/A; es decir, existe una clase $c + A$, $c \in R$, tal que

$$(b + A)(c + A) = bc + A = 1 + A$$

Entonces $1 - bc \in A \subsetneq B$. Como B es un ideal, sabemos que $bc \in B$. Así, $1 = (1 - bc) + bc \in B$. Por el lema 3.7, $B = R$. Esto demuestra que A es maximal.

Supongamos ahora que A es un ideal maximal de R. Demostraremos que cualquier elemento distinto de cero en R/A es una unidad. Si $b + A \neq 0 + A$, $b \in R$, debemos tener que $b \notin A$. Consideremos

$$\langle b \rangle + A = \{br + a : r \in R, a \in A\}$$

Por el *ejercicio 3.1*, $\langle b \rangle + A$ un ideal de R, para el cual $A \subsetneq \langle b \rangle + A \subseteq R$. Como A es maximal, debemos tener que $\langle b \rangle + A = R$. Esto implica que $1 \in \langle b \rangle + A$ y que

$$1 = bc + a$$

para algunas $c \in R$, $a \in A$. Luego,

$$1 + A = bc + a + A = bc + A = (b + A)(c + A)$$

Con esto se demuestra que $(c + A) \in R/A$ es el inverso multiplicativo de $(b + A) \in R/A$. Por lo tanto, R/A es un campo. ■

4.1 Ejercicios

4.1. Sea R un anillo, A un subanillo y $a, b \in R$. Demuestra que:

a) $a + A = A$ si y sólo si $a \in A$.

b) $a + A = b + A$ si y sólo si $b - a \in A$.

4.2. Sea R un anillo y A un subanillo de R. Demuestra que todas las clases laterales de A en R tienen la misma cardinalidad.

4.3. Si R es un anillo conmutativo con identidad y A un ideal propio de R, muestra que R/A cumple todas las propiedades de un anillo conmutativo con identidad.

4.4. Sea $R = \mathbb{Z}[i]$ el anillo de enteros gaussianos.

a) Si $I = \langle 4 - i \rangle$, ¿cuántos elementos hay en $\mathbb{Z}[i]/I$? ¿Cuál es la característica de este anillo?

b) Demuestra que $\langle 2 + 2i \rangle$ no es un ideal primo en $\mathbb{Z}[i]$.

4.5. Sea R un anillo conmutativo con identidad. Demuestra que R es un campo si y sólo si R no contiene ideales propios no triviales.

4.6. Sea R un anillo conmutativo con identidad. Demuestra que todo ideal maximal es primo. Demuestra también que si R es finito, entonces todo ideal primo es maximal.

4.7. Demuestra que en un anillo booleano R con identidad (definición en el *ejercicio 1.11*) todo ideal primo es maximal.

5

Homomorfismos de anillos

Los matemáticos no estudian objetos, sino relaciones entre objetos.

Henri Poincaré, matemático francés

En general, los morfismos de estructuras algebraicas son funciones que preservan las operaciones de la estructura. Para el caso de los anillos (al igual que el de los grupos) estos morfismos son llamados homomorfismos, y su característica principal es que preservan ambas la suma y la multiplicación.

Definición 5.1 (homomorfismo). Sean R y S anillos. Un homomorfismo de anillos es una función $\phi : R \to S$ que cumple con las siguientes propiedades para toda $a, b \in R$:

1) $\phi(a+b) = \phi(a) + \phi(b)$.

2) $\phi(ab) = \phi(a)\,\phi(b)$.

En las propiedades 1) y 2) de la definición 5.1 hay que tener en cuenta que las operaciones realizadas del lado izquierdo de la igualdad son las operaciones del anillo R, mientras que las operaciones realizadas del lado derecho son las operaciones de S.

Ejemplo 5.2 ($\mathbb{Z}$). La función $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ definida como $\phi(a) = [a] \in \mathbb{Z}_n$ es un homomorfismo llamado el homomorfismo natural de $\mathbb{Z}$ a $\mathbb{Z}_n$. Observemos que

$$\begin{aligned} \phi(a+b) &= [a+b] = [a] + [b] = \phi(a) + \phi(b) \\ \phi(ab) &= [ab] = [a]\,[b] = \phi(a)\,\phi(b) \end{aligned}$$

Ejemplo 5.3 (R). Si R es un anillo e I un ideal, la función $\phi : R \longrightarrow R/I$ definida como $\phi(r) = r + I$, $r \in R$, es un homomorfismo llamado el homomorfismo natural de R a R/I (*ejercicio 5.4.*).

Ejemplo 5.4 ($\mathbb{Z}_n$). La función $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_{10}$ definida por $\phi([x]_4) = [5x]_{10}$ es un homomorfismo, donde $[.]_4$ representa una clase de equivalencia módulo 4 y $[.]_{10}$ representa una clase de equivalencia módulo 10. Escribamos $[r_1]_4 = [x+y]_4$, es decir $r_1 = x + y + 4q_1$ para algún $q_1 \in \mathbb{Z}$. Entonces

$$\begin{aligned} \phi([x]_4 + [y]_4) &= \phi([r_1]_4) \\ &= [5r_1]_{10} \\ &= [5(x+y+4q_1)]_{10} \\ &= [5x]_{10} + [5y]_{10} + [20q_1]_{10} \\ &= [5x]_{10} + [5y]_{10} + [0]_{10} \\ &= \phi([x]_4) + \phi([y]_4) \end{aligned}$$

De manera similar, tomando $[r_2]_4 = [x]_4 [y]_4$, con $r_2 = xy + 4q_2$, $q_2 \in \mathbb{Z}$, y usando el hecho de que $[5]_{10} = [5]_{10} [5]_{10}$,

$$\begin{aligned} \phi([x]_4 [y]_4) &= \phi([r_2]_4) \\ &= [5r_2]_{10} \\ &= [5(xy + 4q_2)]_{10} \\ &= [5]_{10} [xy]_{10} + [20q_2]_{10} \\ &= [5x]_{10} [5y]_{10} \\ &= \phi([x]_4)\, \phi([y]_4) \end{aligned}$$

En el siguiente lema denotaremos como $|a|$ al orden aditivo del elemento $a \in R$; esto es, el menor entero positivo $n \in \mathbb{N}$ tal que $n \cdot a = 0$. No debe confundirse la característica del anillo R con el orden de un elemento (de hecho, la característica de un anillo con identidad 1 es el orden aditivo de 1).

Lema 5.5 (homomorfismos). Sean R y S anillos y $\phi : R \longrightarrow S$ un homomorfismo. Entonces

1) $\phi(0_R) = 0_S$, donde 0_R es la identidad aditiva en R y 0_S la identidad aditiva en S.
2) $\phi(-a) = -\phi(a)$ para toda $a \in R$.
3) Si R tiene identidad multiplicativa 1, $\phi(1)$ es la identidad multiplicativa en $\phi(R)$.
4) $\phi(n \cdot r) = n \cdot \phi(r)$ y $\phi(r^n) = \phi(r)^n$ para cualquier $r \in R$, $n \in \mathbb{N}$.
5) Si $|a|$ es finito, $a \in R$, entonces $|\phi(a)|$ divide a $|a|$.

Demostración.

1) Para cualquier $a \in R$,

$$\phi(a) = \phi(0_R + a) = \phi(0_R) + \phi(a)$$

Y entonces $\phi(0_R) = 0_S$.

2) Por la propiedad 1) de este lema,

$$\begin{aligned} 0_S &= \phi(0_R) \\ &= \phi(a + (-a)) \\ &= \phi(a) + \phi(-a) \end{aligned}$$

Restando $\phi(a)$ de ambos lados obtenemos $\phi(-a) = -\phi(a)$ para toda $a \in R$.

3) *Ejercicio 5.1. (a).*

4) *Ejercicio 5.1. (b).*

5) Sea $|a| = n \in \mathbb{N}$. Entonces $n \cdot a = 0$. Usando las propiedades 1) y 4) de este lema, $\phi(n \cdot a) = n \cdot \phi(a) = \phi(0_R) = 0_S$. Por lo tanto, $|\phi(a)|$ divide a n (veáse la demostración de la proposición 2.24).

■

Ejemplo 5.6 ($\mathbb{Z}_n$). En este ejemplo determinaremos todos los homomorfismos que existen de la forma $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$. Por la propiedad 4) del lema 5.5 de homomorfismos, la imagen de cualquier elemento está completamente determinada por la imagen de $[1]_{12}$: si $[a]_{12} \in \mathbb{Z}_{12}$, con $a \in \mathbb{N}$, tenemos que $\phi([a]_{12}) = \phi(a \cdot [1]_{12}) = a \cdot \phi([1]_{12})$. Por la propiedad 5) del lema 5.5 de homomorfismos, $|\phi([1]_{12})|$ debe dividir a $|[1]_{12}| = 12$. Sin embargo, por el teorema de Lagrange (teorema B.27), $|\phi([1]_{12})|$ también debe dividir a $|\mathbb{Z}_{30}| = 30$. Así, $|\phi([1]_{12})| = 1, 2, 3$ o 6. Haciendo cálculos directos, podemos darnos cuenta de que los únicos elementos en $\mathbb{Z}_{30}$ con estos órdenes son $[0]_{30}$, $[15]_{30}$, $[10]_{30}$, $[20]_{30}$, $[5]_{30}$ o $[25]_{30}$. Ahora, debido a que $[1]_{12}[1]_{12} = [1]_{12}$ en $\mathbb{Z}_{12}$, debemos tener que $\phi([1]_{12})\phi([1]_{12}) = \phi([1]_{12})$ en $\mathbb{Z}_{30}$. Esto descarta las posibilidades de que $\phi([1]_{12})$ sea igual a $[20]_{30}$ o $[5]_{30}$. Podemos probar que las alternativas restantes ($\phi([1]_{12}) = [0]_{30}, [15]_{30}, [10]_{30}, [25]_{30}$) realmente son homomorfismos y, por lo tanto, sólo existen exactamente cuatro homomorfismos diferentes de $\mathbb{Z}_{12}$ a $\mathbb{Z}_{30}$.

Ejemplo 5.7 ($\mathbb{Z}$). En este ejemplo determinaremos todos los homomorfismos de la forma $\phi : \mathbb{Z} \to \mathbb{Z}$. Al igual que en el caso anterior, bastará con determinar las posibilidades para $\phi(1)$. Como $1 \cdot 1 = 1$, debemos tener que $\phi(1)\phi(1) = \phi(1)$. Pero los únicos elementos de $\mathbb{Z}$ con tales propiedades son 1 y 0. Por lo tanto, los únicos homomorfismos de $\mathbb{Z}$ en $\mathbb{Z}$ son el homomorfismo identidad y el homomorfismo cero.

Lema 5.8. Sean R y S anillos y $\phi : R \longrightarrow S$ un homomorfismo de anillos. Entonces

1) Si A es un subanillo de R, $\phi(A) = \{\phi(a) : a \in A\}$ es un subanillo de S.

2) Si A es un ideal de R, entonces $\phi(A)$ es un ideal de $\phi(R)$.

3) Si B es un subanillo (o ideal) de S, $\phi^{-1}(B) = \{r \in R : \phi(r) \in B\}$ es un subanillo (o ideal) de R.

4) Si R es conmutativo, entonces $\phi(R)$ es conmutativo.

Demostración.

1) Sean $\phi(a), \phi(b) \in \phi(A)$. Claramente

$$\phi(a) - \phi(b) = \phi(a-b) \in \phi(A)$$
$$\phi(a)\phi(b) = \phi(ab) \in \phi(A)$$

Por el test del subanillo (teorema 1.23), $\phi(A)$ es un subanillo de S.

2) Sean $\phi(a), \phi(b) \in \phi(A)$ y $\phi(r) \in \phi(R)$. Entonces

$$\phi(a) - \phi(b) = \phi(a-b) \in \phi(A)$$

$$\phi(r)\phi(a) = \phi(ra) \in \phi(A)$$

Por lo tanto, por el test del ideal (teorema 3.2), $\phi(A)$ es un ideal de $\phi(R)$.

3) *Ejercicio 5.2. (a).*

4) *Ejercicio 5.2. (b).*

■

Definición 5.9 (isomorfismo). Sean R y S anillos. Una función $\phi : R \to S$ es un isomorfismo si es un homomorfismo biyectivo. Si tal función existe, decimos que R es isomorfo a S y escribimos $R \cong S$.

Definición 5.10 (automorfismo). Sea R un anillo. Un isomorfismo $\phi : R \to R$ es llamado automorfismo.

Observación 5.11. Recordemos que una función $\phi : R \to S$ es biyectiva si es inyectiva (es decir, que es uno a uno) y sobreyectiva (es decir, que $\phi(R) = S$). La técnica estándar para comprobar que ϕ es inyectiva es suponer que $\phi(a) = \phi(b)$ para algunos $a, b \in R$, y demostrar que esto implica que $a = b$. La técnica estándar para comprobar que ϕ es sobreyectiva consiste en tomar un elemento arbitrario $s \in S$, y encontrar un $r \in R$ tal que $\phi(r) = s$ (de hecho, esto demuestra que $S \subseteq \phi(R)$; luego podemos concluir que $S = \phi(R)$ ya que $\phi(R) \subseteq S$ por definición).

Ejemplo 5.12 ($\mathbb{Z}_n$). El anillo $\mathbb{Z}_n$ es isomorfo al anillo cociente $\mathbb{Z}/n\mathbb{Z}$. Para comprobar esto hay que verificar que la función $\beta : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ definida como $\beta([x]) = x + n\mathbb{Z}$, $[x] \in \mathbb{Z}_n$ es un isomorfismo. Usando el *ejemplo 5.2* es fácil comprobar que β cumple las propiedades de un homomorfismo de anillos. Para demostrar que β es inyectivo, supongamos que $x + n\mathbb{Z} = y + n\mathbb{Z}$ para $x, y \in \mathbb{Z}$. Por el lema 4.2, $x - y \in n\mathbb{Z}$, así que $n \mid x - y$. Esto implica que $[x] = [y]$, así que β es inyectiva. Para demostrar que β es sobreyectiva, tomemos una clase lateral arbitraria en $\mathbb{Z}/n\mathbb{Z}$. Cualquiera de estas clases laterales debe tener la forma $x + n\mathbb{Z}$, para algún $x \in \mathbb{Z}$. Por lo tanto, $[x] \in \mathbb{Z}_n$ es la preimagen de $x + n\mathbb{Z}$ porque $\beta([x]) = x + n\mathbb{Z}$. Esto demuesta que β es un isomorfismo.

Teorema 5.13. La relación $\cong$ de isomorfía de anillos es una relación de equivalencia.

Demostración. Debemos comprobar que se cumplen las siguientes propiedades.

1) *Reflexividad.* $A \cong A$ para cualquier anillo A (*ejercicio 5.3.*).

2) *Simetría.* Debemos demostrar que si $A \cong B$ entonces $B \cong A$. Si $A \cong B$, existe un isomorfismo $\phi : A \longrightarrow B$. Demostraremos que $\phi^{-1} : B \longrightarrow A$ es un isomorfismo. Es claro que ϕ^{-1} es una función biyectiva dado que ϕ es biyectiva. Ahora hay que comprobar que ϕ^{-1} cumple las propiedades de los homomorfismos de anillos. Debido a que ϕ es sobreyectiva, para cualquier $x, y \in B$ existen $a, b \in A$ tales que $\phi(a) = x$ y $\phi(b) = y$. Como ϕ es un homomorfismo, se cumple que

$$x + y = \phi(a) + \phi(b) = \phi(a + b)$$
$$xy = \phi(a)\,\phi(b) = \phi(ab)$$

Aplicando ϕ^{-1} a la primera relación,

$$\phi^{-1}(x + y) = \phi^{-1}\phi(a + b) = a + b = \phi^{-1}(x) + \phi^{-1}(y)$$

Y también

$$\phi^{-1}(xy) = \phi^{-1}\phi(ab) = ab = \phi^{-1}(x)\,\phi^{-1}(y)$$

Esto demuestra que $\phi^{-1} : B \longrightarrow A$ es un isomorfismo y $B \cong A$.

3) *Transitividad.* Si $A \cong B$ y $B \cong C$ entonces $A \cong C$ (*ejercicio 5.3.*).

■

Nuestro objetivo ahora es demostrar el llamado primer teorema de isomorfía. Para esto necesitaremos algunas definiciones y proposiciones previas.

Definición 5.14 (kernel). Sea $\phi : R \to S$ un homomorfismo de anillos. El subanillo $\phi^{-1}(0_S) = \{r \in R : \phi(r) = 0_S\}$ es llamado el kernel de ϕ y se denota como $\ker(\phi)$.

Proposición 5.15. Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos. Entonces $\ker(\phi)$ es un ideal de R.

Demostración. Observemos que 0_S es un ideal de S, así que

$$\phi^{-1}(0_S) = \ker(\phi)$$

es un ideal de R, por lema 5.8 inciso 3). ■

Proposición 5.16. El homomorfismo de anillos $\phi : R \longrightarrow S$ es inyectivo si y sólo si $\ker(\phi) = \{0_R\}$.

Demostración. Supongamos que ϕ es inyectivo. Por el lema 5.5 de homomorfismos, sabemos que $0_R \in \ker\phi$ porque $\phi(0_R) = 0_S$. Supongamos que $a \in \ker\phi$. Entonces $\phi(a) = 0_S = \phi(0_R)$, así que $a = 0_R$ debido a que ϕ es inyectivo. Esto demuestra que $\ker(\phi) = \{0_R\}$.

Supongamos que $\ker(\phi) = \{0_R\}$. Sean $a, b \in R$ tales que $\phi(a) = \phi(b)$. Entonces, $\phi(a - b) = 0$, así que $a - b \in \ker\phi = \{0_R\}$. Esto implica que $a - b = 0_R$ y $a = b$. Por lo tanto ϕ es inyectivo. ■

Teorema 5.17 (primer teorema de isomorfía). Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos. Entonces $R/\ker(\phi) \cong \phi(R)$.

Demostración. Definamos una función $\mu : R/\ker(\phi) \longrightarrow \phi(R)$ como $\mu(r + \ker(\phi)) = \phi(r)$ para $r \in R$. Demostremos que μ es un isomorfismo:

1) *Bien definida.* Antes que nada es necesario demostrar que μ es una función bien definida. Supongamos que $r + \ker(\phi) = s + \ker(\phi)$, $r, s \in R$. Entonces $r - s \in \ker(\phi)$, por el lema 4.2. Esto implica que $\phi(r - s) = \phi(r) - \phi(s) = 0_S$, así que $\phi(r) = \phi(s)$. Por lo tanto,

$$\begin{aligned} \mu(r + \ker(\phi)) &= \phi(r) \\ &= \phi(s) \\ &= \mu(s + \ker(\phi)) \end{aligned}$$

2) *Inyectividad.* Supongamos que $\mu(r + \ker(\phi)) = \mu(s + \ker(\phi))$. Entonces $\phi(r) = \phi(s)$. Observemos que

$$\phi(r - s) = \phi(r) - \phi(s) = 0_S$$

Esto implica que $r - s \in \ker(\phi)$, y luego $r + \ker(\phi) = s + \ker(\phi)$.

3) *Sobreyectividad.* Claramente μ es sobreyectiva por definición. La preimagen de $\phi(r) \in \phi(R)$ es $r + \ker(\phi)$.

4) *Homomorfismo.* Para $r, s \in R$

$$\begin{aligned}\mu((r + \ker(\phi)) + (s + \ker(\phi))) &= \mu(r + s + \ker(\phi)) \\ &= \phi(r + s) \\ &= \phi(r) + \phi(s) \\ &= \mu(r + \ker(\phi)) + \\ &\quad \mu(s + \ker(\phi))\end{aligned}$$

De manera similar

$$\begin{aligned}\mu((r + \ker(\phi))(s + \ker(\phi))) &= \mu(rs + \ker(\phi)) \\ &= \phi(rs) \\ &= \phi(r)\phi(s) \\ &= \mu(r + \ker(\phi))\mu(s + \ker(\phi))\end{aligned}$$

■

Ejemplo 5.18 ($\mathbb{Z}_n$). Sea $n \in \mathbb{N}$ y definamos $\phi : \mathbb{Z} \to \mathbb{Z}_n$ como $\phi(a) = [a] \in \mathbb{Z}_n$ para $a \in \mathbb{Z}$. Por el *ejemplo 5.2*, ϕ es un homomorfismo de anillos. Observemos que

$$\begin{aligned}\ker\phi &= \{a \in \mathbb{Z} : \phi(a) = [a] = [0]\} \\ &= \{a \in \mathbb{Z} : n \mid a\} = n\mathbb{Z}\end{aligned}$$

Además $\phi(\mathbb{Z}) = \mathbb{Z}_n$, porque cualquier clase en $\mathbb{Z}_n$ tiene una preimagen en $\mathbb{Z}$. Por lo tanto, por el primer teorema de isomorfía, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Este resultado ya lo habíamos obtenido en el *ejemplo* 5.12.

Cerramos este capítulo con una aplicación del primer teorema de isomorfía que nos será de mucha utilidad en el capítulo 12, “Campos finitos”.

Teorema 5.19. Sea R un anillo con identidad 1_R. Si $char(R) = n \neq 0$, entonces R contiene un subanillo isomorfo a $\mathbb{Z}_n$. Si $char(R) = 0$, R contiene un subanillo isomorfo a $\mathbb{Z}$.

Demostración. Supongamos que $char(R) = n \neq 0$. Consideremos el homomorfismo $\phi : \mathbb{Z} \longrightarrow R$ definido como $\phi(a) = a \cdot 1_R$ para $a \in \mathbb{Z}$. En el *ejercicio 5.6* se pide verificar que ϕ es verdaderamente un homomorfismo. Por el lema 5.8, sabemos que $S = \phi(\mathbb{Z}) = \{a \cdot 1_R : a \in \mathbb{Z}\}$ es un subanillo de R. Usando ahora el primer teorema de isomorfía (teorema 5.17), $\mathbb{Z}/\ker(\phi) \cong S$. Observemos que

$$\begin{aligned} \ker(\phi) &= \{a \in \mathbb{Z} : \phi(a) = 0_R\} \\ &= \{a \in \mathbb{Z} : a \cdot 1_R = 0_R\} \end{aligned}$$

Demostraremos que $n\mathbb{Z} = \ker(\phi)$. Como $n \cdot 1_R = 0_R$, claramente $n \in \ker(\phi)$. Debido a que $\ker(\phi)$ es un ideal de $\mathbb{Z}$, $\langle n \rangle = n\mathbb{Z} \subseteq \ker(\phi)$. Sea $k \in \ker(\phi)$. Entonces, $k \cdot 1_R = 0_R$ implica que $n \mid k$ (proposición 2.24), por lo que $k \in n\mathbb{Z}$. Así, $\ker(\phi) \subseteq n\mathbb{Z}$. Por lo tanto $n\mathbb{Z} = \ker(\phi)$, y

$$S \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Si $char(R) = 0$, $\ker(\phi) = \langle 0 \rangle$, y

$$S \cong \mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$$

■

Corolario 5.20. Sea $p \in \mathbb{N}$ un número primo y F un campo de característica p. Entonces F contiene un subcampo isomorfo a $\mathbb{Z}_p$. Si F es de característica 0, entonces F contiene un subcampo isomorfo a $\mathbb{Q}$.

Demostración. Si F es de característica p, F contiene un subanillo isomorfo a $\mathbb{Z}_p$. Por el teorema de los dominios enteros finitos, este subanillo es un subcampo. Si F es de característica 0, entonces por el teorema anterior F contiene un subanillo $S \cong \mathbb{Z}$. Ahora sólo hay que demostrar que el subcampo

$$T = \left\{ab^{-1} : a, b \in S, b \neq 0\right\} \subseteq F$$

es isomorfo a $\mathbb{Q}$ (*ejercicio 5.12.*). ■

5.1 Ejercicios

5.1. Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos. Demuestra que:

a) Si R es un anillo con identidad multiplicativa 1, $\phi(1)$ es la identidad multiplicativa en $\phi(R)$.

b) $\phi(n \cdot r) = n \cdot \phi(r)$ y $\phi(r^n) = \phi(r)^n$ para cualquier $r \in R$, $n \in \mathbb{N}$.

5.2. Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos. Demuestra que:

a) Si B es un ideal de S, $\phi^{-1}(B) = \{r \in R : \phi(r) \in B\}$ es un ideal de R.

b) Si R es conmutativo entonces $\phi(R)$ es conmutativo.

5.3. Demuestra que la relación $\cong$ de isomorfía de anillos es reflexiva y transitiva.

5.4. Sea $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$ y

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\}$$

Muestra que $\mathbb{Z}\left[\sqrt{2}\right] \cong H$.

5.5. Si R es un anillo e I un ideal, muestra que $\phi : R \longrightarrow R/I$ definida como $\phi(r) = r + I$, $r \in R$, es un homomorfismo (el homomorfismo natural de R a R/I).

5.6. Sea R un anillo con identidad 1_R. Demuestra que la función $\phi : \mathbb{Z} \longrightarrow R$ dada por $\phi(a) = a \cdot 1_R$, $a \in \mathbb{Z}$, es un homomorfismo de anillos.

5.7. Determina todos los homomorfismos de $\mathbb{Z}_6$ a $\mathbb{Z}_6$ y todos los homomorfismos de $\mathbb{Z}_{20}$ a $\mathbb{Z}_{30}$.

5.8. Determina todos los homomorfismos de $\mathbb{Z} \times \mathbb{Z}$ en $\mathbb{Z} \times \mathbb{Z}$. Justifica. Sugerencia: considera que $\phi(1,0) = \phi(1,0)\phi(1,0)$, $\phi(0,1) = \phi(0,1)\phi(0,1)$ y $\phi((1,0)(0,1)) = \phi((1,1))$.

5.9. Sea $\phi : R \longrightarrow S$ un homomorfismo de anillos. Muestra, sin usar el lema 5.8 que $\ker(\phi)$ es un ideal de R.

5.10. Sean K y L campos y $\phi : K \longrightarrow L$ un homomorfismo distinto de cero. Muestra que ϕ es inyectivo.

5.11. Sea R un anillo conmutativo de característica prima p. Muestra que la función $\phi(x) = x^p$ es un homomorfismo de R en R. A ϕ se le llama homomorfismo de Frobenius.

5.12. Sea F un campo de característica 0 y $S \cong \mathbb{Z}$ un subanillo. Muestra que el conjunto $T = \{ab^{-1} : a, b \in S, b \neq 0\}$ es isomorfo a $\mathbb{Q}$.

6

Anillos de polinomios

Los matemáticos son como los franceses: cualquier cosa que les dices la traducen a su propio lenguaje, e inmediatamente suena como algo totalmente diferente.

Wolfgang von Goethe, poeta alemán

6.1 Definiciones

En este capítulo se estudiará más a fondo un anillo particular: el anillo de polinomios. Posiblemente la siguiente definición de polinomio parezca distante a la idea intuitiva del concepto; sin embargo, más adelante se establecerá una representación más familiar.

Definición 6.1 (polinomio). Sea R un anillo conmutativo. Un polinomio f sobre R es una sucesión de la forma $(a_0, a_1, a_2, \ldots)$, con $a_i \in R$ para toda $i \in \mathbb{N}_0$, la cual sólo contiene un número finito de términos distintos de cero; es decir, existe $N \in \mathbb{N}_0$ tal que $a_k = 0$ para toda $k \geq N$. Los términos a_i son llamados coeficientes del polinomio.

Los siguientes son varios términos relacionados con polinomios.

Definición 6.2 (grado). Sea $f = (a_0, a_1, a_2, \ldots)$, $a_i \in R$ un polinomio sobre R. Si $a_n \neq 0$ y $a_m = 0$ para toda $m > n$, decimos que el grado de f es n, y escribimos $\deg f = n$. No definimos grado para el polinomio $f = (0, 0, 0, \ldots)$.

Definición 6.3 (polinomio mónico). Sea f un polinomio de grado n. El coeficiente a_n es llamado coeficiente principal. Si el coeficiente principal $a_n = 1$, decimos que f es un polinomio mónico.

Definición 6.4 (polinomio constante). Decimos que un polinomio de grado 0 es un polinomio constante.

También definimos la suma y multiplicación de polinomios como sigue

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

$$(a_0, a_1, \ldots)\,(b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

donde

$$c_k = \sum_{i+j=k} a_i b_j \text{ para } k \in \mathbb{N}_0$$

El conjunto de polinomios sobre R, junto con las dos operaciones antes descritas, forma un anillo conmutativo con identidad $(1, 0, 0, \ldots)$. Es sencillo verificar que se cumplen las propiedades de anillos; por ejemplo, $(0, 0, \ldots)$ es la identidad aditiva, $(-a_0, -a_1, \ldots)$ es el inverso aditivo de $(a_0, a_1, \ldots)$, etcétera.

A través del homomorfismo inyectivo $\theta(a) = (a, 0, 0, \ldots)$ identificamos al polinomio $(a, 0, 0, \ldots)$ con el elemento $a \in R$. Definamos ahora

$$x = (0, 1, 0, 0, \ldots)$$

Con base en la regla de multiplicación de polinomios, obtenemos que

$$\begin{aligned} x^2 &= (0, 0, 1, 0, \ldots) \\ x^3 &= (0, 0, 0, 1, \ldots) \\ &\vdots \\ x^n &= (0, 0, \ldots, 1, \ldots) \end{aligned}$$

Esto nos brinda una nueva forma de representar los polinomios, con la cual podemos trabajar más cómodamente. Si f es un polinomio de grado n,

$$\begin{aligned} f &= (a_0, a_1, \ldots, a_n, 0, 0, \ldots) \\ &= \theta(a_0) + \theta(a_1)\, x + \theta(a_2)\, x^2 + \ldots + \theta(a_n)\, x^n \end{aligned}$$

Para simplificar notación, identificamos $\theta(a_i)$ con a_i, y así

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

Esta representación es mucho más familiar al lector. Sin embargo, es importante considerar que los símbolos $x, x^2, x^3, \ldots$ simplemente son indicadores, no incógnitas ni variables que resolver como en el caso de una ecuación. De acuerdo con esto, expresiones como

$$x^2 - 4 = 0$$

no tienen sentido, porque el polinomio $x^2 - 4 = (-4, 0, 1, 0, \ldots)$ no es igual al polinomio cero $(0, 0, \ldots)$. Esta última notación tiene la ventaja de que la suma y multiplicación de polinomios se realizan en forma convencional. A partir de ahora escribiremos $f(x)$ para representar a un polinomio f y $R[x]$ para representar al anillo de polinomios sobre R.

Ejemplo 6.5 ($\mathbb{Z}_5[x]$). El anillo $\mathbb{Z}_5[x]$ consiste en el anillo de polinomios con coeficientes en $\mathbb{Z}_5$. Por ejemplo, tomemos $f(x) = [3]x^3 + [2]x^2 + [1]$ y $g(x) = [4]x^2 + [2]$. Para simplificar notación,

escribiremos a en lugar de $[a]$, sin olvidar que a representará una clase de equivalencia módulo 5. Entonces,

$$\begin{aligned} f(x)\,g(x) &= \left(3x^3 + 2x^2 + 1\right)\left(4x^2 + 2\right) \\ &= 12x^5 + 8x^4 + 4x^2 + 6x^3 + 4x^2 + 2 \\ &= 2x^5 + 3x^4 + x^3 + 3x^2 + 2 \end{aligned}$$

Teorema 6.6. Si D es un dominio entero, entonces $D[x]$ es un dominio entero.

Demostración. Como se vio anteriormente, $D[x]$ es un anillo conmutativo con identidad. Debemos demostrar que $D[x]$ no tiene divisores de cero. Sean $f(x), g(x) \in D[x]$ tales que $f(x)\,g(x) = 0$. Supongamos que $f(x) \neq 0$ y $g(x) \neq 0$. Si $f(x) = a_0 + \ldots + a_n x^n$, $a_n \neq 0$, y $g(x) = b_0 + \ldots + b_m x^m$, $b_m \neq 0$; entonces, por la definición de multiplicación en $D[x]$, el coeficiente principal de $f(x)\,g(x)$ es $a_n b_m$. Como D es un dominio entero, $a_n b_m \neq 0$, lo que contradice el hecho de que $f(x)\,g(x) = 0$. Por lo tanto, $g(x) = 0$ o $f(x) = 0$. Esto demuestra que $D[x]$ es un dominio entero. ■

6.2 Algoritmo de la división para polinomios

El siguiente teorema hace uso de los homomorfismos para darle sentido a la idea intuitiva de evaluar un polinomio.

Teorema 6.7 (homomorfismo de evaluación). Sea R un anillo conmutativo y S un subanillo de R. Sea $\alpha \in R$. Entonces la función $\phi_\alpha : S[x] \longrightarrow R$ definida como

$$\phi_\alpha(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

con $a_i \in S$, $i \geq 0$, es un homomorfismo de anillos.

Demostración. Comprobaremos que se cumplen las propiedades de homomorfismo.

1) *Bien definida.* Es claro que ϕ_α está bien definida ya que si $a_0 + a_1 x + \ldots + a_n x^n = b_0 + b_1 x + \ldots + b_m x^m$, con $m \geq n$, entonces $a_i = b_i$ para toda $0 \leq i \leq n$ y $b_j = 0$ para toda $j > m$. Luego

$$b_0 + b_1\alpha + \ldots + b_m\alpha^m = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

2) *Homomorfismo (suma).* Sea ahora $f(x) = a_0 + a_1x + \ldots + a_nx$ y $g(x) = b_0 + b_1x + \ldots + b_mx^m$ con $m \geq n$. Entonces

$$\begin{aligned}\phi_\alpha(f(x) + g(x)) &= \phi_\alpha((a_0 + b_0) + \ldots + (a_n + b_n)x^n \\ &\quad + b_{n+1}x^{n+1} + \ldots + b_mx^m) \\ &= (a_0 + b_0) + \ldots + (a_n + b_n)\alpha^n \\ &\quad + b_{n+1}\alpha^{n+1} + \ldots + b_m\alpha^m \\ &= (a_0 + \ldots + a_n\alpha^n) + (b_0 + \ldots + b_m\alpha^m) \\ &= \phi_\alpha(f(x)) + \phi_\alpha(g(x))\end{aligned}$$

3) *Homomorfismo (multiplicación).* Sea $f(x)g(x) = c_0 + c_1\alpha + \ldots + c_{m+n}x^{n+m}$ con $c_k = \sum_{i+j=k} a_ib_j$.

$$\begin{aligned}\phi_\alpha(f(x)g(x)) &= c_0 + c_1\alpha + \ldots + c_{m+n}\alpha^{n+m} \\ &= (a_0 + \ldots + a_n\alpha^n)(b_0 + \ldots + b_m\alpha^m) \\ &= \phi_\alpha(f(x))\,\phi_\alpha(g(x))\end{aligned}$$

■

Cuando trabajamos con un anillo de polinomios con coeficientes en un campo, el siguiente teorema nos da una herramienta muy poderosa, la cual es análoga al algoritmo de la división para números enteros del apéndice A.

Teorema 6.8 (algoritmo de la división). Sea F un campo y $f(x), g(x) \in F[x]$, $g(x) \neq 0$. Entonces existen polinomios únicos $q(x)$ y $r(x)$ en $F[x]$ tales que

$$f(x) = g(x)q(x) + r(x)$$

donde $r(x) = 0$ o $\deg r(x) < \deg g(x)$.

Demostración. Primero demostraremos la existencia de dichos polinomios. Si $\deg f(x) < \deg g(x)$, podemos tomar $q(x) = 0$ y $r(x) = f(x)$. Supongamos entonces que $n = \deg f(x) \geq m = \deg g(x)$. Demostraremos el teorema por inducción sobre n. Si $n = 0$, debemos tener que $m = 0$, así que $f(x) = a_0, g(x) = b_0 \in F$. En este caso tomemos $q(x) = b_0^{-1}a_0 \in F$ y $r(x) = 0$. Asumamos que el teorema se cumple para cualquier entero positivo menor que n. Sean

$$\begin{aligned}f(x) &= a_nx^n + \ldots + a_0 \in F[x],\ a_n \neq 0 \\ g(x) &= b_mx^m + \ldots + b_0 \in F[x],\ b_m \neq 0\end{aligned}$$

donde $n \geq m$. Definamos

$$f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x) \qquad (*)$$

Observemos que el coeficiente de x^n en $f_1(x)$ es cero, por lo que $\deg f_1(x) < n$. Por hipótesis de inducción, existen $q_1(x), r_1(x) \in F[x]$ tales que

$$f_1(x) = q_1(x) g(x) + r_1(x)$$

con $r_1(x) = 0$ o $\deg r_1(x) < \deg g(x)$. Sustituyendo la relación anterior en $(*)$ obtenemos que

$$\begin{aligned} f(x) &= f_1(x) + \frac{a_n}{b_m} x^{n-m} g(x) \\ &= \left(q_1(x) + \frac{a_n}{b_m} x^{n-m} \right) g(x) + r_1(x) \end{aligned}$$

Por lo tanto, el teorema se cumple con $q(x) = q_1(x) + \frac{a_n}{b_m} x^{n-m}$ y $r(x) = r_1(x)$.

Finalmente, para demostrar la unicidad supongamos que

$$\begin{aligned} f(x) &= g(x) q_1(x) + r_1(x) \\ f(x) &= g(x) q_2(x) + r_2(x) \end{aligned}$$

donde $r_1(x) = 0$ o $\deg r_1(x) < \deg g(x)$ y $r_2(x) = 0$ o $\deg r_2(x) < \deg g(x)$. Luego, deducimos que $\deg(r_2(x) - r_1(x)) < \deg g(x)$ siempre que $r_1(x) - r_2(x) \neq 0$. Restando las relaciones anteriores,

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

Así que por el *ejercicio 6.3*,

$$\begin{aligned} \deg(r_2(x) - r_1(x)) &= \deg g(x) + \deg(q_1(x) - q_2(x)) \\ &\geq \deg(g(x)). \end{aligned}$$

Esto es una contradicción, lo que implica que debemos tener $r_2(x) - r_1(x) = 0$. Por lo tanto $r_1(x) = r_2(x)$ y $q_1(x) = q_2(x)$. ■

Al igual que en el caso de los enteros, el polinomio $q(x)$ se llama cociente y el polinomio $r(x)$ se llama residuo de la división de $f(x)$ por $g(x)$.

Ejemplo 6.9. Consideremos los polinomios $f(x) = 2x^4+x$ y $g(x) = x^2+2x+1$ en $\mathbb{Z}_3[x]$. La forma de encontrar los polinomios cociente y residuo del algoritmo de la división es la llamada "división larga":

$$\begin{array}{r|l} & 2x^2 - x \\ \hline x^2 + 2x + 1 & 2x^4 + x \\ & -2x^4 - 4x^3 - 2x^2 \\ \hline & -x^3 - 2x^2 + x \\ & x^3 + 2x^2 + x \\ \hline & 2x \end{array}$$

El procedimiento se detiene cuando encontramos un residuo de grado menor que $2 = \deg g(x)$. De esta manera,

$$f(x) = \left(2x^2 - 1\right) g(x) + 2x$$

Recordemos que en $\mathbb{Z}_3[x]$, $2x^2 - 1 = 2x^2 + 2$, y podemos trabajar el representante que más nos convenga.

Definición 6.10 (factor). Sea D un dominio entero y $f(x), g(x) \in D[x]$. Decimos que $g(x)$ es un factor de $f(x)$ (o que $g(x)$ divide a $f(x)$) si $f(x) = g(x)\,h(x)$ para algún $h(x) \in D[x]$.

Definición 6.11 (raíz). Sea R un anillo conmutativo, $\alpha \in R$ y $f(x) \in R[x]$. Decimos que α es una raíz de $f(x)$ si $f(\alpha) = 0$.

Corolario 6.12 (teorema del residuo). Sea F un campo

$$\alpha \in F \quad \text{y} \quad f(x) \in F[x].$$

Entonces $f(\alpha)$ es el residuo de la división de $f(x)$ por $x - \alpha$.

Demostración. *Ejercicio 6.5.* ■

Corolario 6.13 (teorema del factor). Sea F un campo, $\alpha \in F$ y $f(x) \in F[x]$. Entonces α es una raíz de $f(x)$ si y sólo si $x - \alpha$ es factor de $f(x)$.

Demostración. *Ejercicio 6.6.* ■

En general, decimos que α es una raíz con multiplicidad $m \geq 1$ de $f(x)$ si $(x - \alpha)^m$ es factor de $f(x)$ pero $(x - \alpha)^{m+1}$ no es factor de $f(x)$.

Teorema 6.14. Sea F un campo y $f(x) \in F[x]$, $\deg f(x) = n$. Entonces $f(x)$ no tiene más de n raíces contando multiplicidad.

Demostración. Usaremos inducción sobre n. Si $n = 0$, entonces el polinomio constante $f(x)$ no tiene ninguna raíz. Sea $f(x)$ un polinomio de grado $n > 0$. La hipótesis de inducción es suponer que cualquier polinomio de grado $m < n$ tiene máximo m raíces contando multiplicidad. Sea $\alpha \in F$ una raíz de $f(x)$ de multiplicidad k. Entonces

$$f(x) = (x - \alpha)^k q(x)$$

con $q(\alpha) \neq 0$. Por el *ejercicio 6.3*, tenemos que

$$n = \deg\left((x - \alpha)^k q(x)\right) = k + \deg q(x)$$

y entonces $k \leq n$. Si $f(x)$ no tiene más raíces, el teorema queda demostrado. En caso contrario, observemos que cualquier otra raíz $\beta \neq \alpha$ de $f(x)$ es una raíz de $q(x)$ porque

$$0 = f(\beta) = (\beta - \alpha)^k q(\beta)$$

implica que $q(\beta) = 0$. Por hipótesis de inducción, $q(x)$ tiene máximo $\deg q(x) = n - k$ raíces contando multiplicidad. Por lo tanto, $f(x)$ tiene máximo $k + (n - k) = n$ raíces. ■

6.3 Ideales y anillos cocientes de polinomios

Esta sección está dedicada a estudiar ejemplos de ideales y anillos cocientes de polinomios.

Ejemplo 6.15 ($\mathbb{R}[x]$). Consideremos el anillo $\mathbb{R}[x]$. El conjunto A de todos los polinomios cuyo término constante es 0 es un ideal de $\mathbb{R}[x]$. De hecho, A es el ideal principal

$$\langle x \rangle = \{g(x)\, x : g(x) \in \mathbb{R}[x]\}.$$

Para comprobar esto, supongamos que $f(x) \in A$. Entonces

$$\begin{aligned} f(x) &= a_1 x + a_2 x^2 + \ldots + a_n x^n \\ &= \left(a_1 + a_2 x + \ldots + a_n x^{n-1}\right) x \in \langle x \rangle \end{aligned}$$

Luego $A \subseteq \langle x \rangle$. Claramente, si $f(x) \in \langle x \rangle$, el término constante de $f(x)$ es 0, así que $f(x) \in A$. Por lo tanto $\langle x \rangle \subseteq A$ y $A = \langle x \rangle$.

Ejemplo 6.16 ($\mathbb{Z}[x]$). El conjunto I de todos los polinomios con términos constantes pares es un ideal del anillo $\mathbb{Z}[x]$. De hecho $I = \langle 2, x\rangle$. La demostración de esto es similar al ejemplo anterior (*ejercicio 6.8.*).

Ejemplo 6.17 ($\mathbb{R}[x]$). Sea

$$\left\langle x^2+1\right\rangle = \left\{g(x)\left(x^2+1\right) : g(x) \in \mathbb{R}[x]\right\}$$

Consideremos el anillo cociente

$$\mathbb{R}[x] / \left\langle x^2+1\right\rangle = \left\{f(x) + \left\langle x^2+1\right\rangle : f(x) \in \mathbb{R}[x]\right\}$$

Si $f(x) \in \mathbb{R}[x]$, podemos usar el algoritmo de la división para escribir $f(x) = q(x)(x^2+1) + r(x)$, donde $r(x) = 0$ o $\deg r(x) < 2$. Por lo tanto, la clase lateral de $f(x)$ es de la forma

$$\begin{aligned} f(x) + \left\langle x^2+1\right\rangle &= q(x)\left(x^2+1\right) + r(x) + \left\langle x^2+1\right\rangle \\ &= r(x) + \left\langle x^2+1\right\rangle \end{aligned}$$

ya que $q(x)(x^2+q) \in \langle x^2+1\rangle$. Así,

$$\mathbb{R}[x] / \left\langle x^2+1\right\rangle = \left\{ax + b + \left\langle x^2+1\right\rangle : a, b \in \mathbb{R}\right\}$$

Debido a que $x^2 + \langle x^2+1\rangle = -1 + \langle x^2+1\rangle$ (lema 4.2) para multiplicar elementos en $\mathbb{R}[x] / \langle x^2+1\rangle$, identificamos a x^2 con -1. Por ejemplo

$$\begin{aligned} &\left(2x+1+\left\langle x^2+1\right\rangle\right)\left(3x+7+\left\langle x^2+1\right\rangle\right) \\ &= (2x+1)(3x+7) + \left\langle x^2+1\right\rangle \\ &= 6x^2 + 3x + 14x + 7 + \left\langle x^2+1\right\rangle \\ &= 17x + 1 + \left\langle x^2+1\right\rangle \end{aligned}$$

Más adelante descubriremos que este anillo cociente es de hecho isomorfo al campo de los números complejos.

Ejemplo 6.18 ($\mathbb{R}[x]$). Ahora observemos que $\langle x^2+1\rangle$ es un ideal maximal en $\mathbb{R}[x]$. Supongamos que A es un ideal de $\mathbb{R}[x]$ tal que $\langle x^2+1\rangle \subsetneq A \subseteq \mathbb{R}[x]$. Sea $f(x) \in A$ tal que $f(x) \notin \langle x^2+1\rangle$. Por el algoritmo de la división,

$$f(x) = q(x)\left(x^2+1\right) + r(x)$$

donde $\deg r(x) < 2$ y $r(x) \neq 0$ (ya que si $r(x) = 0$, $f(x) \in \langle x^2+1 \rangle$). Luego, $r(x) = ax + b$ con $a \neq 0$ o $b \neq 0$. Por cerradura

$$ax + b = f(x) - q(x)\left(x^2+1\right) \in A$$

Como A es un ideal de $\mathbb{R}[x]$,

$$(ax - b)(ax + b) = a^2x^2 - b^2 \in A$$

y

$$a^2\left(x^2+1\right) = a^2x^2 + a^2 \in A$$

porque $(x^2+1) \in A$. Una vez más por cerradura

$$\left(a^2x + a^2\right) - \left(a^2x^2 - b^2\right) = a^2 + b^2 \in A$$

Debido a que $a^2 + b^2 \in \mathbb{R}$ es distinto de cero,

$$\frac{1}{a^2+b^2}\left(a^2+b^2\right) = 1 \in A$$

Por el lema 3.7, $A = \mathbb{R}[x]$, y así $\langle x^2+1 \rangle$ es un ideal maximal.

Ejemplo 6.19 ($\mathbb{Z}_2[x]$). El ideal $\langle x^2+1 \rangle$ no es un ideal primo en $\mathbb{Z}_2[x]$, ya que

$$\begin{aligned}(x+1)(x+1) &= x^2 + 2x + 1 \\ &= x^2 + 1 \in \left\langle x^2+1 \right\rangle\end{aligned}$$

pero $x + 1 \notin \langle x^2+1 \rangle$.

Ejemplo 6.20 ($\mathbb{Z}[x]$). El ideal $\langle x \rangle$ es un ideal primo en $\mathbb{Z}[x]$ pero no es maximal. Para demostrar esto primero debemos observar que $\langle x \rangle = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$. Entonces, si $g(x)h(x) \in \langle x \rangle$ se tiene que $g(0)h(0) = 0$. Como $\mathbb{Z}$ es un dominio entero, $g(0) = 0$ o $h(0) = 0$, lo que implica que $g(x) \in \langle x \rangle$ o $h(x) \in \langle x \rangle$. Por lo tanto, $\langle x \rangle$ es primo. El ideal $\langle x \rangle$ no es maximal ya que $\langle x \rangle \subsetneq \langle x, 2 \rangle \subsetneq \mathbb{Z}[x]$. Ciertamente, $\langle x \rangle \neq \langle x, 2 \rangle$ porque $2 \in \langle x, 2 \rangle$ pero $2 \notin \langle x \rangle$. Además, $\langle x, 2 \rangle \neq \mathbb{Z}[x]$ ya que por el *ejemplo 6.16*, $1 \notin \langle x, 2 \rangle$.

Teorema 6.21. Sea F un campo. Entonces $F[x]$ es un dominio de ideales principales.

Demostración. Como F es un dominio entero, sabemos que $F[x]$ es un dominio entero por el teorema 6.6. Sea I un ideal de $F[x]$. Si $I = \{0\}$, $I = \langle 0 \rangle$. Si $I \neq \{0\}$, por el principio del buen orden existe un elemento $g(x)$ de grado mínimo en I. Mostraremos que $\langle g(x) \rangle = I$. Como $g(x) \in I$ tenemos que $\langle g(x) \rangle \subseteq I$. Tomemos ahora cualquier $f(x) \in I$. Por el algoritmo de la división

$$f(x) = g(x)\,q(x) + r(x)$$

donde $r(x) = 0$ o $\deg r(x) < \deg g(x)$. Debido a que $r(x) = f(x) - g(x)\,q(x) \in I$, y por la minimalidad del grado de $g(x)$, no puede cumplirse que $\deg r(x) < \deg g(x)$. Entonces $r(x) = 0$, y $f(x) = g(x)\,q(x) \in \langle g(x) \rangle$. Por lo tanto $I \subseteq \langle g(x) \rangle$. ■

Corolario 6.22. Sea F un campo, $I \neq \langle 0 \rangle$ un ideal y $g(x) \in F[x]$. Entonces $I = \langle g(x) \rangle$ si y sólo si $g(x) \neq 0$ es un polinomio de grado mínimo en I.

Demostración. Si $g(x) \neq 0$ es un polinomio de grado mínimo en I, la demostración del teorema 6.21 muestra que $I = \langle g(x) \rangle$. Si $I = \langle g(x) \rangle$, por reducción al absurdo supongamos que $g(x)$ no es de grado mínimo en I. Sea entonces $r(x) \neq 0$ un polinomio de grado mínimo en I. Así $r(x) = q(x)\,g(x)$ y $\deg r(x) = \deg q(x) + \deg g(x)$. Esto contradice el supuesto de que $\deg r(x) < \deg g(x)$. ■

Ejemplo 6.23. Por fin demostraremos la afirmación antes hecha de que $\mathbb{R}[x] / \langle x^2 + 1 \rangle$ es isomorfo al campo de los números complejos $\mathbb{C} = \{ai + b : a, b \in \mathbb{R}\}$. Sea $\phi_i : \mathbb{R}[x] \longrightarrow \mathbb{C}$ el homomorfismo de evaluación en $i \in \mathbb{C}$. Claramente $x^2 + 1 \in \ker \phi$, y además $x^2 + 1$ es un polinomio de grado mínimo en $\ker \phi$ (cualquier polinomio distinto de cero de la forma $ax + b$ o a en $\mathbb{R}[x]$, no resulta 0 al evaluarlo en i). Por el corolario 6.22, $\ker \phi = \langle x^2 + 1 \rangle$. Luego, debido a que ϕ_i es sobreyectivo, por el primer teorema de isomorfía tenemos que $\mathbb{C} \cong \mathbb{R}[x] / \langle x^2 + 1 \rangle$. Obviamente, otra forma de demostrar este hecho es definiendo directamente el isomorfismo $\beta(ax + b + \langle x^2 + 1 \rangle) = ai + b$.

6.4 Ejercicios

6.1. Dados $f(x)$ y $g(x)$, encuentra polinomios $q(x)$ y $r(x)$ tales que $f(x) = g(x)\,q(x) + r(x)$ con $r(x) = 0$ o $\deg r(x) < \deg g(x)$.

a) $f(x) = 5x^3 + 2x + 1$, $g(x) = x + 3$ en $\mathbb{Q}[x]$.

b) $f(x) = 5x^4 + 3x^3 + 1$, $g(x) = 3x^2 + 2x + 1$ en $\mathbb{Z}_7[x]$.

6.2. Usa el algoritmo de la división para polinomios y una adaptación del algoritmo de Euclides del apéndice A para encontrar el máximo común divisor entre $f(x) = x^5 + x^4 - 2x^3 - x^2 + x$ y $g(x) = x^3 + x - 2$ en $\mathbb{Q}[x]$. Expresa también el $mcd(f(x), g(x))$ como una combinación lineal de $f(x)$ y $g(x)$.

6.3. Sea D un dominio entero y $f(x), g(x) \in D[x]$. Demuestra que $\deg(f(x)g(x)) = \deg f(x) + \deg(g(x))$.

6.4. Sea D un dominio entero. Muestra que $D[x]^* = D^*$. Sugerencia: usa el *ejercicio 6.3*.

6.5. Demuestra el teorema del residuo.

6.6. Demuestra el teorema del factor.

6.7. Sea $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ con $a_n \neq 0$. Si r y s son dos enteros tales que $mcd(r, s) = 1$ y $f\left(\frac{r}{s}\right) = 0$, entonces $r \mid a_0$ y $s \mid a_n$. Usando este resultado, encuentra todas las raíces racionales del polinomio $f(x) = 6x^3 - 11x^2 - 3x + 2$.

6.8. Muestra que $\langle 2, x\rangle = \{f(x) \in \mathbb{Z}[x] : f(0) \text{ es par}\}$ en $\mathbb{Z}[x]$. ¿Es $\langle 2, x\rangle$ un ideal primo? ¿Es maximal? ¿Cuántos elementos hay en $\mathbb{Z}[x] / \langle 2, x\rangle$? Justifica.

6.9. Muestra que $\mathbb{Z}[x]$ no es un dominio de ideales principales. Sugerencia: usa el *ejercicio 6.8*.

6.10. Muestra que $\langle x\rangle$ es maximal en $\mathbb{Q}[x]$.

6.11. Demuestra que $\mathbb{Q}[x] / \langle x^2 - 2\rangle$ es isomorfo a $\mathbb{Q}\left[\sqrt{2}\right]$.

7

Factorización de polinomios

La única forma de aprender matemáticas es hacer matemáticas.

Richard Halmos, matemático estadounidense

En el capítulo 2, "Dominios enteros" definimos los elementos primos e irreducibles en un dominio entero. Las siguientes definiciones son las equivalentes para el caso de un dominio entero de polinomios.

Definición 7.1 (polinomio irreducible). Sea D un dominio entero. Decimos que un polinomio $p(x) \in D[x]$, $p(x) \neq 0$, es irreducible sobre D si $p(x)$ no es una unidad en $D[x]$ y si siempre que $p(x) = g(x)\,h(x)$, con $g(x), h(x) \in D[x]$, tenemos que $g(x)$ o $h(x)$ es una unidad en $D[x]$.

Definición 7.2 (polinomio reducible). Sea D un dominio entero. Decimos que un polinomio $p(x) \in D[x]$, $p(x) \neq 0$ es reducible sobre D si no es una unidad en $D[x]$ y no es irreducible sobre D.

En el *ejercicio 6.4* se pidió que se demostrara que si D es un dominio entero, entonces las unidades de $D[x]$ coinciden con las unidades de D. Si el dominio entero es un campo F, $F[x]^* = F^* = F \setminus \{0\}$, por lo que podemos decir que un polinomio no constante $p(x) \in F[x]$ es irreducible sobre F si siempre que $p(x) = g(x)\,h(x)$, $g(x), h(x) \in F[x]$ tenemos que $g(x)$ o $h(x)$ es un polinomio constante.

Ejemplo 7.3 ($\mathbb{Q}[x]$). El polinomio $p(x) = 2x^2 - 4$ es reducible sobre $\mathbb{R}$ porque $p(x) = \left(2x - 2\sqrt{2}\right)\left(x + \sqrt{2}\right)$. También, $p(x)$ es reducible sobre $\mathbb{Z}$ porque $p(x) = 2\left(x^2 - 2\right)$, donde ni 2 ni $x^2 - 2$ son unidades en $\mathbb{Z}[x]$. Más adelante desarrollaremos herramientas para demostrar que $p(x)$ es irreducible sobre $\mathbb{Q}$.

Ejemplo 7.4 ($\mathbb{R}[x]$). El polinomio $p(x) = x^2 + 4$ es irreducible sobre $\mathbb{R}$, pero es reducible sobre $\mathbb{C}$ porque $p(x) = (x + 2i)(x - 2i)$.

La importancia principal de los polinomios irreducibles es su conexión con los ideales maximales y los campos. Establecemos esta conexión en el siguiente teorema.

Teorema 7.5 ($\langle p(x) \rangle$ maximal). Sea F un campo y $p(x) \in F[x]$. Entonces $\langle p(x) \rangle$ es un ideal maximal en $F[x]$ si y sólo si $p(x)$ es irreducible sobre F.

Demostración. Supongamos primero que $\langle p(x) \rangle$ es un ideal maximal. Supongamos que $p(x) = g(x)\,h(x)$, donde $g(x), h(x) \in F[x]$. Debemos demostrar que $g(x)$ o $h(x)$ es una unidad en $F[x]$. Claramente, $\langle p(x) \rangle \subseteq \langle h(x) \rangle$ porque $h(x) \mid p(x)$ (lema

3.14). Supongamos que $\langle p(x)\rangle = \langle h(x)\rangle$. Entonces $h(x) \in \langle p(x)\rangle$ y existe $f(x) \in F[x]$, tal que $f(x)\,p(x) = h(x)$. Sustituyendo $p(x)$,

$$f(x)\,g(x)\,h(x) = h(x)$$
$$f(x)\,g(x) = 1$$

por cancelación. Luego $g(x)$ es una unidad. Supongamos ahora que $\langle p(x)\rangle \subsetneqq \langle h(x)\rangle$. Por la maximalidad de $\langle p(x)\rangle$, debemos tener que $\langle h(x)\rangle = F[x]$, lo que implica que $h(x)$ es una unidad (lema 3.14). Por lo tanto, $p(x)$ es irreducible sobre F.

Supongamos ahora que $p(x)$ es irreducible sobre F. Sea I un ideal de $F[x]$ tal que $\langle p(x)\rangle \subsetneqq I \subseteq F[x]$. Por el teorema 6.21, $F[x]$ es un dominio de ideales principales, así que $I = \langle h(x)\rangle$ para algún $h(x) \in F[x]$. Debido a que $p(x) \in I = \langle h(x)\rangle$,

$$p(x) = g(x)\,h(x)$$

para algún $h(x) \in F[x]$. Como $p(x)$ es irreducible, $g(x)$ o $h(x)$ es una unidad. Si $g(x)$ es una unidad, $p(x)$ y $h(x)$ son asociados y entonces $\langle p(x)\rangle = I$ (lema 3.14), lo cual es una contradicción. Por lo tanto, $h(x)$ es una unidad y $I = \langle h(x)\rangle = F[x]$. Esto demuestra que $\langle p(x)\rangle$ es un ideal maximal. ■

Corolario 7.6. Sea F un campo. Un polinomio $p(x) \in F[x]$ es irreducible sobre F si y sólo si $F[x]/\langle p(x)\rangle$ es un campo.

Demostración. Por el teorema 7.5, $p(x)$ es irreducible sobre F si y sólo si $\langle p(x)\rangle$ es un ideal maximal en $F[x]$. Por el teorema 4.9, el ideal $\langle p(x)\rangle$ es maximal si y sólo si $F[x]/\langle p(x)\rangle$ es un campo. ■

En el teorema 2.17 se demostró que cualquier elemento primo de un dominio entero es irreducible. Ahora veremos que para el caso de $F[x]$ también se cumple que cualquier elemento irreducible es primo (esta afirmación no es verdadera para cualquier dominio entero, véase el *ejemplo 2.19)*.

Teorema 7.7 (primos e irreducibles). Sea F un campo y $p(x) \in F[x]$ un polinomio irreducible sobre F. Entonces $p(x)$ es un elemento primo de $F[x]$.

Demostración. Por el corolario anterior sabemos que $F[x]/\langle p(x)\rangle$ es un campo, y por lo tanto un dominio entero. Por el teorema 4.8, $F[x]/\langle p(x)\rangle$ es un dominio entero si y sólo si $\langle p(x)\rangle$ es un ideal primo. Esto implica que $p(x)$ es un elemento primo de $F[x]$. ■

Ahora nos preocuparemos por saber distinguir, en la práctica, cuándo un polinomio es irreducible. Debido al teorema fundamental del álgebra (teorema 11.29) y el teorema del factor, cualquier polinomio en $\mathbb{C}[x]$ puede expresarse como un producto de polinomios lineales. Es fácil observar que estos polinomios lineales son irreducibles (si $f(x) = g(x)\,h(x)$, con $\deg f(x) = 1$, entonces $\deg g(x) = 0$ o $\deg h(x) = 0$), así que, de hecho, los polinomios lineales son los únicos polinomios irreducibles en $\mathbb{C}[x]$ (más de esto en el corolario 11.25). Para el caso de $\mathbb{R}[x]$ tenemos el siguiente resultado.

Teorema 7.8 (polinomios irreducibles sobre $\mathbb{R}$). Cualquier polinomio irreducible sobre $\mathbb{R}$ es lineal o cuadrático.

Demostración. Consideremos el polinomio

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{R}[x]$$

con $n \geq 3$. Demostraremos que $g(x)$ es reducible. Si $\beta \in \mathbb{R}$ es una raíz de $g(x)$, entonces por el teorema del factor, $(x-\beta)$ es un factor de $g(x)$. Por otro lado, si $\gamma \in \mathbb{C} \setminus \mathbb{R}$ es una raíz de $g(x)$ entonces tenemos que

$$a_n\gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_1\gamma + a_0 = 0$$

Aplicando conjugación compleja a la relación previa,

$$\begin{aligned}\overline{a_n\gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_1\gamma + a_0} &= \overline{0}\\ a_n\overline{\gamma}^n + a_{n-1}\overline{\gamma}^{n-1} + \ldots + a_1\overline{\gamma} + a_0 &= 0\end{aligned}$$

Esto último porque $\overline{z+w} = \overline{z} + \overline{w}$, y $\overline{zw} = \overline{z}\,\overline{w}$, para $z, w \in \mathbb{C}$. Así el conjugado complejo $\overline{\gamma}$ también es una raíz de $g(x)$. Esto significa que las raíces no reales de $g(x)$ ocurren en pares, y podemos obtener la factorización

$$\begin{aligned}g(x) \;=\; & a_n(x-\beta_1)\ldots\\ & (x-\beta_r)(x-\gamma_1)(x-\overline{\gamma}_1)\ldots\\ & (x-\gamma_s)(x-\overline{\gamma}_s)\end{aligned}$$

en $\mathbb{C}[x]$, donde $\beta_i \in \mathbb{R}$, $\gamma_j \in \mathbb{C} \setminus \mathbb{R}$ y $r + 2s = n$. Ahora podemos escribir

$$\begin{aligned}g(x) \;=\; & a_n(x-\beta_1)\ldots\\ & (x-\beta_r)\left(x^2 - (\gamma_1+\overline{\gamma}_1)x + \gamma_1\overline{\gamma}_1\right)\ldots\\ & \left(x^2 - (\gamma_s+\overline{\gamma}_s)x + \gamma_s\overline{\gamma}_s\right)\end{aligned}$$

la cual es una factorización en $\mathbb{R}[x]$, porque $(\gamma_1 + \overline{\gamma}_1) \in \mathbb{R}$ y $\gamma_1\overline{\gamma}_1 \in \mathbb{R}$. Como $n \geq 3$, deben aparecer por lo menos dos factores en el producto anterior. Esto implica que $g(x)$ es reducible. ■

Sin embargo, la situación no es tan sencilla en $\mathbb{Q}[x]$ o $\mathbb{Z}_p[x]$ (recordemos que $\mathbb{Z}_p$ es un campo cuando $p \in \mathbb{N}$ es un primo), ya que pueden presentarse polinomios irreducibles de grado arbitrariamente grande. El siguiente teorema es una herramienta poderosa cuando los polinomios son de grados pequeños.

Teorema 7.9. Sea F un campo y sea $f(x) \in F[x]$ tal que $\deg f(x) = 2$ o 3. Entonces $f(x)$ es reducible sobre F si y sólo si $f(x)$ tiene una raíz en F.

Demostración. Supongamos primero que $f(x)$ es reducible sobre F. Entonces $f(x) = g(x)h(x)$ para algunos $g(x), h(x) \in F[x]$ no constantes. Como $\deg f(x) = 2$ o 3 y $\deg f(x) = \deg g(x) + \deg h(x)$, necesariamente alguno de los polinomios $g(x)$ o $h(x)$ debe tener grado 1. Sin pérdida de generalidad, digamos que $g(x) = ax + b$, $a, b \in F$, $a \neq 0$. De esta manera, $-ba^{-1} \in F$ es una raíz de $g(x)$ y por lo tanto es una raíz de $f(x)$ en F.

Supongamos ahora que $\alpha \in F$ es una raíz de $f(x)$. Por el teorema del factor tenemos que $f(x) = (x - \alpha)q(x)$, donde $q(x) \in F[x]$ y $\deg q(x) = 1$ o 2. Como ni $(x - \alpha)$ ni $q(x)$ son unidades de $F[x]$, $f(x)$ es reducible sobre F. ■

El teorema anterior es especialmente útil cuando F es un campo finito, porque podemos intentar con todos los elementos del campo en búsqueda de raíces.

Ejemplo 7.10 ($\mathbb{Z}_5[x]$). El polinomio $f(x) = x^2 + 1$ es reducible sobre $\mathbb{Z}_5$ porque $f(2) = 0$ y $f(3) = 0$. Por otro lado, $f(x)$ es irreducible sobre $\mathbb{Z}_3$ porque $f(x)$ no tiene raíces en $\mathbb{Z}_3$: $f(0) = 1$, $f(1) = 2$ y $f(2) = 2$.

Ejemplo 7.11 ($\mathbb{Q}[x]$). Mostraremos que el polinomio $g(x) = x^3 + 2x^2 + 4x - 6$ es irreducible sobre $\mathbb{Q}$. Por el *ejercicio 6.7*, las posibles raíces racionales de $g(x)$ son $\pm 1, \pm 2, \pm 3, \pm 6$. Calculando cada caso observamos que $g(x)$ no tiene raíces en $\mathbb{Q}$, así que por el teorema 7.9, $g(x)$ es irreducible sobre $\mathbb{Q}$.

Ejemplo 7.12 ($\mathbb{Q}[x]$). El teorema anterior no es verdadero si el grado del polinomio es mayor que 3. Por ejemplo, el polinomio $f(x) = x^4 + 2x^2 + 1$ es reducible sobre $\mathbb{Q}$ porque $f(x) = (x^2 + 1)^2$, pero $f(x)$ no tiene raíces en $\mathbb{Q}$.

7.1 Factorización en $\mathbb{Q}[x]$ y $\mathbb{Z}[x]$

Las siguientes definiciones presentan conceptos necesarios para nuestros siguientes teoremas relacionados con la factorización de polinomios en $\mathbb{Q}[x]$ y $\mathbb{Z}[x]$.

Definición 7.13 (contenido). Sea $f(x) \in \mathbb{Z}[x]$ con $f(x) \neq 0$, donde $f(x) = a_0 + a_1x + \ldots + a_nx^n$. El contenido de $f(x)$ es el máximo común divisor de los enteros $a_0, a_1, \ldots, a_n$.

Definición 7.14 (primitivo). Decimos que un polinomio $f(x) \in \mathbb{Z}[x]$, $f(x) \neq 0$, es primitivo si su contenido es 1.

Lema 7.15 (de Gauss). El producto de dos polinomios primitivos es primitivo.

Demostración. Sean

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$$
$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_0$$

dos polinomios primitivos y supongamos que $f(x)\,g(x)$ no es primitivo. Esto significa que el contenido de $f(x)\,g(x)$ es un entero $d > 1$. Sea $p \in \mathbb{N}$ un número primo tal que $p \mid d$. Entonces p divide a todos los coeficientes de $f(x)\,g(x)$. Como $f(x)$ y $g(x)$ son primitivos, p no divide a alguno de los coeficientes de ambos polinomios. Supongamos que a_k es el primer coeficiente de $f(x)$ tal que $p \nmid a_k$, y b_j es el primer coeficiente de $g(x)$ tal que $p \nmid b_j$. Entonces, en $f(x)\,g(x)$, el coeficiente de x^{k+j} es

$$c_{k+j} = a_kb_j + \left(a_{k+1}b_{j-1} + a_{k+2}b_{j-2} + \ldots + a_{k+j}b_0\right) + \left(a_{k-1}b_{j+1} + a_{k-2}b_{j+2} + \ldots + a_0b_{j+k}\right)$$

Debido a la forma en que elegimos a a_k y b_j, sabemos que $p \mid a_{k-1}, a_{k-2}, \ldots, a_0$ y que $p \mid b_{j-1}, b_{j-2}, \ldots, b_0$, por lo que

$$p \mid \left(a_{k-1}b_{j+1} + a_{k-2}b_{j+2} + \ldots + a_0b_{j+k}\right)$$

y

$$p \mid \left(a_{k+1}b_{j-1} + a_{k+2}b_{j-2} + \ldots + a_{k+j}b_0\right)$$

Además $p \mid c_{k+j}$, así que debemos tener que $p \mid a_kb_j$. Por el lema A.13 de Euclides, $p \mid a_k$ o $p \mid b_j$, lo cual es una contradicción. Por lo tanto, $f(x)\,g(x)$ es primitivo. ■

Lema 7.16 (contenido). Sea $f(x) \in \mathbb{Z}[x]$. Supongamos que $f(x) = dg(x)$, $d \in \mathbb{N}$, $g(x) \in \mathbb{Z}[x]$. Entonces, d es el contenido de $f(x)$ si y sólo si $g(x)$ es primitivo.

Demostración. Sean

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$
$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0$$

Supongamos que d es el contenido de $f(x)$. Tenemos que $a_i = db_i$ para toda i, y que $d = mcd(a_0, \ldots, a_n)$. Por una generalización del *ejercicio A.4*, podemos obtener que $mcd(b_0, \ldots, b_n) = 1$. Por lo tanto, $g(x)$ es primitivo.

Supongamos ahora que $g(x)$ es primitivo. Demostraremos que $d = mcd(db_0, \ldots, db_n)$. Como $mcd(b_0, \ldots b_n) = 1$, entonces $1 = b_0 s_1 + \ldots + b_n s_n$ es el entero más pequeño que puede formarse con una combinación lineal de $b_0, \ldots, b_n$ (teorema A.10). Por lo tanto, el entero más pequeño que tiene la forma $db_0 s_1 + \ldots + db_1 s_n = d(b_0 s_1 + \ldots + b_n s_n)$ ocurre cuando $b_0 s_1 + \ldots + b_n s_n = 1$. Luego, $d = mcd(db_0, \ldots, db_n)$, es decir, d es el contenido de $f(x)$. ■

Observación 7.17. Si $f(x) = dg(x)$ con $d < 0$, entonces $f(x) = (-d)(-g(x))$, por lo que el lema 7.16 del contenido puede usarse con $-d$. Por lo tanto, podemos decir que si $f(x) = dg(x)$, $d \in \mathbb{Z}$, y $g(x)$ primitivo, entonces $|d|$ es el contenido de $f(x)$.

Observación 7.18. Por el lema del contenido, si d es el contenido de $f(x) \in \mathbb{Z}[x]$, tenemos que $g(x) = \frac{1}{d} f(x)$ es un polinomio primitivo.

Teorema 7.19 (reducibilidad sobre $\mathbb{Q}$). Sea $f(x) \in \mathbb{Z}[x]$. Si $f(x)$ es reducible sobre $\mathbb{Q}$ entonces $f(x)$ es reducible sobre $\mathbb{Z}$.

Demostración. Supongamos que $f(x) = g(x) h(x)$ de los cuales $g(x), h(x) \in \mathbb{Q}[x]$ no son constantes. Sin perder generalidad, podemos asumir que $f(x)$ es primitivo, ya que si no lo fuera y tuviera contenido d, el polinomio $\frac{1}{d} f(x)$ es primitivo y es reducible sobre $\mathbb{Q}$ si y sólo si $f(x)$ es reducible sobre $\mathbb{Q}$ (*ejercicio 7.5.*). Sea a el mínimo común múltiplo de los denominadores de los coeficientes de $g(x)$ y b el mínimo común múltiplo de los denominadores de los coeficientes de $h(x)$. Entonces

$$abf(x) = ag(x) \cdot bh(x)$$

donde $ag(x), bh(x) \in \mathbb{Z}[x]$. Sea c_1 el contenido de $ag(x)$ y c_2 el contenido de $bh(x)$. Por el lema 7.16, $ag(x) = c_1 g_1(x)$ y $bh(x) = c_2 h_1(x)$, donde $g_1(x), h_1(x) \in \mathbb{Z}[x]$ son primitivos. Así

$$abf(x) = c_1 c_2 g_1(x) h_1(x)$$

Como $f(x)$ es primitivo, nuevamente por el lema 7.16, el contenido de $abf(x)$ es ab. Además, por el lema 7.15 de Gauss, $g_1(x) h_1(x)$ es primitivo, así que el contenido de $c_1 c_2 g_1(x) h_1(x)$ es $c_1 c_2$. Por lo tanto, $ab = c_1 c_2$ y

$$\begin{aligned} c_1 c_2 f(x) &= c_1 c_2 g_1(x) h_1(x) \\ f(x) &= g_1(x) h_1(x) \end{aligned}$$

con $g_1(x), h_1(x) \in \mathbb{Z}[x]$. Debido a que $\deg g_1(x) = \deg g(x)$ y $\deg h_1(x) = \deg h(x)$, $g_1(x)$ y $h_1(x)$ no son constantes, por lo que $f(x)$ es reducible sobre $\mathbb{Z}$. ■

Ejemplo 7.20 ($\mathbb{Z}[x]$). Ejemplificaremos el teorema 7.19 con el polinomio

$$f(x) = \left(\frac{20}{3}x + \frac{10}{3}\right)\left(\frac{3}{2}x - \frac{3}{5}\right) = 10x^2 + x - 2 \in \mathbb{Z}[x]$$

En este caso $g(x) = \frac{20}{3}x + \frac{10}{3}$ y $h(x) = \frac{3}{2}x - \frac{3}{5}$ son polinomios en $\mathbb{Q}[x]$. El mínimo común múltiplo de los denominadores de $g(x)$ es $a = 3$ y el de los denominadores de $h(x)$ es $b = 10$. Entonces, los polinomios $3g(x) = 20x + 10$ y $10h(x) = 15x - 6$ están en $\mathbb{Z}[x]$. El contenido de $3g(x)$ es $c_1 = 10$ y el contenido de $10h(x)$ es $c_2 = 3$. Así

$$3g(x) = 10(2x + 1) \text{ y } 10h(x) = 3(5x - 2)$$

donde $g_1(x) = 2x + 1$ y $g_2(x) = 5x - 2$ son primitivos. Por lo tanto

$$\begin{aligned} abf(x) &= c_1 c_2 g_1(x) g_2(x) \\ 3 \cdot 10 \cdot f(x) &= 10 \cdot 3(2x + 1)(5x - 2) \end{aligned}$$

Y finalmente

$$f(x) = (2x + 1)(5x - 2)$$

Una de las consecuencias más importantes del teorema 7.19 es el criterio de Eisenstein, el cual nos permite determinar en algunos casos la irreducibilidad de un polinomio de grado arbitrariamente grande.

Teorema 7.21 (criterio de Eisenstein). Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Si existe un primo p tal que $p \nmid a_n$, $p \mid a_i$, $0 \leq i < n$ y $p^2 \nmid a_0$ entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

Demostración. Supongamos que $f(x)$ es reducible sobre $\mathbb{Q}$. Por el teorema 7.19 sabemos que $f(x)$ entonces reducible sobre $\mathbb{Z}$, es decir, que existen polinomios no constantes $g(x)$, $h(x) \in \mathbb{Z}[x]$ tales que $f(x) = g(x)\,h(x)$. Digamos por ejemplo, que

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0 \text{ con } 1 \leq m < n$$
$$h(x) = c_r x^r + c_{r-1}x^{r-1} + \ldots + c_0 \text{ con } 1 \leq r < n$$

Como $p \mid a_0 = b_0 c_0$ pero $p^2 \nmid a_0$, tenemos que p divide a b_0 o c_0 pero no divide a ambos. Supongamos que $p \mid b_0$ y $p \nmid c_0$. Como $p \nmid a_n = b_m c_r$, tenemos que $p \nmid b_m$. Ahora bien, sea t el entero más pequeño tal que $p \nmid b_t$. Consideremos

$$a_t = b_t c_0 + b_{t-1}c_1 + \ldots + b_0 c_t$$

Por hipótesis, $p \mid a_t$ y, por la elección de t, $p \mid b_{t-1}, \ldots, b_0$, así que $p \mid (b_{t-1}c_1 + \ldots + b_0 c_t)$. Por lo tanto, $p \mid b_t c_0$, pero $p \nmid c_0$ y $p \nmid b_t$, lo cual es una contradicción con el lema A.13 de Euclides. ■

Ejemplo 7.22 ($\mathbb{Q}[x]$). El polinomio $f(x) = 25x^5 - 9x^4 - 3x^2 - 12$ es irreducible sobre $\mathbb{Q}$. Para comprobar esto usemos el criterio de Eisenstein con $p = 3$: veamos que $3 \nmid 25$, $3 \mid 9$, $3 \mid 3$ y $3 \mid 12$, pero $3^2 \nmid 12$.

Ejemplo 7.23 ($\mathbb{Q}[x]$). El polinomio $f(x) = x^5 + 2x^3 + \frac{8}{7}x^2 - \frac{4}{7}x + \frac{2}{7}$ es irreducible sobre $\mathbb{Q}$, porque el polinomio $7f(x) = 7x^5 + 14x^3 + 8x^2 - 4x + 2$ satisface el criterio de Eisenstein con $p = 2$ (véase el *ejercicio 7.5.*).

Ejemplo 7.24 ($\mathbb{Q}[x]$). Para cualquier primo p, el polinomio

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

es irreducible sobre $\mathbb{Q}$. A este polinomio se le llama el polinomio ciclotómico de orden p. Para demostrar esta afirmación, sea

$$\begin{aligned} f(x) = \Phi_p(x-1) &= \frac{(x-1)^p - 1}{(x-1) - 1} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + p \end{aligned}$$

Como todos los coeficientes excepto el primero son divisibles entre p, y el último coeficiente no es divisible entre p^2, por el criterio de Eisenstein $f(x)$ es irreducible sobre $\mathbb{Q}$. Así, por el *ejercicio 7.5* $\Phi_p(x)$ es irreducible sobre $\mathbb{Q}$.

Teorema 7.25 (irreducibilidad sobre $\mathbb{Z}_p$). Sea p un primo y sea

$$f(x) \in \mathbb{Z}[x]$$

con $\deg f(x) \geq 1$. Sea $\overline{f}(x) \in \mathbb{Z}_p[x]$ el polinomio obtenido de reducir los coeficientes de $f(x)$ módulo p. Si $\overline{f}(x)$ es irreducible sobre $\mathbb{Z}_p$ y $\deg \overline{f}(x) = \deg f(x)$ entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

Demostración. Por reducción al absurdo, supongamos que $f(x)$ es reducible sobre $\mathbb{Q}$. Entonces, por el teorema de reducibilidad sobre $\mathbb{Q}$, existen polinomios no constantes $g(x), h(x) \in \mathbb{Z}[x]$ tales que $f(x) = g(x)h(x)$. Sean $\overline{f}(x)$, $\overline{g}(x)$ y $\overline{h}(x)$ los polinomios obtenidos de $f(x)$, $g(x)$ y $h(x)$ al reducir sus coeficientes módulo p. Como $\deg f(x) = \deg \overline{f}(x)$, entonces

$$\deg \overline{g}(x) \leq \deg g(x) < \deg \overline{f}(x)$$
$$\deg \overline{h}(x) \leq \deg h(x) < \deg \overline{f}(x)$$

Como $\deg \overline{g}(x) + \deg \overline{h}(x) = \deg \overline{f}(x) = \deg g(x) + \deg h(x)$, tenemos que $\deg \overline{g}(x) = \deg g(x)$ y $\deg \overline{h}(x) = \deg h(x)$. Por el *ejercicio 7.3*, $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ (ya que $\phi(f(x)) = \overline{f}(x)$ es un homomorfismo), lo cual contradice el supuesto de que $\overline{f}(x)$ es irreducible sobre $\mathbb{Z}_p$. ■

Para simplificar notación, si $[a] \in \mathbb{Z}_p$ simplemente escribiremos a.

Ejemplo 7.26. Sea $f(x) = 21x^3 - 3x^2 + 2x + 9$. Sobre $\mathbb{Z}_2$, tenemos que $\overline{f}(x) = x^3 + x^2 + 1$ es irreducible, porque $\overline{f}(0) = 1$ y $\overline{f}(1) = 1$. Por lo tanto, $f(x)$ es irreducible sobre $\mathbb{Q}$.

Ejemplo 7.27. Debemos usar cuidadosamente el teorema 7.25. Por ejemplo, si $f(x) = 21x^3 - 3x^2 + 2x + 8$, en $\mathbb{Z}_2[x]$, $\overline{f}(x) = x^3 + x^2 = x^2(x+1)$ es un polinomio reducible. Sin embargo, el teorema no asegura nada en estos casos; no es posible concluir con esto que $f(x)$ sea reducible sobre $\mathbb{Q}$. Observemos que en $\mathbb{Z}_5$, el polinomio $\overline{f}(x) = x^3 + 2x^2 + 2x + 3$ no tiene raíces, así que por el teorema 7.9 y el teorema 7.25, $f(x)$ es irreducible sobre $\mathbb{Q}$.

Ejemplo 7.28. Sea $f(x) = 7x^4 + 10x^3 - 2x^2 + 4x - 5$. Demostraremos que $f(x)$ es irreducible sobre $\mathbb{Q}$. En $\mathbb{Z}_2[x]$, $\overline{f}(x) = x^4 - 1 = (x^2 - 1)(x^2 + 1)$, el cual es reducible sobre $\mathbb{Z}_2$. Trabajemos ahora en $\mathbb{Z}_3[x]$. Primero, tenemos que $\overline{f}(x) = x^4 + x^3 + x^2 + x + 1$. Este polinomio no tiene factores lineales porque $\overline{f}(0) = 1$, $\overline{f}(1) = 2$ y $\overline{f}(2) = 1$. Sin embargo, aún puede tener factores cuadráticos. Supongamos que

$$\overline{f}(x) = \left(x^2 + ax + bx\right)\left(x^2 + cx + d\right)$$

Igualando coeficientes obtenemos que

$$\begin{array}{llll} 1) & a + c = 1 & 2) & b + ac + d = 1 \\ 3) & bd = 1 & 4) & ad + bc = 1 \end{array}$$

Como $bd = 1$ por 3), tenemos que $b = d = 1$ o $b = d = -1$. Suponiendo que ambos son 1, de 2) obtenemos que $ac = -1$, así que $a = \pm 1$ y $c = \mp 1$. En cualquier caso, $a + c = 0$, lo que contradice 1). Suponiendo ahora que $b = d = -1$, entonces $ac = 0$ por 2). Si $a = 0$, entonces $c = 1$ por 1), y $1 = ad + bc = b$, por 4), lo cual es una contradicción. Si $c = 0$, $a = 1$ y $1 = ad + bc = d$ es otra vez una contradicción. Por lo tanto, la factorización propuesta de $\overline{f}(x)$ no puede existir y $\overline{f}(x)$ es irreducible sobre $\mathbb{Z}_3$. Por el teorema 7.25, $f(x)$ es irreducible sobre $\mathbb{Q}$.

7.2 Ejercicios

7.1. Responde lo siguiente:

a) ¿Es $x^2 + x + 1$ irreducible sobre $\mathbb{Z}_2$?

b) ¿Es $x^3 + 2x + 3$ irreducible sobre $\mathbb{Z}_5$? Exprésalo como producto de polinomios irreducibles en $\mathbb{Z}_5[x]$.

7.2. Demuestra que el polinomio $f(x) = x^3 + 2x^2 - 3x + 5$ es irreducible sobre $\mathbb{Q}$.

7.3. Sea m un entero positivo fijo. Muestra que la función $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_m[x]$ definida como

$$\begin{aligned} & \phi\left(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0\right) \\ = \; & [a_n]x^n + [a_{n-1}]x^{n-1} + \ldots + [a_0] \end{aligned}$$

donde $[a] \in \mathbb{Z}_m$, es un homomorfismo de anillos.

7.4. Muestra lo siguiente usando el lema del contenido:

a) Todo polinomio no constante de $\mathbb{Z}[x]$ que es irreducible sobre $\mathbb{Z}$ es primitivo.

b) Si $f(x) \in \mathbb{Z}[x]$ es un polinomio primitivo tal que $f(x) = g(x)\,h(x), g(x), h(x) \in \mathbb{Z}[x]$, entonces $g(x)$ y $h(x)$ son primitivos.

7.5. Sea F un campo y $a \in F$, $a \neq 0$. Muestra que:

a) $af(x)$ es irreducible sobre F si y sólo si $f(x)$ es irreducible sobre F.

b) $f(ax)$ es irreducible sobre F si y sólo si $f(x)$ es irreducible sobre F.

c) $f(x + a)$ es irreducible sobre F si y sólo si $f(x)$ es irreducible sobre F.

7.6. Usando el test de irreducibilidad módulo p demuestra que el polinomio $f(x) = 4x^4 - 2x^2 + x - 5$ es irreducible sobre $\mathbb{Q}$.

7.7. Usa el criterio de Eisenstein para mostrar que los siguientes polinomios son irreducibles sobre $\mathbb{Q}$.

a) $f(x) = x^5 + 5x^2 + 15x - 10$.

b) $g(x) = x^3 + 3x^2 + \frac{6}{5}x + \frac{12}{5}$.

c) $h(x) = 8x^3 - 6x + 1$. Sugerencia: usa la parte c) del *ejercicio 7.5*.

7.8. Supongamos que $f(x) \in \mathbb{Z}_p[x]$ es irreducible sobre $\mathbb{Z}_p$, donde p es primo. Si $\deg f(x) = n$, demuestra que $\mathbb{Z}_p[x] / \langle f(x) \rangle$ es un campo con p^n elementos.

7.9. Sea F un campo y $p(x)$ un polinomio irreducible sobre F. Si E es un campo que contiene a F y existe un elemento $a \in E$ tal que $p(a) = 0$, muestra que el homomorfismo de evaluación en a, $\phi_a : F[x] \to E$, tiene kernel $\langle p(x) \rangle$.

7.10. Muestra que $\langle x^2 + 1 \rangle$ es un ideal primo en $\mathbb{Z}[x]$ pero no maximal en $\mathbb{Z}[x]$.

8

Más de dominios enteros

Las matemáticas no mienten, lo que hay son muchos matemáticos mentirosos.

David Thoreau, filósofo estadounidense

Para concluir con nuestro estudio de los anillos, estudiaremos un poco más a fondo tres dominios enteros especiales: los dominios de ideales principales, los dominios de factorización única y los dominios euclidianos.

8.1 Dominios de ideales principales

Definimos un dominio de ideales principales como un dominio entero en el que todos sus ideales son principales. Ya hemos trabajado un poco con este tipo de dominios; demostramos que $\mathbb{Z}$, $\mathbb{Z}_p$ y $F[x]$, donde F es un campo, son todos dominios de ideales principales (*ejemplo 3.12*, *ejemplo 3.13* y teorema 6.21).

Ejemplo 8.1. Un campo F es un dominio de ideales principales porque sus únicos ideales son $\langle 0 \rangle$ y $F = \langle 1 \rangle$ (*ejercicio 4.5.*).

La demostración del siguiente teorema es muy similar a la del teorema 7.5. Por tal motivo, la demostración se deja como ejercicio.

Teorema 8.2. En un dominio de ideales principales D, el elemento $p \in D$ es irreducible si y sólo si $\langle p \rangle$ es maximal.

Demostración. *Ejercicio 8.2.* ■

Corolario 8.3. En un dominio de ideales principales D, un ideal es primo si y sólo si es maximal.

Demostración. Por el *ejercicio 4.6*, todo ideal maximal es primo en cualquier anillo conmutativo con identidad. Supongamos que $I = \langle p \rangle$ es un ideal primo de D. Por la proposición 3.22, $p \in D$ es un elemento primo, así que es irreducible por el teorema 2.17. Por el teorema anterior, $I = \langle p \rangle$ es un ideal maximal. ■

En general, sabemos que en cualquier dominio entero todo elemento primo es irreducible. Sin embargo, en un dominio de ideales principales ambos conceptos son equivalentes. La demostración del siguiente teorema es muy similar a la del teorema 7.7, y por tal motivo se deja como ejercicio.

Teorema 8.4 (primos e irreducibles). En un dominio de ideales principales, un elemento es irreducible si y sólo si es primo.

Demostración. *Ejercicio 8.4.* ■

Definición 8.5 (Noetheriano). Decimos que un anillo conmutativo R es Noetheriano si cualquier cadena creciente de ideales $I_1 \subseteq I_2 \subseteq \ldots$ se estabiliza; es decir, si existe $k \in \mathbb{N}$ tal que $I_k = I_j$ para toda $j \geq k$.

Finalmente, demostraremos el siguiente lema, el cual nos será de gran utilidad posteriormente.

Lema 8.6. Cualquier dominio de ideales principales es Noetheriano.

Demostración. Sea D un dominio de ideales principales y

$$I_1 \subseteq I_2 \subseteq \ldots$$

una cadena creciente de ideales. Sea

$$I = \bigcup I_i$$

Es sencillo demostrar que I es un ideal (*ejercicio 8.4.*). Como D es de ideales principales, debemos tener que $I = \langle a \rangle$ para algún $a \in D$. Claramente, $a \in I$, así que $a \in I_k$ para algún índice k. De esta manera, si $x \in I = \langle a \rangle$, entonces $x = ra$, $r \in R$, y luego $x = ra \in I_k$. Así $I \subseteq I_k$. Debido a que

$$I_i \subseteq I \subseteq I_k \text{ para todo índice } i$$

debemos tener que $I = I_k$, y por lo tanto la cadena se estabiliza porque $I_k = I_j$ para toda $j \geq k$. ■

8.2 Dominios de factorización única

Definición 8.7 (dominio de factorización única). Un dominio entero D es un dominio de factorización única si satisface que:

1) Cualquier elemento $a \in D \setminus D^*$, $a \neq 0$, puede escribirse como el producto finito de elementos irreducibles de D.
2) Si $a = p_1 \ldots p_s = q_1 \ldots q_r$, con p_i y q_i irreducibles, entonces $s = r$ y es posible reordenar los elementos p_i de tal forma que p_i y q_i sean asociados.

Ejemplo 8.8 ($\mathbb{Z}$). Los enteros $\mathbb{Z}$, por el teorema fundamental de la aritmética, son un dominio de factorización única. Observemos que, por ejemplo

$$12 = (2)(2)(3) = (-2)(2)(-3)$$

donde 2 es asociado de -2 y 3 es asociado de -3.

Teorema 8.9. Todo dominio de ideales principales es un dominio de factorización única.

Demostración. Sea D un dominio de ideales principales y $a \in D \setminus D^*$, $a \neq 0$. Mostraremos que se cumplen las propiedades 1) y 2) de la definición de dominio de factorización única.

1) Si a es irreducible no hay nada que hacer, así que supongamos que a no es irreducible. Primero mostraremos que a tiene por lo menos un factor irreducible. Sabemos que $a = b_1a_1$ donde $a_1, b_1 \in D \setminus D^*$, $a_1 \neq 0$, $b_1 \neq 0$. Por el lema 3.14 de ideales principales, $\langle a\rangle \subseteq \langle a_1\rangle$. Si a_1 es irreducible, entonces demostramos lo que queríamos, ya que a_1 es factor de a. Si a_1 no es irreducible, $a_1 = b_2a_2$ donde $a_2, b_2 \in D \setminus D^*$, $a_2 \neq 0$, $b_2 \neq 0$. Otra vez, por el lema 3.14, $\langle a_1\rangle \subseteq \langle a_2\rangle$. Continuando este procedimiento obtenemos una cadena creciente de ideales

$$\langle a\rangle \subseteq \langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \dots$$

la cual debe estabilizarse por el lema 8.6. Supongamos que la cadena se estabiliza en $\langle a_k\rangle$. Demostraremos que a_k es irreducible. Por reducción al absurdo, supongamos que a_k no es irreducible, así que $a_k = b_{k+1}a_{k+1}$ donde $a_{k+1}, b_{k+1} \in D \setminus D^*$, $a_{k+1} \neq 0$, $b_{k+1} \neq 0$. Entonces $\langle a_k\rangle \subseteq \langle a_{k+1}\rangle$, y $\langle a_k\rangle = \langle a_{k+1}\rangle$ ya que la cadena se estabiliza en $\langle a_k\rangle$. Por el lema 3.14, a_k y a_{k+1} son asociados, así que $a_k = ua_{k+1}$ con $u \in D^*$. Luego $ua_{k+1} = b_{k+1}a_{k+1}$, y $u = b_{k+1}$, lo que contradice que b_{k+1} no es una unidad. Como $\langle a\rangle \subseteq \langle a_k\rangle$, a_k es un factor irreducible de a. Esto demuestra que cualquier elemento distinto de cero que no es unidad tiene un factor irreducible.

Ahora, podemos escribir $a = p_1c_1$ donde $p_1 = a_k$ es irreducible y $c_1 \in D \setminus D^*$ (observemos que si $c_1 \in D^*$, $p_1 = ac_1^{-1} = b_1a_1c_1^{-1}$, lo que contradice que p_1 es irreducible). Luego, $\langle a\rangle \subseteq \langle c_1\rangle$. Si c_1 es irreducible, a es un producto de irreducibles. En caso contrario, $c_1 = p_2c_2$ donde p_2 es irreducible y $c_2 \in D \setminus D^*$. Así $\langle c_1\rangle \subseteq \langle c_2\rangle$. Continuando este procedimiento obtenemos una cadena creciente de ideales

$$\langle a\rangle \subseteq \langle c_1\rangle \subseteq \langle c_2\rangle \subseteq \dots$$

La cual debe estabilizarse por el lema 8.6. Supongamos que la cadena se estabiliza en $\langle c_r\rangle$. Por el mismo argumento que en el párrafo anterior, c_r debe ser irreducible. Por lo tanto, $a = p_1p_2 \dots p_rc_r$ es un producto de elementos irreducibles.

2) Supongamos que

$$a = p_1 \dots p_s = q_1 \dots q_r$$

donde q_j y p_i son irreducibles para toda j, i. Sin perder generalidad, supongamos que $s \leq r$. Como D es de ideales principales, por el teorema 8.4 sabemos que p_1 es también un elemento primo, así que $p_1 \mid q_1 \dots q_r$ implica que $p_1 \mid q_k$ para algún índice k. Reordenando si es necesario, podemos asumir que $k = 1$, así que $p_1 \mid q_1$. De esta forma, $q_1 = u_1 p_1$ con $u_1 \in D$. Debido a que q_1 es irreducible y p_1 no es una unidad, $u_1 \in D^*$. Esto implica que p_1 y q_1 son asociados. Luego, por cancelación

$$p_2 \dots p_s = u_1 q_2 \dots q_r$$

Ahora $p_2 \mid u_1 q_2 \dots q_r$, así que $p_2 \mid q_t$ para algún índice t (no es posible que $p_2 \mid u_1$ ya que $u_1 = p_2 c$, $c \in D$, implica que $1 = p_2 \left(c u_1^{-1}\right)$, y $p_2 \in D^*$, lo cual es una contradicción). Reordenando si es necesario, podemos asumir que $t = 2$, así que $p_2 \mid q_2$ y $q_2 = u_2 p_2$ con $u_2 \in D^*$. Luego

$$p_3 \dots p_s = u_1 u_2 q_3 \dots q_r$$

Continuando este proceso, finalmente llegamos a que

$$1 = u_1 u_2 \dots u_s q_{s+1} \dots q_r$$

Como los q_i son irreducibles (y por lo tanto no son unidades), la igualdad anterior sólo es posible cuando $r = s$.

■

Corolario 8.10. Sea F un campo. Entonces $F[x]$ es un dominio de factorización única.

Ejemplo 8.11. Un campo F es un dominio de factorización única porque es un dominio de ideales principales.

El siguiente teorema nos da un ejemplo importante de un dominio de factorización única que no es de ideales principales (véase *ejercicio 6.9.*).

Teorema 8.12. $\mathbb{Z}[x]$ es un dominio de factorización única.

Demostración. Sea $f(x) \in \mathbb{Z}[x]$, donde $f(x)$ no es ni cero ni una unidad. Si $\deg f(x) = 0$, entonces $f(x)$ es constante y, por el teorema fundamental de la aritmética (teorema A.15), $f(x)$ puede factorizarse de manera única en elementos irreducibles de $\mathbb{Z}$. Supongamos que $\deg f(x) > 0$. Demostraremos que se cumplen las dos propiedades de la definición de dominios de factorización única.

1) Sea $b \in \mathbb{Z}$ el contenido de $f(x)$. Ahora es posible factorizar b como un producto de elementos irreducibles en $\mathbb{Z}$, digamos $b = b_1 \dots b_s$. Entonces, por el lema 7.16 del contenido,

$$f(x) = b_1 \dots b_s f_1(x)$$

donde $f_1(x)$ es un polinomio primitivo y

$$\deg f(x) = \deg f_1(x).$$

Por lo tanto, para demostrar que existe una factorización en irreducibles de $f(x)$ basta con demostrar que existe una factorización en irreducibles para el primitivo $f_1(x)$. Procederemos por inducción sobre el grado de $f_1(x)$. Sea $\deg f_1(x) = 1$. Si $f_1(x) = g(x)h(x)$ debemos tener que $\deg g(x) = 0$ o $\deg h(x) = 0$. Por el *ejercicio 7.4 (b)*, $g(x)$ y $h(x)$ son primitivos. Como las únicas constantes primitivas son las unidades 1 y -1, concluimos que $f_1(x)$ es irreducible.

Supongamos que si $\deg f_1(x) < k$, entonces $f_1(x)$ puede escribirse como el producto de irreducibles. Sea $\deg f_1(x) = k$. Si $f_1(x)$ es irreducible no hay nada que hacer, así que supongamos que $f_1(x)$ es reducible. Luego, $f_1(x) = g(x)h(x)$ donde $g(x)$ y $h(x)$ son primitivos y $\deg g(x), \deg h(x) < k = \deg f_1(x)$. Por hipótesis de inducción, $g(x)$ y $h(x)$ pueden escribirse como el producto de irreducibles, así que $f_1(x)$ también es el producto de irreducibles.

2) Supongamos que

$$f(x) = b_1 \dots b_s p_1(x) \dots p_m(x) = c_1 \dots c_t q_1(x) \dots q_n(x)$$

donde las b's y c's son constantes irreducibles y los polinomios $p_i(x)$ y $q_j(x)$ son irreducibles de grado mayor a 0. Sin perder generalidad, supongamos también que $n \leq m$. Sea $b = b_1 \dots b_s$ y $c = c_1 \dots c_t$. Por el *ejercicio 7.4 (a)*, los polinomios $p_i(x)$ y $q_j(x)$ son primitivos, y por el lema 7.15 de Gauss los productos $p_1(x) \dots p_m(x)$ y $q_1(x) \dots q_n(x)$ son

primitivos. El lema 7.16 del contenido implica que $|b| = |c|$, así que por el teorema A.15 fundamental de la aritmética tenemos que $s = t$ y $b_i = \pm c_i$. Cancelando obtenemos que

$$p_1(x) \dots p_m(x) = \pm q_1(x) \dots q_n(x)$$

Considerando los polinomios $p_i(x)$ y $q_j(x)$ como elementos de $\mathbb{Q}[x]$, sabemos que al ser irreducibles, son primos por el teorema 7.7. De esta forma, si $p_1(x) \mid q_1(x) \dots q_n(x)$, entonces $p_1(x) \mid q_k(x)$ para algún k. Reordenando, podemos suponer que $k = 1$. Así $q_1(x) = d(x)\, p_1(x)$ con $d(x) \in \mathbb{Q}[x]$. Como $q_1(x)$ es irreducible, y $p_1(x)$ no es una unidad, debemos tener que $d(x)$ es una unidad, así que $d(x) = \frac{y}{z}$, $y, z \in \mathbb{Z}$, $z \neq 0$. Sin embargo, $p_1(x)$ y $q_1(x)$ son primitivos, así que el lema 7.16 del contenido implica que $\frac{y}{z} = \pm 1$. Por lo tanto $q_1(x) = \pm p_1(x)$. Cancelando

$$p_2(x) \dots p_m(x) = \pm q_2(x) \dots q_n(x)$$

Repitiendo este proceso n veces obtenemos que

$$p_{n+1}(x) \dots p_m(x) = \pm 1$$

Como $p_{n+1}(x), \dots, p_m(x)$ no son unidades, la igualdad anterior sólo tiene sentido si $m = n$.

■

El teorema 8.12 puede generalizarse; de hecho, si D es un dominio de factorización única, entonces $D[x]$ es un dominio de factorización única.

Ejemplo 8.13 ($\mathbb{Z}\left[\sqrt{-5}\right]$). El dominio entero $\mathbb{Z}[\sqrt{-5}]$ no es de factorización única. Para demostrar esto definimos una función $N : D \setminus \{0\} \longrightarrow \mathbb{N}_0$ como $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Por la proposición 2.18, sabemos que $N(xy) = N(x)\, N(y)$ para toda $x, y \in \mathbb{Z}[\sqrt{-5}]$ y que $N(x) = 1$ si y sólo si x es una unidad. Observemos que los únicos elementos $x \in \mathbb{Z}[\sqrt{-5}]$ tales que $N(x) = 1$ son 1 y -1, por lo que las únicas unidades en $\mathbb{Z}[\sqrt{-5}]$ son 1 y -1. Consideremos las factorizaciones

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) \end{aligned}$$

Demostraremos que 2, 3 y $(1 \pm \sqrt{-5})$ son irreducibles, lo cual implica que la factorización de 6 en irreducibles en $\mathbb{Z}[\sqrt{-5}]$ no es única, porque $1 \pm \sqrt{-5}$ no es asociado de 2 ni de 3.

Supongamos que $2 = xy$, donde $x, y \in \mathbb{Z}[\sqrt{-5}]$ no son unidades. Entonces $N(2) = 4 = N(x)N(y)$. Como $N(x), N(y) \neq 1$, debemos tener que $N(x) = N(y) = 2$. Sin embargo, esto es imposible porque la ecuación

$$N\left(a + b\sqrt{-5}\right) = a^2 + 5b^2 = 2$$

no tiene soluciones con $a, b \in \mathbb{Z}$. Luego, 2 es irreducible. De manera similar, si $3 = xy$ donde ni x ni y son unidades, tenemos que $N(3) = 9 = N(x)N(y)$ y $N(x) = N(y) = 3$. Sin embargo, la ecuación

$$a^2 + 5b^2 = 3$$

no puede satisfacerse con enteros. Finalmente, si $1 \pm \sqrt{-5} = xy$ donde ni x ni y son unidades,

$$N\left(1 \pm \sqrt{-5}\right) = 6 = N(x)N(x)$$

Entonces $N(x) = 2$ o $N(x) = 3$, lo cual siempre lleva a una contradicción.

8.3 Dominios euclidianos

Definición 8.14 (dominio euclidiano). Un dominio entero D es llamado dominio euclidiano si existe una función $d : D \setminus \{0\} \to \mathbb{N}_0$ tal que

1) $d(a) \leq d(ab)$ para cualquier $a, b \in D \setminus \{0\}$.
2) Si $a, b \in D$, $b \neq 0$, existen elementos $q, r \in D$ tales que $a = qb + r$, donde $r = 0$ o $d(r) < d(b)$.

La función $d : D \setminus \{0\} \longrightarrow \mathbb{N}_0$ es llamada norma euclidiana.

Ejemplo 8.15 ($\mathbb{Z}$). Los enteros son un dominio euclidiano. Definamos $d : \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0$ como $d(a) = |a|$ para toda $a \in \mathbb{Z} \setminus \{0\}$. Veamos que d cumple con la definición de norma euclidiana. Claramente

$$|a| \leq |a|\,|b| = |ab|$$

para toda $a, b \in \mathbb{Z} \setminus \{0\}$, así que la primera propiedad se cumple. Para verificar la segunda propiedad, observemos que si $b > 0$, el

algoritmo de la división (teorema A.6) garantiza que para cualquier $a \in \mathbb{Z}$ existen $q, r \in \mathbb{Z}$ tales que

$$a = qb + r \text{ con } 0 \leq r < b$$

Si $b < 0$, entonces $-b > 0$ y podemos usar el algoritmo de la división para encontrar $q, r \in \mathbb{Z}$ tales que

$$a = q(-b) + r \text{ con } 0 \leq r < -b$$

Por lo que, tomando $q' = -q$

$$a = q'b + r \text{ con } 0 \leq r < -b$$

Podemos juntar ambos casos en uno solo diciendo que para cualquier $a, b \in \mathbb{Z}$, $b \neq 0$, existen $q, r \in \mathbb{Z}$ tales que

$$a = qb + r \text{ con } r = 0 \text{ ó } |r| < |b|$$

Ejemplo 8.16 (F). Cualquier campo F es un dominio euclidiano. Simplemente hay que definir $d(x) = 1$, para toda $x \in F \setminus \{0\}$. Claramente, $d(a) \leq d(ab)$ para toda $a, b \in F \setminus \{0\}$. Además si $a, b \in F$, $b \neq 0$, podemos tomar $q = ab^{-1}$ y $r = 0$, de tal forma que $a = qb + r$.

Ejemplo 8.17 ($F[x]$). Si F es un campo, $F[x]$ es un dominio euclidiano. Definamos la norma euclidiana d como $d(f(x)) = \deg f(x)$, para todo $f(x) \in F[x] \setminus \{0\}$. Por el *ejercicio 6.3*,

$$\deg f(x) \leq \deg f(x) + \deg g(x) = \deg f(x) g(x)$$

para cualquier $g(x) \neq 0$. Además, por el algoritmo de la división para polinomios (teorema 6.8), para cualquier $f(x), g(x) \in F[x]$, $g(x) \neq 0$ existen polinomios $q(x), r(x) \in F[x]$ tales que

$$f(x) = g(x) q(x) + r(x)$$

con

$$r(x) = 0 \quad \text{o} \quad \deg r(x) < \deg g(x)$$

Ejemplo 8.18 ($\mathbb{Z}[i]$). Los enteros gaussianos $\mathbb{Z}[i]$ son un dominio euclidiano con la norma euclidiana d definida como $d(a + bi) = a^2 + b^2$, con $a, b \in \mathbb{Z}$. Por la proposición 2.18, sabemos que $d(xy) = d(x) d(y)$ para toda $x, y \in \mathbb{Z}[i]$. De esta manera

$$d(x) \leq d(x) d(y) = d(xy)$$

Demostraremos ahora la segunda propiedad de la definición. Sean $x = a + bi$ y $y = c + di$, $y \neq 0$, $a, b, c, d \in \mathbb{Z}$. Entonces,

$$\begin{aligned}\frac{x}{y} &= \frac{a+bi}{c+di}\frac{c-di}{c-di} \\ &= \frac{ac+bd+(bc-ad)\,i}{c^2+d^2} \\ &= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \in \mathbb{Q}[i]\end{aligned}$$

Sean

$$s = \frac{ac+bd}{c^2+d^2} \text{ y } t = \frac{bc-ad}{c^2+d^2}$$

Entonces

$$\frac{x}{y} = s + ti,$$

donde $t, s \in \mathbb{Q}$. Sea m el entero más cercano a s, y n el entero más cercano a t. Así

$$\begin{aligned}|m-s| \leq \frac{1}{2} &\rightarrow (m-s)^2 \leq \frac{1}{4} \\ |n-t| \leq \frac{1}{2} &\rightarrow (n-t)^2 \leq \frac{1}{4}\end{aligned}$$

Además

$$\begin{aligned}\frac{x}{y} = s + ti &= (m-m+s) + (n-n+t)\,i \\ &= (m+ni) + [(s-m) + (t-n)\,i]\end{aligned}$$

Multiplicando por y obtenemos

$$x = (m+ni)\,y + [(s-m) + (t-n)\,i]\,y$$

Sean $q = m + ni$ y $r = [(s-m) + (t-n)\,i]\,y$. Claramente, $q \in \mathbb{Z}[i]$, y $r = x - qy \in \mathbb{Z}[i]$ por cerradura. Luego, si $r \neq 0$

$$\begin{aligned}d(r) &= d([(s-m) + (t-n)\,i])\,d(y) \\ &= \left[(s-m)^2 + (t-n)^2\right] d(y) \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right) d(y) < d(y)\end{aligned}$$

Por lo tanto, para cualquier $x, y \in \mathbb{Z}[i]$, $y \neq 0$, existen $q, r \in \mathbb{Z}[i]$ tales que

$$x = qy + r \text{ con } r = 0 \text{ o } d(r) < d(y)$$

Teorema 8.19. Todo dominio euclidiano es un dominio de ideales principales.

Demostración. Sea D un dominio euclidiano y d su norma euclidiana. Sea I un ideal de D. Si $I = \{0\}$, entonces $I = \langle 0 \rangle$ es un ideal principal. Supongamos que $I \neq \{0\}$. Sea $b \in I$ tal que $b \neq 0$ y tal que $d(b)$ sea un elemento mínimo del conjunto $\{d(x) : x \in I \setminus \{0\}\}$ (esto es posible por el principio del buen orden). Demostraremos que $I = \langle b \rangle$. Claramente $\langle b \rangle \subseteq I$. Sea $a \in I$. Por la segunda propiedad de la definición de dominios euclidianos, existen $q, r \in D$ tales que

$$a = qb + r \text{ con } r = 0 \text{ o } d(r) < d(b)$$

Observemos que

$$r = a - qb \in I$$

porque $a, b \in I$. Por lo tanto, que $d(r) < d(b)$ es imposible por la minimalidad de $d(b)$ entre las normas de los elementos de I. Luego $r = 0$, y $a = qb \in \langle b \rangle$. Esto demuestra que $I = \langle b \rangle$. ■

Corolario 8.20. Todo dominio euclidiano es un dominio de factorización única.

Hasta ahora hemos demostrado que

$$\text{D.E.} \rightarrow \text{D.I.P.} \rightarrow \text{D.F.U.}$$

donde D.E. significa dominio euclidiano, D.I.P. significa dominio de ideales principales y D.F.U. significa dominio de factorización única. Sin embargo, las implicaciones opuestas no se cumplen; es decir, existen D.F.U. que no son D.I.P., y existen D.I.P. que no son D.E. Es difícil encontrar un ejemplo de este último caso. Sin embargo, como lo demostró el argentino Óscar Campoli, el dominio $\mathbb{Z}[\alpha] = \{a + \alpha b : a, b \in \mathbb{Z}\}$ con $\alpha = \frac{1+\sqrt{-19}}{2}$ es un dominio de ideales principales que no es un dominio euclidiano (véase Campoli, 1999).

8.4 Ejercicios

8.1. Si U es el conjunto de todos los dominios enteros, realiza un diagrama de Venn donde se muestren los siguientes subconjuntos de U: los dominios de factorización única, los dominios de ideales principales, los dominios euclidianos y los campos. Da un ejemplo de un dominio entero en cada región del diagrama.

8.2. Demuestra que en un dominio de ideales principales D, el elemento $p \in D$ es irreducible si y sólo si $\langle p \rangle$ es maximal.

8.3. Demuestra que si $I_1 \subseteq I_2 \subseteq \ldots$ es una cadena de ideales de un anillo conmutativo R, entonces $I = \bigcup I_i$ es un ideal de R.

8.4. Demuestra que en un dominio de ideales principales, un elemento es irreducible si y sólo si es primo.

8.5. Demuestra, sin usar el lema de Zorn, que en un dominio Noetheriano todo ideal está contenido en un ideal maximal.

8.6. Sea D un dominio euclidiano y d su norma euclidiana. Muestra que:

a) $u \in D$ es una unidad si y sólo si $d(u) = d(1)$.

b) Si $a, b \in D$ son asociados entonces $d(a) = d(b)$.

8.7. Usando como guía el ejemplo 8.18, encuentra $q, r \in \mathbb{Z}[i]$ tales que $5 - 4i = (3 + 2i)q + r$, donde $r = 0$ o $d(r) < d(5 - 4i)$.

8.8. En $\mathbb{Z}[i]$,

a) Muestra que $1 - i$ es irreducible.

b) Muestra que 3 es irreducible.

c) Muestra que 5 no es irreducible.

8.9. Demuestra que $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de factorización única.

8.10. Demuestra que en un dominio de factorización única D, $p \in D$ es irreducible si y sólo si p es primo.

8.11. Demuestra que un dominio D es Noetheriano si y sólo si cualquier ideal I de D es generado por un número finito de elementos.

Parte II

Campos

Las ciencias matemáticas particularmente exhiben orden, simetría y limitación; y esas son las más grandes formas de la belleza.

Aristóteles, filósofo griego

9

El campo de las fracciones

Caballeros, esto es sin duda cierto, es absolutamente paradójico; no podemos comprenderlo y no sabemos lo que significa, pero lo hemos demostrado y, por lo tanto, sabemos que debe ser verdad.

Charles Sanders Peirce, lógico estadounidense

Desde el capítulo 1, "Propiedades básicas de los anillos", definimos un campo como un anillo conmutativo con identidad y con división. En este capítulo estudiaremos más a fondo este tipo de estructuras algebraicas y sus propiedades principales.

Aunque un dominio entero como $\mathbb{Z}$ tiene muchas propiedades interesantes (es conmutativo, tiene un elemento identidad, no tiene divisores de cero, etc.), no podemos dividir sus elementos. Sin embargo, sabemos que $\mathbb{Z}$ está contenido en un campo: el campo de los números racionales $\mathbb{Q}$, el cual está formado por las fracciones de los elementos de $\mathbb{Z}$. Es decir

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

Tomando como ejemplo esta construcción podemos demostrar que dado cualquier dominio entero D es isomorfo a un subdominio contenido en un campo F, el cual es llamado el campo de las fracciones de D.

Lo primero que hay que hacer es considerar el siguiente subconjunto del producto cartesiano

$$A = \{(a, b) : a, b \in D, b \neq 0\} \subset D \times D$$

y la relación $\sim$ definida sobre A como $(a, b) \sim (c, d)$ si $ad = bc$.

Proposición 9.1. La relación $\sim$ definida anteriormente sobre A es una relación de equivalencia.

Demostración. Verifiquemos las propiedades:

1) *Reflexiva.* $(a, b) \sim (a, b)$, porque $ab = ba$ en D.
2) *Simétrica.* Si $(a, b) \sim (c, d)$, $ad = bc$, lo que implica que $cb = da$, por lo que $(c, d) \sim (a, b)$.
3) *Transitiva.* Si $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$, entonces $ad = bc$ y $cf = de$. Multiplicando la primera ecuación por f

$$\begin{aligned} adf &= bcf \\ (af)\, d &= b\,(de) \\ (af)\, d &= (be)\, d \\ af &= be \end{aligned}$$

por lo que $(a, b) \sim (e, f)$.

■

Denotemos como

$$\frac{a}{b}$$

a la clase de equivalencia que contiene a (a, b)

$$\frac{a}{b} = \{(c, d) \in A : (a, b) \sim (c, d)\}$$

y sea

$$F = \left\{ \frac{a}{b} : (a, b) \in A \right\}$$

Este conjunto F será nuestro campo de fracciones. La suma y multiplicación sobre F están definidas de la siguiente forma, para cualquier

$$\frac{a}{b}, \frac{c}{d} \in F,$$

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

Proposición 9.2. Las operaciones de suma y multiplicación definidas previamente sobre F están bien definidas.

Demostración. Supongamos que

$$\frac{a}{b} = \frac{a'}{b'} \text{ y } \frac{c}{d} = \frac{c'}{d'}$$

Entonces $ab' = a'b$ y $cd' = c'd$, por definición. Ahora veamos que

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

y

$$\frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'}$$

Debido a que

$$\begin{aligned}(a'd' + b'c')\, bd &= (a'b)\, dd' + (c'd)\, bb' \\ &= (ab')\, dd' + (cd')\, bb' \\ &= (ad + bc)\, b'd'\end{aligned}$$

tenemos que

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

De manera similar,

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

Luego,

$$\begin{aligned}(ac)\,(b'd') &= (ab')\,(cd') \\ &= (a'b)\,(c'd) \\ &= (bd)\,(a'c')\end{aligned}$$

por lo que

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

■

Teorema 9.3. El conjunto F, junto con la suma y multiplicación, previamente definidas, forman un campo.

Demostración. Es necesario verificar que se cumplen todas las propiedades de un campo. Se deja como ejercicio (*ejercicio 9.1*) demostrar que tanto la suma como la multiplicación sobre F son conmutativas y cumplen la propiedad distributiva. Claramente, la identidad aditiva es $\frac{0}{1}$ y la identidad multiplicativa es $\frac{1}{1}$. El inverso aditivo de $\frac{a}{b} \in F$ es $\frac{-a}{b} \in F$ ya que

$$\begin{aligned}\frac{a}{b} + \frac{-a}{b} &= \frac{ab - ab}{b^2} \\ &= \frac{0}{b^2} \\ &= \frac{0}{1}\end{aligned}$$

Si $\frac{a}{b} \neq \frac{0}{1}$, entonces $a \neq 0$, y su inverso multiplicativo es $\frac{b}{a} \in F$,

$$\begin{aligned}\frac{a}{b}\frac{b}{a} &= \frac{ab}{ba} \\ &= \frac{1}{1}\end{aligned}$$

porque $1ab = 1ba$. Finalmente, para cualquier $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3} \in F$ la asociatividad de la suma se cumple

$$\begin{aligned}\left(\frac{a_1}{b_1}+\frac{a_2}{b_2}\right)+\frac{a_3}{b_3} &= \frac{a_1b_2+a_2b_1}{b_1b_2}+\frac{a_3}{b_3}\\ &= \frac{(a_1b_2+a_2b_1)\,b_3+a_3\,(b_1b_2)}{(b_1b_2)\,b_3}\\ &= \frac{a_1\,(b_2b_3)+b_1\,(a_2b_3+a_3b_2)}{b_1\,(b_2b_3)}\\ &= \frac{a_1}{b_1}+\frac{a_2b_3+a_3b_2}{b_2b_3}\\ &= \frac{a_1}{b_1}+\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right)\end{aligned}$$

y la asociatividad de la multiplicación se cumple

$$\begin{aligned}\left(\frac{a_1}{b_1}\frac{a_2}{b_2}\right)\frac{a_3}{b_3} &= \frac{(a_1a_2)\,a_3}{(b_1b_2)\,b_3}\\ &= \frac{a_1\,(a_2a_3)}{b_1\,(b_2b_3)}\\ &= \frac{a_1}{b_1}\left(\frac{a_2}{b_2}\frac{a_3}{b_3}\right)\end{aligned}$$

■

Teorema 9.4. F contiene un subdominio isomorfo a D.

Demostración. Definamos la función $\beta : D \longrightarrow F$ como

$$\beta\,(a) = \frac{a}{1}.$$

Demostraremos que se trata de un homomorfismo de anillos inyectivo. Claramente β está bien definida porque si $a = b$, entonces

$$\frac{a}{1} = \frac{b}{1}.$$

Veamos que para $a, b \in D$

$$\begin{aligned}\beta\,(a+b) &= \frac{a+b}{1}\\ &= \frac{a}{1}+\frac{b}{1}\\ &= \beta\,(a)+\beta\,(b)\end{aligned}$$

y

$$\begin{aligned}\beta(ab) &= \frac{ab}{1} \\ &= \frac{a}{1}\frac{b}{1} \\ &= \beta(a)\,\beta(b)\end{aligned}$$

Además, β es inyectivo porque si $\beta(a) = \beta(b)$, entonces

$$\frac{a}{1} = \frac{b}{1},$$

lo que implica que $a1 = 1b$. De esta manera, $\beta(D)$ es un subdominio de F isomorfo a D. ■

Ejemplo 9.5. Tomando $D = \mathbb{Z}[x]$, entonces el campo de las fracciones de $\mathbb{Z}[x]$ es

$$\left\{\frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{Z}[x], g(x) \neq 0\right\}$$

En particular, si D es un dominio entero, el campo de las fracciones de $D[x]$ se denotará como $D(x)$.

Ejemplo 9.6. Sea p un primo. Entonces

$$\mathbb{Z}_p(x) = \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0\right\}$$

es un campo infinito de característica p. Para demostrar esto observemos que

$$\begin{aligned}p \cdot \frac{f(x)}{g(x)} &= \frac{f(x)}{g(x)} + \ldots + \frac{f(x)}{g(x)} \\ &= \frac{p \cdot f(x)}{g(x)} \\ &= \frac{0}{g(x)} = 0\end{aligned}$$

Además es claro que $\mathbb{Z}_p(x)$ es infinito porque $\mathbb{Z}_p[x]$ lo es.

Teorema 9.7. Sea D un dominio entero y F el campo de las fracciones de D. Si E es un campo tal que $D \subseteq E$, entonces F es isomorfo a un subcampo de E.

Demostración. Definamos $\phi : F \longrightarrow E$ como $\phi\left(\frac{a}{b}\right) = ab^{-1}$ donde $\frac{a}{b} \in F$. Demostraremos que ϕ es un homomorfismo inyectivo. Primero, para mostrar que ϕ está bien definido, supongamos que $\frac{a}{b} = \frac{c}{d}$. Entonces $ad = bc$, lo que implica que $ab^{-1} = cd^{-1}$. También

$$\begin{aligned}\phi\left(\frac{a}{b} + \frac{c}{d}\right) &= \phi\left(\frac{ad + bc}{bd}\right) \\ &= (ad + bc)\,(bd)^{-1} \\ &= adb^{-1}d^{-1} + bcb^{-1}d^{-1} \\ &= ab^{-1} + cd^{-1} \\ &= \phi\left(\frac{a}{b}\right) + \phi\left(\frac{c}{d}\right)\end{aligned}$$

y de manera similar,

$$\begin{aligned}\phi\left(\frac{a}{b}\frac{c}{d}\right) &= \phi\left(\frac{ac}{bd}\right) \\ &= ac\,(bd)^{-1} \\ &= \left(ab^{-1}\right)\left(cd^{-1}\right) \\ &= \phi\left(\frac{a}{b}\right)\phi\left(\frac{c}{d}\right)\end{aligned}$$

Finalmente, supongamos que $\phi\left(\frac{a}{b}\right) = \phi\left(\frac{c}{d}\right)$, entonces

$$\begin{aligned}ab^{-1} &= cd^{-1} \\ ad &= cb\end{aligned}$$

y luego

$$\frac{a}{b} = \frac{c}{d}.$$

Por lo tanto, $\phi(F)$ es un subcampo de E isomorfo a F. ■

En otras palabras, el teorema anterior asegura que el campo de las fracciones de D es el campo más pequeño que contiene a D.

9.1 Ejercicios

9.1. Sea D un dominio entero y F el conjunto de las fracciones de D. Demuestra que la suma y multiplicación definidas en este capítulo sobre F son ambas conmutativas. Demuestra además que se cumple la propiedad distributiva.

9.2. Demuestra que el anillo de las fracciones de $\mathbb{Z}[i]$ es isomorfo a $\mathbb{Q}[i] = \{x + iy : x, y \in \mathbb{Q}\}$.

9.3. Sea D un dominio entero. Decimos que un subconjunto $S \subset D$ es un sistema multiplicativo si $1 \in S$, $0 \notin S$, y si S es cerrado bajo la multiplicación en D. Sea I un ideal de D. Demuestra que I es primo si y sólo si $D \setminus I$ es un sistema multiplicativo.

9.4. Sea D un dominio entero y S un sistema multiplicativo. Demuestra que el conjunto $S^{-1}D = \left\{\frac{a}{b} : a \in D, b \in S\right\}$ es un subdominio del campo de las fracciones de D. Llamamos a $S^{-1}D$ la localización de D con respecto a S.

9.5. Decimos que un dominio entero D es un dominio local si D tiene un único ideal maximal. Demuestra que D es un dominio local con ideal maximal M si y sólo si $D^* = D \setminus M$ para algún ideal M de D. Sugerencia: usa el teorema 3.25, recuerda también que D^* es el grupo de unidades de D.

9.6. Sea D un dominio entero y sea I un ideal primo de D. Sea $S = D \setminus I$. Demuestra que $S^{-1}D$ es un dominio local con ideal maximal $S^{-1}I$. Sugerencia: usa el *ejercicio 9.5*.

9.7. Sea $p \in \mathbb{Z}$ un número primo y sea $S = \mathbb{Z} \setminus \langle p \rangle$. Describe el dominio local $S^{-1}\mathbb{Z}$ y su único ideal maximal.

10

Extensiones de campos

No se preocupen por sus problemas en matemáticas. Puedo asegurarles que los míos son mayores.

Albert Einstein, físico alemán

El concepto de campo fue usado por primera vez implícitamente por los matemáticos Henrik Abel y Évariste Galois a principios del siglo XIX. Sin embargo, hasta 1893 Heinrich M. Weber dio la primera definición de campo abstracto. Gran parte de la teoría de campos fue desarrollada más tarde por Ernst Steinitz y Emil Artin.

Los objetos de estudio principales de la teoría de campos son las extensiones de campos. La idea principal detrás de una extensión de campo es, a partir de un campo dado, obtener un nuevo campo "más grande" que contenga algunas propiedades adicionales.

Definición 10.1 (extensión de campo). Sean F y E campos. Decimos que E es una extensión de campo de F si existe un homomorfismo inyectivo $\phi : F \to E$.

Observemos que si E es una extensión de campo de F, entonces F es isomorfo al subcampo $\phi(F)$ de E. Por tal motivo, podríamos decir que E es una extensión de campo de F si y sólo si F es isomorfo a un subcampo de E. Muchas veces incluso identificaremos a F con $\phi(F)$, y supondremos que $F \subseteq E$.

Ejemplo 10.2 ($\mathbb{C}$). El campo de los números complejos $\mathbb{C}$ es una extensión de campo de los reales $\mathbb{R}$. Asimismo, $\mathbb{C}$ y $\mathbb{R}$ son extensiones de campos de $\mathbb{Q}$.

Ejemplo 10.3 ($F(x)$). Sea F un campo. Entonces el campo de las fracciones de $F[x]$ denotado como $F(x)$ es una extensión de campo de F. El homomorfismo inyectivo $\phi : F \longrightarrow F(x)$ puede definirse como $\phi(a) = \frac{a}{1}$ para toda $a \in F$. Obviamente, $F(x)$ no es una extensión de campo de $F[x]$ porque este último anillo no es un campo.

El teorema fundamental de la teoría de campos fue demostrado por el matemático alemán Leopold Kronecker en 1887. A grandes rasgos, el teorema afirma que todo polinomio no constante tiene una raíz en algún campo.

Teorema 10.4 (teorema fundamental de la teoría de campos). Sea F un campo y $f(x) \in F[x]$ un polinomio no constante. Entonces existe una extensión de campo E de F tal que $f(x)$ tiene una raíz en E.

Demostración. Sea $p(x) \in F[x]$ un factor irreducible de $f(x)$. Bastará con demostrar que existe una extensión de campo E de F donde $p(x)$ tenga una raíz. Debido a la irreducibilidad de $p(x)$, el ideal

$\langle p(x)\rangle$ es maximal en $F[x]$ (teorema 7.5), así que $F[x]/\langle p(x)\rangle$ es un campo. Demostraremos primero que $F[x]/\langle p(x)\rangle$ es una extensión de campo de F. Para esto definamos la función $\varphi : F \longrightarrow F[x]/\langle p(x)\rangle$ como $\varphi(a) = a + \langle p(x)\rangle$, con $a \in F$. Claramente, φ es un homomorfismo. Además, φ es inyectivo porque si $\varphi(a) = \varphi(b)$, $a, b \in F$, entonces $a - b \in \langle p(x)\rangle$. Por lo tanto, $a - b = q(x)\,p(x)$ para algún $q(x) \in F[x]$. Sin embargo, como $\deg p(x) \geq 1$, la relación anterior sólo es posible si $a - b = 0$, y $a = b$. Así, por definición, $E = F[x]/\langle p(x)\rangle$ es una extensión de campo de F. Observemos que $F \cong \varphi(F) = \{a + \langle p(x)\rangle : a \in F\} \subseteq E$.

Para demostrar que $p(x)$ tiene una raíz en E supongamos que

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \text{ donde } a_i \in F$$

Identificando F con $\varphi(F)$, podemos considerar los coeficientes de $p(x)$ como elementos de $\varphi(F)$. De esta forma, si $\alpha = x + \langle p(x)\rangle$,

$$\begin{aligned} p(\alpha) &= (a_n + \langle p(x)\rangle)(x + \langle p(x)\rangle)^n + \\ &\quad (a_{n-1} + \langle p(x)\rangle)(x + \langle p(x)\rangle)^{n-1} + \ldots + (a_0 + \langle p(x)\rangle) \\ &= (a_n x^n + \langle p(x)\rangle) + \left(a_{n-1}x^{n-1} + \langle p(x)\rangle\right) + \ldots \\ &\quad + (a_0 + \langle p(x)\rangle) \\ &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle \end{aligned}$$

Luego, $\alpha \in E$ es una raíz de $p(x) \in F[x]$. ■

Corolario 10.5. Sea F un campo y $f(x) \in F[x]$ un polinomio de grado $\deg f(x) = n > 0$. Entonces existe una extensión de campo E de F tal que $f(x)$ tiene exactamente n raíces en E.

Demostración. La demostración será por inducción sobre n. Si $n = 1$, el polinomio $f(x) = a_1 x + a_0$ tiene una raíz en F (la cual es $-a_1^{-1}a_0 \in F$). Supongamos que el corolario se cumple para $n = k \in \mathbb{N}$. Sea $n = k + 1$. Por el teorema fundamental de la teoría de campos, $f(x)$ tiene una raíz α en una extensión de campo E de F. Por el teorema del factor, $f(x) = (x - \alpha)\,g(x)$ para $g(x) \in E[x]$, $\deg g(x) = k$. Por hipótesis de inducción, existe una extensión de campo K de E en la cual $g(x)$ tiene exactamente k raíces. Por lo tanto, $f(x)$ tiene exactamente $k + 1$ raíces en K. ■

Ejemplo 10.6 ($\mathbb{R}[x]$). El polinomio $f(x) = x^2 + 1 \in \mathbb{R}[x]$ no tiene raíces sobre $\mathbb{R}$. De acuerdo con el teorema fundamental de la teoría de campos, $f(x)$ tiene raíz $\alpha = x + \langle x^2 + 1\rangle$ en $\mathbb{R}[x] / \langle x^2 + 1\rangle$;

$$\begin{aligned} f(\alpha) &= \left(x + \left\langle x^2 + 1\right\rangle\right)^2 + \left(1 + \left\langle x^2 + 1\right\rangle\right) \\ &= x^2 + 1 + \left\langle x^2 + 1\right\rangle = 0 + \left\langle x^2 + 1\right\rangle \end{aligned}$$

Por el *ejemplo* 6.23, sabemos que $\mathbb{R}[x] / \langle x^2 + 1\rangle$ es isomorfo a $\mathbb{C}$, y el elemento $x + \langle x^2 + 1\rangle$ en $\mathbb{R}[x] / \langle x^2 + 1\rangle$ corresponde a i en $\mathbb{C}$.

Ejemplo 10.7 ($\mathbb{Z}_3[x]$). Sea $f(x) = x^4 + 2x^2 + 1 \in \mathbb{Z}_3[x]$. Su factorización en irreducibles es $f(x) = (x^2 + 1)^2$ por lo que $f(x)$ tiene una raíz en el campo $\mathbb{Z}_3[x] / \langle x^2 + 1\rangle$ con nueve elementos (véase *ejercicio 7.8.*).

Ejemplo 10.8 ($\mathbb{Z}_3[x]$). Consideremos el polinomio

$$f(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$$

Como $\deg f(x) = 3$ y $f(x)$ no tiene raíces en $\mathbb{Z}_3$, es irreducible sobre $\mathbb{Z}_3$. Así, el teorema fundamental de la teoría de campos nos dice que $\beta = x + \langle x^3 + 2x + 1\rangle$ es una raíz de $f(x)$ en $E = \mathbb{Z}_3[x] / \langle x^3 + 2x + 1\rangle$. Ahora podemos descomponer a $f(x)$ en factores lineales en $E[x]$. Identifiquemos las clases laterales

$$a + \left\langle x^3 + 2x + 1\right\rangle \in E$$

con los elementos $a \in \mathbb{Z}_3$. Además, sabemos que $\beta^3 + 2\beta + 1 = 0$. Por el teorema del factor, $x - \beta$ es un factor de $f(x)$, así que dividimos

$$\begin{array}{r|l} & x^2 + \beta x + (2 + \beta^2) \\ \hline x - \beta & x^3 + 2x + 1 \\ & -x^3 + \beta x^2 \\ \hline & \beta x^2 + 2x + 1 \\ & -\beta x^2 + \beta^2 x \\ \hline & (2 + \beta^2)x + 1 \\ & -(2 + \beta^2)x + 2\beta + \beta^3 \\ \hline & \beta^3 + 2\beta + 1 = 0 \end{array}$$

Luego,

$$\begin{aligned} x^2 + \beta x + \left(2 + \beta^2\right) &= x^2 - 2\beta x + \left(\beta^2 - 1\right) \\ &= \left(x^2 - 2\beta x + \beta^2\right) - 1 \\ &= (x - \beta)^2 - 1 \\ &= (x - \beta - 1)(x - \beta + 1) \end{aligned}$$

Por lo tanto en E,

$$f(x) = (x - \beta)(x - \beta - 1)(x - \beta + 1)$$

10.1 Elementos algebraicos y trascendentes

Si E es una extensión de campo de F, dividimos los elementos de E en dos categorías: los algebraicos y los trascendentes sobre F.

Definición 10.9 (elemento algebraico). Sea E una extensión de campo F y $\alpha \in E$. Decimos que α es un elemento algebraico sobre F si existe un polinomio $f(x) \in F[x]$ distinto de cero tal que $f(\alpha) = 0$.

Definición 10.10 (elemento trascendente). Sea E una extensión de campo de F y $\alpha \in E$. Decimos que α es un elemento trascendente sobre F si no es algebraico sobre F.

En 1744, Leonhard Euler fue el primero en hacer la distinción entre estos dos tipos de elementos; sin embargo, fue hasta 1844, cien años después, cuando Joseph Liouville pudo demostrar la existencia de elementos trascendentes sobre $\mathbb{Q}$.

Ejemplo 10.11 ($\mathbb{Q}$). Debido a que $\sqrt{2} \in \mathbb{R}$ es raíz del polinomio $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, tenemos que $\sqrt{2}$ es un elemento algebraico sobre $\mathbb{Q}$. También, $i \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$ porque es raíz de $g(x) = x^2 + 1 \in \mathbb{Q}[x]$.

Ejemplo 10.12 ($\mathbb{Q}$). Los números π, $e \in \mathbb{R}$ son trascendentes sobre $\mathbb{Q}$. Demostrar este hecho no es tan sencillo; puede consultarse (1983), por ejemplo, para encontrar una demostración sobre la trascendencia de e. Hasta la fecha no se sabe si $\pi + e$ es trascendente sobre $\mathbb{Q}$, lo cual puede darnos una idea de las complicaciones que pueden surgir en este tipo de demostraciones. Sin embargo, notemos que ambos números, π y e, son algebraicos sobre $\mathbb{R}$ ya que son raíces de los polinomios $f(x) = x - \pi \in \mathbb{R}[x]$ y $g(x) = x - e \in \mathbb{R}[x]$.

Ejemplo 10.13 ($\mathbb{Q}$). Es sencillo demostrar que $\sqrt{2+\sqrt{3}} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$. Sea $\alpha = \sqrt{2+\sqrt{3}}$. Entonces $\alpha^2 = 2+\sqrt{3}$ y $(\alpha^2-2)^2 = 3$. Luego, $\alpha^4 - 4\alpha^2 + 1 = 0$, por lo que α es raíz del polinomio $f(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$.

Ahora presentaremos una nueva forma de construir un campo.

Observación 10.14. Al igual que la intersección de grupos o de anillos, la intersección de campos es un campo.

Definición 10.15 (subcampo generado). Sea E una extensión de campo de F y A un subconjunto de E. Sea

$$Int = \{K \text{ es un campo} : F \subseteq K \subseteq E\}$$

el conjunto de campos intermedios entre F y E. Definimos al subcampo generado por A sobre F como

$$F(A) = \bigcap_{K \in Int,\ A \subseteq K} K$$

En otras palabras, $F(A)$ es el subcampo de E más pequeño que contiene a F y A.

Si el subconjunto $A = \{a_1, \ldots, a_n\}$ es finito nosotros escribimos $F(a_1, \ldots, a_n)$ en lugar de $F(\{a_1, \ldots, a_n\})$ para representar al subcampo generado por A sobre F.

Ejemplo 10.16. Dada cualquier extensión de campo E de F, por definición tenemos que $F(\emptyset) = F$ y $F(E) = E$. Además, es obvio que si $\alpha \in F$, $F(\alpha) = F$.

Teorema 10.17 (subcampo generado). Sea E una extensión de campo de F y $A \subseteq E$. Entonces $F(A) = H$, donde H consiste en elementos de la forma $\frac{\alpha}{\beta} \in E$, donde α y $\beta \neq 0$ son combinaciones lineales finitas con coeficientes en F de productos finitos de los elementos de A.

Demostración. Primero demostraremos que H es un subcampo de E. Sean $x, y \in H$, $x = \frac{\alpha_1}{\beta_1}$ y $y = \frac{\alpha_2}{\beta_2}$. Entonces

$$x - y = \frac{\alpha_1\beta_2 - \alpha_2\beta_1}{\beta_1\beta_2} \in H$$

ya que tanto el numerador como el denominador son combinaciones lineales de elementos de A. De manera similar

$$\frac{x}{y} = \frac{\alpha_1\beta_2}{\alpha_2\beta_1} \in H$$

Lo que muestra que H es un subcampo. Claramente $A \subseteq H$ y $F \subseteq H$, así que $F(A) \subseteq H$ porque $F(A)$ es el subcampo más pequeño que contiene a A y F.

Además, por cerradura, si α es una combinación lineal finita con coeficientes en F de productos finitos de elementos de A, entonces $\alpha \in F(A)$. Por lo tanto, $\frac{\alpha}{\beta} \in F(A)$ y $H \subseteq F(A)$. ■

Corolario 10.18. Sea E una extensión de campo de F y $\alpha \in E$. Entonces

$$F(\alpha) = \left\{ \frac{a_n\alpha^n + \ldots + a_0}{b_m\alpha^m + \ldots + b_0} : a_i, b_j \in F, b_m \neq 0, n, m \in \mathbb{N} \right\}$$

En particular, denotamos al conjunto de combinaciones lineales finitas de potencias de $\alpha \in E$ con coeficientes en F como

$$F[\alpha] = \left\{ a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 : a_i \in F,\ n \in \mathbb{N} \right\}$$

De hecho, es fácil demostrar que $F[\alpha]$ es un dominio entero, y por lo tanto puede verse a $F(\alpha)$ como el campo de las fracciones de $F[\alpha]$.

Ejemplo 10.19 ($\mathbb{Q}(\pi)$). Consideremos a $\mathbb{R}$ como extensión de $\mathbb{Q}$. Entonces

$$\mathbb{Q}(\pi) = \left\{ \frac{a_n\pi^n + \ldots + a_0}{b_m\pi^m + \ldots + b_0} : a_i, b_j \in \mathbb{Q},\ b_m \neq 0, n, m \in \mathbb{N} \right\}$$

Ejemplo 10.20 ($\mathbb{Q}\left(\sqrt{2}\right)$). Por el corolario anterior,

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{ \frac{a_n\left(\sqrt{2}\right)^n + \ldots + a_0}{b_m\left(\sqrt{2}\right)^m + \ldots + b_0} : a_i, b_j \in \mathbb{Q},\ b_m \neq 0, n, m \in \mathbb{N} \right\}$$

Observemos que para cualquier potencia par $\left(\sqrt{2}\right)^{2k} = 2^k$, con $k \in \mathbb{Z}$, y que para cualquier potencia impar $\left(\sqrt{2}\right)^{2k+1} = 2^k\sqrt{2}$. Así podemos reescribir el conjunto anterior como

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{ \frac{a_1 + a_2\sqrt{2}}{b_1 + b_2\sqrt{2}} : a_i, b_i \in \mathbb{Q},\ b_1 \neq 0 \text{ o } b_2 \neq 0 \right\}$$

Racionalizando el denominador

$$\frac{a_1 + a_2\sqrt{2}}{b_1 + b_2\sqrt{2}} \frac{b_1 - b_2\sqrt{2}}{b_1 - b_2\sqrt{2}} = \frac{(a_1 b_1 + 2a_2 b_2) + (a_2 b_1 - a_1 b_2)\sqrt{2}}{b_1^2 - 2b_2^2}$$
$$= \frac{(a_1 b_1 + 2a_2 b_2)}{b_1^2 - 2b_2^2} + \frac{(a_2 b_1 - a_1 b_2)}{b_1^2 - 2b_2^2}\sqrt{2}$$

Por la irracionalidad de $\sqrt{2}$, $b_1^2 - 2b_2^2 = 0$ si y sólo si $b_1 = 0$ y $b_2 = 0$. Pero esto nunca ocurre en el conjunto $\mathbb{Q}\left(\sqrt{2}\right)$, así que

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$$

En los siguientes teoremas desarrollaremos las herramientas necesarias para describir con precisión el campo $F(\alpha)$, sabiendo de antemano si α se trata de un elemento algebraico o trascendente sobre F. El siguiente teorema aborda el segundo caso.

Teorema 10.21. Sea E una extensión de campo de F y $\alpha \in E$. Si α es trascendente sobre F entonces $F(x) \cong F(\alpha)$.

Demostración. Consideremos el homomorfismo de evaluación $\phi_\alpha : F[x] \longrightarrow F[\alpha]$ como $\phi_\alpha(f(x)) = f(\alpha)$. Como α es trascendente, el único polinomio tal que $p(\alpha) = 0$ es $p(x) = 0$. Así, $\ker \phi_\alpha = \{0\}$ y ϕ_α es inyectivo. Además, ϕ_α es sobreyectivo porque la preimagen de $a_n\alpha^n + \ldots + a_0 \in F[\alpha]$ es $a_n x^n + \ldots + a_0 \in F[x]$. Luego, $F[x] \cong F[\alpha]$, lo que implica que sus respectivos campos de fracciones son isomorfos, es decir $F(x) \cong F(\alpha)$. ■

Ejemplo 10.22. Puesto que π es trascendente sobre $\mathbb{Q}$, tenemos que $\mathbb{Q}(x) \cong \mathbb{Q}(\pi)$.

Ahora nos enfocaremos en el caso de los elementos algebraicos.

Teorema 10.23 (polinomio mínimo). Si α es algebraico sobre un campo F, entonces existe un único polinomio mónico irreducible $p(x) \in F[x]$ tal que $p(\alpha) = 0$.

Demostración. Sea $\phi_\alpha : F[x] \longrightarrow F[\alpha]$ el homomorfismo de evaluación. En este caso, $\ker \phi_\alpha \neq \{0\}$ porque existe al menos un polinomio $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Como $F[x]$ es un dominio de ideales principales, debemos tener que $\ker \phi_\alpha = \langle p(x) \rangle$, con $p(x) \in F[x]$. Demostraremos que $p(x)$ es irreducible. Por el corolario 6.22, $p(x)$ es un polinomio de grado mínimo en $\ker \phi_\alpha$. Supongamos que $p(x) = q(x)\, r(x)$, donde $0 < \deg q(x), \deg r(x) <$

$\deg p(x)$. Entonces $p(\alpha) = 0$ implica que $q(\alpha) r(\alpha) = 0$. Como $F[\alpha]$ es un dominio entero, $q(\alpha) = 0$ o $r(\alpha) = 0$, lo que contradice en cualquier caso que $p(x)$ es un polinomio de grado mínimo en $\ker \phi_\alpha$. Luego, $p(x)$ es irreducible. Además, es claro que podemos suponer que $p(x)$ es mónico, ya que si $a_n \neq 1$ es el coeficiente principal de $p(x)$, entonces $\frac{1}{a_n} p(x)$ es mónico e irreducible.

Para demostrar la unicidad de $p(x)$, supongamos que $q(x) \in F[x]$ es un polinomio mónico irreducible tal que $q(\alpha) = 0$. Entonces, $q(x) \in \ker \phi_\alpha = \langle p(x) \rangle$, por lo que $q(x) = g(x) p(x)$ para algún $g(x) \in F[x]$. Por la irreducibilidad de $q(x)$ debemos tener que $g(x) = a \in F$ es una unidad de $F[x]$. Luego, $q(x) = ap(x)$, y como ambos $p(x)$ y $q(x)$ son mónicos, $a = 1$. ■

Definición 10.24 (polinomio mínimo). Sea α un elemento algebraico sobre F. El único polinomio mónico irreducible $p(x) \in F[x]$ tal que $p(\alpha) = 0$ es llamado el polinomio mínimo de α sobre F.

Definición 10.25 (grado de un elemento algebraico). El grado de un elemento algebraico α sobre F es el grado del polinomio mínimo de α sobre F.

Ejemplo 10.26. El polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $p(x) = x^2 - 2$, ya que $p(x)$ es un polinomio mónico irreducible sobre $\mathbb{Q}$ tal que $p\left(\sqrt{2}\right) = 0$. Así, el grado de $\sqrt{2}$ sobre $\mathbb{Q}$ es $\deg p(x) = 2$.

Teorema 10.27. Sea E una extensión de campo de F y $\alpha \in E$. Supongamos que α es algebraico sobre F y sea $p(x)$ el polinomio mínimo de α sobre F. Entonces $F(\alpha) \cong F[x] / \langle p(x) \rangle$.

Demostración. Consideremos el homomorfismo de evaluación $\phi_\alpha : F[x] \longrightarrow F[\alpha]$. Como $\ker \phi_\alpha = \langle p(x) \rangle$, por el primer teorema de isomorfía tenemos que $\phi_\alpha(F[x]) \cong F[x] / \langle p(x) \rangle$. Como ϕ_α es sobreyectivo, $\phi_\alpha(F[x]) = F[\alpha]$. Además, como $\langle p(x) \rangle$ es irreducible, por el corolario 7.6, tenemos que $F[\alpha] \cong F[x] / \langle p(x) \rangle$ es un campo. Ahora sólo demostraremos que $F[\alpha] = F(\alpha)$. Claramente $F[\alpha] \subseteq F(\alpha)$. Por otro lado, observemos que $\alpha \in F[\alpha]$ y que $F \subseteq F[\alpha]$. Así, $F(\alpha) \subseteq F[\alpha]$ porque $F(\alpha)$ es el campo más pequeño que contiene a α y a F. ■

Corolario 10.28. Sea E una extensión de campo de F y $\alpha \in E$ un elemento algebraico sobre F. Entonces $F[\alpha] = F(\alpha)$.

Definición 10.29 (extensión simple). Sea E una extensión de campo de F. Decimos que E es una extensión simple de F si $E \cong F(\alpha)$ para algún $\alpha \in E$.

Ejemplo 10.30. El campo $E = \mathbb{Q}(x)$ es una extensión simple de $\mathbb{Q}$.

Teorema 10.31 (elementos en $F(\alpha)$). Sea $E = F(\alpha)$ una extensión simple de F, donde α es algebraico sobre F. Sea n el grado de α sobre F. Entonces,

$$F(\alpha) = \left\{ b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \ldots + b_0 : b_i \in F \right\}$$

donde la representación de los elementos de $F(\alpha)$ es única.

Demostración. Sea $p(x)$ el polinomio mínimo de α sobre F. Sea $f(\alpha) \in F(\alpha)$. Por el corolario 10.28, $F(\alpha) = F[\alpha]$, así que $f(\alpha)$ es una combinación lineal de potencias de α con coeficientes en F. Sea $f(x) \in F[x]$ el polinomio obtenido al reemplazar α por x en $f(\alpha)$. Por el algoritmo de la división para polinomios (teorema 6.8) existen $q(x)$, $r(x)$ tales que

$$f(x) = q(x)\,p(x) + r(x)$$

con

$$r(x) = 0 \quad \text{o} \quad \deg r(x) < \deg p(x) = n$$

Evaluando en α obtenemos que

$$f(\alpha) = q(\alpha)\,p(\alpha) + r(\alpha) = r(\alpha)$$

ya que $p(\alpha) = 0$. Como $\deg r(\alpha) < n$, la combinación lineal $r(\alpha)$ tiene la forma deseada.

Para demostrar la unicidad, supongamos que

$$b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \ldots + b_0 = b'_{n-1}\alpha^{n-1} + b'_{n-2}\alpha^{n-2} + \ldots + b'_0$$

Entonces el polinomio

$$g(x) = (b_{n-1} - b'_{n-1})\,x^{n-1} + \ldots + (b_0 - b'_0)$$

está en $F[x]$ y $g(\alpha) = 0$. Sin embargo, si $g(x)$ fuera distinto de cero tendríamos que $\deg g(x) < \deg p(x)$, lo cual contradice la minimalidad de $p(x)$. Así $g(x) = 0$ y $b_i = b'_i$ para toda i. ■

Ejemplo 10.32 ($\mathbb{Z}_2$). Consideremos el polinomio $p(x) = x^2 + x + 1$ en $\mathbb{Z}_2[x]$. El polinomio $p(x)$ es irreducible sobre $\mathbb{Z}_2$ puesto que $\deg p(x) = 2$ y no tiene raíces en $\mathbb{Z}_2$. Por el teorema fundamental de la teoría de campos, $p(x)$ tiene una raíz α en una extensión de campo de $\mathbb{Z}_2$. Por el teorema 10.31, todos los elementos de $\mathbb{Z}_2(\alpha)$ deben tener la forma $\beta = b_1\alpha + b_0$ con $b_1, b_0 \in \mathbb{Z}_2$. Así

$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$$

es un campo finito con cuatro elementos.

Ejemplo 10.33 ($\mathbb{Q}$). Sea $\alpha \in \mathbb{C}$ una raíz del polinomio $f(x) = x^2 + x + 1 \in \mathbb{Q}[x]$. Observemos que $f(x)$ es el polinomio mínimo de α porque $f(x)$ es irreducible sobre $\mathbb{Q}$. Entonces debemos poder expresar cualquier elemento β del campo $\mathbb{Q}(\alpha)$ de la forma $\beta = b_1\alpha + b_0$ con $b_1, b_0 \in \mathbb{Q}$. Consideremos por ejemplo

$$\beta = \frac{\alpha^2 + 1}{\alpha^2 - 1} \in \mathbb{Q}(\alpha)$$

Debido a que $\alpha^2 + \alpha + 1 = 0$, tenemos que $\alpha^2 = -\alpha - 1$. Así

$$\begin{aligned} \beta &= \frac{-\alpha}{-\alpha - 2} \\ &= \frac{\alpha}{\alpha + 2} \\ &= 1 - \frac{2}{\alpha + 2} \end{aligned}$$

Usando el algoritmo de la división entre $f(x)$ y $x + 2$

$$f(x) = (x + 2)(x - 1) + 3$$

Por lo que $(\alpha + 2)(\alpha - 1) + 3 = 0$. Así

$$\frac{1}{\alpha + 2} = -\frac{1}{3}(\alpha - 1)$$

Y finalmente

$$\begin{aligned} \beta &= 1 + \frac{2}{3}(\alpha - 1) \\ &= \frac{2}{3}\alpha + \frac{1}{3} \end{aligned}$$

10.2 Campos de descomposición

Definición 10.34 (polinomio separable). Sea E una extensión de campo de F. Decimos que un polinomio $f(x) \in F[x]$ es separable en E si $f(x)$ puede descomponerse en un producto de factores lineales en $E[x]$.

Ejemplo 10.35 ($\mathbb{R}$). El polinomio $f(x) = x^2 + 1 \in \mathbb{R}[x]$ es separable en $\mathbb{C}$ porque $f(x) = (x + i)(x - i)$.

Observación 10.36. Si F es un campo y $f(x) \in F[x]$, siempre existirá una extensión de campo E de F donde $f(x)$ es separable. Esto es verdad ya que por el corolario 10.5, siempre existe una extensión de campo E de F en la cual $f(x)$ tiene exactamente $n = \deg f(x)$ raíces. Entonces por el teorema del factor, $f(x)$ es separable en E.

Definición 10.37 (campo de descomposición). Sea E una extensión de campo de F y $f(x) \in F[x]$. Decimos que E es un campo de descomposición de $f(x)$ sobre F si $f(x)$ es separable en E, pero no es separable en ningún otro subcampo intermedio entre E y F.

Ejemplo 10.38 ($\mathbb{Q}$). $\mathbb{C}$ es un campo de descomposición de x^2+1 sobre $\mathbb{R}$. Sin embargo, $\mathbb{C}$ no es un campo de descomposición de x^2+1 sobre $\mathbb{Q}$ porque $f(x)$ también es separable en

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$$

y $\mathbb{Q}(i)$ es un subcampo propio de $\mathbb{C}$. De manera similar, $x^2 - 2 \in \mathbb{Q}[x]$ es separable sobre $\mathbb{R}$, pero el campo de descomposición de x^2-2 sobre $\mathbb{Q}$ es $\mathbb{Q}\left(\sqrt{2}\right)$.

Observación 10.39. Si F es un campo y $f(x) \in F[x]$, $n = \deg f(x)$, siempre podemos construir el campo de descomposición de $f(x)$ sobre F de la siguiente forma. Por el corolario 10.5, sabemos que existe una extensión de campo E de F tal que E contiene exactamente n raíces de $f(x)$. Sean $\alpha_1, \ldots, \alpha_n \in E$ las raíces de $f(x)$. No es posible asegurar que E es el campo de descomposición de $f(x)$ sobre F porque $f(x)$ puede ser separable sobre algún campo intermedio entre E y F. Sin embargo, el subcampo $F(\alpha_1, \ldots, \alpha_n) \subseteq E$ es el campo más pequeño que contiene a F y las raíces de $f(x)$. Por lo tanto, $F(\alpha_1, \ldots, \alpha_n)$ es el campo de descomposición de $f(x)$ sobre F.

Ejemplo 10.40 ($\mathbb{Q}$). Sea $f(x) = x^4 - x^2 - 2 = (x^2-2)(x^2+1) \in \mathbb{Q}[x]$. Las raíces de $f(x)$ son $\pm\sqrt{2}$ y $\pm i$ en $\mathbb{C}$, por lo que el campo de descomposición de $f(x)$ sobre $\mathbb{Q}$ es

$$\mathbb{Q}\left(\sqrt{2}, -\sqrt{2}, i, -i\right) = \mathbb{Q}\left(\sqrt{2}, i\right)$$

Sabemos que $\sqrt{2}$ e i son elementos algebraicos de grado 2 sobre $\mathbb{Q}$, así que por el teorema 10.31,

$$\begin{aligned}\mathbb{Q}\left(\sqrt{2}, i\right) &= \left\{x + yi : x, y \in \mathbb{Q}\left(\sqrt{2}\right)\right\} \\ &= \left\{a + b\sqrt{2} + ci + di\sqrt{2} : a, b, c, d \in \mathbb{Q}\right\}\end{aligned}$$

Ejemplo 10.41 ($\mathbb{Q}$). Para encontrar el campo de descomposición de x^3-1 sobre $\mathbb{Q}$, observemos que $x^3-1=(x+1)(x-1)\left(x+e^{i\frac{2\pi}{3}}\right)$ en $\mathbb{C}$, donde

$$e^{i\frac{2\pi}{3}}=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$$

Luego, el campo de descomposición de x^3-1 sobre $\mathbb{Q}$ es

$$\mathbb{Q}\left(1,-1,-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)=\mathbb{Q}\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)=\mathbb{Q}\left(i\sqrt{3}\right)$$

ya que $-\frac{1}{2}+i\frac{\sqrt{3}}{2}\in\mathbb{Q}\left(i\sqrt{3}\right)$ (con esto concluimos que $\mathbb{Q}\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)\subseteq\mathbb{Q}\left(i\sqrt{3}\right)$), y también $i\sqrt{3}\in\mathbb{Q}\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)$ (con esto concluimos que $\mathbb{Q}\left(i\sqrt{3}\right)\subseteq\mathbb{Q}\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)$).

10.3 Ejercicios

10.1. Sea $f(x)=x^4+x+1\in\mathbb{Z}_2[x]$. Escribe $f(x)$ como el producto de factores lineales sobre alguna extensión E de $\mathbb{Z}_2$. Sugerencia: usa el hecho de que $a^2+b^2=(a+b)^2$ en $\mathbb{Z}_2$.

10.2. Clasifica los siguientes elementos como algebraicos o trascendentes. En caso de ser algebraicos, encuentra su grado.

a) $\sqrt{\pi}$ sobre $\mathbb{Q}$.

b) $1+i$ sobre $\mathbb{R}$.

c) $\sqrt{\pi}$ sobre $\mathbb{R}$.

10.3. Encuentra los polinomios mínimos de $\sqrt{2}+i$ y de $\sqrt{\frac{1}{3}+\sqrt{7}}$ sobre $\mathbb{Q}$. Justifica.

10.4. Sea α algebraico sobre F, y sea $p(x)$ el polinomio mínimo de α sobre F. Muestra que si α es raíz de $f(x)\in F[x]$, entonces $p(x)\mid f(x)$ en $F[x]$.

10.5. Sabemos que π es trascendente sobre $\mathbb{Q}$. Encuentra un subcampo F de $\mathbb{R}$ donde π sea algebraico de grado 3.

10.6. Con respecto al ejemplo del polinomio $p(x)=x^2+x+1$ en $\mathbb{Z}_2[x]$, escribe una tabla de multiplicar para los elementos de $F(\alpha)$, donde α es una raíz de $p(x)$ en alguna extensión de $\mathbb{Z}_2$. Escribe α^5, α^{-2} y α^{100} en la forma $b_1\alpha+b_0$, $b_i\in\mathbb{Z}_2$, $i=0,1$.

10.7. Sea $\alpha \in \mathbb{C}$ una raíz de $f(x) = x^3 + x + 1$. Expresa $\frac{1}{\alpha}$ y $\frac{1}{\alpha+2} \in \mathbb{Q}(\alpha)$ de la forma $b_2\alpha^2 + b_1\alpha + b_0$ con $b_i \in \mathbb{Q}$, $i = 0, 1, 2$.

10.8. Encuentra el campo de descomposición de

$$x^4 + x^2 + 1 = \left(x^2 + x + 1\right)\left(x^2 - x + 1\right)$$

sobre $\mathbb{Q}$.

10.9. Sea E una extensión de F y $\alpha \in E$ un elemento trascendente sobre F. Muestra que todos los elementos de $F(\alpha) \setminus F$ son también trascendentes sobre F.

10.10. Un número algebraico α sobre $\mathbb{Q}$ se dice que es un entero algebraico si α es la raíz de un polinomio mónico en $\mathbb{Z}[x]$. Si α es un número algebraico sobre $\mathbb{Q}$ muestra que $n\alpha$ es un entero algebraico para algún $n \in \mathbb{N}$.

11

Extensiones algebraicas

Si no sabes a dónde estás yendo, cualquier camino te llevará.

Lewis Carroll, lógico y escritor británico

Para el estudio de los siguientes capítulos se recomienda recordar los conceptos de álgebra lineal tratados en el apéndice C. En este capítulo estudiaremos un tipo especial de extensiones de campos: las extensiones algebraicas.

Definición 11.1 (extensión algebraica). Sea E una extensión de campo de F. Decimos que E es una extensión algebraica de F si todo elemento de E es algebraico sobre F. Si E no es una extensión algebraica sobre F decimos que E es una extensión trascendente sobre F.

11.1 Extensiones finitas

Antes de definir lo que es una extensión finita y su relación con las extensiones algebraicas, presentaremos algunos nuevos conceptos. Si E es una extensión de campo de F, entonces E puede verse como un espacio vectorial sobre F. Claramente se satisfacen todos los axiomas de un espacio vectorial porque el campo E es un grupo abeliano bajo la suma y además se cumplen las siguientes propiedades para todo $\alpha, \beta \in F$ y $x, y \in E$

1) *Identidad escalar.* $1x = x$ con $1 \in F$.
2) *Asociatividad escalar.* $(\alpha\beta)\, x = \alpha\,(\beta x)$.
3) *Distributividad.* $\alpha\,(x + y) = \alpha x + \alpha y$ y $(\alpha + \beta)\, x = \alpha x + \beta x$.

Definición 11.2 (extensión finita). Decimos que la extensión E de F es finita si E visto como espacio vectorial sobre F es de dimensión finita (véase definición C.21). En caso contrario decimos que la extensión es infinita.

Definición 11.3 (grado de una extensión). Sea E una extensión finita de F. Decimos que E tiene grado n sobre F y escribimos $[E : F] = n$ si E tiene dimensión n visto como espacio vectorial sobre F.

Ejemplo 11.4 ($\mathbb{C}$). Consideremos a $\mathbb{C}$ como una extensión de $\mathbb{R}$. Sostenemos que el conjunto $B = \{1, i\}$ es una base para $\mathbb{C}$ visto como espacio vectorial sobre $\mathbb{R}$. Claramente, todo elemento de $\mathbb{C}$ tiene la forma $x + iy$ con $x, y \in \mathbb{R}$, por lo que $gen_{\mathbb{R}}(B) = \mathbb{C}$. Para demostrar que 1 e i son linealmente independientes, supongamos que

$$\alpha + \beta i = 0$$

con $\alpha, \beta \in \mathbb{R}$. Si, $\beta \neq 0$, obtenemos que $i = -\frac{\alpha}{\beta} \in \mathbb{R}$, lo cual es una contradicción. De esta forma, $\beta = 0$ y por lo tanto $\alpha = 0$. Esto demuestra que $[E : F] = 2$, y $\mathbb{C}$ es una extensión finita de $\mathbb{R}$.

Ejemplo 11.5 ($\mathbb{R}$). Demostraremos que el campo de números reales $\mathbb{R}$ no es una extensión finita de $\mathbb{Q}$. Supongamos que $B = \{b_1, \ldots, b_n\}$ es una base para $\mathbb{R}$ sobre $\mathbb{Q}$. Entonces, podemos escribir cualquier $x \in \mathbb{R}$ de forma única como

$$x = \alpha_n b_n + \alpha_{n-1} b_{n-1} + \ldots + \alpha_1 b_1$$

donde $\alpha_i \in \mathbb{Q}$. De esta forma, podemos definir una biyección $\beta : \mathbb{R} \to \mathbb{Q}^n = \mathbb{Q} \times \ldots \times \mathbb{Q}$ como $\beta(x) = (\alpha_n, \alpha_{n-1}, \ldots, \alpha_1)$. Debido a que el conjunto $\mathbb{Q}$ es numerable (es decir, existe una biyección $\mathbb{N} \to \mathbb{Q}$), sabemos que $\mathbb{Q}^n$ es numerable. Sin embargo, esto es una contradicción porque $\mathbb{R}$ no es numerable. Por lo tanto, $\mathbb{R}$ es una extensión infinita de $\mathbb{Q}$. (Para un repaso sobre conjuntos numerables puede consultarse la sección 12 de Stewart y Tall, 1977).

En la siguiente proposición encontramos el grado de la extensión $F(\alpha)$ de F, donde α es algebraico sobre F. En particular, la proposición implica que $F(\alpha)$ es una extensión finita de F siempre que α sea algebraico sobre F.

Proposición 11.6. Sea E una extensión de campo de F y sea $\alpha \in E$ un elemento algebraico de grado n sobre F. Entonces $[F(\alpha) : F] = n$.

Demostración. Los teoremas 10.31 y C.18 implican que

$$\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$$

es una base para $F(\alpha)$ sobre F. Así, $\dim_F F(\alpha) = n$. ■

Ejemplo 11.7 ($\mathbb{Q}(\alpha)$). El número $\sqrt{2} \in \mathbb{C}$ es algebraico de grado 2 sobre $\mathbb{Q}$ porque $x^2 - 2$ es su polinomio mínimo. Entonces

$$\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2.$$

De manera similar,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$$

y

$$\left[\mathbb{Q}\left(\sqrt[5]{2}\right) : \mathbb{Q}\right] = 5.$$

El siguiente teorema explica la relación de las extensiones finitas con las extensiones algebraicas.

Teorema 11.8 (finita implica algebraica). Toda extensión de campos finita es algebraica.

Demostración. Sea E una extensión finita de F con $[E:F] = n$. Sea $\alpha \in E$. Sabemos que el conjunto $\{1, \alpha, \ldots \alpha^n\}$ es linealmente dependiente en E porque $\dim_F E = n$ (teorema C.19). Así, existen escalares $a_i \in F$ no todos cero tales que

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$$

De esta manera, α es algebraico sobre F porque es raíz del polinomio $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in F[x]$. Como $\alpha \in E$ era un elemento arbitrario, la extensión E de F es algebraica. ■

Corolario 11.9. Sea E una extensión de campo de F y α un elemento algebraico sobre F. Entonces $F(\alpha)$ es una extensión algebraica de F.

Demostración. Sabemos que $F(\alpha)$ es una extensión finita de F por la proposición 11.6. Así, por el teorema anterior, $F(\alpha)$ es una extensión algebraica de F. ■

Corolario 11.10. Sea E una extensión de F y $\alpha \in E$. Entonces α es algebraico de grado n sobre F si y sólo si $[F(\alpha):F] = n$.

Demostración. *Ejercicio 11.2.* ■

Teorema 11.11. Sea K una extensión finita de E y sea E una extensión finita de F. Entonces K es una extensión finita de F y

$$[K:F] = [K:E][E:F]$$

Demostración. Sea $B_1 = \{x_1, x_2, \ldots, x_n\}$ una base para K sobre E, y sea $B_2 = \{y_1, y_2, \ldots, y_m\}$ una base para E sobre F. Demostraremos que

$$B_3 = \left\{x_i y_j : i = 1, \ldots, n,\ j = 1, \ldots, m\right\}$$

es una base para K sobre F. Sea $\alpha \in K$. Entonces existen escalares $b_i \in E$ tales que

$$\alpha = b_1x_1 + b_2x_2 + \ldots + b_nx_n$$

Además, para cada $b_i \in E$, existen escalares $a_{ij} \in F$ tales que

$$\begin{aligned} b_i &= a_{i1}y_1 + a_{i2}y_2 + \ldots + a_{im}y_m \\ &= \sum_{j=1}^{m} a_{ij}y_j \end{aligned}$$

Sustituyendo obtenemos que

$$\begin{aligned} \alpha &= \sum_{j=1}^{m} a_{1j}y_j x_1 + \sum_{j=1}^{m} a_{2j}y_j x_2 + \ldots + \sum_{j=1}^{m} a_{nj}y_j x_n \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}y_j x_i \\ &= \sum_{i,j} a_{ij}\left(y_j x_i\right) \end{aligned}$$

Esto demuestra que B_3 es un conjunto generador de K. Para demostrar que B_3 es linealmente independiente supongamos que existen elementos $c_{ij} \in F$ tales que

$$\sum_{i,j} c_{ij}\left(y_j x_i\right) = 0$$

Entonces

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} c_{ij}y_j\right)x_i = 0$$

Como $\sum_{j=1}^{m} c_{ij}y_j \in E$ y los elementos x_i son linealmente independientes sobre E, entonces

$$\sum_{j=1}^{m} c_{ij}y_j = 0$$

para toda i. De manera similar, como $c_{ij} \in F$ y los elementos y_j son linealmente independientes sobre F, debemos tener que

$$c_{ij} = 0$$

para toda i y j. Por lo tanto, B_3 es linealmente independiente sobre F. Hay nm elementos en B_3, así que $[K : F] = nm$. ■

Corolario 11.12. Sean $F_1, \ldots, F_n$ campos donde F_{i+1} es una extensión finita de F_i. Entonces F_n es una extensión finita de F_1 y

$$[F_n : F_1] = [F_n : F_{n-1}]\,[F_{n-1} : F_{n-2}] \ldots [F_2 : F_1]$$

Demostración. *Ejercicio 11.3.* ■

Corolario 11.13. Sea E una extensión de campo de F y $\alpha \in E$ un elemento algebraico de grado n sobre F. Entonces, si $\beta \in F(\alpha)$, el grado de β sobre F divide a n.

Demostración. Sabemos que β es algebraico sobre F por el corolario 11.9. Sea m el grado de β sobre F. Entonces $[F(\beta) : F] = m$ y $[F(\alpha) : F] = n$. Es claro que $F \subseteq F(\beta) \subseteq F(\alpha)$. Así, por el teorema 11.11,

$$\begin{aligned}[F(\alpha) : F] &= [F(\alpha) : F(\beta)]\,[F(\beta) : F] \\ n &= [F(\alpha) : F(\beta)]\, m\end{aligned}$$

Lo que implica que m divide a n. ■

Ejemplo 11.14 ($\mathbb{Q}\left(\sqrt{3}\right)$). En este ejemplo demostraremos que ningún elemento de $\mathbb{Q}(\sqrt{3})$ es raíz del polinomio $f(x) = x^3 + 2$. Sea $\beta \in \mathbb{Q}(\sqrt{3})$. Por el corolario 11.13, el grado de β sobre $\mathbb{Q}$ debe dividir a 2, que es el grado de $\sqrt{3}$ sobre $\mathbb{Q}$. Sin embargo, si β es raíz de $f(x)$, entonces $f(x)$ debe ser su polinomio mínimo porque es irreducible sobre $\mathbb{Q}$. Así β debe tener grado 3, lo cual es una contradicción porque $3 \nmid 2$.

Ejemplo 11.15 ($\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[4]{3}\right)$). En este ejemplo encontraremos el grado de la extensión $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{5}\right)$ de $\mathbb{Q}$. Sea $\alpha = \sqrt{2}$ y $\beta = \sqrt[3]{5}$. Por el teorema 11.11,

$$\begin{aligned}[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] &= [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)]\,[\mathbb{Q}(\beta) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)]\,(3)\end{aligned}$$

Ahora debemos encontrar $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)]$. Observemos que α es raíz del polinomio $x^2 - 2 \in \mathbb{Q}(\beta)[x]$. Demostraremos que $x^2 - 2$ es irreducible sobre $\mathbb{Q}(\beta)$ mostrando que $x^2 - 2$ no tiene raíces en $\mathbb{Q}(\beta)$. Las raíces de $x^2 - 2$ son $\pm\alpha$. Si $\alpha \in \mathbb{Q}(\beta)$, como el grado de α sobre $\mathbb{Q}$ es 2, y el grado de β sobre $\mathbb{Q}$ es 3, por el corolario 11.13 tenemos que $2 \mid 3$, lo cual es una contradicción. Por lo tanto, $\pm\alpha \notin \mathbb{Q}(\beta)$, y $x^2 - 2$ es el polinomio mínimo de α sobre $\mathbb{Q}(\beta)$. Luego $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = 2$ y $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2 \cdot 3 = 6$.

Ejemplo 11.16 ($\mathbb{Q}\left(\sqrt{3}, \sqrt{5}\right)$). Demostraremos que

$$\mathbb{Q}\left(\sqrt{3}, \sqrt{5}\right) = \mathbb{Q}\left(\sqrt{3} + \sqrt{5}\right).$$

Claramente

$$\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right) \subseteq \mathbb{Q}\left(\sqrt{3},\sqrt{5}\right)$$

porque

$$\sqrt{3}+\sqrt{5} \in \mathbb{Q}\left(\sqrt{3},\sqrt{5}\right).$$

Si demostramos que $\sqrt{3} \in \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$ y que $\sqrt{5} \in \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$, podemos concluir que $\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right) \subseteq \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$ ya que $\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right)$ es el campo más pequeño que contiene a $\mathbb{Q}$, $\sqrt{3}$ y $\sqrt{5}$. Observemos que $\left(\sqrt{3}+\sqrt{5}\right)^{-1} \in \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$, así que

$$\begin{aligned}\left(\sqrt{3}+\sqrt{5}\right)^{-1} &= \frac{1}{\sqrt{3}+\sqrt{5}}\frac{\sqrt{3}-\sqrt{5}}{\sqrt{3}-\sqrt{5}} \\ &= -\frac{1}{2}\left(\sqrt{3}-\sqrt{5}\right) \in \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)\end{aligned}$$

Por lo tanto,

$$\frac{1}{2}\left(\sqrt{3}+\sqrt{5}\right)-\frac{1}{2}\left(\sqrt{3}-\sqrt{5}\right) = \sqrt{5} \in \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$$
$$\frac{1}{2}\left(\sqrt{3}+\sqrt{5}\right)+\frac{1}{2}\left(\sqrt{3}-\sqrt{5}\right) = \sqrt{3} \in \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$$

Ejemplo 11.17 ($\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right)$). El grado de la extensión $\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$ de $\mathbb{Q}$ es

$$\begin{aligned}\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\right] &= \left[\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right):\mathbb{Q}\right] \\ &= \left[\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right):\mathbb{Q}\left(\sqrt{5}\right)\right]\left[\mathbb{Q}\left(\sqrt{5}\right):\mathbb{Q}\right] \\ &= 2\cdot 2 = 4\end{aligned}$$

Ya que $\left[\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right):\mathbb{Q}\left(\sqrt{5}\right)\right] = 2$. Para demostrar esto último, notemos que $\sqrt{3}$ es raíz de $x^2-3 \in \mathbb{Q}\left(\sqrt{5}\right)[x]$. Demostraremos que x^2-3 es irreducible sobre $\mathbb{Q}\left(\sqrt{5}\right)$ mostrando que no tiene raíces en $\mathbb{Q}\left(\sqrt{5}\right)$. Supongamos que $\sqrt{3} \in \mathbb{Q}\left(\sqrt{5}\right)$. Entonces,

$$\sqrt{3} = a + b\sqrt{5} \text{ con } a,b \in \mathbb{Q}$$

Si $a = 0$, $\sqrt{\frac{3}{5}} = b \in \mathbb{Q}$, lo cual es una contradicción. Luego $a \neq 0$. Claramente, $b \neq 0$, ya que si $b = 0$, $\sqrt{3} = a \in \mathbb{Q}$. Elevando al cuadrado,

$$3 = a^2 + 2ab\sqrt{5} + 5b^2$$
$$\sqrt{5} = \frac{3-a^2-b^2}{2ab} \in \mathbb{Q}$$

Lo cual es una contradicción. Así $x^2 - 3$ es el polinomio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{5})$. Una forma alternativa para calcular

$$\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right):\mathbb{Q}\right]$$

es encontrando el polinomio mínimo de $\sqrt{3}+\sqrt{5}$ sobre $\mathbb{Q}$.

Ejemplo 11.18. Sea $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{C}$. Encontraremos el polinomio mínimo de α sobre $\mathbb{Q}$. Observemos que

$$\left(\alpha - \sqrt{2}\right)^2 = 3 \longrightarrow \alpha^2 - 1 = 2\sqrt{2}\alpha \longrightarrow \left(\alpha^2-1\right)^2 = 8\alpha^2$$

Así que α es una raíz de $p(x) = x^4 - 10x^2 + 1$. Hasta ahora no queda claro si $p(x)$ es irreducible sobre $\mathbb{Q}$. Por el *ejercicio 11.4*, $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$. Luego, por el teorema 11.11,

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] = 2\cdot 2 = 4$$

Como $\deg p(x) = 4$ y es mónico, debemos tener que $p(x)$ es el polinomio mínimo de α sobre $\mathbb{Q}$. Esto da una demostración indirecta de que el polinomio $p(x)$ es irreducible sobre $\mathbb{Q}$.

Ejemplo 11.19 ($\mathbb{Q}\left(\sqrt[3]{3},\sqrt{3}\right)$). En este ejercicio encontraremos una base para $\mathbb{Q}(\sqrt[3]{3},\sqrt{3})$ sobre $\mathbb{Q}$. Puesto que

$$\left[\mathbb{Q}\left(\sqrt[3]{3}\right):\mathbb{Q}\right] = 3, \left\{1, 3^{\frac{1}{3}}, 3^{\frac{2}{3}}\right\}$$

es una base para $\mathbb{Q}(\sqrt[3]{3})$ sobre $\mathbb{Q}$. Observemos que $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{3})$ porque el grado de $\sqrt{3}$ sobre $\mathbb{Q}$ no divide al grado de $\sqrt[3]{3}$ sobre $\mathbb{Q}$. Así, el conjunto $B = \left\{1, 3^{\frac{1}{2}}\right\}$ es una base para $\mathbb{Q}(\sqrt[3]{3},\sqrt{3})$ sobre $\mathbb{Q}(\sqrt[3]{3})$ porque $[\mathbb{Q}(\sqrt[3]{3},\sqrt{3}):\mathbb{Q}(\sqrt[3]{3})] = 2$. Por la demostración del teorema 11.11, el conjunto

$$\left\{1, 3^{\frac{1}{3}}, 3^{\frac{2}{3}}, 3^{\frac{1}{2}}, 3^{\frac{5}{6}}, 3^{\frac{7}{6}}\right\}$$

es una base para $\mathbb{Q}(\sqrt[3]{3},\sqrt{3})$ sobre $\mathbb{Q}$ y $[\mathbb{Q}(\sqrt[3]{3},\sqrt{3}):\mathbb{Q}] = 6$.

Teorema 11.20. Sea E una extensión algebraica de F. Entonces $E = F(\alpha_1,\ldots,\alpha_n)$, para algunos $\alpha_i \in E$ si y sólo si E es una extensión finita de F.

Demostración. Supongamos que $E = F(\alpha_1, \ldots, \alpha_n)$. Como E es una extensión algebraica de F, los elementos $\alpha_1, \ldots, \alpha_n$ son algebraicos sobre F. Así, por la proposición 11.6, $F(\alpha_1)$ es una extensión finita de F. De manera similar, como α_2 es algebraico sobre $F(\alpha_1)$, $F(\alpha_1, \alpha_2)$ es una extensión finita de $F(\alpha_1)$. En general,

$$F\left(\alpha_1, \alpha_2, \ldots, \alpha_j\right)$$

es una extensión finita de $F\left(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}\right)$. Luego, por el *ejercicio 11.3*

$$[E : F] = [E : F(\alpha_1 \ldots \alpha_{n-1})] \ldots [F(\alpha_1, \alpha_2) : F(\alpha_1)]\,[F(\alpha_1) : F]$$

lo que implica que $[E : F]$ es finito y E una extensión finita de F.

Supongamos que E es una extensión finita de F. Sea $\{a_1, \ldots, a_n\}$ una base para E sobre F. Entonces $E = F(\alpha_1, \ldots, \alpha_n)$. ■

Corolario 11.21. Si K es una extensión algebraica de E y E es una extensión algebraica de F, entonces K es una extensión algebraica de F.

Demostración. Sea $\alpha \in K$. Bastará con demostrar que α pertenece a alguna extensión finita de F, ya que todos los elementos de cualquier extensión finita de F son algebraicos sobre F. Como α es algebraico sobre E, α es raíz de algún polinomio $f(x) \in E[x]$. Supongamos que

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

con $a_n, a_{n-1}, \ldots, a_0 \in E$. Debido a que E es una extensión algebraica de F, por el teorema anterior, el campo $F_n = F(a_0, \ldots, a_{n-1}, a_n)$ es una extensión finita de F. Observemos que $f(x) \in F_n[x]$, por lo que α es algebraico sobre F_n. Luego, $F_n(\alpha)$ es una extensión finita de F_n. De esa manera, $F_n(\alpha)$ es una extensión finita de F ya que

$$[F_n(\alpha) : F] = [F_n(\alpha) : F_n]\,[F_n : F]$$

Con esto el corolario queda demostrado. ■

Proposición 11.22. Sea E una extensión de campo de F. Entonces el conjunto de elementos algebraicos sobre F

$$A = \{\alpha \in E : \alpha \text{ es algebraico sobre } F\}$$

es un subcampo de E.

Demostración. Sean $\alpha, \beta \in \overline{A}$. Claramente $F(\alpha, \beta)$ es una extensión finita de F porque α y β son algebraicos sobre F. Por el teorema 11.8, $F(\alpha, \beta)$ es una extensión algebraica de F y $F(\alpha, \beta) \subseteq \overline{A}$. Como $F(\alpha, \beta)$ es un subcampo de E, $\alpha \pm \beta, \alpha\beta \in F(\alpha, \beta) \subseteq \overline{A}$ y $\alpha\beta^{-1} \in F(\alpha, \beta) \subseteq \overline{A}$ si $\beta \neq 0$. Por lo tanto, $\overline{A}$ es un subcampo de E. ■

11.2 Cerradura algebraica

Definición 11.23 (algebraicamente cerrado). Un campo F es algebraicamente cerrado si todo polinomio no constante en $F[x]$ tiene una raíz en F.

El siguiente teorema y sus corolarios ilustran las ventajas de trabajar en un campo que sea algebraicamente cerrado.

Teorema 11.24. Un campo F es algebraicamente cerrado si y sólo si todo polinomio no constante en $F[x]$ es separable en F.

Demostración. Supongamos que F es algebraicamente cerrado y sea $f(x) \in F[x]$ un polinomio no constante con $n = \deg f(x) > 1$. Debemos mostrar que $f(x)$ puede descomponerse en factores lineales. Por hipótesis, $f(x)$ tiene una raíz en F, así que sea $\alpha_1 \in F$ una raíz de $f(x)$. Por el teorema del factor, $f(x) = (x - \alpha_1) f_1(x)$ donde $f_1(x) \in F[x]$, $\deg f_1(x) = n - 1$. Si $f_1(x)$ no es constante, como F es algebraicamente cerrado, tenemos que $f_1(x)$ tiene una raíz $\alpha_2 \in F$. Así que $f(x) = (x - \alpha_1)(x - \alpha_2) f_2(x)$ con $f_2(x) \in F[x]$, $\deg f_2(x) = n - 2$. Continuando este proceso, obtenemos que

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) f_n(x)$$

donde $\deg f_n(x) = 0$.

Supongamos ahora que todo polinomio no constante en $F[x]$ es separable en F. Debemos mostrar que todo polinomio $f(x) \in F[x]$ no constante tiene una raíz en F. Sea $ax + b$ un factor lineal de $f(x)$. Entonces $ba^{-1} \in F$ es una raíz de $f(x)$ y el teorema queda demostrado. ■

Corolario 11.25. Un campo F es algebraicamente cerrado si y sólo si los únicos polinomios irreducibles en $F[x]$ son los de grado 1.

Demostración. *Ejercicio 11.9.* ■

Corolario 11.26. Un campo algebraicamente cerrado no tiene extensiones algebraicas propias.

Demostración. Sea F un campo algebraicamente cerrado y supongamos que E es una extensión algebraica de F. Si $\alpha \in E$, por el corolario anterior, el polinomio mínimo de α debe ser lineal, digamos $p(x) = ax + b \in F[x]$. De esta forma, $a\alpha + b = 0$ y $\alpha = -b/a \in F$. Así $E = F$. ■

Definición 11.27 (cerradura algebraica). Sea F un campo. Decimos que un campo $\overline{F}$ es una cerradura algebraica de F si $\overline{F}$ es una extensión algebraica de F y $\overline{F}$ es algebraicamente cerrado.

Teorema 11.28. Cualquier campo tiene una cerradura algebraica.

Demostración. Sea F un campo. Usaremos el lema de Zorn (axioma 3.24) para demostrar que existe la cerradura algebraica. Consideremos el conjunto

$$S = \{E \text{ es un campo} : E \text{ es una extensión algebraica de } F\}$$

Claramente, $S \neq \emptyset$ porque $F \in S$. Además, S es un conjunto parcialmente ordenado junto con la relación $\subseteq$. Sea $C = \{E_i\}$ una cadena de S y sea $K = \cup E_i$. Demostraremos que K es un campo. Si $a, b \in K$, $b \neq 0$, entonces $a \in E_i$ y $b \in E_j$ para algunas i, j. Como C es una cadena, podemos asumir que $E_i \subseteq E_j$, así que $a, b \in E_j$. Por cerradura, $a - b, ab^{-1} \in E_j \subseteq K$. Es sencillo verificar que K cumple con todas las propiedades de un campo. También tenemos que K es una extensión algebraica de F: si $a \in K$, $a \in E_i$ para alguna i, y como $E_i \in S$, el elemento a es algebraico sobre F. Por lo tanto, $K \in S$ es una cota superior para C. Con esto se cumple la hipótesis del lema de Zorn, así que existe un elemento maximal $\overline{F}$ en S.

Finalmente demostraremos que el campo $\overline{F}$ es algebraicamente cerrado. Sea $f(x) \in \overline{F}[x]$ un polinomio no constante. Por reducción al absurdo, supongamos que $f(x)$ no tiene ninguna raíz en $\overline{F}$. Por el teorema fundamental de la teoría de campos, existe una extensión de campo de $\overline{F}$ en la cual $f(x)$ tiene una raíz α. Como α es algebraico sobre $\overline{F}$, el campo $\overline{F}(\alpha)$ es una extensión algebraica de $\overline{F}$ por el corolario 11.9. Además, $\overline{F}$ es una extensión algebraica de F, así que por el corolario 11.21, $\overline{F}(\alpha)$ es una extensión algebraica de F. De esta forma, $\overline{F}(\alpha) \in S$. Sin embargo, $\overline{F} \subsetneq \overline{F}(\alpha)$, ya que $\alpha \notin \overline{F}$, lo cual contradice que $\overline{F}$ sea un elemento maximal en S. Por lo tanto, $f(x)$ tiene una raíz en $\overline{F}$ y $\overline{F}$ es algebraicamente cerrado. ■

Es bien conocido que cualquier polinomio no constante con coeficientes complejos tiene una raíz en $\mathbb{C}$. Este es el llamado teorema fundamental del álgebra. Omitimos su demostración ya que la forma más directa de hacerlo utiliza varios conceptos propios del análisis complejo (puede consultarse el capítulo 2.4 de Marsden y Hoffman 1999).

Teorema 11.29 (teorema fundamental del álgebra). El campo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.

Ejemplo 11.30 ($\mathbb{C}$). El campo de los complejos $\mathbb{C}$ es una cerradura algebraica de $\mathbb{R}$.

Ejemplo 11.31 ($\mathbb{Q}$). El campo de los números algebraicos

$$A = \{\alpha \in \mathbb{C} : \alpha \text{ es algebraico sobre } \mathbb{Q}\}$$

es una cerradura algebraica de $\mathbb{Q}$. Para mostrar que A es algebraicamente cerrado, sea $f(x)$ un polinomio no constante en $A[x]$. Como $\mathbb{C}$ es algebraicamente cerrado, existe un $\beta \in \mathbb{C}$ tal que $f(\beta) = 0$. Esto implica que β es algebraico sobre A y por el *ejercicio 11.10* $\beta \in A$.

11.3 Ejercicios

11.1. Sea E una extensión finita de F. Demuestra que $[E : F] = 1$ si y sólo si $E = F$.

11.2. Sea E una extensión de F y $\alpha \in E$. Demuestra que α es algebraico de grado n sobre F si y sólo si $[F(\alpha) : F] = n$.

11.3. Sean F_i campos, $i = 1, \ldots, n$, donde F_{i+1} es extensión finita de F_i. Demuestra que F_n es una extensión finita de F_1 y

$$[F_n : F_1] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_2 : F_1]$$

11.4. Sean $a, b \in \mathbb{Q}$. Demuestra que $\mathbb{Q}\left(\sqrt{a}, \sqrt{b}\right) = \mathbb{Q}\left(\sqrt{a} + \sqrt{b}\right)$.

11.5. Encuentra el grado y una base para las siguientes extensiones finitas:

a) $\mathbb{Q}\left(\sqrt{2}\sqrt{3}\right)$ sobre $\mathbb{Q}$.

b) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{18}\right)$ sobre $\mathbb{Q}$.

c) $\mathbb{Q}\left(\sqrt{2}, \sqrt{6}\right)$ sobre $\mathbb{Q}(\sqrt{3})$.

11.6. Encuentra el grado y la base para $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ sobre $\mathbb{Q}(\sqrt{15})$.

11.7. Sea E una extensión finita de F. Demuestra que:

a) Si $p(x) \in F[x]$ es un polinomio irreducible sobre F con una raíz en E, entonces $\deg p(x)$ divide a $[E:F]$.

b) Si $[E:F]$ es un número primo, entonces E es una extensión simple de F.

11.8. Demuestra que x^2-3 es irreducible sobre $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

11.9. Demuestra que un campo F es algebraicamente cerrado si y sólo si los únicos polinomios irreducibles en $F[x]$ son los de grado 1.

11.10. Sea E una extensión de F, y

$$A = \{\alpha \in E : \alpha \text{ es algebraico sobre } F\}.$$

Demuestra que para cualquier $\alpha \in E$, si a es algebraico sobre A entonces $\alpha \in A$. Sugerencia: usa el corolario 11.21.

11.11. Sea E una extensión de F. Sea $\alpha \in E$ un elemento algebraico de grado impar sobre F. Muestra que α^2 es algebraico de grado impar sobre F y que $F(\alpha) = F(\alpha^2)$.

12

Campos finitos

Quien no ha cometido nunca un error, nunca ha intentado nada nuevo.

Albert Einstein, físico alemán

12.1 Estructura

Hasta ahora ya hemos trabajado con algunos campos finitos. Sabemos que si p es un número primo, $\mathbb{Z}_p$ es un campo finito de orden p. Obviamente, todos los campos finitos deben tener característica finita; de hecho, al ser dominios enteros, cualquier campo finito debe tener característica prima (teorema 2.25). En el corolario 5.20 demostramos que cualquier campo F de característica prima p contiene un subcampo isomorfo a $\mathbb{Z}_p$.

Definición 12.1 (subcampo primo). Sea F un campo finito de característica p. Al subcampo isomorfo a $\mathbb{Z}_p$ de F lo llamamos el subcampo primo de F.

Los siguientes teoremas nos dan un poco más de información básica.

Proposición 12.2. Sea F un campo finito de característica $p \in \mathbb{N}$. Entonces F tiene p^n elementos, para algún $n \in \mathbb{N}$.

Demostración. El subcampo primo de F es $\mathbb{Z}_p$. Claramente F es una extensión finita de $\mathbb{Z}_p$ ya que F es finito y no puede contener un subconjunto infinito linealmente independiente. De esta forma, sea $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base para F sobre $\mathbb{Z}_p$. Cada $\beta \in F$ puede ser escrito de forma única como

$$\beta = b_1\alpha_1 + b_2\alpha_2 + \ldots + b_n\alpha_n$$

para algunos $b_i \in \mathbb{Z}_p$. Como hay p alternativas para elegir los n distintos b_is, concluimos que hay exactamente p^n elementos distintos en F, donde $n = \dim_{\mathbb{Z}_p}(F)$. ■

Corolario 12.3. Si F es un campo de orden p^n, $\left[F : \mathbb{Z}_p\right] = n$.

Teorema 12.4. Sea F un campo de orden p^n. Entonces F tiene característica p.

Demostración. Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base para F sobre $\mathbb{Z}_p$, cualquier elemento $\beta \in F$ puede escribirse como

$$\beta = b_1\alpha_1 + \ldots + b_n\alpha_n$$

Para algunos $b_i \in \mathbb{Z}_p$. Así

$$\begin{aligned} p \cdot \beta &= (p \cdot b_1)\,\alpha_1 + \ldots + (p \cdot b_n)\,\alpha_n \\ &= 0 \end{aligned}$$

Por lo tanto, $char(F) \mid p$. Como p es primo, y $char(F) \neq 1$, $char(F) = p$. ■

Teorema 12.5 (grupo aditivo de un campo finito). Sea F un campo de orden p^n. Entonces, como grupo bajo la suma, $F \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$, donde hay n sumandos $\mathbb{Z}_p$.

Demostración. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base para F sobre $\mathbb{Z}_p$. Definamos la función $\phi : F \to \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$ como

$$\phi(b_1\alpha_1 + \ldots + b_n\alpha_n) = (b_1, \ldots, b_n) \text{ donde } b_i \in \mathbb{Z}_p$$

Considerando a F como grupo bajo la suma, es rutinario verificar que ϕ se trata de un isomorfismo de grupos. ■

Para estudiar la estructura de los campos finitos como grupos multiplicativos serán necesarias algunas herramientas de teoría de grupos.

Definición 12.6 (exponente de un grupo). El exponente $e(G)$ de un grupo finito G es el mínimo común múltiplo de los órdenes de todos los elementos de G.

Lema 12.7. Cualquier grupo abeliano finito G contiene un elemento de orden $e(G)$.

Demostración. Por el teorema fundamental de la aritmética, tenemos que $o(G) = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ donde los p_is son primos distintos y $\alpha_i \geq 1$. Por la definición de $e(G)$, debe existir un elemento $h_1 \in G$ cuyo orden sea divisible por $p_1^{\alpha_1}$; es decir $|h_1| = p_1^{\alpha_1} q_1$ donde $q_1 \mid p_2^{\alpha_2} \ldots p_n^{\alpha_n}$. Sea $g_1 = h_1^{q_1}$. Entonces para toda $m \geq 1$, $g_1^m = h_1^{mq_1} = 1$ si y sólo si $|h_1| = p_1^{\alpha_1} q_1 \mid mq_1$, lo cual ocurre si y sólo si $p_1^{\alpha_1} \mid m$. Por lo tanto $|g_1| = p_1^{\alpha_1}$.

De manera similar, para cada $i \in \{1, 2, \ldots, n\}$, podemos encontrar elementos g_i de órdenes $p_i^{\alpha_i}$. Sea

$$a = g_1 \ldots g_n$$

Si $|a| = k$, como G es abeliano

$$a^k = g_1^k \ldots g_n^k = 1$$

y

$$g_1^k = g_2^{-k} \ldots g_n^{-k}$$

Sea $r_1 = p_2^{\alpha_2} \dots p_n^{\alpha_n}$. Luego

$$g_1^{kr_1} = g_2^{-kr_1} \dots g_n^{-kr_1} = 1$$

ya que $g_i^{-kr_1} = 1$ para $i \in \{2, \dots, n\}$. De esta forma, $|g_1| = p_1^{\alpha_1} \mid kr_1$, y, debido a que p_1 y r_1 son primos relativos, $p_1^{\alpha_1} \mid k$.

Repitiendo este proceso observamos que $p_i^{\alpha_i} \mid k$ para toda $i \geq 1$, así que $e(G) \mid k$. Sin embargo, por definición $k \mid e(G)$. Por lo tanto $k = e(G)$. ■

Corolario 12.8. Si G es un grupo abeliano finito tal que $|G| = e(G)$, entonces G es cíclico.

Demostración. Por el lema anterior, existe un elemento $g \in G$ de orden $e(G) = |G|$. Esto implica que $G = \langle g \rangle$, así que G es cíclico. ■

Teorema 12.9 (grupo multiplicativo de un campo finito). Sea F un campo de orden p^n. Como grupo bajo la multiplicación, $F^* = F \setminus \{0\}$ es cíclico.

Demostración. Sea s el exponente de F^*. Entonces $a^s = 1$ para toda $a \in F^*$, así que todos los elementos de F^* son raíces del polinomio $x^s - 1$. Por el teorema 6.14, este polinomio tiene máximo s raíces, así que $|F^*| \leq s$. Por otro lado, $s \leq |F^*|$ ya que $s \mid |F^*|$ por el teorema de Lagrange. Luego $s = |F^*|$ y F^* es cíclico por el corolario anterior. ■

Corolario 12.10. Sea F un campo de orden p^n. Si $\alpha \in F$, entonces α es raíz del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$.

Demostración. El conjunto F^* forma un grupo bajo la multiplicación de orden $p^n - 1$. Así, para cualquier $\alpha \in F^*$, $\alpha^{p^n - 1} = 1$ por el *ejercicio B.10*. Así $\alpha^{p^n} = \alpha$. ■

Definición 12.11 (elemento primitivo). Sea F un campo finito. Decimos que $\alpha \in F$ es un elemento primitivo si α es un elemento generador del grupo cíclico F^*.

Observación 12.12. Si α es un elemento primitivo del campo finito F, entonces cualquier elemento distinto de cero de F puede escribirse como una potencia de α.

Corolario 12.13. Sea F un campo finito de orden p^n y $\alpha \in F$ un elemento primitivo. Entonces α es algebraico de grado n sobre $\mathbb{Z}_p$.

Demostración. Observemos que $\mathbb{Z}_p(\alpha) = F$. Por lo tanto, por el corolario 12.3,

$$\left[\mathbb{Z}_p(\alpha), \mathbb{Z}_p\right] = \left[F, \mathbb{Z}_p\right] = n$$

■

Corolario 12.14. Sea F un campo de orden p^n. Entonces cualquier extensión finita E de F es simple.

Demostración. Como E es una extensión finita de F, entonces E es un campo finito porque tiene una base finita y todos sus elementos son generados por combinaciones lineales de los elementos de F. Por el teorema 12.9, E^* es cíclico. Sea $\alpha \in E$ un elemento primitivo. Entonces $E = F(a)$. ■

12.2 Existencia y unicidad

Antes de continuar con el desarrollo de la teoría de los campos finitos, es necesario introducir el concepto de derivada formal.

Definición 12.15 (derivada formal). Sea F un campo y $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ un polinomio en $F[x]$. El polinomio $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$ en $F[x]$ es llamado la derivada formal de $f(x)$.

Lema 12.16. Sea F un campo y $f(x), g(x) \in F[x]$, $a \in F$. Entonces:

1) $(f(x) + g(x))' = f'(x) + g'(x)$.
2) $(af(x))' = af'(x)$.
3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Demostración. *Ejercicio 12.1.* ■

Nuestro objetivo ahora es demostrar que existe un campo finito de orden p^n para cualquier primo $p, n \in \mathbb{N}$. En el *ejercicio 7.8*, dado un polinomio $f(x)$ irreducible de grado n sobre $\mathbb{Z}_p$, construimos un campo $\mathbb{Z}_p[x] / \langle f(x) \rangle$ de orden p^n. Sin embargo, si quisiéramos llegar a nuestro objetivo por este camino tendríamos que demostrar que existe un polinomio irreducible de cualquier grado sobre $\mathbb{Z}_p$, lo cual no es sencillo. En lugar de esto, usaremos el concepto de cerradura algebraica desarrollado en el capítulo anterior. Demostraremos primero dos lemas antes del teorema de existencia.

Lema 12.17. Sea F un campo de característica p con cerradura algebraica $\overline{F}$. Entonces $x^{p^n} - x$ tiene p^n raíces distintas en $\overline{F}$.

Demostración. Debido a que $\overline{F}$ es algebraicamente cerrado, $x^{p^n} - x$ puede factorizarse como un producto de factores lineales $x - \alpha$. Basta demostrar que cada uno de estos factores aparece sólo una vez. Supongamos que hay algún factor repetido; esto es, $f(x) = (x-\alpha)^r g(x)$ donde $r > 1$, $\alpha \in \overline{F}$, $g(x) \in \overline{F}[x]$. Entonces, por el *ejercicio 12.2* y el lema anterior,

$$\begin{aligned} f'(x) &= r(x-\alpha)^{r-1} g(x) + (x-\alpha)^r g'(x) \\ &= (x-\alpha)^{r-1} \left(r g(x) + (x-\alpha) g'(x)\right) \end{aligned}$$

Así que α es una raíz de $f'(x)$. Sin embargo, por otro lado

$$\begin{aligned} f'(x) &= p^n x^{p^n-1} - 1 \\ &= -1 \end{aligned}$$

porque p es la característica de F. Esto implica que $f'(x)$ no tiene raíces, lo cual es una contradicción. ■

Lema 12.18. Si F es un campo de característica p entonces

$$(\alpha + \beta)^p = \alpha^p + \beta^p$$

para toda $\alpha, \beta \in F$.

Demostración. Aplicando el teorema del binomio

$$(\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \binom{p}{2}\alpha^{p-2}\beta^2 + \ldots + \binom{p}{p-1}\alpha\beta^{p-1} + \beta^p$$

como $p \mid \binom{p}{k}$ para toda $0 < k < p$ (véase la solución del *ejercicio 5.11*),

$$\begin{aligned} (\alpha+\beta)^p &= \alpha^p + 0\alpha^{p-1}\beta + \ldots + 0\alpha\beta^{p-1} + \beta^p \\ &= \alpha^p + \beta^p \end{aligned}$$

■

Corolario 12.19. Si F es un campo de característica p entonces

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$$

para toda $\alpha, \beta \in F$, $n \in \mathbb{N}$.

Teorema 12.20 (existencia de los campos finitos). Para cada primo p y cada $n \in \mathbb{N}$ existe un campo finito de orden p^n.

Demostración. Sea $\overline{\mathbb{Z}}_p$ la cerradura algebraica de $\mathbb{Z}_p$ y $g(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Sea

$$F = \left\{\alpha \in \overline{\mathbb{Z}}_p : g(\alpha) = 0\right\}$$

Por el lema 12.17, $|F| = p^n$. Demostraremos que F es un campo. Claramente $0, 1 \in F$. Si $\alpha, \beta \in F$, entonces $\alpha + \beta \in F$ ya que

$$(\alpha+\beta)^{p^n} - (\alpha+\beta) = \left(\alpha^{p^n} - \alpha\right) + \left(\beta^{p^n} - \beta\right) = 0 + 0 = 0$$

También $\alpha\beta \in F$ porque

$$\begin{aligned}(\alpha\beta)^{p^n} - \alpha\beta &= \alpha^{p^n}\beta^{p^n} - \alpha\beta \\ &= \alpha\beta - \alpha\beta = 0\end{aligned}$$

ya que $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. De manera similar, $-\alpha \in F$. Para observar esto, veamos que si $p > 2$, $(-1)^{p^n} = -1$ y

$$\begin{aligned}(-\alpha)^{p^n} + \alpha &= (-1)^{p^n}\alpha^{p^n} + \alpha \\ &= -\alpha + \alpha = 0\end{aligned}$$

Si $p = 2$, entonces $-1 = 1$, así que $\alpha = -\alpha \in F$. Ahora, si $\alpha \neq 0$, que $\alpha^{p^n} = \alpha$ implica que

$$\left(\frac{1}{\alpha}\right)^{p^n} = \frac{1}{\alpha}$$

Así que $\frac{1}{\alpha} \in F$. Esto demuestra que F es un subcampo finito de $\overline{\mathbb{Z}}_p$ con p^n elementos. ■

Definición 12.21 (campo de Galois). Llamamos al campo finito de orden p^n construido en el teorema 12.20 el campo de Galois de orden p^n, y lo denotamos $GF(p^n)$.

Observación 12.22. Claramente $GF(p) \cong \mathbb{Z}_p$.

Observación 12.23. Todos los elementos de $GF(p^n)$ son algebraicos sobre $\mathbb{Z}_p$ porque son raíces del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$. Así, $GF(p^n)$ es una extensión algebraica de $\mathbb{Z}_p$.

Corolario 12.24. Sea $n \in \mathbb{N}$. Entonces existe un polinomio irreducible sobre $\mathbb{Z}_p$ de grado n, para cualquier primo $p \in \mathbb{N}$.

Demostración. Por el corolario 12.13 y el teorema 12.20. ■

Teorema 12.25 (unicidad de $GF(p^n)$). Sea p un primo y $n \in \mathbb{N}$. Si F y F' son campos de orden p^n entonces $F \cong F'$.

Demostración. Ambos F y F' contienen un subcampo isomorfo a $\mathbb{Z}_p$ como subcampo primo. Digamos $\mathbb{Z}_p \cong K \subseteq F$, $\mathbb{Z}_p \cong K' \subseteq F'$. Sea $\alpha \in F$ un elemento primitivo. Entonces $F = K(\alpha)$ y por el corolario 12.13, α es un elemento algebraico de grado n sobre K. Sea $f(x) \in \mathbb{Z}_p[x]$ el polinomio mínimo de α. Entonces $K(\alpha) \cong \mathbb{Z}_p[x] / \langle f(x) \rangle$ por el teorema 10.27. Como los elementos de F son raíces de $g(x) = x^{p^n} - x$, en particular α es raíz de $g(x)$ y $f(x)$ es factor de $g(x)$ por el *ejercicio 10.4*. Como F' también consiste en las raíces de $g(x)$ (corolario 12.10), F' también contiene las raíces de $f(x)$, digamos que $\alpha' \in F'$ es tal que $f(\alpha') = 0$. De esta manera, $K'(\alpha') \cong \mathbb{Z}_p[x] / \langle f(x) \rangle$. Hasta ahora no podemos asegurar que α' es un generador de $(F')^*$. Sin embargo, observemos que $K'(\alpha') \subseteq F'$ y que ambos campos tienen p^n elementos por el *ejercicio 7.8*. Por lo tanto $K'(\alpha') = F'$ y $F \cong F'$. ■

Corolario 12.26. Si $f(x)$ es un polinomio irreducible de grado n sobre $\mathbb{Z}_p$, entonces $GF(p^n) \cong \mathbb{Z}_p[x] / \langle f(x) \rangle$.

Demostración. Por el *ejercicio 7.8*, $\mathbb{Z}_p[x] / \langle f(x) \rangle$ es un campo finito de orden p^n. ■

Teorema 12.27 (subcampos). Para cada divisor m de n, $GF(p^n)$ tiene un único subcampo de orden p^m. Además, esos son los únicos subcampos de $GF(p^n)$.

Demostración. Sea m un divisor de n. Sea

$$K = \left\{ x \in GF(p^n) : x^{p^m} = x \right\}$$

Claramente K es un subcampo de $GF(p^n)$ por el corolario 12.19. Para demostrar que tiene p^m elementos primero veamos que $|K| \leq p^m$ ya que $x^{p^m} - x$ tiene un máximo de p^m raíces. Ahora

$$p^n - 1 = (p^m - 1)\left(p^{n-m} + p^{n-2m} + \ldots + p^m + 1\right)$$

implica que $p^m - 1 \mid p^n - 1$. Por simplicidad escribiremos $p^n - 1 = (p^m - 1)t$. Sea $a \in GF(p^n)$ un elemento primitivo. Entonces $|a^t| = p^m - 1$ y además $a^t \in K$ porque

$$\left(a^t\right)^{p^m} = a^t a^{t(p^m - 1)} = a^t$$

Por el teorema de Lagrange (teorema B.27), $(p^m - 1) \mid |K^*|$, lo que implica que $(p^m - 1) \leq |K^*|$. Por lo tanto, $|K| = p^m$.

Para probar la unicidad basta con darse cuenta de que si $GF(p^n)$ tuviera dos subcampos de orden p^m distintos, entonces el polinomio $x^{p^m} - x$ tendría más de p^m raíces.

Finalmente supongamos que F es un subcampo de $GF(p^n)$. Entonces F es isomorfo a $GF(p^m)$ para alguna m y

$$\begin{aligned} n &= \left[GF(p^n) : \mathbb{Z}_p\right] \\ &= \left[GF(p^n) : GF(p^m)\right]\left[GF(p^m) : \mathbb{Z}_p\right] \\ &= \left[GF(p^n) : GF(p^m)\right] m \end{aligned}$$

Por el corolario 12.3. Así $m \mid n$. ■

Ejemplo 12.28 (GF (16)). Consideremos $GF(16)$. En este caso $16 = 2^4$, así que por el teorema anterior este campo tiene sólo tres subcampos de órdenes 2^1, 2^2 y 2^4. Obviamente, estos subcampos son $\mathbb{Z}_2 = \{0, 1\}$, $GF(4)$ y $GF(16)$.

12.3 Ejemplos

Ejemplo 12.29 (GF (8)). Construiremos una tabla de sumar y de multiplicar para $GF(8)$. Consideremos el polinomio irreducible $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ y sea $a \in \overline{\mathbb{Z}}_2$ una raíz de $f(x)$. Sea $F = \mathbb{Z}_2(a) \cong \mathbb{Z}_2[x] / \langle f(x) \rangle$. Claramente, $|F^*| = 7$, así que por el teorema de Lagrange (teorema B.27), $|a| \mid |F^*| = 7$. Como $a \neq 1$, $|a| = 7$. Esto implica que a es un elemento primitivo en F y

$$F = \left\{0, 1, a, a^2, a^3, a^4, a^5, a^6\right\}$$

Ahora es muy fácil construir una tabla de multiplicar para F:

$*$	0	1	a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0	0	0	0
1	0	1	a	a^2	a^3	a^4	a^5	a^6
a	0	a	a^2	a^3	a^4	α^5	a^6	1
a^2	0	a^2	a^3	a^4	α^5	α^6	1	a
a^3	0	a^3	a^4	α^5	a^6	1	a	a^2
a^4	0	a^4	α^5	a^6	1	a	a^2	a^3
a^5	0	a^5	a^6	1	α	a^2	a^3	a^4
a^6	0	α^6	1	a	a^2	a^3	a^4	a^5

Construyamos ahora la tabla de sumar de F. Podemos obtener bastante información de la relación $a^3+a+1=0$. Multiplicando por a, a^2 y a^3 obtenemos que $a^4=a^2+a$, $a^5=a^2+\alpha^3$ y $a^6=a^2+1$. Además sabemos que $\left(\alpha^2+1\right)^2=\alpha^4+1=\alpha^{12}=\alpha^5$ ya que $char\,(F)=2$. Para saber a qué es igual a^5+a escribimos $a^5+a=a^2+\alpha^3+\alpha=\alpha^2+1=\alpha^6$. También $\alpha^4+\alpha^3=a^2+a+\alpha+1=\alpha^6$. De esta forma, podemos completar la tabla de sumar:

$+$	0	1	a	a^2	a^3	a^4	a^5	a^6
0	0	1	a	a^2	a^3	a^4	a^5	a^6
1	1	0	α^3	a^6	a	α^5	α^4	α^2
a	a	a^3	0	a^4	1	α^2	α^6	α^5
a^2	a^2	a^6	a^4	0	α^5	α	α^3	1
a^3	a^3	a	1	α^5	0	α^6	α^2	α^4
a^4	a^4	α^5	α^2	a	α^6	0	1	α^3
a^5	a^5	α^4	α^6	α^3	α^2	1	0	α
a^6	a^6	α^2	α^5	1	α^4	α^3	α	0

Esta tabla es isomorfa a la tabla de sumar de $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$. Las imágenes de cada elemento bajo el isomorfismo $\phi:F\to\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$ son las siguientes: $\phi(0)=(0,0,0)$, $\phi(1)=(1,0,0)$, $\phi(a)=(0,1,0)$, $\phi\left(a^2\right)=(0,0,1)$, $\phi\left(a^3\right)=(1,1,0)$, $\phi\left(a^4\right)=(0,1,1)$, $\phi\left(a^5\right)=(1,1,1)$, $\phi\left(a^6\right)=(1,0,1)$.

Ejemplo 12.30 (*GF* (8)). Como en el ejemplo anterior, sea $f(x)=x^3+x+1\in\mathbb{Z}_2[x]$, $a\in\overline{\mathbb{Z}}_2$ una raíz de $f(x)$ y $F=\mathbb{Z}_2(a)$. Demostraremos que F es el campo de descomposición de $f(x)$ sobre $\mathbb{Z}_2$. Para esto, usando la tabla de sumar construida anteriormente, buscaremos más raíces de $f(x)$ en F.

$$f\left(a^2\right)=a^6+a^2+1=0$$
$$f\left(a^3\right)=\left(a^3\right)^3+a^3+1=a^2+a^3+1=a^4\neq 0$$
$$f\left(a^4\right)=\left(a^4\right)^3+a^4+1=a^5+a^4+1=0$$

Como $f(x)$ no puede tener más de tres raíces, concluimos que

$$f(x)=(x-a)\left(x-a^2\right)\left(x-a^4\right),$$

donde $a,a^2,a^4\in F$.

Ejemplo 12.31 (*GF* (16)). Consideremos el campo finito $F = GF(16)$. Como el polinomio $f(x) = x^4 + x + 1$ es irreducible sobre $\mathbb{Z}_2[x]$ sabemos que $F \cong \mathbb{Z}_2[x] / \langle f(x) \rangle$. También sabemos que el elemento $b = x + \langle f(x) \rangle$ es una raíz de $f(x)$. Demostraremos que b es un elemento primitivo. Para hacerlo simplemente necesitamos demostrar que $|b| = 15$ ya que $|F^*| = 15$. Por el teorema de Lagrange, $|b| = 1, 3, 5$ o 15. Claramente, $|b| \neq 1$ porque $b \neq 1$ en F^*. Si $b^3 = 1$, entonces debido a que $b^4 + b + 1 = 0$ tenemos que

$$\begin{aligned} bb^3 + b + 1 &= 0 \\ b1 + b + 1 &= 0 \\ 1 &= 0 \end{aligned}$$

Lo cual es una contradicción. Suponiendo que $b^5 = 1$, entonces $b^4 + b + 1 = 0$ implica que

$$\begin{aligned} b^5 + b^2 + b &= 0 \\ b^2 + b &= 1 \\ b^2 &= b + 1 \end{aligned}$$

Sustituyendo,

$$\begin{aligned} (b+1)(b+1) + b + 1 &= 0 \\ b^2 + 1 + b + 1 &= 0 \\ b^2 + b &= 0 \end{aligned}$$

Lo cual es nuevamente una contradicción. Por lo tanto $|b| = 15$.

Ejemplo 12.32 (*GF* (27)). La raíz de un polinomio irreducible $f(x)$ sobre $\mathbb{Z}_p$ no siempre será un elemento primitivo del campo

$$\mathbb{Z}_p[x] / \langle f(x) \rangle .$$

Por ejemplo, en el campo $\mathbb{Z}_3[x] / \langle x^3 + 2x + 2 \rangle$ el elemento $\alpha = x + \langle x^3 + 2x + 2 \rangle$ de $(\mathbb{Z}_3[x] / \langle x^3 + 2x + 2 \rangle)^*$ no es primitivo debido a

que

$$\begin{aligned}\alpha^{13} &= \left(\alpha^3\right)^4 \alpha = (-2\alpha - 2)^4 \alpha \\ &= (\alpha + 1)^4 \alpha \\ &= \left(\alpha^4 + 4\alpha^3 + 6\alpha^2 + 4\alpha + 1\right) \alpha \\ &= \alpha^5 + \alpha^4 + \alpha^2 + \alpha \\ &= (\alpha + 1)\,\alpha^2 + (\alpha + 1)\,\alpha + \alpha^2 + \alpha \\ &= \alpha^3 + \alpha^2 + \alpha^2 + \alpha + \alpha^2 + \alpha \\ &= \alpha + 1 + 2\alpha = 1\end{aligned}$$

En general no existe un procedimiento para encontrar un elemento primitivo en un campo finito, aunque sabemos que éste siempre debe existir.

12.4 Ejercicios

12.1. Sea F un campo y $f(x), g(x) \in F[x]$, $a \in F$. Demuestra que:

a) $(f(x) + g(x))' = f'(x) + g'(x)$

b) $(af(x))' = af'(x)$

c) $(f(x)\,g(x))' = f'(x)\,g(x) + f(x)\,g'(x)$

12.2. Muestra por inducción sobre n que

$$((x + a)^n)' = n(x - a)^{n-1}.$$

12.3. Sea $\alpha \in \overline{\mathbb{Z}}_2$ una raíz del polinomio $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Demuestra que si $\beta \in \overline{\mathbb{Z}}_2$ es una raíz de $x^3 + x + 1 \in \mathbb{Z}_2[x]$ entonces $\beta \in \mathbb{Z}_2(\alpha)$.

12.4. Sea $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$, $b \in \overline{\mathbb{Z}}_2$ una raíz de $f(x)$ y $K = \mathbb{Z}_2(b) \cong GF(8)$. Construye una tabla de multiplicar y de sumar para K. Encuentra un isomorfismo entre K y el campo F del *ejemplo 12.29*.

12.5. Sea $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Demuestra que el campo de descomposición de $f(x)$ sobre $\mathbb{Z}_2$ es el campo finito de ocho elementos.

12.6. Construye una tabla de multiplicar y de sumar para algún campo isomorfo a $GF(9)$.

12.7. Decimos que un campo F de característica p es perfecto si $F^p = \{a^p : a \in F\} = F$. Demuestra que todo campo finito es perfecto. Sugerencia: usa el *ejercicio 5.11*.

12.8. Muestra que si $\alpha \in \overline{\mathbb{Z}}_3$ es raíz de $f(x) = x^3 + 2x + 2$, entonces α es un elemento primitivo en el campo

$$\mathbb{Z}_3(\alpha) \cong \mathbb{Z}_3[x] / \left\langle x^3 + 2x + 2 \right\rangle.$$

12.9. Demuestra que ningún campo finito es algebraicamente cerrado.

12.10. Supongamos que L y K son subcampos de $GF(p^n)$ tales que $|L| = p^s$ y $|K| = p^t$. Encuentra $|L \cap K|$.

13

Introducción a la teoría de Galois

En toda la historia de la ciencia no hay ejemplo más completo del triunfo de la crasa estupidez sobre el indomable genio que el proporcionado por la vida extraordinariamente breve de Évariste Galois.

E. T. Bell, matemático escocés

Hasta ahora hemos trabajado bastante con polinomios y raíces de polinomios, pero no hemos dado una fórmula o un algoritmo para encontrar las raíces de un polinomio particular. Desde los antiguos griegos, los matemáticos han sabido que las raíces de un polinomio cuadrático $ax^2 + bx + c$ están dadas por

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

En el siglo XVI, los matemáticos del Renacimiento encontraron una fórmula general para las raíces de un polinomio cúbico y cuártico. Sin embargo, nadie pudo encontrar una fórmula general para las raíces de un polinomio de grado mayor o igual que cinco. A principios del siglo XIX, el matemático noruego Niels Henrik Abel demostró que no existe ni puede existir tal fórmula. Poco tiempo después, el matemático francés Évariste Galois construyó, antes de cumplir veintidós años, una teoría completamente nueva en la cual se investigaban las razones más profundas de la inexistencia de estas fórmulas generales. Así, la teoría de Galois surgió como una rama de las matemáticas que hace una bella conexión entre la teoría de campos y la teoría de grupos. Galois fue asesinado en un duelo a los veintiún años en circunstancias que permanecen poco claras hasta la fecha. Para leer más sobre la historia de Galois recomendamos la introducción del libro *Galois theory* (Stewart, 2004).

Generalmente, el primer concepto que separa el estudio de la teoría de campos clásica y la teoría de Galois es el de automorfismo de campo. Recordemos que si F es un campo, un automorfismo ϕ es un isomorfismo de la forma $\phi : F \to F$.

Proposición 13.1. Sea F un campo. El conjunto

$$Aut\,(F) = \{\phi : F \to F : \phi \text{ es un automorfismo}\}$$

es un grupo bajo la composición de funciones.

Demostración. Sean $\phi, \psi \in Aut\,(F)$. Entonces $\phi\psi$ es una biyección y

$$\begin{aligned} \phi\psi\,(a+b) &= \phi\,(\psi\,(a) + \psi\,(b)) \\ &= \phi\psi\,(a) + \phi\psi\,(b) \end{aligned}$$

De manera similar, $\phi\psi$ preserva la multiplicación en F. Así, por lo tanto, $\phi\psi \in Aut\,(F)$. Es claro que la composición de funciones es

asociativa, y que la función $e \in Aut(F)$ definida como $e(a) = a$ para toda $a \in F$ es la identidad en $Aut(F)$. Finalmente, por el teorema 5.13, si $\phi \in Aut(F)$ tenemos que ϕ^{-1} es también un automorfismo. ■

En contraste con el capítulo anterior, aquí trabajaremos principalmente con campos de característica 0. Recordemos que cualquiera de estos campos tiene un subcampo isomorfo a $\mathbb{Q}$, llamado su subcampo primo. Por simplicidad, también nos referiremos a este subcampo como $\mathbb{Q}$.

Proposición 13.2. Sea F un campo de característica 0. Si

$$\phi \in Aut(F),$$

entonces $\phi(x) = x$ para toda $x \in \mathbb{Q}$.

Demostración. Por el *ejercicio 5.1 a)*, $\phi(1)$ es la identidad multiplicativa en $\phi(F) = F$; esto es, $\phi(1) = 1$. De manera similar $\phi(0) = 0$. También para cualquier $n \in \mathbb{N}$,

$$\begin{aligned}\phi(n) &= \phi(1 + \ldots + 1)\\ &= \phi(1) + \ldots + \phi(1)\\ &= 1 + \ldots + 1 = n\end{aligned}$$

Podemos aplicar el mismo argumento para demostrar que $\phi(n) = n$ para toda $n \in \mathbb{Z}$. Por lo tanto $\phi(mn^{-1}) = \phi(m)\,\phi(n)^{-1} = mn^{-1}$ para toda $n, m \in \mathbb{Z}$ y la proposición queda demostrada. ■

Ejemplo 13.3 ($\mathbb{Q}$). Observemos que $Aut(\mathbb{Q}) = \{e\}$ por la proposición 13.2.

Ejemplo 13.4 ($\mathbb{Q}\left(\sqrt{2}\right)$). Sea $F = \mathbb{Q}\left(\sqrt{2}\right) = \left\{x + y\sqrt{2} : x, y \in \mathbb{Q}\right\}$. Calculemos $Aut(F)$. Si $\phi \in Aut(F)$, entonces

$$\begin{aligned}\phi\left(\sqrt{2}\right)^2 &= \phi\left(\left(\sqrt{2}\right)^2\right)\\ &= \phi(2) = 2\end{aligned}$$

Así que $\phi\left(\sqrt{2}\right) = \pm\sqrt{2}$. Si $\phi\left(\sqrt{2}\right) = \sqrt{2}$, entonces tenemos la función identidad, ya que si $x, y \in \mathbb{Q}$

$$\begin{aligned}\phi\left(x + y\sqrt{2}\right) &= \phi(x) + \phi(y)\,\phi\left(\sqrt{2}\right)\\ &= x + y\sqrt{2}\end{aligned}$$

Escribamos $\phi = e$ en este caso. Si $\phi\left(\sqrt{2}\right) = -\sqrt{2}$, entonces tenemos la función $\phi\left(x + y\sqrt{2}\right) = x - y\sqrt{2}$. Escribamos $\phi = \phi_0$ en este caso. Es sencillo verificar que ϕ_0 es un automorfismo (*ejercicio 13.1.*). Por lo tanto, $Aut(F) = \{e, \phi_0\} \cong \mathbb{Z}_2$, donde nos referimos a $\mathbb{Z}_2$ como grupo bajo la suma.

Ejemplo 13.5 ($\mathbb{Q}\left(\sqrt[3]{2}\right)$). Sea $\alpha = \sqrt[3]{2} \in \mathbb{C}$. Calculemos ahora $Aut(F)$ con $F = \mathbb{Q}(\alpha)$. El polinomio mínimo de α sobre $\mathbb{Q}$ es $x^3 - 2$, así que

$$F = \left\{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\right\}.$$

Si $\phi \in Aut(F)$,

$$\phi(\alpha)^3 = \phi(2) = 2$$

Entonces $\phi(\alpha)$ puede ser cualquiera de las tres raíces complejas de 2; es decir, $\phi(\alpha) = \alpha, \alpha\omega$ o $\alpha\omega^2$, donde $\omega = e^{\frac{2\pi i}{3}}$. Como $F \subseteq \mathbb{R}$, pero $\alpha\omega, \alpha\omega^2 \notin \mathbb{R}$, el automorfismo ϕ no puede tomar valores $\alpha\omega$ o $\alpha\omega^2$. Por lo tanto, $\phi(\alpha) = \alpha$ y $\phi = e$. En este caso $Aut(F) = \{e\}$.

Definición 13.6 (grupo de Galois). Sean $F \subseteq E$ campos. El grupo de Galois de E sobre F es el conjunto

$$Gal(E : F) = \{\phi \in Aut(E) : \phi(x) = x \text{ para toda } x \in F\}$$

Observación 13.7. Por la proposición 13.2, para cualquier campo F de característica 0, $Gal(F : \mathbb{Q}) = Aut(F)$.

Proposición 13.8. El conjunto $Gal(E : F)$ es un subgrupo de $Aut(E)$.

Demostración. Claramente $e \in Gal(E : F)$. Sean $\phi, \psi \in Gal(E : F)$. Entonces $\phi\psi(x) = \phi(x) = x$ para cualquier $x \in F$, así que $\phi\psi \in Gal(E : F)$. Además tenemos que si $\phi(x) = x$ para toda $x \in F$ entonces $\phi^{-1}(x) = x$ para toda $x \in F$. Luego $\phi^{-1} \in Gal(E : F)$. ■

Ejemplo 13.9 ($\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$). Calculemos

$$Gal(E : \mathbb{Q})$$

con $E = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Sabemos que

$$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}$$

Si $\phi \in Gal(E : \mathbb{Q})$, entonces $\phi\left(\sqrt{2}\right) = \pm\sqrt{2}$ y $\phi(\sqrt{3}) = \pm\sqrt{3}$, así que las cuatro posibilidades para ϕ son

1) $e\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$.

2) $\phi_1\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$.

3) $\phi_2\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$.

4) $\phi_3\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$.

Con cálculos directos podemos demostrar que todas ellas son automorfismos. Por lo tanto,

$$Gal\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\right)=\{e,\phi_1,\phi_2,\phi_3\}\cong\mathbb{Z}_2\times\mathbb{Z}_2, \text{ ya que } \phi_i^2=e$$

Definición 13.10 (conjugados de un elemento algebraico). Sea F un campo y $r\in\overline{F}$ un elemento algebraico sobre F con polinomio mínimo $p(x)\in F[x]$. Decimos que los conjugados de r sobre F son las raíces del polinomio $p(x)$.

Ejemplo 13.11. Los conjugados de $\sqrt{2}$ sobre $\mathbb{Q}$ son $\pm\sqrt{2}\in\mathbb{C}$.

Ejemplo 13.12. Los conjugados de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ son

$$2^{1/3},\ 2^{1/3}\omega \text{ y } 2^{1/3}\omega^2\in\mathbb{C}\ , \text{ con } \omega=e^{2\pi i/3}$$

Proposición 13.13. Sea F un campo. Supongamos que $\alpha,\beta\in\overline{F}$ son conjugados sobre F. Entonces existe un único isomorfismo

$$\phi:F(\alpha)\to F(\beta)$$

tal que $\phi(\alpha)=\beta$ y $\phi(x)=x$ para toda $x\in F$.

Demostración. Sea $p(x)\in F[x]$ el polinomio mínimo de α y β sobre F. Por la proposición 11.6, sabemos que $1,\alpha,\ldots,\alpha^{n-1}$ es una base para $F(\alpha)$ visto como espacio vectorial sobre F y que demás $1,\beta,\ldots,\beta^{n-1}$ es una base para $F(\beta)$ sobre F, donde $n=\deg p(x)$. Entonces,

$$F(\alpha)=\{g(\alpha):g(x)\in F[x],\ \deg g(x)<n\}$$
$$F(\beta)=\{g(\beta):g(x)\in F[x],\ \deg g(x)<n\}$$

Definamos $\phi:F(\alpha)\to F(\beta)$ como

$$\phi\left(g(\alpha)\right)=g(\beta)\ \text{ para cualquier } g(\alpha)\in F(\alpha)$$

Observemos que en particular $\phi(\alpha)=\beta$ y $\phi(x)=x$ para toda $x\in F$. Demostraremos que ϕ es un isomorfismo.

1) *Bien definido e inyectivo.* Sean $g(x), h(x) \in F[x]$. Entonces $g(\alpha) = h(\alpha)$ si y sólo si $(g-h)(\alpha) = 0$ si y sólo si $p(x) \mid (g-h)(x)$ si y sólo si $(g-h)(\beta) = 0$ debido a que $p(\beta) = 0$. Esta última afirmación ocurre si y sólo si $\phi(g(\alpha)) = \phi(h(\alpha))$. Por lo tanto, ϕ está bien definido y es inyectivo.

2) *Isomorfismo.* Claramente ϕ es sobreyectivo. Además,

$$\begin{aligned} \phi(g(\alpha) + h(\alpha)) &= \phi((g+h)(\alpha)) \\ &= (g+h)(\beta) \\ &= g(\beta) + h(\beta) \\ \phi(g(\alpha)\, h(\alpha)) &= \phi(gh(\alpha)) \\ &= gh(\beta) \\ &= g(\beta)\, h(\beta) \end{aligned}$$

Para demostrar la unicidad de ϕ, supongamos que $\psi : F(\alpha) \to F(\beta)$ es un isomorfismo tal que $\psi(\alpha) = \beta$ y $\psi(x) = x$ para toda $x \in F$. Entonces, para cualquier

$$\begin{aligned} g(\alpha) &\in F(\alpha), \\ g(\alpha) &= a_{n-1}\alpha^{n-1} + \ldots + a_0 \ \text{ con } \ \alpha_i \in F \end{aligned}$$

tenemos que

$$\begin{aligned} \psi(g(\alpha)) &= \psi(a_{n-1})\, \psi(\alpha)^{n-1} + \ldots + \psi(a_0) \\ &= a_{n-1}\beta^{n-1} + \ldots + a_0 \\ &= g(\beta) \\ &= \phi(g(\alpha)) \end{aligned}$$

Luego $\phi = \psi$.

■

Corolario 13.14. Sea F un campo y $\alpha, \beta \in \overline{F}$ conjugados sobre F. Entonces $F(\alpha) \cong F(\beta)$.

Ejemplo 13.15 ($\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$). Por el *ejemplo 11.18* sabemos que el polinomio mínimo de $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{C}$ sobre $\mathbb{Q}$ es

$$p(x) = x^4 - 10x^2 + 1.$$

Las raíces de $p(x)$ (y, por lo tanto, los conjugados de α) son $\pm\sqrt{2} \pm \sqrt{3}$. Por la proposición 13.13, existe un único isomorfismo ϕ_i que

envía α a alguno de sus conjugados y fija los elementos de $\mathbb{Q}$. Como $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\pm\sqrt{2} \pm \sqrt{3}\right)$ (lo cual se demuestra fácilmente usando el *ejercicio 11.4*) todos los isomorfismos ϕ_i son de hecho automorfismos. Esto se corresponde con nuestros cálculos previos del grupo de Galois $Gal(\mathbb{Q}(\alpha) : \mathbb{Q})$.

Teorema 13.16. Sea F un campo y $r \in \overline{F}$ un elemento algebraico sobre F. Sean $r = r_1, r_2, \ldots, r_n \in \overline{F}$ los conjugados de r sobre F, y sea $G = Gal(F(r) : F)$. Entonces hay una biyección entre el conjunto $C = F(r) \cap \{r_1, \ldots, r_n\}$ y el grupo G.

Demostración. Construiremos una función $\beta : C \to G$. Sea $r_i \in C$. Como $r_i \in F(r)$, sabemos que $F(r_i) \subseteq F(r)$. Debido a que r y r_i tienen el mismo polinomio mínimo, $|F(r_i) : F| = |F(r) : F|$. Por lo tanto, $F(r) = F(r_i)$. Por la proposición 13.13, existe un único isomorfismo $\phi_i : F(r) \to F(r_i)$ que fija los elementos de F tal que $\phi_i(r) = r_i$. Como $F(r) = F(r_i)$, ϕ_i es un automorfismo y $\phi_i \in G$. Definamos $\beta(r_i) = \phi_i \in G$.

Demostraremos que β es una biyección. Debido a que el automorfismo $\beta(r_i) = \phi_i$ es único por la proposición 13.13, β es inyectivo. Para demostrar que β es sobreyectivo, sea $\phi \in G$ y $p(x)$ el polinomio mínimo de r sobre F. El automorfismo ϕ fija todos los coeficientes de $p(x)$, así que $p(\phi(r)) = \phi(p(r)) = 0$. Esto implica que $\phi(r)$ es una raíz de $p(x)$, y $\phi(r) = r_i$ para alguna i donde $r_i \in F(r)$ (porque $\phi(r) \in F(r)$). Luego, $\beta(r_i) = \phi$. Esto demuestra que β es una biyección. ■

Corolario 13.17. Si $G = Gal(F(r) : F)$, $|G|$ es igual al número de conjugados de r sobre F que estén en $F(r)$.

Corolario 13.18. Si $G = Gal(F(r) : F)$, entonces $|G| \leq [F(r) : F]$.

Demostración. *Ejercicio 13.6.* ■

Ejemplo 13.19. Como los conjugados de $\sqrt{2}$ sobre $\mathbb{Q}$ son $\pm\sqrt{2}$ y ambos están en $\mathbb{Q}\left(\sqrt{2}\right)$, tenemos que $\left|Gal\left(\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right)\right| = 2$. De manera similar sabemos que $\left|Gal\left(\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right)\right| = 1$, ya que sólo uno de los conjugados de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ está en $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

Definición 13.20 (grupo de Galois de $f(x)$). Sea F un campo,

$$f(x) \in F[x]$$

Sea E el campo de descomposición de $f(x)$ sobre F. El grupo de Galois de $f(x)$ sobre F es el grupo $Gal(E:F)$. Si F es el campo más pequeño que contiene los coeficientes de $f(x)$, llamamos a $Gal(E:F)$ simplemente el grupo de Galois de $f(x)$, y escribimos $Gal(f)$.

Ejemplo 13.21. Por ejemplos previos,

$$Gal\left(x^2-2\right) = Gal\left(\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right) \cong \mathbb{Z}_2$$
$$Gal\left(x^4-10x^2+1\right) = Gal\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Ejemplo 13.22 ($\mathbb{Q}(\alpha, i)$). Sea $f(x) = x^4 - 2$ y $G = Gal(f)$. Las raíces de $f(x)$ son $\pm\alpha, \pm\alpha i$, donde $\alpha = \sqrt[4]{2}$. El campo de descomposición de $f(x)$ es $E = \mathbb{Q}(\alpha, i)$. Por el *ejercicio 11.4*, $E = \mathbb{Q}(\alpha, i) = \mathbb{Q}(\alpha + i)$. Sea $r = \alpha + i$. Entonces,

$$(r-i)^4 = 2$$
$$r^4 - 4ir^3 - 6r^2 + 4ir + 1 = 2$$
$$4i\left(r^3 - r\right) = r^4 - 6r^2 - 1$$

Así que r es una raíz del polinomio

$$p(x) = \left(x^4 - 16x^2 - 1\right)^2 + 16\left(x^3 - x\right)^2.$$

Observemos que por el teorema 11.11,

$$|E:\mathbb{Q}| = |\mathbb{Q}(\alpha, i):\mathbb{Q}(\alpha)|\,|\mathbb{Q}(\alpha):\mathbb{Q}| = 2 \cdot 4 = 8$$

Luego, $p(x)$ es el polinomio mínimo de r sobre $\mathbb{Q}$ y sus raíces son $\pm\alpha \pm i$ y $\pm\alpha i \pm i$. Como todos los conjugados de r están en $E = \mathbb{Q}(\alpha, i)$, tenemos que $|G| = 8$.

Ejemplo 13.23 ($\mathbb{Q}(\alpha, i)$). Con

$$f(x) = x^4 - 2 \quad \text{y} \quad G = Gal(f) = Gal(E:\mathbb{Q}),$$

como en el ejemplo anterior, calcularemos ahora explícitamente los elementos de G. Si $\phi \in G$, $\phi(\alpha)$ debe satisfacer el polinomio mínimo de α, $x^4 - 2$, y de manera similar $\phi(i)$ debe satisfacer $x^2 + 1$, así que

$$\phi(\alpha) = \pm\alpha \text{ o } \pm\alpha i$$
$$\phi(i) = \pm i$$

Además sabemos que

$$E = \mathbb{Q}(\alpha, i) = \{a + b\alpha + ci + d\alpha i : a, b, c, d \in \mathbb{Q}\}.$$

Luego, los posibles automorfismos de G están completamente determinados por las imágenes de $\phi(\alpha)$ y $\phi(i)$:

1) $e(a + b\alpha + ci + d\alpha i) = a + b\alpha + ci + d\alpha i$.
2) $\phi_1(a + b\alpha + ci + d\alpha i) = a + b\alpha i + ci - d\alpha$.
3) $\phi_2(a + b\alpha + ci + d\alpha i) = a - b\alpha + ci - d\alpha i$.
4) $\phi_3(a + b\alpha + ci + d\alpha i) = a - b\alpha i + ci + d\alpha$.
5) $\phi_4(a + b\alpha + ci + d\alpha i) = a + b\alpha - ci - d\alpha i$.
6) $\phi_5(a + b\alpha + ci + d\alpha i) = a + b\alpha i - ci + d\alpha$.
7) $\phi_6(a + b\alpha + ci + d\alpha i) = a - b\alpha - ci + d\alpha i$.
8) $\phi_7(a + b\alpha + ci + d\alpha i) = a - b\alpha - ci - d\alpha i$.

Es fácil verificar que todas esas posibilidades definen en realidad automorfismos, así que estos son todos los elementos de G. Etiquetemos ahora los vértices de un cuadrado como α, αi, $-\alpha$ y $-\alpha i$, podemos darnos cuenta de que el grupo G es en realidad el grupo de simetrías del cuadrado. Por ejemplo, ϕ_1 permuta los vértices de la forma $\alpha \mapsto \alpha i \mapsto -\alpha \mapsto -\alpha i$, por lo que ϕ_1 hace una rotación del cuadrado de 90 grados. De manera similar, ϕ_3 hace una rotación de 270 grados. El automorfismo ϕ_4 permuta los vértices de la forma $\alpha i \mapsto -\alpha i$, por lo que ϕ_4 hace una reflexión del cuadrado a través de la diagonal $\alpha, -\alpha$. De esta forma podemos encontrar las transformaciones del cuadrado a las que son equivalentes el resto de los automorfismos.

Ahora desarrollaremos una herramienta para establecer una conexión entre el grupo de Galois $Gal(E : F)$ y los campos intermedios entre E y F.

Definición 13.24 (correspondencia de Galois). Sea $F \subseteq E$ una extensión de campos, $\Delta = \{H \leq Gal(E : F)\}$ y $\Omega = \{K : F \subseteq K \subseteq E\}$. La correspondencia de Galois de la extensión $F \subseteq E$ es un par de funciones

$$\dagger : \Delta \to \Omega$$
$$* : \Omega \to \Delta$$

Para subgrupos $H \leq Gal(E:F)$, definimos

$$H^{\dagger} = \{a \in E : h(a) = a \text{ para toda } h \in H\}$$

Para campos intermedios K, definimos

$$\begin{aligned} K^{*} &= Gal(E:K) \\ &= \{\phi \in Gal(E:F) : \phi(k) = k \text{ para toda } k \in K\} \end{aligned}$$

Observación 13.25. Es claro que K^{*} es un subgrupo puesto que $Gal(E:K)$ es un grupo en sí mismo. Si $H \leq Gal(E:F)$, $H^{\dagger}$ es un campo ya que si $a, b \in H^{\dagger}$, $a - b \in H^{\dagger}$ porque $h(a-b) = h(a) - h(b) = a - b$, y de manera similar $ab^{-1} \in H^{\dagger}$, $b \neq 0$. Obviamente $F \subseteq H^{\dagger} \subseteq E$ porque $h(a) = a$ para toda $h \in G$, $a \in F$.

Ejemplo 13.26. Sea $E = \mathbb{Q}\left(\sqrt{2}\right)$ y $G = Gal(E:\mathbb{Q}) = \{e, \phi_0\} \cong C_2$, donde

$$\phi_0\left(a + b\sqrt{2}\right) = a - b\sqrt{2} \ , \ a, b \in \mathbb{Q}.$$

Los subgrupos de G son $I = \{e\}$ y G. Observemos que $I^{\dagger} = E$ y que $G^{\dagger} = \mathbb{Q}$. Los campos intermedios de $\mathbb{Q} \subseteq E$ son sólo $\mathbb{Q}$ y E (por el teorema 11.11). En este caso, $\mathbb{Q}^{*} = G$ y $E^{*} = 1$.

Ejemplo 13.27. Sea $E = \mathbb{Q}\left(2^{\frac{1}{3}}\right)$, $G = Gal(E:\mathbb{Q}) \cong \{e\}$. El único subgrupo de G es G y los campos intermedios de $\mathbb{Q} \subseteq E$ son $\mathbb{Q}$ y E. Así, $G^{\dagger} = E$, $\mathbb{Q}^{*} = G$ y $E^{*} = G$.

Ejemplo 13.28. Sea $E = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$, $G = Gal(E:\mathbb{Q})$. Por el *ejemplo 13.9*,

$$G = \{e, \phi_1, \phi_2, \phi_3\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

donde

$$\begin{aligned} \phi_1 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \phi_2 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \\ \phi_3 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \end{aligned}$$

Los subgrupos de G son $I = \{e\}$, G y $\langle \phi_i \rangle$ para $i = 1, 2, 3$. Entonces, $I^{\dagger} = E$ y $G^{\dagger} = \mathbb{Q}$. Encontraremos $\langle \phi_3 \rangle^{\dagger}$. Si ϕ_3 fija $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, $a, b, c, d \in \mathbb{Q}$, entonces

$$\begin{aligned} a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &= \phi_3\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right) \\ &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \end{aligned}$$

Como $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ es una base para $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$, tenemos que $b = c = 0$. De esta manera, $\langle \phi_3 \rangle^\dagger \subseteq \mathbb{Q}(\sqrt{6})$. Sin embargo, es claro que ϕ_3 fija todos los elementos de $\mathbb{Q}(\sqrt{6})$. Por lo tanto, $\langle \phi_3 \rangle^\dagger = \mathbb{Q}(\sqrt{6})$. De manera similar encontramos que $\langle \phi_1 \rangle^\dagger = \mathbb{Q}(\sqrt{3})$ y $\langle \phi_2 \rangle^\dagger = \mathbb{Q}\left(\sqrt{2}\right)$. Para describir $*$ es necesario tener más información sobre los campos intermedios de $\mathbb{Q} \subseteq E$.

Proposición 13.29. Sean $F \subseteq E$ campos y $G = Gal(E:F)$. Sean H, H_1, H_2 subgrupos de G y K, K_1, K_2 campos intermedios.

1) Si $H_1 \leq H_2$ entonces $H_2^\dagger \subseteq H_1^\dagger$.

2) Si $K_1 \subseteq K_2$ entonces $K_2^* \leq K_1^*$.

3) $H \leq H^{\dagger *}$ y $K \subseteq K^{* \dagger}$.

Demostración. *Ejercicio 13.9.* ■

Nuestro objetivo ahora es demostrar que el tamaño de cualquier subgrupo H de $Gal(E:F)$ es igual al grado de la extensión $[E:H^\dagger]$. Esto es un ejemplo de que es posible deducir muchas propiedades de los campos intermedios entre E y F a través de los subgrupos de $Gal(E:F)$. Antes de llegar a nuestro objetivo, demostraremos el teorema del elemento primitivo, el cual es verdadero cuando trabajamos con campos de característica 0.

Teorema 13.30 (elemento primitivo). Sea F un campo de característica 0 y $b, c \in \overline{F}$ elementos algebraicos sobre F. Entonces $F(b,c) = F(a)$ para alguna $a \in \overline{F}$.

Demostración. Sea $f(x)$ el polinomio mínimo de b sobre F con raíces $b = b_1, b_2, \ldots, b_q \in \overline{F}$, y sea $g(x)$ el polinomio mínimo de c sobre F con raíces $c = c_1, c_2, \ldots, c_m \in \overline{F}$. Por el *ejercicio 13.5*, todas las raíces de $f(x)$ y $g(x)$ son distintas. Consideremos las siguientes $q(m-1)$ ecuaciones:

$$b_i + xc_j = b_1 + xc_1 \quad (1 \leq i \leq q, 2 \leq j \leq m) \qquad (*)$$

Cada ecuación tiene solución única

$$x = \frac{b_i - b_1}{c_1 - c_j}$$

Como F es un campo infinito, existe $k \in F$ tal que $x = k$ no satisface ninguna de las ecuaciones en $(*)$. En otras palabras,

$$b_i + kc_j \neq b_1 + kc_1 \quad (1 \leq i \leq q, 2 \leq j \leq m)$$

Sea $a = b + kc \in F(b, c)$.

Mostraremos que $F(b, c) = F(a)$. Claramente $F(a) \subseteq F(b, c)$. Demostraremos que $c \in F(a)$ y esto implica que $b = a - kc \in F(a)$. Ahora, $b = a - kc$ es raíz del polinomio $f(x)$, así que c es una raíz de $g(x)$ y del polinomio $f(a - kx)$. Por el teorema del factor, $x - c$ divide a $g(x)$ y $f(a - kx)$. Sea $h(x) = mcd(g(x), f(a - kx)) \in F(a)[x]$. Entonces, $x - c \mid h(x)$ y $h(c) = 0$. Como c es una raíz simple de $g(x)$, también debe ser una raíz simple de $h(x)$.

Supongamos que $d \neq c$ es otra raíz de $h(x)$. Entonces d es una raíz de $g(x)$, así que $d = c_j$ para alguna $j > 1$, y también d es una raíz de $f(a - kx) = 0$, así que $a - kd = b_i$ para alguna i. Esto implica que $a - kc_j = b_i$, lo que es una contradicción por la elección de k. Por lo tanto, $h(x)$ no tiene más raíces y $h(x) = x - c \in F(a)[x]$. Luego $c \in F(a)$. ■

Corolario 13.31. Sea F un campo de característica 0. Si E es una extensión finita de F, entonces $E = F(\alpha)$ para alguna $a \in E$.

Demostración. Como $F \subseteq E$ es una extensión finita, por el teorema 11.20, $E = F(a_1, ..., a_n)$ para algunos $a_1, \ldots, a_n \in E$. Ahora puede usarse el teorema de elemento primitivo repetidas veces para concluir que $E = F(\alpha)$ para algún $\alpha \in E$. ■

Teorema 13.32. Sea F un campo de característica 0, y E una extensión finita de F. Sea $G = Gal(E : F)$. Si $H \leq G$, entonces

$$|H| = \left[E : H^{\dagger}\right]$$

Demostración. Sea $K = H^{\dagger}$, así que $F \subseteq K \subseteq E$ y $H \leq H^{\dagger *} = Gal(E : K)$. Por el teorema del elemento primitivo existe $\alpha \in E$ tal que $E = K(\alpha)$. Por el corolario 13.18,

$$|H| \leq |Gal(E : K)| \leq [E : K]$$

Demostraremos que $|H| \geq [E : K]$.

Sea $p(x) \in K[x]$ el polinomio mínimo de α sobre K, así que

$$|E : K| = |K(\alpha) : K| = \deg p(x).$$

Supongamos que $|H| = r < \deg p(x)$ y

$$H = \{\phi_1 = e, \phi_2, \ldots, \phi_r\}$$

Definamos $\alpha_i = \phi_i(\alpha) \in E$. Sea

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_r) \in E[x]$$

Observemos que cada ϕ_i permuta el conjunto $\{\alpha_1, \ldots, \alpha_r\}$ ya que

$$\phi_i\left(\alpha_j\right) = \phi_i\left(\phi_j(\alpha)\right) = \phi_k(\alpha) = \alpha_k$$

donde $\phi_k = \phi_i\phi_j \in H$. Por lo tanto, ϕ_i fija cada coeficiente de $f(x)$, lo que implica que dichos coeficientes están en $K = H^\dagger$. Así $f(x) \in K[x]$. Como $\alpha = \alpha_1$ es una raíz de $f(x)$, $p(x) \mid f(x)$. Pero $\deg f(x) = r < \deg p(x)$. Esto es una contradicción. Por lo tanto, $|H| \geq [E : K]$ como se deseaba. ■

Corolario 13.33. Sea F un campo de característica 0, y E una extensión finita de F. Sea $G = Gal(E : F)$. Entonces, para cualquier $H \leq G$,

$$H^{\dagger *} = H$$

Demostración. Por la proposición 13.29, $H \leq H^{\dagger *}$. Como $H^{\dagger *} = Gal\left(E : H^\dagger\right)$, por el corolario 13.18 y el teorema 13.32,

$$\left|H^{\dagger *}\right| = \left|Gal\left(E : H^\dagger\right)\right| \leq \left[E : H^\dagger\right] = |H|$$

Luego $H^{\dagger *} = H$. ■

Ejemplo 13.34. Sea

$$E = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right), G = Gal(E : \mathbb{Q}) = \{e, \phi_1, \phi_2, \phi_3\}$$

como antes. Si $H = \langle\phi_3\rangle$, $H^\dagger = \mathbb{Q}(\sqrt{6})$, entonces el teorema 13.32 dice que

$$2 = |H| = \left|\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt{6}\right)\right|$$

Finalmente abordaremos el problema de la insolubilidad de la quíntica. Decimos que un polinomio $f(x) \in F[x]$ es soluble por radicales si existe una fórmula para las raíces que utilice las operaciones aritméticas básicas involucrando los coeficientes de $f(x)$. Galois descubrió que $f(x)$ es soluble por radicales si y sólo si existe una sucesión de campos $F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n$, tal que F_n es un campo que contiene al campo de descomposición de $f(x)$ sobre F, y cada extensión $F_i \subseteq F_{i+1}$ es una *extensión radical* (esto significa que $F_{i+1} = F_i(\alpha)$, donde $\alpha^m \in F_i$ para alguna $m \in \mathbb{N}$).

Definición 13.35 (grupo soluble). Decimos que un grupo finito G es soluble si existe una sucesión de subgrupos normales

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$$

tal que el grupo cociente

$$G_{i+1}/G_i$$

es abeliano para toda $i \in \{0, \ldots, n-1\}$.

A través de la correspondencia de Galois, podemos encontrar un criterio para decidir cuándo un polinomio es soluble por radicales.

Teorema 13.36. Sea F un campo y $f(x) \in F[x]$. Entonces, $f(x)$ es soluble por radicales si y sólo si $Gal(f)$ es un grupo soluble.

Es posible demostrar que hay polinomios de grado 5 con coeficientes racionales cuyo grupo de Galois es isomorfo a S_5, el grupo de permutaciones de cinco objetos. Este grupo no es soluble porque la única serie de subgrupos normales que tiene es $\{e\} \lhd A_5 \lhd S_5$, donde A_5 es el subgrupo de permutaciones pares, y el cociente $A_5/\{e\} \cong A_5$ no es abeliano. Por lo tanto, este tipo de polinomios no son solubles por radicales. Un ejemplo de un polinomio con $Gal(f) \cong S_5$ es $f(x) = x^5 - 6x + 3$.

13.1 Ejercicios

13.1. Demuestra que la función $\phi : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{Q}\left(\sqrt{2}\right)$ definida como $\phi\left(x + y\sqrt{2}\right) = x - y\sqrt{2}$ es un automorfismo.

13.2. Encuentra $Gal(\mathbb{C} : \mathbb{R})$.

13.3. Sea $p \in \mathbb{N}$ un primo. Si $\omega = e^{\frac{2\pi i}{p}}$, demuestra que

$$|Gal(\mathbb{Q}(\omega), \mathbb{Q})| = p - 1.$$

13.4. Sea F un campo. Demuestra que la relación definida en $\overline{F}$ de ser conjugados sobre F es una relación de equivalencia.

13.5. Sea F un campo de característica 0 y $f(x) \in F[x]$ irreducible sobre F. Demuestra que $f(x)$ no tiene raíces múltiples en $\overline{F}$. Sugerencia: usa la derivada formal, definición 12.15.

13.6. Demuestra el corolario 13.18. Sugerencia: usa el *ejercicio 13.5*.

13.7. Encuentra $|Gal(f)|$ cuando:

a) $f(x) = x^2 + 2ix + 1 \in \mathbb{C}[x]$.

b) $f(x) = x^6 - 1 \in \mathbb{C}[x]$.

c) $f(x) = x^6 - 2 \in \mathbb{C}[x]$.

13.8. Encuentra los conjugados de $\alpha = i + \sqrt{3}$ sobre $\mathbb{Q}$. ¿Cuáles son los conjugados de α sobre $\mathbb{R}$?

13.9. Demuestra la proposición 13.29.

13.10. Encuentra $Gal(x^4 + 1)$ y $H^\dagger$ para todo subgrupo H.

Apéndices

A

Teoría de números elemental

Dios hizo los enteros. Todo lo demás es invento del hombre.

Leopold Kronecker, matemático alemán

A.1 Introducción a la teoría de números

La teoría de números estudia principalmente el conjunto de los números enteros y sus propiedades. Posee una estrecha relación con ciertas áreas del álgebra abstracta. Denotaremos como $\mathbb{Z}$ al conjunto de números enteros, es decir

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

La costumbre de usar la letra Z para este conjunto proviene de los alemanes, ya que *zahlen* es la palabra alemana para "números". Asimismo, denotaremos como $\mathbb{N}$ al conjunto de números naturales

$$\mathbb{N} = \{1, 2, \ldots\} \text{ y } \mathbb{N}_0 = \mathbb{N} \cup \{0\}$$

Comenzaremos nuestro estudio formal de los números enteros enunciando el axioma llamado el *principio del buen orden*. Los axiomas, en matemáticas, no son teoremas, sino expresiones aceptadas como verdaderas sin necesidad de una demostración. Podríamos decir, así, que los axiomas (junto con las definiciones) son las reglas del juego de las cuales debemos partir para comenzar la construcción de una enorme red matemática formada por teoremas, lemas y proposiciones. Si no establecemos clara y explícitamente las reglas del juego, a la larga las reglas se pueden tornar confusas y podemos caer en contradicciones. El principio del buen orden es importante porque de él se desprende la demostración de teoremas como el algoritmo de la división.

Axioma A.1 (principio del buen orden). Cualquier conjunto no vacío de números naturales posee un elemento mínimo.

Intuitivamente el axioma es bastante claro. Ahora comenzaremos con algunas definiciones propias de la teoría de números.

Definición A.2 (divisor). Sean $a, b \in \mathbb{Z}$, con $a \neq 0$. Decimos que a es divisor (o factor) de b si existe $t \in \mathbb{Z}$ tal que $b = at$. Escribimos $a \mid b$ si a es divisor de b, y $a \nmid b$ si a no es divisor de b.

Si $a \mid b$, también decimos que b es múltiplo de a, o que b es divisible entre a. Observemos que la definición de divisor involucra al producto de números enteros, y no a la división, como su nombre haría pensar. La razón de esto es que la división no es una operación bien definida en los enteros; es decir, que la división de dos números enteros no siempre es un entero. De todas maneras,

en ocasiones puede resultar cómodo pensar en que a es divisor de b, si de la división de a entre b resulta un entero. Por ejemplo, 5 es divisor de 10 porque $10 = 5 \cdot 2$ o en forma equivalente porque $\frac{10}{5} = 2$ es un entero.

Definición A.3 (primo). Sea $p \in \mathbb{Z}$, con $p > 1$. Decimos que p es un número primo si sus únicos divisores positivos son 1 y él mismo.

Definición A.4 (compuesto). Si $t \in \mathbb{Z}$, con $t > 1$, y t no es primo, decimos que t es compuesto.

Son ya bastante conocidos los primeros números primos: 2, 3, 5, 7, 11,... El misterioso comportamiento de esta secuencia ha obsesionado a los matemáticos durante siglos. Numerosos esfuerzos fallidos se han hecho por encontrar alguna fórmula que describa su comportamiento. Nosotros descubriremos su relevancia primordial más adelante, cuando se aborde el teorema fundamental de la aritmética.

Las siguientes son algunas propiedades de la divisibilidad.

Lema A.5 (divisibilidad). Sean $a, b, c \in \mathbb{Z}$. Entonces:

1) Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.
2) Si $b \neq 0$ y $a \mid b$ entonces $|a| \leq |b|$.
3) Si $c \mid a$ y $c \mid b$ entonces $c \mid (au + bv)$. para todo $u, v \in \mathbb{Z}$
4) $a \mid b$ y $b \mid a$ si y sólo si $a = \pm b$.

Demostración.

1) Si $a \mid b$ y $b \mid c$, entonces $b = t_1 a$ y $c = t_2 b$ para algunos $t_1, t_2 \in \mathbb{Z}$. Sustituyendo la primera relación en la segunda, $c = t_2 (t_1 a) = (t_2 t_1) a$, por lo que $a \mid c$.

2) Si $a \mid b$ entonces $b = ta$ para algún $t \in \mathbb{Z}$. Además $t \neq 0$ porque $b \neq 0$. De esta forma,

$$|a| \leq |t|\,|a| = |ta| = |b|$$

3) Si $c \mid a$ y $c \mid b$, entonces $a = t_1 c$ y $b = t_2 c$ para algunos $t_1, t_2 \in \mathbb{Z}$. Así, para cualquier $u, v \in \mathbb{Z}$ tenemos que $au = t_1 cu$ y $bv = t_2 cv$. Sumando las dos relaciones anteriores

$$\begin{aligned} au + bv &= t_1 cu + t_2 cv \\ &= (t_1 u + t_2 v)\, c \end{aligned}$$

Por lo tanto, $c \mid (au + bv)$.

4) Si $a = \pm b$, entonces es claro que $a = q_1 b$ y $b = q_2 a$, donde $q_1 = q_2 = \pm 1$. Luego, $a \mid b$ y $b \mid a$.

   Supongamos ahora que $a \mid b$ y $b \mid a$. De esta manera, $a = q_1 b$ y $b = q_2 a$ para algunos $q_1, q_2 \in \mathbb{Z}$. Sustituyendo la segunda ecuación en la primera y cancelando,

$$a = q_1 q_2 a$$
$$1 = q_1 q_2$$

   La única forma de que el producto de dos enteros sea igual a 1 es que $q_1 = q_2 = \pm 1$. Por lo tanto, $a = \pm b$.

■

Teorema A.6 (algoritmo de la división). Sean $a, b \in \mathbb{Z}$ con $b > 0$. Entonces existen únicos enteros q y r tales que

$$a = bq + r$$

donde $0 \leq r < b$.

Demostración. Primero se demostrará que existen tales enteros q y r. Sea S el conjunto

$$S = \{a - bk : k \in \mathbb{Z}\}$$

Si $0 \in S$, entonces $0 = a - bk_1$ para algún $k_1 \in \mathbb{Z}$, por lo que $a = bk_1$. En tal caso tenemos que $q = k_1$ y $r = 0$. Supongamos que $0 \notin S$. El conjunto $S \cap \mathbb{N}$ es no vacío porque $a + 2|a|\, b \in S$ (si $a > 0$, $a + 2ab = a(1 + 2b) > 0$, y si $a < 0$, $a - 2ab = a(1 - 2b) > 0$). Por el principio del buen orden, $S \cap \mathbb{N}$ posee un elemento mínimo, digamos $r = a - qb$ para algún $q \in \mathbb{Z}$. Por lo tanto,

$$a = qb + r, \text{ con } r \geq 0$$

Es necesario probar que $r < b$. Por reducción al absurdo, supongamos que $r \geq b$. Si $r = b$, entonces

$$a - b(q + 1) = a - bq - b = r - b = 0 \in S$$

lo cual no es posible porque $0 \notin S$. Si $r > b$, entonces

$$a - b(q + 1) = r - b > 0$$

y

$$a - b(q + 1) \in S \cap \mathbb{N}.$$

Sin embargo,

$$a - b\,(q+1) = r - b < r$$

lo cual es una contradicción porque r es un elemento mínimo de $S \cap \mathbb{N}$. Luego $r < b$.

Finalmente, sólo resta demostrar que q y r son únicos. Supongamos que existen q' y r' tales que

$$a = q'b + r' \text{ con } 0 \leq r' < b$$

Por conveniencia, supongamos que $r' \geq r$. Entonces,

$$qb + r = q'b + r'$$

y de ahí tenemos que

$$b\,(q - q') = r' - r.$$

Así, $b \mid r' - r$. Supongamos que $r' - r \neq 0$. Entonces por el inciso 2) del lema A.5, $b \leq r' - r$ (no usamos valor absoluto porque ambos números son no negativos). Sin embargo, también $0 \leq r' - r \leq r' < b$, lo cual es una contradicción. Luego, $r' - r = 0$. Por lo tanto $r = r'$ y $q = q'$. ■

El entero q en el algoritmo de la división es llamado el cociente de dividir a entre b, y el entero r es llamado el residuo.

Definición A.7 (máximo común divisor). Decimos que $d \in \mathbb{N}$ es el máximo común divisor de $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, si se cumplen las siguientes propiedades:

1) $d \mid a$ y $d \mid b$ (es divisor común).
2) Si c es un entero tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Si d es el máximo común divisor de a y b escribimos

$$d = mcd\,(a, b)\,.$$

Definición A.8 (mínimo común múltiplo). Decimos que $m \in \mathbb{N}$ es mínimo común múltiplo de $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, si

1) $a \mid m$ y $b \mid m$ (es múltiplo común).
2) Si m' es un entero tal que $a \mid m'$ y $b \mid m'$ entonces $m \mid m'$.

Si m es el mínimo común múltiplo de a y b escribimos

$$m = mcm\,(a, b)\,.$$

Definición A.9 (primos relativos). Decimos que a y b son primos relativos siempre que $mcd\,(a,b) = 1$.

Una forma de obtener el máximo común divisor entre dos números es escribir los divisores de ambos números y observar cuál es el mayor de los divisores comunes. Por ejemplo, para encontrar $mcd\,(12,18)$ escribimos los divisores de 12: $1,2,3,4,6$ y 12; y los divisores de 18: $1,2,3,6,9$ y 18. El máximo de los divisores comunes es 6. Sin embargo, este puede ser un procedimiento muy lento si se usan números más grandes. Un método más eficiente es el llamado *algoritmo de Euclides*, pero antes de presentarlo mostraremos el siguiente teorema.

Teorema A.10 (del MCD). Para cualquier par $a,b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, existen $s_1, s_2 \in \mathbb{Z}$ tales que $mcd\,(a,b) = as_1 + bs_2$. Además $mcd\,(a,b)$ es el menor entero positivo de la forma $as_1 + bs_2$.

Demostración. Sea S el conjunto

$$S = \{am + bn : m,n \in \mathbb{Z},\, am + bn > 0\}$$

Es claro que S es no vacío porque si $am + bn < 0$ para alguna m,n entonces reemplazamos m por $-m$ y n por $-n$, $a\,(-m) + b\,(-n) > 0$. Por el principio del buen orden, existe un elemento mínimo, digamos $d = as_1 + bs_2$. Ahora se demostrará que $mcd\,(a,b) = d$.

Usando el algoritmo de la división con a y d tenemos que $a = qd + r$ donde $0 \leq r < d$. Si $r > 0$,

$$\begin{aligned} r &= a - dq \\ &= a - (as_1 + bs_2)\,q \\ &= a\,(1 - s_1 q) + b\,(-s_2 q) \in S \end{aligned}$$

Como $r < d$, esto contradice el hecho de que d es un elemento mínimo de S. Así, $r = 0$, y $d \mid a$. De manera similar, $d \mid b$.

Supongamos que d' es un entero tal que $d' \mid a$ y $d' \mid b$. Por el inciso 3) del lema A.5, $d' \mid as_1 + bs_2 = d$. Por lo tanto, $d = mcd\,(a,b)$. ■

Lema A.11. Si $a = qb + r$ entonces $mcd\,(a,b) = mcd\,(b,r)$.

Demostración. Sea $c = mcd\,(a,b)$ y $d = mcd\,(b,r)$. Por el inciso 3) del lema A.5, $d \mid (qb + r) = a$. Así, como $d \mid a$ y $d \mid b$, sabemos por definición que $d \mid c$. De manera similar, $c \mid (a - qb) = r$ por el inciso 3) del lema A.5. Como $c \mid b$ y $c \mid r$, tenemos que $c \mid d$. Usando el inciso 4) del lema A.5 obtenemos que $d = \pm c$, pero debido a que por definición $c,d \geq 1$, $d = c$. ■

Asumamos que $a, b > 0$ ya que $mcd(a,b) = mcd(\pm a, \pm b)$. La idea principal del algoritmo de Euclides es el uso repetido del algoritmo de la división:

$$\begin{aligned} a &= bq_1 + r_1 \quad \text{con } 0 < r_1 < b \\ b &= r_1 q_2 + r_2 \text{ con } 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 \text{ con } 0 < r_3 < r_2 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k \text{ con } 0 < r_k < r_{k-1} \\ r_{k-1} &= r_k q_{k+1} + 0 \end{aligned}$$

Ya que $b > r_1 > r_2 > \ldots \geq 0$, es posible afirmar que debe llegarse a un residuo $r_k = 0$ después de un máximo de b pasos. El algoritmo de Euclides garantiza que

$$r_k = mcd(a,b)$$

Para mostrar esto, observemos que por el lema anterior

$$mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2) = \ldots = mcd(r_{k-1}, r_k)$$

De la última ecuación vemos que $r_k \mid r_{k-1}$, así que $mcd(r_{k-1}, r_k) = r_k$.

El algoritmo de Euclides también permite escribir al máximo común divisor como una combinación lineal de a y b, de acuerdo con al teorema A.10. El procedimiento consiste en despejar de la penúltima ecuación r_k

$$r_k = r_{k-2} - r_{k-1} q_k$$

y sustituir el resto de las ecuaciones anteriores

$$\begin{aligned} r_{k-1} &= r_{k-3} - r_{k-2} q_{k-1} \\ r_{k-2} &= r_{k-4} - r_{k-3} q_{k-2} \\ &\vdots \end{aligned}$$

hasta llegar a una expresión que contenga a y b.

Ejemplo A.12. Usaremos el algoritmo de Euclides para obtener el máximo común divisor de 15 y 49.

$$\begin{aligned} 49 &= 15 \cdot 3 + 4 \\ 15 &= 4 \cdot 3 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Por lo tanto, $mcd\,(15, 49) = 1$. Despejando los residuos

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ 3 &= 15 - 4 \cdot 3 \\ 4 &= 49 - 15 \cdot 3 \end{aligned}$$

Ahora podemos escribir 1 como combinación lineal de 15 y 49.

$$\begin{aligned} 1 &= 4 - \mathbf{3} \cdot 1 \\ &= 4 - (15 - 4 \cdot 3) \cdot 1 \\ &= \mathbf{4} \cdot 4 - 15 \\ &= (49 - 15 \cdot 3) \cdot 4 - 15 \\ &= 49 \cdot 4 - 15 \cdot 13 \end{aligned}$$

Lema A.13 (de Euclides). Sean $a, b \in \mathbb{Z}$. Si p es un primo tal que $p \mid ab$ entonces $p \mid a$ o $p \mid b$.

Demostración. Supongamos que $p \nmid a$. Se demostrará que $p \mid b$. Como $p \nmid a$, tenemos que $mcd\,(p, a) = 1$, y por el teorema A.10, para algunos $s_1, s_2 \in \mathbb{Z}$

$$1 = ps_1 + as_2$$

Multiplicando por b obtenemos

$$b = ps_1 b + abs_2$$

Como $p \mid abs_2$ y $p \mid ps_1 b$, tenemos que $p \mid b$. ■

Un modo alternativo de enunciar el lema de Euclides es, si $p \mid ab$ donde p es primo relativo con a, entonces p divide a b.

Es un error pensar que el lema de Euclides se cumple si p no es un número primo. Es decir, que si $p \mid ab$ no es necesariamente cierto que $p \mid a$ o $p \mid b$. Por ejemplo, $6 \mid 3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$.

Lema A.14 (generalizado de Euclides). Sean $a_i \in \mathbb{Z}$, $i = 1, \ldots n$. Si p es un primo tal que $p \mid a_1 a_2 \ldots a_n$ entonces $p \mid a_i$, para alguna i.

Demostración. *Ejercicio A.5.* ■

Euclides fue un matemático griego nacido en Alejandría hacia el año 325 a.C. A pesar de que prácticamente no se sabe nada sobre su vida, Euclides se ha transformado en uno de los iconos de las matemáticas más conocidos actualmente. En su obra más importante, *Elementos*, desarrolla de manera axiomática la geometría y la

aritmética. Él fue uno de los primeros matemáticos en utilizar en sus demostraciones la poderosa técnica de reducción al absurdo. El lema de Euclides nos servirá en muchas ocasiones.

Por fin, el siguiente teorema revela la importancia de los números primos.

Teorema A.15 (teorema fundamental de la aritmética). Cualquier entero mayor que 1 es un primo o es producto de primos. Además, este producto es único excepto por el orden en el que aparecen los factores.

Demostración. Demostraremos la primera parte del teorema por inducción. Para $n = 2$, n es un primo, así que el teorema se cumple. Supongamos que se cumple para toda $k \leq n$. Sea ahora $n = k + 1$. Si n es un primo no hay nada que hacer. Si n es un número compuesto, significa que existen otros divisores distintos de 1 y él mismo. Así $n = ab$, para algunos $a, b \in \mathbb{Z}$, $1 < a < n$, $1 < b < n$. Por hipótesis de inducción, a es primo o producto de primos, y b es primo o producto de primos. Por lo tanto, n es producto de primos.

Para demostrar la unicidad supongamos que $n = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$, donde p_i y q_j son primos $i = 1, \dots, n$, $j = 1, \dots, m$. Sin perder generalidad, supongamos que $n \leq m$. Como $p_1 \mid n$, por el lema generalizado de Euclides, $p_1 \mid q_k$ para alguna k. Sin embargo, debido a que p_1 y q_k son primos tenemos que $p_1 = q_k$. Renombremos a q_k como q_1. Entonces $p_2 \dots p_n = q_2 \dots q_m$ por cancelación. Repitiendo el mismo argumento obtenemos que $p_2 = q_2$, $p_3 = q_3$, $\dots$, $p_n = q_n$. Así, de nuevo por cancelación, obtenemos que $1 = q_{n+1} \dots q_m$, por lo que $q_{n+1} = \dots = q_m = 1$, lo que implica que $n = m$. ■

A.2 Congruencias módulo n

Definición A.16 (congruencia módulo n). Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$. Decimos que a es congruente con b módulo n si $n \mid a - b$. En tal caso escribimos $a \equiv b \pmod{n}$.

La relación "a es congruente con b módulo n" es una relación de equivalencia. Esta relación de equivalencia es muy útil en la construcción de tipos especiales de anillos del capítulo 1.

Proposición A.17. Si $a \equiv b \pmod{n}$ entonces para cualquier $s \in \mathbb{Z}$, $a + s \equiv b + s \pmod{n}$.

Demostración. Como a es congruente con b módulo n, $n \mid a-b$; es decir, para algún $q \in \mathbb{Z}$

$$a - b = qn$$

De esta forma, para cualquier $s \in \mathbb{Z}$

$$(a+s) - (b+s) = qn$$

por lo que $a + s \equiv b + s \pmod{n}$. ■

Proposición A.18. Si $as \equiv bs \pmod{n}$, donde s y n son primos relativos, entonces $a \equiv b \pmod{n}$.

Demostración. La expresión $as \equiv bs \pmod{n}$ significa que para algún $q \in \mathbb{Z}$

$$\begin{aligned} as - bs &= qn \\ s(a-b) &= qn \end{aligned}$$

De aquí observamos que $s \mid qn$, y sabemos que $mcd(s,n) = 1$. Por el lema de Euclides obtenemos que $s \mid q$. Entonces $q = sk$ para algún $k \in \mathbb{Z}$ y

$$\begin{aligned} s(a-b) &= skn \\ a - b &= kn \end{aligned}$$

Por lo tanto $a \equiv b \pmod{n}$. ■

Si se desea profundizar en este tema (o en el tema de teoría de números en general), se recomienda ampliamente el libro *Elementary number theory* (Jones y Josephine, 1998).

A.3 Ejercicios

A.1. Responde y justifica los siguientes incisos:

a) Determina

$$mcd\left(2^4 \cdot 3^2 \cdot 5 \cdot 7, 2 \cdot 3^3 \cdot 7 \cdot 11\right) \quad \text{y}$$
$$mcm\left(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11\right).$$

b) Usa el algoritmo de Euclides para encontrar el

$$mcd\,(1485, 1745)$$

y escríbelo como una combinación lineal de 1485 y 1745.

A.2. Demuestra las siguientes afirmaciones:

a) Si $a \mid b$ y $c \mid d$ entonces $ac \mid bd$.

b) Si $m \neq 0$, entonces $a \mid b$ si y sólo si $ma \mid mb$.

A.3. Sean $p_1, p_2, \ldots, p_n$ primos. Muestra que $p_1 p_2 \ldots p_n + 1$ no es divisible por ninguno de esos primos. Usa este hecho para demostrar que hay infinitos números primos.

A.4. Sea $d = mcd\,(a, b)$, $a, b \in \mathbb{Z}$. Muestra que si $a = da'$ y $b = db'$ entonces $mcd\,(a', b') = 1$.

A.5. Demuestra el *lema generalizado de Euclides* (lema A.14).

A.6. Demuestra que si $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, y $a \equiv b \pmod{n}$ entonces $as \equiv bs \pmod{n}$ para toda $s \in \mathbb{Z}$.

A.7. Demuestra que la relación "a es congruente con b módulo n" es una relación de equivalencia.

B

Teoría de grupos

Una pieza musical puede ser acompañada por palabras, movimiento, o baile, o simplemente apreciada por sí misma. Es lo mismo con los grupos. Pueden ser vistos como grupos de simetrías, permutaciones, o movimientos, o pueden ser simplemente estudiados y admirados por sí mismos.

Mark Ronan, matemático inglés

En este apéndice desarrollaremos los conceptos básicos de la teoría de grupos. Es muy recomendable que el lector esté familiarizado con estos conceptos antes de comenzar el capítulo 1, "Propiedades básicas de los anillos".

Definición B.1 (operación binaria). Sea S un conjunto. Una operación binaria $\cdot$ es una función de la forma $\cdot : S \times S \to S$.

Definición B.2 (grupo). Sea G un conjunto no vacío y $\cdot$ una operación binaria. Decimos que el par $(G, \cdot)$ es un grupo si se cumplen las siguientes condiciones:

1) *Asociatividad.* Para toda $a, b, c \in G$ se cumple que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2) *Identidad.* Existe un elemento $e \in G$ tal que $a \cdot e = a$ para toda $a \in G$.
3) *Inversos.* Para cada $a \in G$ existe un elemento $b \in G$ tal que $ab = e$. En ese caso escribimos $b = a^{-1}$.

Cuando se quiera verificar que un conjunto G y una operación binaria $\cdot$ forman un grupo, es importante asegurarse de que la operación binaria esté bien definida; esto es, que $a \cdot b \in G$ para toda $a, b \in G$. Comúnmente llamamos a esta propiedad la propiedad de cerradura de un grupo. Otra condición necesaria para que la operación binaria esté bien definida es que si $a = a'$ y $b = b'$ entonces $a \cdot b = a' \cdot b'$.

A partir de ahora si $(G, \cdot)$ es un grupo, escribiremos sólo la letra G para representarlo. Además escribiremos ab en lugar de $a \cdot b$.

Ejemplo B.3 ($\mathbb{Z}$). El conjunto $\mathbb{Z}$ junto con la suma usual de números enteros es un grupo. El elemento identidad es el 0, y el inverso de $a \in \mathbb{Z}$ es $-a \in \mathbb{Z}$.

Ejemplo B.4 ($GL_2(\mathbb{R})$). Consideremos el conjunto

$$GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \det A \neq 0,\ a, b, c, d \in \mathbb{R} \right\}$$

donde $\det A = ad - bc$. Este conjunto, junto con la multiplicación de matrices, forma un grupo. La propiedad de cerradura se cumple ya que si $A, B \in GL_2(\mathbb{R})$, $\det A \neq 0$, $\det B \neq 0$, entonces $\det AB = (\det A)(\det B) \neq 0$, por lo que $AB \in GL_2(\mathbb{R})$. La propiedad asociativa se cumple porque la multiplicación de matrices es

asociativa. El elemento identidad del grupo es

$$Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, el inverso de A es

$$A^{-1} = \begin{pmatrix} \dfrac{d}{ad-bc} & -\dfrac{b}{ad-bc} \\ -\dfrac{c}{ad-bc} & \dfrac{a}{ad-bc} \end{pmatrix}$$

Ejemplo B.5. Sea $n \in \mathbb{N}$. Consideremos el conjunto de clases de equivalencia $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ de la relación módulo n (véase definición A.16). Definamos la suma de clases como $[m] + [k] = [m+k] \in \mathbb{Z}_n$, donde $[m], [k] \in \mathbb{Z}_n$. Para demostrar que esta operación está bien definida, supongamos que $[m] = [m']$ y que $[k] = [k']$. Esto significa que $n \mid (m - m')$ y que $n \mid (k - k')$. Por el lema A.5,

$$n \mid (m - m') + (k - k') = (m + k) - (m' + k')$$

así que $[m + k] = [m' + k']$. Así, $\mathbb{Z}_n$ junto con la suma de clases de equivalencia, forma un grupo. La identidad es $[0] \in \mathbb{Z}_n$, y el inverso de $[a] \in \mathbb{Z}_n$ es $[-a] \in \mathbb{Z}_n$. Además, se cumple la propiedad asociativa porque, para cualquier $[a], [b], [c] \in \mathbb{Z}_n$,

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

Lema B.6 (cancelación). Se G un grupo. Si $a, b, c \in G$ y $ac = bc$ entonces $a = b$.

Demostración. Usando las propiedades de la definición, si $ac = bc$ entonces

$$\begin{aligned} (ac)\, c^{-1} &= (bc)\, c^{-1} \\ a\left(cc^{-1}\right) &= b\left(cc^{-1}\right) \\ ae &= be \\ a &= b \end{aligned}$$

■

Teorema B.7 (unicidad de los inversos). Sea G un grupo. Si a^{-1} es el inverso de a, entonces $aa^{-1} = a^{-1}a = e$ y a^{-1} es único.

Demostración. Primero mostraremos que $a^{-1}a = e$. Observemos que

$$\begin{aligned}\left(a^{-1}a\right)\left(a^{-1}a\right) &= a^{-1}\left(aa^{-1}\right)a \\ &= a^{-1}ea \\ &= a^{-1}a \\ &= e\left(a^{-1}a\right)\end{aligned}$$

y por cancelación

$$a^{-1}a = e$$

Para demostrar la unicidad supongamos que $b \in G$ es tal que $ab = e$. Entonces

$$\begin{aligned}a^{-1} &= a^{-1}e = a^{-1}(ab) \\ &= \left(a^{-1}a\right)b = eb \\ &= b\end{aligned}$$

■

Teorema B.8 (unicidad de la identidad). Sea G un grupo. Si $e \in G$ es la identidad en G, entonces $ae = ea = a$ para toda $a \in G$ y e es única.

Demostración. *Ejercicio B.1.* ■

Una vez demostrados estos teoremas es sencillo darse cuenta de que la cancelación izquierda también existe: si $ca = cb$ entonces $a = b$ para cualesquiera $a, b, c \in G$.

Definición B.9 (orden de un grupo). El orden de un grupo G es la cardinalidad del conjunto G.

Definición B.10 (grupo abeliano). Decimos que un grupo G es abeliano si se cumple la siguiente propiedad:

4) *Conmutatividad.* Para toda $a, b \in G$ se cumple que $ab = ba$.

Ejemplo B.11. El grupo $\mathbb{Z}$ es abeliano, mientras que el grupo $GL_2(\mathbb{R})$ no es abeliano. Por ejemplo,

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Definición B.12 (subgrupo). Sea G un grupo y $H \subseteq G$. Decimos que H es un subgrupo de G si H es en sí mismo un grupo bajo la misma operación de G. En tal caso escribimos $H \leq G$.

Decimos que H es un subgrupo propio de G y escribimos $H < G$ si H es un subconjunto propio de G (es decir, $H \subsetneq G$).

Teorema B.13 (test del subgrupo). Sea G un grupo y $H \subseteq G$, $H \neq \emptyset$. Entonces $H \leq G$ si y sólo si se cumple que para toda $a, b \in H$, $ab^{-1} \in H$.

Demostración. Obviamente, si H es un subgrupo de G, $ab^{-1} \in H$ para toda $a, b \in H$ por cerradura. Supongamos ahora que se cumple que $ab^{-1} \in H$ para toda $a, b \in H$. Como H es no vacío, existe al menos un $g \in H$. Tomando $a = b = g$, obtenemos que $ab^{-1} = gg^{-1} = e \in H$. Por lo tanto H contiene al elemento identidad. Ahora, si $g \in G$, tomando $a = e$, $b = g$, tenemos que $ab^{-1} = eg^{-1} = g^{-1} \in H$. Por lo tanto H contiene al inverso de cada elemento. La cerradura se cumple porque si $g, h \in H$, podemos tomar $a = g$, $b = h^{-1}$, así que $ab^{-1} = g\left(h^{-1}\right)^{-1} = gh \in H$, por el *ejercicio B.2*. La propiedad asociativa se cumple porque la operación en H es la misma que la operación en G. De esta forma, H es un grupo en sí mismo, y un subgrupo de G. ■

Si G es un grupo y $g \in G$, definimos el conjunto $\langle g \rangle$ como

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

Es sencillo verificar que $\langle g \rangle$ es un subgrupo de G (*ejercicio B.5.*).

Definición B.14 (grupo cíclico). Sea G un grupo. Decimos que G es cíclico si $G = \langle g \rangle$ para algún $g \in G$. Llamamos al elemento g un generador de G.

Ejemplo B.15. Consideremos el grupo de enteros $\mathbb{Z}$ con la suma. Obviamente en este caso, si $g \in \mathbb{Z}$, entonces g^n significa $g + g + \ldots + g$ donde hay n sumandos. Por tal motivo, cuando la operación del grupo es la suma, en lugar de escribir g^n escribimos $n \cdot g$. El grupo $\mathbb{Z}$ es cíclico ya que $\mathbb{Z} = \langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\}$.

Definición B.16 (orden de un elemento). Sea G un grupo y $g \in G$. El orden de g, denotado como $|g|$ es el orden del grupo $\langle g \rangle$.

Ejemplo B.17. Sea

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Observemos que $A^2 = Id$, $A^3 = A^2A = A$, etc., así que $\langle A \rangle = \{A, Id\}$. Por lo tanto, $|A| = |\langle A \rangle| = 2$.

Teorema B.18. Sea $G = \langle g \rangle$ un grupo cíclico. Si $H \leq G$, entonces H es cíclico.

Demostración. Si $H = \{e\}$ entonces H es cíclico generado por la identidad $e \in G$. Supongamos que $H \neq \{e\}$. Como el conjunto G consiste en elementos de la forma g^k para $k \in \mathbb{Z}$, los elementos de H tienen la misma forma. Consideremos el conjunto

$$S = \left\{k \in \mathbb{Z} : g^k \in H\right\} \cap \mathbb{N}$$

Obviamente, S es no vacío, ya que si $g^r \in H$, con $r < 0$, entonces su inverso $(g^r)^{-1} = g^{-r} \in H$, donde $-r > 0$. Así $-r \in S$. Por el principio del buen orden, sea n un elemento mínimo de S. Ahora demostraremos que $H = \langle g^n \rangle$. Como $g^n \in H$, es claro que $\langle g^n \rangle \subseteq H$. Tomemos $g^k \in H$. Por el algoritmo de la división (teorema A.6), para algunos $q, r \in \mathbb{Z}$

$$k = qn + r \text{ con } 0 \leq r < n$$

Entonces $g^k = g^{qn+r} = g^{qn}g^r$, y $g^r = g^{-qn}g^k \in H$, porque $g^{-qn} = (g^n)^{-q} \in H$ y $g^k \in H$. Como n es un elemento mínimo en S, y $0 \leq r < n$, debemos tener que $r = 0$. Por lo tanto $k = qn$, y $g^k = (g^n)^q \in \langle g^n \rangle$. Por lo tanto, $H \subseteq \langle g^n \rangle$, y $H = \langle g^n \rangle$. ■

Definición B.19 (clase lateral). Sea G un grupo, $H \leq G$ y $a \in G$. El conjunto $Ha = \{ha \in G : h \in H\}$ es llamado la clase lateral derecha de H en G que contiene a a. El conjunto $aH = \{ah : h \in H\}$ es llamado la clase lateral izquierda de H en G que contiene a a.

Lema B.20. Sea G un grupo, $H \leq G$ y $a, b \in G$. Entonces $aH = bH$ si y sólo si $a \in bH$ si y sólo si $b^{-1}a \in H$.

Demostración. Primero mostraremos que $aH = bH \implies a \in bH$. Como $e \in H$ por ser subgrupo, entonces $a = ae \in aH = bH$.

Ahora mostraremos que $a \in bH \implies b^{-1}a \in H$. Si $a \in bH$, entonces existe un $h \in H$ tal que $a = bh$. Multiplicando por b^{-1} la relación anterior obtenemos que

$$b^{-1}a = b^{-1}bh = h \in H$$

Finalmente mostraremos que $b^{-1}a \in H \implies aH = bH$. Sea $ah \in aH$ con $h \in H$. Entonces

$$\begin{aligned} ah &= \left(bb^{-1}\right)ah \\ &= b\left(b^{-1}ah\right) \in bH \end{aligned}$$

ya que $(b^{-1}a)\,h \in H$ por cerradura. Así $aH \subseteq bH$. Ahora bien, sea $bh \in bH$ con $h \in H$. Debido a que H es un subgrupo, el inverso de $b^{-1}a$ debe pertenecer a H. Por el *ejercicio B.2* $(b^{-1}a)^{-1} = a^{-1}b \in H$. Entonces

$$\begin{aligned} bh &= \left(aa^{-1}\right)bh \\ &= a\left(a^{-1}bh\right) \in aH \end{aligned}$$

ya que $(a^{-1}b)\,h \in H$ por cerradura. Así $bH \subseteq aH$. Por lo tanto $aH = bH$. ■

Puede demostrarse, de manera similar, un lema análogo al lema B.20 para clases laterales derechas, $Ha = Hb$ si y sólo si $a \in Hb$ si y sólo si $ba^{-1} \in H$.

Lema B.21. Si $H \leq G$, entonces

$$G = \bigcup_{a \in G} aH$$

Demostración. Sea $x \in G$. Entonces $x \in xH$, así que $x \in \bigcup_{a \in G} aH$. Esto implica que $G \subseteq \bigcup_{a \in G} aH$. Sea $x \in \bigcup_{a \in G} aH$. Entonces $x \in yH$ para alguna $y \in G$. De esta forma $x = yh$ para alguna $h \in H$. Como $H \leq G$ por cerradura debemos tener que $x \in G$. Por lo tanto, $\bigcup_{a \in G} aH \subseteq G$. ■

Lema B.22. Sean $a, b \in G$ y $H \leq G$. Si $aH \neq bH$ entonces $aH \cap bH = \emptyset$.

Demostración. Por reducción al absurdo, supongamos que $aH \cap bH \neq \emptyset$ y sea $g \in aH \cap bH$. Entonces $g = ah_1 = bh_2$ para algunos $h_1, h_2 \in H$. De esta forma $b^{-1}a = h_2 h_1^{-1} \in H$, lo cual implica que $aH = bH$ por el lema B.20. Esto es una contradicción. Por lo tanto, $aH \cap bH = \emptyset$. ■

Lema B.23. Si $H \leq G$, entonces $|H| = |aH| = |Ha|$ para toda $a \in G$.

Demostración. Una manera de demostrar que dos conjuntos tienen el mismo número de elementos es construir una biyección entre ambos conjuntos. Sea $\beta : H \longrightarrow aH$ la función definida como $\beta(h) = ah$ para $h \in H$. Notemos que $ah_1 = ah_2$ si y sólo si $h_1 = h_2$, para cualquier $h_1, h_2 \in H$, así que la función β está bien definida y es inyectiva. Además, β es sobreyectiva porque la preimagen de $ah \in aH$ es $h \in H$. Así β es una biyección y $|H| = |aH|$. En forma análoga se demuestra que $|H| = |Ha|$. ■

Lema B.24. Si $H \leq G$, el número de clases laterales derechas es igual al número de clases laterales izquierdas.

Demostración. Construiremos una función β entre el conjunto de clases laterales derechas y el conjunto de clases laterales izquierdas. Si $a \in G$, definamos $\beta(aH) = Ha^{-1}$. Observemos que $aH = bH$ si y sólo si $b^{-1}a \in H$ por el lema B.20. Por el *ejercicio B.2*, $b^{-1}a = b^{-1}\left(a^{-1}\right)^{-1}$ así que usando la versión del lema B.20 para clases laterales derechas sabemos que $b^{-1}a \in H$ si y sólo si $Ha^{-1} = Hb^{-1}$. Esto demuestra que β está bien definida y es inyectiva. Para demostrar que β es sobreyectiva, observemos que si Ha es una clase lateral derecha su preimagen es $a^{-1}H$. ■

Gracias al lema B.24 podemos referirnos sin ambigüedad al número de clases laterales en general, ya que este número no es alterado si utilizamos clases laterales derechas o izquierdas.

Definición B.25 (índice). Sea $H \leq G$. El número de clases laterales de H en G es llamado el índice de H en G. Se denota como $[G : H]$.

Ejemplo B.26 ($\mathbb{Z}_{12}$). Consideremos el grupo $\mathbb{Z}_{12} = \{[0], [1], \ldots, [11]\}$. Consideremos el subgrupo

$$H = \langle [3] \rangle = \{[0], [3], [6], [9]\}$$

Como la operación en $\mathbb{Z}_{12}$ es la suma, denotamos a la clase lateral $[k]H$ como $[k]+H$. Las clases laterales de H en $\mathbb{Z}_{12}$ son:

$$[0]+H=[3]+H=[6]+H=[9]+H=\{[0],[3],[6],[9]\}$$
$$[1]+H=[4]+H=[7]+H=[10]+H=\{[1],[4],[7],[10]\}$$
$$[2]+H=[5]+H=[8]+H=[11]+H=\{[2],[5],[8],[11]\}$$

Observemos que efectivamente todas las clases laterales son del mismo tamaño y forman una partición de $\mathbb{Z}_{12}$ (es decir que la unión de ellas es $\mathbb{Z}_{12}$ y la intersección de cualquier par de clases distintas es vacía). Además, el número de clases laterales es $[\mathbb{Z}_{12}:H]=3$.

Teorema B.27 (teorema de Lagrange). Si $H \leq G$ entonces

$$|G| = |H|\,[G:H]$$

Demostración. Por el lema B.21 y el lema B.22, el conjunto G es la unión disjunta de sus clases laterales. Además, por el lema B.23, todas las clases laterales tienen la misma cardinalidad. Así, el orden de G debe ser igual al tamaño de las clases laterales (que es $|H|$) por el número de clases laterales. Esto último es precisamente lo que representa $[G:H]$. ■

Corolario B.28. Si $H \leq G$, entonces $|H| \mid |G|$.

Corolario B.29. Si $a \in G$, entonces $|a| \mid |G|$.

Demostración. Debido a que $|a| = |\langle a\rangle|$ debemos tener que $|a| \mid |G|$ ya que por el teorema de Lagrange el orden de cualquier subgrupo debe dividir al orden del grupo. ■

B.1 Ejercicios

B.1. Demuestra el teorema unicidad de la identidad.

B.2. Demuestra que para toda $a, b \in G$:

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

b) $\left(a^{-1}\right)^{-1} = a$.

B.3. Verifica que los números complejos $\mathbb{C}$ junto con la multiplicación de números complejos, cumplen con todas las propiedades de la definición de un grupo.

B.4. Sea $n \in \mathbb{N}$, G un grupo y $a \in G$. Hagamos las siguientes convenciones: $a^n = aa \ldots a$ donde a está operado n veces del lado derecho, $a^{-n} = (a^{-1})(a^{-1}) \ldots (a^{-1})$ donde a^{-1} está operado n veces del lado derecho, y $a^0 = e$. Demuestra por inducción que para toda $a \in G$, y $r, s \in \mathbb{Z}$

a) $a^{r+s} = a^r a^s$.

b) $(a^r)^s = a^{rs}$.

B.5. Sea G un grupo y $g \in G$. Demuestra que $\langle g \rangle$ es un subgrupo de G.

B.6. Demuestra que el conjunto de números enteros pares es un subgrupo de los enteros $\mathbb{Z}$.

B.7. Calcula el orden de $\mathbb{Z}_6$ y el orden de cada uno de sus elementos. Haz lo mismo para $\mathbb{Z}_8$. ¿Esto contradice al teorema de Lagrange?

B.8. Sea $p \in \mathbb{N}$ un número primo. Demuestra que cualquier grupo de orden p es cíclico.

B.9. Demuestra que todo grupo cíclico es abeliano.

B.10. Sea G un grupo con $|G| = n$. Demuestra que $a^n = e$ para toda $a \in G$.

C

Espacios vectoriales

En matemáticas no entiendes las cosas. Sólo te acostumbras a ellas.

John von Neumann, matemático estadounidense

En este apéndice desarrollaremos los conceptos básicos de espacios vectoriales como subespacios, combinaciones lineales, conjuntos linealmente independientes, bases y dimensión. Es recomendable que el lector esté familiarizado con estos conceptos antes de comenzar el estudio del capítulo 11, "Extensiones algebraicas".

Definición C.1 (espacio vectorial). Sea F un campo y V un conjunto. Un espacio vectorial sobre F es una tríada $(V, +, \cdot)$ donde $+$ es una operación binaria sobre V llamada suma y $\cdot : F \times V \to V$ una operación llamada multiplicación por escalar. Además deben cumplirse las siguientes condiciones:

1) $(V, +)$ es un grupo abeliano.
2) *Identidad escalar*. Para toda $v \in V$, $1 \cdot v = v$, donde $1 \in F$.
3) *Asociatividad escalar*. Para toda $\alpha, \beta \in F$, $v \in V$, se cumple que $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$.
4) *Distributividad*. Para toda $\alpha, \beta \in F$, $u, v \in V$ se cumple que $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ y $\alpha \cdot (v + u) = \alpha \cdot v + \alpha \cdot u$.

Escribiremos αv en lugar de $\alpha \cdot v$ para denotar la multiplicación por escalar. A partir de ahora si $(V, +, \cdot)$ es un espacio vectorial, escribiremos sólo la letra V para representarlo.

Ejemplo C.2 ($\mathbb{R}^n$). Consideremos el conjunto $\mathbb{R}^n = \mathbb{R} \times \ldots \times \mathbb{R}$. Definamos en $\mathbb{R}^n$ la suma y la multiplicación por escalares de $\mathbb{R}$ como

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$\alpha\,(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n)$$

donde $\alpha, a_i, b_i \in \mathbb{R}$. De esta forma, $\mathbb{R}^n$ es un espacio vectorial sobre $\mathbb{R}$ *ejercicio C.2*.

Ejemplo C.3 ($M_2(\mathbb{R})$). El conjunto de matrices

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} : a_i \in \mathbb{R} \right\}$$

junto con la suma de matrices y la multiplicación por escalar definida como

$$\alpha \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} \alpha a_1 & \alpha a_2 \\ \alpha a_3 & \alpha a_4 \end{pmatrix} \text{ para } \alpha \in \mathbb{R}$$

es un espacio vectorial sobre $\mathbb{R}$. Demostraremos cada una de las propiedades de la definición de espacio vectorial:

1) Es claro que $(M_2(\mathbb{R}), +)$ es un grupo abeliano. Además, se cumple para cualesquiera $\alpha, \beta, a_i, b_i \in \mathbb{R}$,

2)

$$1\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

3)

$$\begin{aligned}(\alpha\beta)\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} &= \begin{pmatrix} (\alpha\beta)a_1 & (\alpha\beta)a_2 \\ (\alpha\beta)a_3 & (\alpha\beta)a_4 \end{pmatrix} \\ &= \begin{pmatrix} \alpha(\beta a_1) & \alpha(\beta a_2) \\ \alpha(\beta a_3) & \alpha(\beta a_4) \end{pmatrix} \\ &= \alpha\left(\beta\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\right)\end{aligned}$$

4)

$$\begin{aligned}(\alpha+\beta)\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} &= \begin{pmatrix} (\alpha+\beta)a_1 & (\alpha+\beta)a_2 \\ (\alpha+\beta)a_3 & (\alpha+\beta)a_4 \end{pmatrix} \\ &= \begin{pmatrix} \alpha a_1 + \beta a_1 & \alpha a_2 + \beta a_2 \\ \alpha a_3 + \beta a_3 & \alpha a_4 + \beta a_4 \end{pmatrix} \\ &= \alpha\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \beta\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\end{aligned}$$

Y también

$$\begin{aligned}\alpha\left(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}\right) &= \alpha\begin{pmatrix} a_1+b_1 & a_2+b_2 \\ a_3+b_3 & a_4+b_4 \end{pmatrix} \\ &= \begin{pmatrix} \alpha(a_1+b_1) & \alpha(a_2+b_2) \\ \alpha(a_3+b_3) & \alpha(a_4+b_4) \end{pmatrix} \\ &= \begin{pmatrix} \alpha a_1 + \alpha b_1 & \alpha a_2 + \alpha b_2 \\ \alpha a_3 + \alpha b_3 & \alpha a_4 + \alpha b_4 \end{pmatrix} \\ &= \alpha\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \alpha\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}\end{aligned}$$

Proposición C.4. Sea V un espacio vectorial sobre F. Entonces para todo $v \in V$ se tiene que $0v = \mathbf{0}$ donde $0 \in F$ y $\mathbf{0} \in V$.

Demostración. Observemos que para $1 \in F$,

$$\begin{aligned} 0v &= (1-1)\,v \\ &= 1v - 1v \\ &= v - v \\ &= \mathbf{0} \end{aligned}$$

■

Definición C.5 (subespacio vectorial). Sea V un espacio vectorial sobre F. Un subconjunto W de V es un subespacio vectorial de V sobre F si W es un espacio vectorial sobre F en sí mismo bajo las mismas operaciones de V.

Teorema C.6 (test del subespacio). Sea V un espacio vectorial sobre F y W un subconjunto no vacío de V. Entonces W es un subespacio vectorial de V sobre F si y sólo si se cumple que para toda $\alpha \in F$, $u, v \in W$, $u + v \in W$ y $\alpha v \in W$.

Demostración. *Ejercicio C.4.* ■

Definición C.7 (combinación lineal). Sea V un espacio vectorial sobre F. Una combinación lineal de $v_1, v_2, \ldots, v_n \in V$ sobre F es un elemento de la forma

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$$

donde $\alpha_1, \ldots, \alpha_n \in F$.

Definición C.8 (espacio generado). Sea V un espacio vectorial sobre F y $A \subseteq V$. El conjunto de combinaciones lineales sobre F de los elementos de A es llamado el espacio generado por A sobre F y se denota como $gen_F(A)$.

Observación C.9. El conjunto $gen_F(A)$ es un subespacio vectorial de V sobre F.

Ejemplo C.10. Consideremos el subconjunto $A = \{(1,0,0), (0,1,1)\}$ del espacio vectorial $\mathbb{R}^3$. Entonces el espacio generado por A sobre $\mathbb{R}$ es

$$\begin{aligned} gen_{\mathbb{R}}(A) &= \{\alpha_1 (1,0,0) + \alpha_2 (0,1,1) : \alpha_i \in \mathbb{R}\} \\ &= \{(\alpha_1, 0, 0) + (0, \alpha_2, \alpha_2) : \alpha_i \in \mathbb{R}\} \\ &= \{(\alpha_1, \alpha_2, \alpha_2) : \alpha_i \in \mathbb{R}\} \end{aligned}$$

Definición C.11 (linealmente dependiente). Sea V un espacio vectorial sobre F y $A \subseteq V$. Si existe un número finito de elementos $v_1, \ldots, v_n \in A$ tales que

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = \mathbf{0} \in V$$

para algunos $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ no todos cero, decimos que A es linealmente dependiente sobre F.

Definición C.12 (linealmente independiente). Sea V un espacio vectorial sobre F y $A \subseteq V$. Decimos que A es linealmente independiente sobre F si no es linealmente dependiente sobre F.

Ejemplo C.13. El subconjunto $A = \{(1,0),(1,1)\}$ de $\mathbb{R}^2$ es linealmente independiente sobre $\mathbb{R}$. Para demostrar esto, supongamos que

$$\alpha_1 (1,0) + \alpha_2 (1,1) = \mathbf{0}$$

para algunos $\alpha_1, \alpha_2 \in \mathbb{R}$. Claramente en este caso $\mathbf{0} \in \mathbb{R}^2$, así que $\mathbf{0} = (0,0)$. Observemos que la relación de arriba implica que

$$\begin{aligned} (\alpha_1, 0) + (\alpha_2, \alpha_2) &= (0,0) \\ (\alpha_1 + \alpha_2, \alpha_2) &= (0,0) \end{aligned}$$

Y entonces $\alpha_1 + \alpha_2 = 0$ y $\alpha_2 = 0$. Por lo tanto, $\alpha_1 = \alpha_2 = 0$ y A es un conjunto linealmente independiente sobre $\mathbb{R}$.

Ejemplo C.14. El subconjunto $A = \{(1,0),(1,1),(0,1)\}$ de $\mathbb{R}^2$ es linealmente dependiente sobre $\mathbb{R}$ porque

$$(1,0) - (1,1) + (0,1) = \mathbf{0}$$

Definición C.15 (base). Sea V un espacio vectorial sobre F y sea $B \subseteq V$. Si $gen_F(B) = V$ y B es linealmente independiente sobre F entonces decimos que B es una base de V sobre F.

Ejemplo C.16. El conjunto $B = \{(1,0),(1,1)\}$ es una base para $\mathbb{R}^2$ sobre $\mathbb{R}$. En un ejemplo previo ya se demostró que B es linealmente independiente sobre $\mathbb{R}$. Por cerradura, sabemos que $gen_{\mathbb{R}}(B) \subseteq \mathbb{R}^2$. Sea ahora $(x,y) \in \mathbb{R}^2$ un elemento arbitrario. Entonces

$$(x,y) = (x-y)(1,0) + y(1,1) \in gen_{\mathbb{R}}(B)$$

Por lo tanto, $\mathbb{R}^2 \subseteq gen_{\mathbb{R}}(B)$, y $gen_{\mathbb{R}}(B) = \mathbb{R}^2$.

Ejemplo C.17. Es fácil demostrar que el conjunto $B = \{(1,0),(0,1)\}$ es una base para $\mathbb{R}^2$ sobre $\mathbb{R}$. Llamamos a B la base canónica de $\mathbb{R}^2$ sobre $\mathbb{R}$.

Teorema C.18. El subconjunto B de un espacio vectorial V sobre F es una base si y sólo si cada elemento de V puede escribirse de forma única como combinación lineal sobre F de elementos de B.

Demostración. Supongamos que B es una base de V sobre F. Es claro que cualquier elemento de V puede escribirse como una combinación lineal sobre F de elementos de B porque $gen_F(B) = V$. Para demostrar la unicidad de esta representación, supongamos que existe un elemento $v \in V$ tal que

$$v = \alpha_1 b_1 + \ldots + \alpha_n b_n = \beta_1 b_1 + \ldots + \beta b_m$$

donde $\alpha_i, \beta_i \in F$, $b_i \in B$. Sin perder generalidad, supongamos que $n \geq m$. Entonces

$$(\alpha_1 - \beta_1) b_1 + \ldots + (\alpha_m - \beta_m) b_m + \alpha_{m+1} b_{m+1} + \ldots + \alpha_n b_n = 0$$

Como B es un conjunto linealmente independiente sobre F debemos tener que

$$\alpha_i - \beta_i = 0 \text{ para } 1 \leq i \leq m$$
$$\alpha_i = 0 \text{ para } i > m$$

Esto demuestra que $\alpha_i = \beta_i$ para toda i, así que ambas representaciones de v son idénticas.

Supongamos ahora que cualquier elemento de V puede escribirse únicamente como combinación lineal sobre F de elementos de B. Entonces $gen_F(B) = V$. Para demostrar que B es linealmente independiente, supongamos que

$$\alpha_1 b_1 + \ldots + \alpha_n b_n = \mathbf{0}$$

para algunos $\alpha_i \in F$, $b_i \in B$. Sabemos que

$$0b_1 + \ldots + 0b_n = \mathbf{0} \in V$$

Por la unicidad de la representación de los elementos de V como combinaciones lineales de elementos de B, debemos tener que $\alpha_i = 0$ para toda i, lo que demuestra que B es un conjunto linealmente independiente sobre F. Por lo tanto, B es una base para V sobre F. ■

Teorema C.19. Sea $B = \{b_1, \ldots, b_n\}$ una base de un espacio vectorial V sobre F. Entonces cualquier subconjunto de V con más de n elementos es linealmente dependiente sobre F. Además, cualquier subconjunto de V con menos de n elementos no genera a V sobre F.

Demostración. Sea $A = \{v_1, \ldots, v_m\}$ un subconjunto de V con $m > n$. Por reducción al absurdo, supongamos que A es linealmente independiente. Si $\mathbf{0} \in A$, A es linealmente dependiente sobre F por el *ejercicio C.4*, así que $\mathbf{0} \notin A$. Debido a que $gen_F(B) = V$, podemos escribir v_1 como

$$v_1 = \alpha_1 b_1 + \ldots + \alpha_n b_n \qquad (*)$$

donde $\alpha_i \in F$ no son todos cero (ya que de lo contrario $v_1 = \mathbf{0}$). Sin perder generalidad, supongamos que $a_1 \neq 0$. Ahora sostenemos que el conjunto $A_1 = \{v_1, b_2, \ldots, b_n\}$ genera a V. Observemos que $b_1 \in gen_F(A_1)$ ya que, de la relación $(*)$,

$$b_1 = \frac{1}{\alpha_1}(v_1 - \alpha_2 b_2 - \ldots - \alpha_n b_n)$$

Así, $B \subseteq gen_F(A_1)$, por lo que $V = gen_F(B) \subseteq gen_F(A_1)$. Luego $gen_F(A_1) = V$. Ahora podemos escribir a v_2 como

$$v_2 = \beta_1 v_1 + \beta_2 b_2 + \ldots + \beta_n b_n$$

donde $\beta_i \in F$ no son todos cero. Sin perder generalidad, podemos suponer que $\beta_2 \neq 0$ (si $\beta_1 \neq 0$ y $\beta_i = 0$ para toda $i \neq 1$, entonces v_1 y v_2 son linealmente dependientes, lo que implica que A es linealmente dependiente). El conjunto $A_2 = \{v_1, v_2, b_3, \ldots, b_n\}$ genera a V porque

$$b_2 = \frac{1}{\beta_2}(v_2 - \beta_1 v_1 - \beta_3 b_3 - \ldots - \beta_n b_n) \in gen_F(A_2)$$

y entonces $A_1 \subseteq gen_F(A_2)$, por lo que $V = gen_F(A_1) \subseteq gen_F(A_2)$. Continuando con este proceso, podemos demostrar que el conjunto $A_n = \{v_1, \ldots, v_n\}$ genera a V. Por lo tanto, $v_{n+1} \in A$ puede ser escrito como una combinación lineal de los elementos de A_n. Es decir,

$$\begin{aligned} v_{n+1} &= \gamma_1 v_1 + \ldots + \gamma_n v_n \\ 0 &= \gamma_1 v_1 + \ldots + \gamma_n v_n - v_{n+1} \end{aligned}$$

donde $\gamma_i \in F$ no son todos cero. Esto implica que el subconjunto $\{v_1, \ldots, v_{n+1}\} \subseteq A$ es linealmente dependiente, por lo que el conjunto A es linealmente dependiente (*ejercicio C.4.*).

Supongamos ahora que $A = \{v_1, \ldots, v_m\}$ con $m < n$. Por reducción al absurdo, supongamos que $gen_F(A) = V$. Repitiendo el procedimiento del párrafo anterior, podemos demostrar que $A_1' = \{b_1, v_2, \ldots, v_m\}$ genera a V, que $A_2' = \{b_1, b_2, v_3, \ldots, v_m\}$ genera a V, y, continuando este proceso, que $A_n' = \{b_1, \ldots, b_m\}$ genera a V. Por lo tanto, $b_{m+1} \in B$ es una combinación lineal sobre F de $b_1, \ldots, b_m$, lo cual contradice que B sea linealmente independiente. Esto demuestra que $gen_F(A) \subsetneq V$. ■

Corolario C.20. Si $B = \{v_1, \ldots, v_n\}$ y $B' = \{w_1, \ldots, w_m\}$ son bases del espacio vectorial V sobre F, entonces $n = m$.

Demostración. Si B es una base de V sobre F con n elementos, por el teorema C.19, cualquier conjunto que genere a V y que sea linealmente independiente sobre F debe tener exactamente n elementos. ■

Definición C.21 (espacio de dimensión finita). Sea V un espacio vectorial no trivial sobre F. Si V posee un subconjunto infinito linealmente independiente, decimos que V es de dimensión infinita. En caso contrario, decimos que V es de dimensión finita.

Teorema C.22. Sea V un espacio vectorial sobre F de dimensión finita. Si $A \subseteq V$ es linealmente independiente sobre F, entonces A puede ser extendido para formar una base de V.

Demostración. Sea $A_0 = A$. Si $gen_F(A_0) = V$, entonces A_0 ya es una base. Si $gen_F(A_0) \subsetneq V$, tomemos $v_1 \in V \setminus gen_F(A_0)$. Demostraremos que el conjunto $A_1 = A_0 \cup \{v_1\}$ es linealmente independiente sobre F. Por reducción al absurdo, supongamos que A_1 es linealmente dependiente sobre F. Entonces,

$$\beta_1 v_1 + \beta_2 a_2 + \ldots + \beta_n a_n = 0 \qquad (**)$$

para algunos $\beta_i \in F$ no todos cero, $a_i \in A_0$. Observemos que $\beta_1 \neq 0$, ya que si $\beta_1 = 0$, la relación $(**)$ de arriba implica que el conjunto A_0 es linealmente dependiente. Por lo tanto,

$$v_1 = \frac{1}{\beta_1}(-\beta_2 a_2 - \ldots - \beta_n a_n) \in gen_F(A)$$

lo cual contradice que $v_1 \notin gen_F(A)$.

Ahora, si $gen_F(A_1) = V$, entonces A_1 es una base para V sobre F. Si $gen_F(A_1) \subsetneq V$, tomemos $v_2 \in V \setminus gen_F(A_1)$. Usando el mismo razonamiento que antes, el conjunto $A_2 = A_1 \cup \{v_2\}$ es linealmente independiente sobre F. Continuemos este proceso construyendo A_3, A_4, etc. Como V es de dimensión finita, debemos tener que el conjunto A_k es linealmente dependiente sobre F para alguna $k \in \mathbb{N}$. Tomemos a k como el menor entero positivo con tal propiedad, por lo tanto, $gen_F(A_{k-1}) = V$, y el conjunto A_{k-1} es una base para V sobre F. ■

Corolario C.23. Todo espacio vectorial de dimensión finita tiene una base.

Demostración. Sea V un espacio vectorial sobre F de dimensión finita. Sea $v \in V$, $v \neq 0$. Entonces, el conjunto $A = \{v\}$ es linealmente independiente sobre F, así que por el teorema anterior puede extenderse a una base. ■

Definición C.24 (dimensión). Sea V un espacio vectorial de dimensión finita sobre F y B una base de V sobre F. Sea $n \in \mathbb{N}$ la cardinalidad del conjunto B. Entonces decimos que la dimensión de V sobre F es n y escribimos $\dim_F V = n$.

C.1 Ejercicios

C.1. Sea V un espacio vectorial sobre F. Demuestra que $(-\alpha)v = \alpha(-v) = -\alpha v$ para toda $\alpha \in F$, $v \in V$.

C.2. Demuestra que $\mathbb{R}^n$ es un espacio vectorial sobre $\mathbb{R}$.

C.3. Sea V un espacio vectorial sobre F y $A \subseteq V$. Demuestra que $gen_F(A)$ es un subespacio vectorial de V.

C.4. Demuestra el test del subespacio.

C.5. Determina si los conjuntos A son linealmente dependientes o independientes sobre F. Justifica tu respuesta.

a) $A = \{(4,2), (6,3)\}$ sobre $\mathbb{R}$.

b) $A = \{(1,1,1), (0,1,1), (0,0,1)\}$ sobre $\mathbb{R}$.

c) $A = \left\{ \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 3 & 1 \end{pmatrix} \right\}$ sobre $\mathbb{R}$.

C.6. Sea V un espacio vectorial sobre F y $A \subseteq V$. Demuestra que

a) Si $\mathbf{0} \in A$, entonces A es linealmente dependiente sobre F.

b) Si $B \subseteq A$ es linealmente dependiente sobre F, entonces A es linealmente dependiente sobre F.

C.7. Sea V un espacio vectorial sobre F. Demuestra que si

$$A = \{v_1, \ldots, v_n\} \subseteq V$$

es un conjunto linealmente dependiente sobre F, entonces, para alguna k, el vector $v_k \in A$ es una combinación lineal del conjunto $A \setminus \{v_k\}$ sobre F.

C.8. Sea V un espacio vectorial sobre F, y sea $A = \{v_1, \ldots, v_n\}$ tal que $gen_F(A) = V$. Demuestra que existe un subconjunto $B \subseteq A$ tal que B es una base para V sobre F.

D

El campo de los números complejos

Un matemático es una máquina para transformar café en teoremas.

Paul Erdős, matemático húngaro

Una obstinación, digna de la mejor imitación, en la historia de las matemáticas se observa en la larga lucha entre los defensores y los enemigos de los números "imaginarios", como fuente de los cuales sirve la ecuación algebraica

$$x^2 + 1 = 0 \tag{D.1}$$

Podemos tomar una posición simplista, limitándonos a la escritura formal de las soluciones de la ecuación (D.1), en forma de $\pm\sqrt{-1}$. Pero esto no era difícil hacerlo en tiempos más lejanos; sólo queda darle sentido a la escritura indicada. Resolveremos este problema introduciendo algunas reflexiones heurísticas.

D.1 Construcción auxiliar

Deseamos ampliar el campo de los números reales $\mathbb{R}$ de tal modo que, en el nuevo campo, la ecuación (D.1) tenga solución. Un modelo de esta ampliación puede ser el conjunto P de todas las matrices cuadradas

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in M_2(\mathbb{R}) \tag{D.2}$$

Se afirma que P es un campo (comparar con el *ejercicio 2.11*).

Efectivamente, en P están contenidos el 0 y la identidad 1 del anillo $M_2(\mathbb{R})$. Luego, de las relaciones

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix}$$

$$-\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} -a & -b \\ -(-b) & -a \end{bmatrix} \tag{D.3}$$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix}$$

se deduce que P es cerrado con respecto a las operaciones de suma y multiplicación. La asociatividad de estas operaciones es consecuencia de su propiedad asociativa en M_2. Lo mismo se refiere a las leyes de distributividad. De este modo, P es un subanillo en M_2. Queda por demostrar la existencia en P de una matriz inversa a cualquier matriz (D.2), con determinante

$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2 \neq 0$$

(la conmutatividad de P se desprende de la fórmula (D.3)). Directamente de la fórmula para los coeficientes de la matriz inversa o por medio de la resolución del sistema lineal

$$\begin{aligned} ax - by &= 1 \\ bx + ay &= 0 \end{aligned}$$

que surge de la condición

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

hallamos, que

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}^{-1} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}, \text{ donde } c = \frac{a}{a^1 + b^2}, \, d = \frac{-b}{a^2 + b^2} \quad \text{(D.4)}$$

Utilizando la regla de multiplicación de matrices por números, cualquier elemento del campo P lo anotamos en la forma

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = aE + bJ, \text{ donde } a, b \in \mathbb{R}, \; J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{(D.5)}$$

El campo P contiene el subcampo $\{aE \mid a \in \mathbb{R}\} \cong \mathbb{R}$, y la relación

$$J^2 + E = U$$

muestra que el elemento $J \in P$ "con exactitud hasta el isomorfismo" es solución de la ecuación (D.1). Aquí no se puede hablar de ninguna mística acerca del "elemento imaginario J".

Sin embargo, se llama campo de los números complejos, no el campo P, sino cierto objeto isomorfo del mismo, cuyos elementos se representan como puntos de un plano. El deseo de tener una realización geométrica del campo P no es casual si se recuerda que el campo $\mathbb{R}$ para nosotros es inseparable de la "recta real" con un punto dado, representante del cero, y una escala determinada, que define la situación del número 1.

D.2 El plano complejo

Queremos construir un campo C cuyos elementos sean puntos del plano $\mathbb{R}^2$, siendo que la suma y multiplicación de los puntos, sometiéndose a todas la reglas de operaciones en un campo, resuelvan

nuestro problema. Elegimos en el plano cartesiano un sistema de coordenadas cartesianas, con eje de abscisas x y con eje de ordenadas y. Escribimos (a,b) para indicar el punto con abscisa a y ordenada b. Para los puntos (a,b) y (c,d), definimos la suma y el producto por las reglas

$$\begin{aligned}(a,b)+(c+d) &= (a+c,b+d)\\ (a,b)(c,d) &= (ac-bd,ad+bc)\end{aligned} \tag{D.6}$$

(el uso de los mismos signos $+$, $\cdot$, que en el campo $\mathbb{R}$ no debe llevar a confusión). Una comprobación directa, pero bastante fatigosa, nos convencería de que las operaciones así definidas dotan al conjunto de pares (de puntos en el plano) para la construcción de un campo con las propiedades necesarias. No hay necesidad, por suerte, de esta comprobación. La comparación

$$(a,b)\mapsto\begin{bmatrix}a & b\\ -b & a\end{bmatrix}$$

de los puntos del plano $\mathbb{C}$ con los elementos del campo P, anteriormente construido, y una ligera mirada a las fórmulas (D.3) y (D.6), nos convencen de que estamos en presencia de un isomorfismo y que, en consecuencia, el conjunto $\mathbb{C}$ es un campo, el que se llama habitualmente campo de los números complejos. Teniendo en cuenta la realización geométrica de este campo, $\mathbb{C}$ también se denomina *plano complejo*.

El eje de abscisas elegido por nosotros, o sea el conjunto de puntos $(a,0)$, no se diferencia en nada, por sus propiedades, de la recta real, y suponemos $(a,0)=a$. El cero $(0,0)$ y la unidad $(1,0)$ del campo se hacen, con esto, números reales corrientes. Para el punto $(0,1)$ en el eje de ordenadas se introduce por tradición la designación i "unidad imaginaria", que es la raíz de la ecuación (D.1): $i^2=(0,1)(0,1)=(-1,0)=-1$. El número complejo arbitrario $z=(x,y)$ se escribe ahora en la forma acostumbrada

$$z=x+iy,\quad x,y\in\mathbb{R} \tag{D.7}$$

sumamente cercana a la forma (D.5) de los elementos del campo P. Notemos, que $\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$. Por eso, $\mathbb{C}$ es un campo con característica cero.

E

Técnicas de demostración

La matemática es la ciencia del orden y la medida, de bellas cadenas de razonamientos, todos sencillos y fáciles.

René Descartes, filósofo y matemático francés

En este apéndice enlistamos algunas de las técnicas de demostración más usadas en el texto.

E.1 Conjuntos y funciones

Sean A y B conjuntos no vacíos y $f : A \to B$ una función. Denotaremos como $|A|$ la cardinalidad del conjunto A. Sea $\sim$ una relación binaria definida sobre A.

E.1.1 **Para demostrar que** $A \subseteq B$: tomar cualquier $a \in A$ y mostrar que $a \in B$.

E.1.2 **Para demostrar que** $A = B$: mostrar que $A \subseteq B$ y que $B \subseteq A$ (véase técnica E.1.1).

E.1.3 **Para demostrar que** $A \neq B$: mostrar que existe $a \in A$ tal que $a \notin B$, o mostrar que existe $b \in B$ tal que $b \notin B$.

E.1.4 **Para demostrar que** $|A| = |B|$: definir una función biyectiva $\beta : A \to B$.

E.1.5 **Para demostrar que** f **está bien definida**: mostrar que si $a = b$, $a, b \in A$, entonces $f(a) = f(b)$. Además hay que mostrar que $f(a) \in B$ para toda $a \in A$.

E.1.6 **Para demostrar que** f **es inyectiva**: mostrar que si $f(a) = f(b)$, $a, b \in A$, entonces $a = b$.

E.1.7 **Para demostrar que** f **es sobreyectiva**: tomar cualquier $b \in B$ y encontrar (o definir) un $a \in A$ tal que $f(a) = b$.

E.1.8 **Para demostrar que** f **es biyectiva**: mostrar que f es inyectiva (véase técnica E.1.6) y que f es sobreyectiva (véase técnica E.1.7).

E.1.9 **Para demostrar que** $\sim$ **es reflexiva en** A: mostrar que $a \sim a$ para toda $a \in A$.

E.1.10 **Para demostrar que** $\sim$ **es simétrica en** A: mostrar que si $a \sim b$, $a, b \in A$, entonces $b \sim a$.

E.1.11 **Para demostrar que** $\sim$ **es transitiva en** A: mostrar que si $a \sim b$ y $b \sim c$, $a, b, c \in A$, entonces $a \sim c$.

E.1.12 **Para demostrar que $\sim$ es una relación de equivalencia sobre A**: mostrar que R es reflexiva (véase técnica E.1.9), simétrica (véase técnica E.1.10) y transitiva (véase técnica E.1.11).

E.1.13 **Para demostrar que una operación binaria $\cdot$ sobre A está bien definida**: mostrar que si $a = a'$ y $b = b'$, entonces $a \cdot b = a' \cdot b'$. Además hay que mostrar que $a \cdot b \in A$ para toda $a, b \in A$ (comparar con la técnica E.1.5).

E.2 Anillos

Sean R y S anillos conmutativos con identidad, $\phi : R \to S$ una función e I un ideal de R.

E.2.1 **Para demostrar que R es un campo**: mostrar que todos los elementos distintos de cero en R son unidades (es decir, que $R^* = R \setminus \{0\}$).

E.2.2 **Para demostrar que un subconjunto $A \subseteq R$ es un subanillo**: mostrar que A es no vacío, y que $a - b \in A$ y $ab \in A$ para toda $a, b \in A$.

E.2.3 **Para demostrar que R es un dominio entero**:

a) Mostrar que la propiedad de cancelación se cumple en R; es decir, que si $ab = ac$, $b, c \in R$, $a \in R \setminus \{0\}$, entonces $b = c$, o bien

b) Mostrar que R no tiene divisores de cero; es decir, que no hay elementos $a, b \in R \setminus \{0\}$ tales que $ab = 0$.

E.2.4 **Para demostrar que $a \in R$ es irreducible (con R dominio entero)**:

a) Mostrar que si $a = bc$, $b, c \in R$, entonces b o c es una unidad, o bien

b) Si R es de ideales principales, mostrar que $\langle a \rangle$ es maximal (véase técnica E.2.11).

E.2.5 **Para demostrar que $a \in R$ es reducible (con R dominio entero)**: encontrar $b, c \in R \setminus \{0\}$ no unidades tales que $a = bc$.

E.2.6 **Para demostrar que $a \in R$ es primo (con R dominio entero)**:

a) Mostrar que si $a \mid bc$, $b, c \in R$, entonces $a \mid b$ o $a \mid c$, o bien

b) Mostrar que $\langle a \rangle$ es un ideal primo (véase técnica E.2.10).

E.2.7 **Para demostrar que un subconjunto $A \subseteq R$ es un ideal**: mostrar que A es un subanillo (véase técnica E.1.2) y que $ra \in A$ para toda $a \in A$, $r \in R$.

E.2.8 **Para demostrar que $I = R$**: mostrar que $1 \in I$. En forma equivalente, puede usarse la técnica E.1.2.

E.2.9 **Para demostrar que $\langle a \rangle \subseteq \langle b \rangle$, $a, b \in D$**: mostrar que $b \mid a$. En forma equivalente, puede usarse la técnica E.1.1.

E.2.10 **Para demostrar que I es primo**:

a) Mostrar que si $ab \in I$ entonces $a \in I$ o $b \in I$, o bien

b) Mostrar que R/I es un dominio entero (véase técnica E.2.3), o bien

c) Mostrar que I es maximal (véase técnica E.2.11).

E.2.11 **Para demostrar que I es maximal**:

a) Mostrar que si A es un ideal tal que $I \subsetneq A \subseteq R$, entonces $A = R$ (véase técnica E.2.8), o bien

b) Mostrar que R/I es un campo (véase técnica E.2.1).

E.2.12 **Para demostrar que ϕ es un homomorfismo de anillos**: mostrar que

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{y que} \quad \phi(ab) = \phi(a)\,\phi(b)$$

para toda $a, b \in R$.

E.2.13 **Para demostrar que ϕ es un isomorfismo de anillos**: mostrar que ϕ es un homomorfismo de anillos (véase técnica E.2.12) y que es biyectivo (véase técnica E.1.8).

E.2.14 **Para demostrar que $R \cong S$**: mostrar que existe un isomorfismo de anillos $\beta : R \to S$ (véase técnica E.2.13).

E.2.15 **Para demostrar que ϕ es inyectivo**: mostrar que $\ker \phi = \{0_R\}$. En forma equivalente, puede usarse la técnica E.1.6.

E.3 Campos

Sea E una extensión de campo de F.

E.3.1 **Para demostrar que $\alpha \in E$ es algebraico sobre F**:

a) Mostrar que existe $f(x) \in F[x] \setminus \{0\}$ tal que $f(\alpha) = 0$, o bien

b) Mostrar que $[F(\alpha) : F] < \infty$.

E.3.2 **Para demostrar que $\alpha \in E$ es trascendente sobre F**: demostrar que α no es algebraico sobre F (véase técnica E.3.1).

E.3.3 **Para encontrar el grado de un elemento algebraico $\alpha \in E$ sobre F**:

a) Encontrar el grado del polinomio mínimo de α sobre F, o bien

b) Encontrar el grado de la extensión $F(\alpha)$ de F.

E.3.4 **Para demostrar que E es una extensión simple de F:** encontrar un $\alpha \in E$ tal que $E \cong F(\alpha)$.

E.3.5 **Para encontrar el campo de descomposición de $f(x)$ sobre F**: obtener las raíces $\alpha_1, \ldots, \alpha_n$ de $f(x)$ en una extensión de F y adjuntarlas a F.

E.3.6 **Para demostrar que E es una extensión finita de F**: mostrar que $[E : F] < \infty$.

E.3.7 **Para demostrar que E es una extensión algebraica de F**:

a) Mostrar que todos los elementos de E son algebraicos sobre F (véase técnica E.3.1), o bien

b) Mostrar que E es una extensión finita de F (véase técnica E.3.6).

E.3.8 **Para demostrar que F es algebraicamente cerrado**:

a) Mostrar que todo polinomio no constante en $F[x]$ tiene una raíz en F, o bien

b) Mostrar que todo polinomio no constante en $F[x]$ es separable en F, o bien

c) Mostrar que los únicos polinomios irreducibles en $F[x]$ son los de grado 1.

E.3.9 **Para encontrar $|Gal(F(r):F)|$, donde r es algebraico sobre F**: calcular el número de conjugados de r sobre F que estén en $F(r)$.

Respuestas a los ejercicios

Capítulo 1, "Propiedades básicas de los anillos"

1.3. $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

1.5. Si u es unidad, $a = a1 = a(u^{-1}u) = (au^{-1})u$ para toda $a \in R$.

1.7. Si $nt_1, nt_2 \in n\mathbb{Z}$, $nt_1 - nt_2 = n(t_1 - t_2) \in n\mathbb{Z}$ y $(nt_1)(nt_2) = n(t_1 nt_2) \in n\mathbb{Z}$.

1.9. Si $x, y \in Z(R)$, para toda $a \in R$, $(x-y)a = xa - ya = ax - ay = a(x-y)$ y $(xy)a = x(ay) = a(xy)$.

1.11. Comprueba que $(a+b)^2 = a^2 + ab + ba + b^2$ y usa el hecho de que $a^2 = a$.

Capítulo 2, "Dominios enteros"

2.1. a) Sí es un dominio entero.

b) No es un dominio entero.

c) No es un dominio entero.

2.3. $\mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{0\}$ y $\mathbb{Z}_7$ no tiene divisores de cero. $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ y los divisores de cero de $\mathbb{Z}_{12}$ son $\mathbb{Z}_{12} \setminus (\mathbb{Z}_{12}^* \cup \{0\})$.

2.5. $char(4\mathbb{Z}) = 0$,
$char(\mathbb{Z}_3 \oplus \mathbb{Z}_4) = 12$,
$char(\mathbb{Z}_3 \oplus 3\mathbb{Z}) = 0$ y
$char(\mathbb{Z}_6 \oplus \mathbb{Z}_{15}) = 30$.

2.7. S es un subanillo de D por el *ejercicio 2.6*. Como $S \subseteq D$, S no tiene divisores de cero. Sea P cualquier subdominio entero de D. Sabemos que $1 \in P$ y por cerradura $n \cdot 1 \in P$ para toda $n \in \mathbb{Z}$. Por lo tanto $S \subseteq P$.

2.9. Propiedad reflexiva: $a \sim a$ porque $a = 1a$. Propiedad simétrica: si $a \sim b$ entonces $a = ub$, u unidad, $b = u^{-1}a$ y $b \sim a$. Propiedad transitiva: Si $a \sim b$ y $b \sim c$, entonces $a = ub$ y $b = vc$, u, v unidades; entonces, $a = uvc$, donde uv es una unidad (con inverso $v^{-1}u^{-1}$) y $a \sim c$.

Capítulo 3, "Ideales"

3.3. Sean $x, y \in Ann(A)$. Entonces $xa = 0$ y $ya = 0$. De esta manera, $(x-y)a = xa - ya = 0 - 0 = 0$. Además, si $r \in R$, $rxa = r0 = 0$ y $rx \in Ann(A)$.

3.5. Sean $x, y \in N(A)$. Entonces

$$(x-y)^{n_1+n_2} = \sum_{k=0}^{n_1+n_2} \binom{n_1+n_2}{k} x^k (-y)^{n_1+n_2-k} \in A,$$

así que $x - y \in N(A)$. Claramente, $(rx)^{n_1} = r^{n_1} x^{n_1} \in A$ y $rx \in N(A)$ para cualquier $r \in R$.

3.7. $N(\langle 0\rangle) = \langle 3\rangle$ en $\mathbb{Z}_{27}$ y $N(\langle 0\rangle) = \langle 6\rangle$ en $\mathbb{Z}_{36}$.

3.9. Sean $(x_1, x_2), (y_1, y_2) \in \mathbb{Z} \oplus \mathbb{Z}$. Si $(x_1, x_2)(y_1, y_2) \in I$, $y_1 y_2 = 0$, por lo que $y_1 = 0$ o $y_2 = 0$. Por lo tanto, $(x_1, x_2) \in I$ o $(y_1, y_2) \in I$. El ideal I no es maximal porque $I \subsetneq A \subsetneq \mathbb{Z} \oplus \mathbb{Z}$, donde A es el ideal $A = \{(a, 2b) : a, b \in \mathbb{Z}\}$.

Capítulo 4, "Anillos cociente"

4.1. a) Si $a + A = A$, como $0 \in A$, $a = a + 0 \in a + A = A$. Supongamos que $a \in A$. Por cerradura, $a + A \subseteq A$. Si $a' \in A$, $a' = a + (a' - a) \in a + A$, así que $A \subseteq a + A$ y $a + A = A$.

b) Supongamos que $a + A = b + A$. Entonces $a + a' = b$, para algún $a' \in A$. Luego $b - a = a' \in A$. Supongamos que $b - a \in A$. Sea $a + a' \in a + A$, con $a' \in A$. Entonces, $a + a' = b + [(a - b) + a'] \in b + A$. De manera similar, si $b + a' \in b + A$, entonces $b + a' = a + [(b - a) + a'] \in a + A$.

4.5. Si R no contiene ideales propios no triviales, $\langle 0\rangle$ es un ideal maximal. Así $R/\langle 0\rangle \cong R$ es un campo. Supongamos ahora que R es un campo e I un ideal no trivial. Entonces cualquier $u \in I$ distinto de cero es una unidad, por lo que $I = R$.

4.7. Sea I un ideal primo de R. Entonces R/I es un dominio entero. Sea $r \in R \setminus \{0\}$. Como R es booleano, $(r + I)(r + I) = (r + I)$ así que $r + I = 1 + I$ por cancelación. Por lo tanto, R/I es un dominio entero finito (con dos elementos), lo que implica que es un campo. Luego, I es un ideal maximal de R.

Capítulo 5, "Homomorfismos de anillos"

5.1. a) Para cualquier $a \in R$, $\phi(a) = \phi(1a) = \phi(1)\phi(a)$.

b) Por inducción, si $n = 1$, $\phi(1r) = 1\phi(r)$ y $\phi(r^1) = \phi(r)^1$. Supongamos que $\phi(n \cdot r) = n \cdot \phi(r)$ y $\phi(r^n) = \phi(r)^n$ se cumple. Entonces $\phi((n+1) \cdot r) = \phi(n \cdot r + r) = n \cdot \phi(r) + \phi(r) = (n+1) \cdot \phi(r)$. También tenemos que $\phi(r^{n+1}) = \phi(r^n)\phi(r) = \phi(r)^n \phi(r) = \phi(r)^{n+1}$.

5.3. Sean A, B, C anillos. La función identidad $id : A \to A$ es un isomorfismo, por lo que $A \cong A$. Si $A \cong B$ y $B \cong C$, sean $\alpha : A \to B$ y $\beta : B \to C$ isomorfismos. Entonces la composición de funciones $\beta \circ \alpha : A \to C$ es una biyección y $\beta \circ \alpha(xy) = \beta(\alpha(x)\alpha(y)) = \beta \circ \alpha(x)\beta \circ \alpha(y)$, $x, y \in A$. Así $A \cong C$.

5.5. Para cualquier $a, b \in R$, $\phi(a+b) = (a+b) + I = (a+I) + (b+I) = \phi(a) + \phi(b)$ y $\phi(ab) = ab + I = (a+I)(b+I) = \phi(a)\phi(b)$.

5.7. Hay cuatro homomorfismos de

$$\mathbb{Z}_6 \text{ a } \mathbb{Z}_6 : \phi([1]_6) = [0]_6, [1]_6, [3]_6 \text{ y } [4]_6.$$

Hay cuatro homomorfismos de

$$\mathbb{Z}_{20} \text{ a } \mathbb{Z}_{30} : \phi([1]_{20}) = [0]_{30}, [6]_{30}, [15]_{30} \text{ y } [21]_{30}.$$

5.9. Si $a, b \in \ker\phi$, $\phi(a) = 0$ y $\phi(b) = 0$, por lo que $\phi(a) - \phi(b) = \phi(a-b) = 0$ y $a - b \in \ker\phi$. Si $r \in R$, entonces $\phi(r)\phi(a) = \phi(ra) = 0$ y $ra \in \ker\phi$.

5.11. Claramente $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$, $x, y \in R$. Observemos que $\phi(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k$. Demostraremos que $p \mid \binom{p}{k}$ si $0 < k < p$. Por definición, sabemos que, $p! = \binom{p}{k} k!(p-k)!$, así que $p \mid \binom{p}{k} k!(p-k)!$. Si $1 \leq k < p$, $p \nmid k!$, $p \nmid (p-k)!$. Luego, $p \mid \binom{p}{k}$ por el lema de Euclides. Debido a que la característica de R es p, $\binom{p}{k} x^{p-k} y^k = 0$ para toda $0 < k < p$. Por lo tanto $\phi(x+y) = (x+y)^p = x^p + y^p = \phi(x) + \phi(y)$.

Capítulo 6, "Anillos de polinomios"

6.1. a) $q(x) = 5x^2 - 15x + 47$, $r(x) = -140$.

b) $q(x) = 4x^2 + 3x - 1$, $r(x) = 6x + 2$.

6.3. Es trivial por la definición de multiplicación de polinomios.

6.5. Por el algoritmo de la división

$$f(x) = q(x)(x - \alpha) + r(x),$$

$r(x) = 0$ o $\deg r(x) < \deg(x - \alpha) = 1$ para algunos $q(x)$, $r(x) \in F[x]$. Así, $r(x) = r \in F$ es un polinomio constante. Evaluando en α, $f(\alpha) = q(\alpha)0 + r(\alpha) = r(\alpha) = r$.

6.7. Sustituyendo en $f(x)$,

$$a_n\left(\frac{r}{s}\right)^n + \ldots + \frac{r}{s} + a_0 = 0$$
$$a_n r^n + a_{n-1} s r^{n-1} + \ldots + s^{n-1} r + s^n a_0 = 0$$

Así que,

$$a_n r^n = -s\left(a_{n-1} r^{n-1} + \ldots + s^{n-2} r + s^{n-1} a_0\right)$$
$$s^n a_0 = -r\left(a_n r^{n-1} + a_{n-1} s r^{n-1} + \ldots + s^{n-1}\right)$$

Esto implica que $s \mid a_n r^n$ y $r \mid s^n a_0$. Como s y r son primos relativos, $s \mid a_n$ y $r \mid a_0$. Las raíces de $f(x) = 6x^3 - 11x^2 - 3x + 2$ son 2, $-\frac{1}{2}$ y $\frac{1}{3}$.

6.9. Supongamos que $\langle 2, x\rangle = \langle g(x)\rangle$ para algún $g(x) \in \mathbb{Z}[x]$. Como $g(x) \in \langle 2, x\rangle$, $g(0)$ es par por el *ejercicio 6.8*. Debido a que $2 \in \langle 2, x\rangle$, tenemos que debe existir un $q(x) \in \mathbb{Z}[x]$ tal que $2 = q(x)\, g(x)$. Sin embargo, $\deg(2) = 0 = \deg q(x) + \deg g(x)$. Así que $\deg q(x) = \deg g(x) = 0$. Esto implica que $g(x)$ y $q(x)$ son constantes enteras y que $g(x) = \pm 2$ y $q(x) = \pm 1$. Esto implica que $\langle 2, x\rangle = \langle 2\rangle$, lo cual es una contradicción porque $x \notin \langle 2\rangle$.

6.11. Usar el homomorfismo de evaluación

$$\phi : \mathbb{Q}[x] \to \mathbb{Q}\left[\sqrt{2}\right],$$

$\phi(f(x)) = f\left(\sqrt{2}\right)$ y el primer teorema de isomorfía.

Capítulo 7, "Factorización de polinomios"

7.1. a) El polinomio es irreducible sobre $\mathbb{Z}_2$ porque es de grado 2 y no tiene raíces en $\mathbb{Z}_2$.

b) $x^3 + 2x + 3 = (x-4)^2 (x-2)$ en $\mathbb{Z}_5[x]$.

7.5. c) Si $f(x)$ es reducible sobre F,

$$f(x) = g(x)\, h(x)$$

donde $\deg g(x), \deg h(x) > 0$. Luego

$$f(x+a) = g(x+a)\, h(x+a)$$

implica que $f(x+a)$ es reducible sobre F. Ahora, si el polinomio $f(x+a)$ es reducible sobre F, tenemos que $f(x+a) = g(x)\,h(x)$, y evaluando en $x-a$, $f(x) = g(x-a)\,h(x-a)$, por lo que $f(x)$ es reducible sobre F.

7.7. a) Eisenstein con $p = 5$.

b) $5g(x)$ es irreducible por Eisenstein con $p = 3$, y $g(x)$ es irreducible por el *ejercicio 7.5*.

c) $h(x+1)$ es irreducible por Eisenstein con $p = 3$, y $h(x)$ es irreducible por el *ejercicio 7.5*.

7.9. Si $f(x) \in \langle p(x) \rangle$, $f(x) = g(x)\,p(x)$. Así

$$\phi_a(f(x)) = \phi_a(g(x)\,p(x)) = g(a)\,p(a) = 0,$$

por lo que $f(x) \in \ker\phi$ y $\langle p(x) \rangle \subseteq \ker\phi$. Observemos que $\ker\phi \subsetneqq F[x]$, ya que por ejemplo $1 \notin \ker\phi$. Por el teorema 7.5, el ideal $\langle p(x) \rangle$ es maximal, así que $\langle p(x) \rangle = \ker\phi$.

Capítulo 8, "Más de dominios enteros"

8.3. Sean $x, y \in I$. Entonces $x \in I_i$ y $y \in I_j$ para algunas i, j. En particular, $x, y \in I_k$, donde $k = \text{máx}\{i, j\}$. Luego $x - y \in I_k$ y $rx \in I_k$ para toda $r \in R$. Por lo tanto, $x - y \in I$ y $rx \in I$.

8.5. Sea D un dominio de ideales principales e I_1 un ideal. Si I_1 es maximal, no hay nada que hacer. Si, I_1, no es maximal, $I_1 \subsetneqq I_2 \subsetneqq D$, para algún ideal I_2. Si I_2 es maximal, se demuestra lo que se quería. Si no, $I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq D$. Continuando este proceso formamos la cadena de ideales estrictamente creciente

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \ldots$$

La cual no puede ser infinita por el teorema 8.6. Por lo tanto, alguno de los ideales I_k debe ser maximal.

8.7. $q = 1 - 2i$, $r = -2$ donde $d(r) = 4 < d(3 + 2i) = 13$.

8.9. Observemos que $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Usando la función $N : D \setminus \{0\} \longrightarrow \mathbb{N}_0$ definida como $N(a + b\sqrt{-3}) = a^2 + 3b^2$, $a, b \in \mathbb{Z}$, hay que demostrar que 2 y $1 \pm \sqrt{-3}$ son elementos irreducibles en $\mathbb{Z}[\sqrt{-3}]$. Además, como $u \in \mathbb{Z}[\sqrt{-3}]^*$ si y sólo si $N(u) = 1$, tenemos que $\mathbb{Z}[\sqrt{-3}]^* = \{1, -1\}$. Por lo tanto, 2 y $1 + \sqrt{-3}$ no son asociados, lo que implica que la factorización en irreducibles de 4 en $\mathbb{Z}[\sqrt{-3}]$ no es única.

8.11. Si D es Noetheriano, sea I un ideal de D y $a \in I$. Si $I = (a)$, obtenemos lo que queríamos; si no, sea $a_1 \in I \setminus (a)$. Si $I = (a_1, a)$, terminamos; si no, sea $a_2 \in I \setminus (a_1, a)$. Este proceso debe detenerse ya que de lo contrario obtenemos una cadena estrictamente creciente de ideales $(a) \subsetneq (a, a_1) \subsetneq (a, a_1, a_2) \subsetneq \ldots$ que no se estabiliza. Por lo tanto, I es generado por un número finito de elementos. Por otro lado, supongamos que cualquier ideal de D es generado por un número finito de elementos. Consideremos una cadena creciente de ideales $I_1 \subseteq I_2 \subseteq \ldots$. Sea $I = \cup I_i$. Este es un ideal de D y por hipótesis $I = (a_1, \ldots, a_n)$ con $a_i \in D$. Así, $a_i \in I_{k_i}$ para alguna k_i, y $a_i \in I_m$ para toda i, donde $m = \text{máx}\{k_1, \ldots, k_n\}$. Por lo tanto, $I = I_m$ y la cadena se estabiliza.

Capítulo 9, "El campo de las fracciones"

9.3. Sea $S = D \setminus I$. Como I es un ideal, $0 \notin S$. Si I es primo, $1 \notin I$, así que $1 \in S$. Si $a, b \in S$, $a, b \notin I$, por lo que $ab \notin I$ y $ab \in S$. Luego S es un sistema multiplicativo. Ahora, si S es un sistema multiplicativo, como $1 \in S$, $I \neq D$. Si $ab \in I$, $ab \notin S$, por lo que $a \notin S$ o $b \notin S$ y $a \in I$ o $b \in I$. Luego I es primo.

9.5. Supongamos que D es un dominio local con ideal maximal M. Si $u \in D^*$, es claro que $u \in D \setminus M$. Sea $u \in D \setminus M$. Supongamos que $u \notin D^*$, así que $\langle u \rangle \neq R$. Por el teorema 3.25, $\langle u \rangle \subseteq M'$, donde M' es un ideal maximal de D. Como D es un dominio local, $M' = M$ y $u \in M$, lo cual es una contradicción. Luego $u \in D^*$ y $D \setminus M = D^*$. Supongamos ahora que $D \setminus M = D^*$ donde M es un ideal de D. Supongamos que $M \subsetneq I \subseteq D$. Entonces I contiene una unidad de D, y por lo tanto $I = D$. Esto demuestra que M es maximal. Sea M' otro ideal maximal de D. Obviamente M' no contiene unidades, así que $M' \subseteq M$ y $M' = M$ por maximalidad.

9.7. $S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} : p \nmid b, a, b \in \mathbb{Z} \right\}$ y su único ideal maximal es

$$S^{-1} \langle p \rangle = \left\{ \frac{a}{b} : p \mid a, p \nmid b \right\}.$$

Capítulo 10, "Extensiones de campos"

10.1. Por el teorema fundamental de la teoría de campos, existe una extensión E de $\mathbb{Z}_2$ en la cual existe $\alpha \in E$ con $f(\alpha) = 0$. Así,

$$f(x) = (x - \alpha)(x + \alpha + 1)\left(x + \alpha^2\right)\left(x + \alpha^2 + 1\right)$$

10.3. El polinomio mínimo de $\sqrt{2} + i$ sobre $\mathbb{Q}$ es $\overline{f}(x) = x^4 - 2x^2 + 9$ y el polinomio mínimo de $\sqrt{\frac{1}{3} + \sqrt{7}}$ sobre $\mathbb{Q}$ es $g(x) = x^4 - \frac{2}{3}x^2 - \frac{62}{9}$.

10.5. En $\mathbb{Q}(\pi^3)$, π es raíz del polinomio $x^3 - \pi^3 \in \mathbb{Q}(\pi^3)[x]$, el cual es irreducible porque es de grado 3 y no tiene raíces en $\mathbb{Q}(\pi^3)$.

10.7. $\dfrac{1}{\alpha} = -\alpha^2 - 1$ y $\dfrac{1}{\alpha + 2} = \dfrac{1}{9}\alpha^2 - \dfrac{2}{9}\alpha + \dfrac{5}{9}$.

10.9. Sea $\beta \in F(\alpha) \setminus F$. Supongamos que β es algebraico sobre F y sea $f(x) \in F[x]$ su polinomio mínimo. Sabemos que

$$\beta = \frac{b_r\alpha^r + \ldots + b_0}{c_s\alpha^s + \ldots + c_0}$$

donde $c_i, b_j \in F$, $b_r, c_s \neq 0$. Entonces α es raíz del polinomio

$$(c_s x^s + \ldots + c_0)^n f\left(\frac{b_r x^r + \ldots + b_0}{c_s x^s + \ldots + c_0}\right) \in F[x]$$

lo que contradice que es trascendente sobre F.

Capítulo 11, "Extensiones algebraicas"

11.1. $[E : F] = 1$ si y sólo si el conjunto $\{1\}$ es una base para E sobre F si y sólo si $E = F$.

11.3. Usa inducción.

11.5. a) $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2$ y $\{1, \sqrt{6}\}$ es una base.

b) $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 4$ y $\left\{1, \sqrt{3}, \sqrt{2}, \sqrt{6}\right\}$ es una base.

c) $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{6}\right) : \mathbb{Q}(\sqrt{3})\right] = 2$ y $\left\{1, \sqrt{2}\right\}$ es una base.

11.7. a) Sea $\alpha \in E$ tal que $p(\alpha) = 0$. Como $p(x)$ es irreducible sobre F, es el polinomio mínimo de α sobre F. Así, $[E : F] = [E : F(\alpha)][F(\alpha) : F] = [E : F(\alpha)] \deg p(x)$.

b) Si $[E:F] = p$ primo, tomemos $\alpha \in E \setminus F$. Entonces $[E:F] = [E:F(\alpha)]\,[F(\alpha):F]$, por lo que

$$[E:F(\alpha)] = 1 \quad \text{o} \quad [F(\alpha):F] = 1.$$

Si $[F(\alpha):F] = 1$, $F = F(\alpha)$ es una contradicción. Por lo tanto $E = F(\alpha)$.

11.9. Si $f(x) \in F[x]$ un polinomio con $\deg f(x) > 1$, por el teorema 11.24, $f(x)$ es reducible sobre F. Supongamos que los únicos polinomios irreducibles en $F[x]$ son los lineales. Sea $f(x) \in F[x]$. Usando inducción, sea $\deg f(x) = k$. Como $f(x)$ es reducible, $f(x) = g(x)\,h(x)$ donde $1 \leq \deg g(x)$, $\deg h(x) < k$. Por hipótesis de inducción $g(x)$ tiene una raíz en F y por lo tanto $f(x)$ tiene una raíz en F.

11.11. Observemos que $[F(\alpha):F] = \left[F(\alpha):F\left(\alpha^2\right)\right]\left[F\left(\alpha^2\right):F\right]$. Como $[F(\alpha):F]$ es impar, $n = \left[F\left(\alpha^2\right):F\right]$ es impar. Sea

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

el polinomio mínimo de α^2 sobre F. Entonces

$$\alpha^{2n} + a_{n-1}\alpha^{2n-1} + \ldots + a_0 = 0$$

Como el grado de α es impar, tenemos que

$$[F(\alpha):F] < 2\left[F\left(\alpha^2\right):F\right]$$

y así,

$$\frac{[F(\alpha):F]}{[F(\alpha^2):F]} = \left[F(\alpha):F\left(\alpha^2\right)\right] = 1$$

Por lo tanto, $F(\alpha) = F\left(\alpha^2\right)$.

Capítulo 12, "Campos finitos"

12.1. Sea $f(x) = a_n x^n + \ldots + a_0$ y $g(x) = b_m x^m + \ldots + b_0$.

a) Si $n \geq m$,

$$\begin{aligned}\left(f(x) + g(x)\right)' &= na_n x^{n-1} + \ldots + m\left(a_m + b_m\right)x^m \ldots \\ &\quad + (a_1 + b_1) \\ &= f'(x) + g'(x).\end{aligned}$$

b) $(af(x))' = naa_n x^{n-1} + \ldots + aa_1 = af'(x)$.

c) Por inducción sobre $\deg f(x)$. Si $\deg f(x) = 0$, usamos la parte b). Si

$$\deg f(x) = n, f(x) = a_n x^n + h(x)$$

donde $\deg h(x) < n$. Entonces, por a) y la hipótesis de inducción,

$$\begin{aligned}(f(x)g(x))' &= (a_n x^n g(x))' + (h(x)g(x))' \\ &= a_n (x^n g(x))' + h'(x)g(x) \\ &\quad + h(x)g'(x)\end{aligned}$$

Ahora es fácil observar que

$$(x^n g(x))' = nx^{n-1}g(x) + x^n g'(x).$$

Sustituyendo en la relación de arriba obtenemos la fórmula deseada.

12.3. Sabemos que $|\mathbb{Z}_2(\alpha)| = |\mathbb{Z}_2(\beta)| = 8$. Si $\mathbb{Z}_2(\alpha) \neq \mathbb{Z}_2(\beta)$, entonces el polinomio $x^8 - x \in \mathbb{Z}[x]$ tendría más de ocho raíces en $\overline{\mathbb{Z}}_2$. Por lo tanto $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2(\beta)$ y en particular $\beta \in \mathbb{Z}_2(\alpha)$.

12.5. Sea $b \in \overline{\mathbb{Z}}_2$ una raíz de $f(x)$ y $K = \mathbb{Z}_2(b) \cong \mathbb{Z}_2[x] / \langle f(x) \rangle$. Entonces, $|K^*| = 7$ y b es un elemento primitivo en K. Usando la tabla de sumar construida en el *ejercicio 12.4*, puede demostrarse que $f(x)$ tiene todas sus raíces en K, y por lo tanto K es el campo de descomposición de $f(x)$ sobre $\mathbb{Z}_2$.

12.7. Por el *ejercicio 5.11*, la función $\phi : F \to F$ definida como $\phi(x) = x^p$ es un homomorfismo donde $\phi(F) = F^p \subseteq F$. Si $x^p = y^p$, entonces $x^p + y^p = (x+y)^p = 0$, por lo que $x = y$. Esto muestra que ϕ es inyectivo y $|\phi(F)| = |F|$. Por lo tanto, $\phi(F) = F$.

12.9. Usa el polinomio $f(x) = 1 + \prod_{a \in F} (x - a) \in F[x]$.

Capítulo 13, "Introducción a la teoría de Galois"

13.3. El polinomio mínimo de ω es

$$x^{p-1} + \ldots + x + 1 = \frac{x^p - 1}{x - 1} = f_p(x),$$

el cual es irreducible por el *ejemplo* 7.24. Los conjugados de ω son $\omega, \omega^2, \ldots, \omega^{p-1}$. Todos ellos están en $\mathbb{Q}(\omega)$ así que

$$|Gal(\mathbb{Q}(\omega), \mathbb{Q})| = p - 1.$$

13.5. Sea $a \in \overline{F}$ una raíz múltiple de $f(x)$. Entonces a también es una raíz de $f'(x) \in F[x]$, donde $f'(x) \neq 0$ porque $char(F) = 0$ y $\deg f(x) > 0$. Como $f(x)$ es irreducible sobre F, $f(x)$ es el polinomio mínimo de a sobre F. Por el *ejercicio 10.4*, $f(x) \mid f'(x)$, lo cual es una contradicción porque

$$\deg(f'(x)) < \deg(f(x)).$$

13.7. Encuentra $|Gal(f)|$ cuando:

a) $|Gal(f)| = 2$.

b) $|Gal(f)| = 2$.

c) $|Gal(f)| = 12$.

13.9. 1) Supongamos que $H_1 \leq H_2$ y sea $a \in H_2^{\dagger}$. Así $h_2(a) = a$ para toda $h_2 \in H_2$. En particular, $h_1(a) = a$ para toda $h_1 \in H_1$. Luego $a \in H_1^{\dagger}$.

2) Supongamos que $K_1 \subseteq K_2$ y sea $\phi \in K_2^*$. Así $\phi(k_2) = k_2$ para toda $k_2 \in K_2$. En particular, $\phi(k_1) = k_1$ para toda $k_1 \in K_1$. Luego $\phi \in K_1^*$.

3) Sea $h \in H$. Así $h(a) = a$ para toda $a \in H^{\dagger}$. Por lo tanto, $h \in Gal(E : H^{\dagger}) = H^{\dagger *}$. De manera similar, sea $k \in K$. Así $\phi(k) = k$ para toda $\phi \in K^*$. Luego $k \in K^{*\dagger}$.

Apéndice A, "Teoría de números elemental"

A.1. a)

$$mcd\left(2^4 \cdot 3^2 \cdot 5 \cdot 7, 2 \cdot 3^3 \cdot 7 \cdot 11\right) =$$
$$2 \cdot 3^2 \cdot 7, mcm\left(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11\right) =$$
$$2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$$

b) $mcd(1485, 1745) = 5 = 1745 \cdot 40 - 1485 \cdot 47$.

A.3. Supongamos que $p_i \mid p_1 p_2 \ldots p_n + 1$. Entonces $p_1 p_2 \ldots p_n + 1 = qp_i$ con $q \in \mathbb{Z}$. Luego $p_i \mid 1 = qp_i - p_1 p_2 \ldots p_n$, lo cual es una contradicción. Si $p_1, \ldots, p_n$ es la lista de todos los números primos, el número $p_1 p_2 \ldots p_n + 1$ no es divisible entre ningún número primo, lo cual es una contradicción.

A.5. Usaremos inducción. Si $n = 2$, si $p \mid a_1 a_2$ entonces $p \mid a_1$ o $p \mid a_2$ por el lema de Euclides. Sea $n = k+1$, y $p \mid a_1 \ldots a_k a_{k+1}$ Si $p \mid a_{k+1}$ el lema queda demostrado. Si $p \nmid a_{k+1}$, por el lema de Euclides $p \mid a_1 \ldots a_k$. Luego, por hipótesis de inducción $p \mid a_i$ para alguna i, $1 \leq i \leq k$.

A.7. Propiedad reflexiva: $a \equiv a \pmod{n}$ porque $n \mid a - a$. Propiedad simétrica: si $a \equiv b \pmod{n}$, $a - b = nq$, $q \in \mathbb{Z}$, y $b - a = n(-q)$. Luego $b \equiv a \pmod{n}$. Propiedad transitiva: si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, $a - b = nq_1$ y $b - c = nq_2$, $q_i \in \mathbb{Z}$; sumando ambas relaciones $a - c = n(q_1 + q_2)$, por lo que $a \equiv c \pmod{n}$.

Apéndice B, "Teoría de grupos"

B.1. Observemos que $(a^{-1}e)(ae) = a^{-1}a = e$, así que $ae = ea$ ya que $e^{-1} = e$. Supongamos que $e' \in G$ es otra identidad. Por definición, $ee' = e$ y $ee' = e'$. Por lo tanto $e = e'$.

B.5. Sean $g^k, g^s \in \langle g \rangle$. Entonces $g^k (g^s)^{-1} = g^k g^{-s} = g^{k-s} \in \langle g \rangle$.

B.7. $|\mathbb{Z}_6| = 6$, $|[1]_6| = |[5]_6| = 6$, $|[2]_6| = |[4]_6| = 3$, $|[3]_6| = 2$, $|[0]_6| = 1$.

B.9. Sea $G = \langle g \rangle$ cíclico y sean $g^k, g^s \in \langle g \rangle$. Entonces $g^k g^s = g^{k+s} = g^{s+k} = g^s g^k$.

Apéndice C, "Espacios vectoriales"

C.1. Observemos que $0v = (\alpha + (-\alpha))v = \alpha v + (-\alpha)v = 0$. Por lo tanto $(-\alpha)v = -\alpha v$. Ahora, $\alpha \mathbf{0} = \alpha(v + (-v)) = \alpha v + \alpha(-v)$, por lo que $\alpha(-v) = -\alpha v$.

C.3. Sean $\alpha_1 v_1 + \ldots + \alpha_n v_n$ y $\beta_1 v_1 + \ldots + \beta_n v_n \in gen_F(A)$, $v_i \in A$, $\alpha_i, \beta_i \in F$. Entonces

$$\lambda(\alpha_1 v_1 + \ldots + \alpha_n v_n) = (\lambda\alpha_1) v_1 + \ldots + (\lambda\alpha_n) v_n \in gen_F(A) \text{ para toda } \lambda \in F$$

$$\begin{aligned} (\alpha_1 v_1 + \ldots + \alpha_n v_n) + (\beta_1 v_1 + \ldots + \beta_n v_n) &= (\alpha_1 + \beta_1) v_1 + \\ \ldots + (\alpha_n + \beta_n) v_n &\in gen_F(A) \end{aligned}$$

C.5. a) A es linealmente dependiente sobre $\mathbb{R}$.

b) A es linealmente independiente sobre $\mathbb{R}$.

c) A es linealmente independiente sobre $\mathbb{R}$.

C.7. Como A es linealmente dependiente tenemos que $\alpha_1 v_1 + \ldots + \alpha_n v_n$ para algunos $\alpha_i \in F$ no todos cero. Supongamos que $\alpha_k \neq 0$. Entonces

$$v_k = \frac{\alpha_1}{\alpha_k} v_1 + \ldots + \frac{\alpha_{k-1}}{\alpha_k} v_{k-1} + \frac{\alpha_{k+1}}{\alpha_k} v_{k+1} + \ldots + \frac{\alpha_n}{\alpha_k} v_n$$

Bibliografía

Bibliografía

Campoli, Oscar A. (1999). A principal ideal domain that is not a Euclidean domain. *The American Mathematical Monthly*, *95*, 868-871.

Fraleigh, John B. (1998). *A first course in abstract algebra*. New Jersey: Prentice Hall.

Gallian, Joseph A. (2004). *Contemporary abstract algebra*. Massachusetts: Houghton Mifflin.

Gowers, Timothy. (2008). *The Princeton companion to mathematics*. Princeton: (ed.) Princeton University Press.

Herstein, Israel N. (1983). *Álgebra moderna*. México: Trillas.

Howie, John M. (2006). *Fields and Galois theory*. Springer.

Jones, Gareth A., y Josephine, Jones M. (1998). *Elementary number theory*. Springer.

Liebeck, Martin W. (2009). *Lecture notes: M3p11 Galois theory*. London: Departamento de Matemáticas Imperial College London.

Milne, J. S. (2011). *Fields and Galois theory (v4.22).* (Disponible en www.jmilne.org/math/)

Murphy, Timothy. (2002). *Finite fields. Course 373 notes*. Dublin: Trinity College University of Dublin.

Rose, Harvey E. (2002). *Linear algebra: A pure mathematical approach*. Basel: Brikhäuser.

Stewart, Ian. (2004). *Galois theory*. London: Chapman & Hall/CRC Mathematics.

Stewart, Ian, y Tall, David. (1977). *The foundations of mathematics*. Oxford: Oxford University Press.

Índice alfabético

Acerca de los autores

Alfonso Manuel Hernández Magdaleno es graduado de la licenciatura y maestría en matemáticas de la Universidad de Guadalajara, en 1998 y 2003 respectivamente. Doctorado en ciencias en física por la Universidad de Guadalajara en 2008, bajo la dirección del doctor Vladimir N. Efremov. Es miembro del Sistema Nacional de Investigadores en el nivel de candidato, cuenta con perfil Promep. Actualmente es profesor de tiempo completo del Centro Universitario de Ciencias Exactas e Ingenierias de la Universidad de Guadalajara. Su línea de investigación es topología de dimensiones bajas y teoría del campo.
e-mail: 137mag@gmail.com

Alonso Castillo Ramírez es licenciado en matemáticas por la Universidad de Guadalajara. Fue reconocido en la XXXVIII Ceremonia de Reconocimiento y Estímulo a Estudiantes Sobresalientes (CREES) en dicha institución. En 2010 obtuvo el grado de maestro en ciencias en matemáticas puras con distinción en el Imperial College de Londres. Recientemente le fue otorgada la Beca Internacional Imperial College para realizar el doctorado en matemáticas bajo la supervisión del profesor Alexander Ivanov. Su línea de investigación es la de representaciones de Majorana de grupos finitos.
e-mail: ac1209@imperial.ac.uk