Michell A. Gómez L.

Breve introducción al

Álgebra Moderna

Pontificia Universidad
JAVERIANA
Cali

Rector: Luis Felipe Gómez Restrepo, S.J.
Vicerrectora Académica: Ana Milena Yoshioka Vargas
Vicerrector del Medio Universitario: Luis Fernando Granados Ospina, S.J.

Facultad de Ingeniería
Decano Académico: Jaime Alberto Aguilar Zambrano
Director del Departamento de Ciencias Naturales y Matemáticas: Daniel Enrique González Gómez

Breve Introducción al Álgebra Moderna
Michell A. Gómez L.

Colección: Texto - Número y Línea

ISBN: 978-958-8856-38-4 / ISBN_e: 978-958-8856-39-1

Coordinador Editorial: Ignacio Murgueitio

Correspondencia, suscripciones y solicitudes de canje:
Calle 18 No. 118-250, Vía Pance
Santiago de Cali, Valle del Cauca
Pontificia Universidad Javeriana
Facultad de Ingeniería
Teléfonos (57-2) 3218200 Ext. 8533

Formato 17 x 24 cms

Diseño carátula: Patricia Mejía
Diseño páginas interiores: Autor

2014

Gómez Leiva, Michell Andrés
Breve introducción al álgebra moderna / Michel A. Gómez L. -- Santiago de Cali: Pontificia Universidad Javeriana, Sello Editorial Javeriano, 2014.
105 páginas; 24 cm. -- (Colección texto-número y línea)
Incluye referencias bibliográficas e índices.

ISBN: 978-958-8856-38-4 / ISBN_e: 978-958-8856-39-1

1. Teoría de grupos 2. Anillos (Álgebra) 3. Campos algebraicos I. Pontificia Universidad Javeriana (Cali). Facultad de Ingeniería. Departamento de Ciencias Naturales y Matemáticas
SCDD 512.2 ed. 23 CO-CaPUJ
malc/14

Índice general

Introducción

El concepto de estructura aparece en todas las áreas de las Matemáticas y desempeña el papel fundamental de unificar ideas que parecen aisladas pero que comparten características comunes, esto permite ordenar y clasificar el conocimiento matemático mediante un lenguaje general. El Álgebra Moderna estudia grupos, anillos y campos, los cuales son ejemplos de dichas estructuras abstractas. En las siguientes páginas nos introduciremos en el estudio de éstas y sus propiedades.

La versión preliminar de este libro orientó el curso de Álgebra Moderna que tuve a cargo en la Pontificia Universidad Javeriana Cali durante el segundo semestre de 2013. Se espera que el libro pueda ser utilizado como guía por profesores y estudiantes en cursos introductorios de Álgebra Abstracta y, en general, por cualquier persona interesada en aprender algunas ideas fundamentales de esta importante área de las Matemáticas.

El lector podrá encontrar en este escrito un amplio número de ejemplos que ilustran las definiciones y teoremas, así como ejercicios propuestos al final de cada sección, algunos de ellos complementan la teoría por lo que se recomienda resolverlos.

Este texto es autocontenido, salvo algunos ejemplos y problemas que requieren conocimientos elementales de divisibilidad de enteros y Álgebra Matricial. La falta de referencias en ciertos ejercicios no presupone originalidad de mi parte, éstos son típicos y se consideran como parte del saber matemático.

Para terminar, se describe brevemente el contenido del libro. En el primer capítulo, se estudian los grupos, los cuales son conjuntos dotados de una operación. Se abordan conceptos básicos como subgrupos, grupos cíclicos, permutaciones, clases laterales, grupo cociente y homomorfismos. El segundo capítulo trata acerca de los anillos, que son grupos en los que se ha definido una segunda operación. Inicialmente, se hace un desarrollo similar al de grupos y después concentramos la atención en anillos de polinomios. El último capítulo, contiene una sección, al inicio, dedicada a espacios vectoriales, y en adelante trata, fundamentalmente, acerca de campos y, en particular, sobre campos de extensión.

Capítulo 1

Grupos

En este capítulo estudiamos los grupos y sus propiedades. La estructura algebraica de un grupo es adecuada para una introducción a la teoría del Álgebra Moderna. En nuestro desarrollo incluimos el estudio de subgrupos, estructura cociente y morfismos entre grupos.

1.1. Definición y propiedades elementales

Estamos familiarizados con operaciones binarias, como la adición y la multiplicación, definidas en conjuntos de números. En general, una operación binaria en un conjunto no vacío G es una regla que a cada par ordenado de elementos de G le hace corresponder un elemento de G.

1.1.1 Definición. Sea G un conjunto no vacío. Una **operación binaria** en G es una función $* : G \times G \longrightarrow G$ que a cada $(a, b) \in G \times G$ le asigna un elemento $a * b \in G$.

Puesto que $a * b \in G$ si $a, b \in G$, se suele decir que G *es cerrado bajo la*

operación $*$. Es común utilizar la notación multiplicativa ab o la notación aditiva $a + b$ para denotar $a * b$.

1.1.2 Definición. Un **grupo** es un conjunto G junto con una operación binaria $(a, b) \mapsto ab$ que satisface las siguientes propiedades:

1. **Asociatividad:** $(ab)c = a(bc)$ para todo $a, b, c \in G$.
2. **Elemento identidad:** Existe un elemento $e \in G$, llamado *identidad*, tal que $ae = ea = a$ para todo $a \in G$.
3. **Inversos:** Para cada $a \in G$ existe $b \in G$, llamado *inverso de* a, tal que $ab = ba = e$.

El elemento identidad y el inverso de un elemento en un grupo son únicos, ver teorema 1.1.4. En notación multiplicativa se acostumbra a denotar el inverso de a por a^{-1}. En notación aditiva el elemento identidad se denota usualmente por 0 y el inverso de a por $-a$.
Un grupo G, en el que se cumple la propiedad **conmutativa**, $xy = yx$ para todo $x, y \in G$, se denomina grupo **abeliano**.

1.1.3. Ejemplos

1. $\mathbb{Z}$ con la adición usual es un grupo y es abeliano. Similarmente otros *conjuntos numéricos* como $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son grupos abelianos con la respectiva adición.
2. $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ con la multiplicación es un grupo abeliano. Análogamente $\mathbb{R}^*$ y $\mathbb{C}^*$ son grupos abelianos. El elemento identidad en cada uno de estos grupos es el número 1.

3. El conjunto $G = \mathbb{R} - \{0\} \times \mathbb{R}$ con la operación $(a, b) * (c, d) = (ac, ad + b)$ es un *grupo no abeliano*. El elemento identidad es $(1, 0)$ y el inverso de (a, b) es $(1/a, -b/a)$.

4. $\mathbb{N}$ *no* es grupo con la suma y $\mathbb{Z}$ *no* es grupo con la multiplicación.

5. $G = \{1, i, -1, -i\}$ es un grupo *finito* con la multiplicación de complejos. La *tabla de grupo* para G es:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

6. El espacio euclídeo $\mathbb{R}^n$ es un grupo con la suma de vectores. En general, todo *espacio vectorial* es un grupo abeliano respecto a la suma de vectores.

7. El conjunto $GL(n, \mathbb{R})$ de matrices invertibles de $n \times n$ es un grupo respecto a la multiplicación de matrices llamado *grupo lineal general*. Note que $GL(n, \mathbb{R})$ es un grupo *no* abeliano.

8. En $\mathbb{Z}$ se define la *relación de equivalencia* $a \equiv b \pmod{n}$ si y sólo si $n|b - a$ (n divide a $b - a$). La *clase de equivalencia* de $a \in \mathbb{Z}$ es $[a] = \{b \in \mathbb{Z} \,|\, a \equiv b \,(\mathrm{mod}\, n)\}$ y el conjunto $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ de *enteros módulos* n es un grupo con la suma de clases $[a]+[b] = [a+b]$.

Para verificar que la operación está bien definida, suponga que $[a] = [a']$ y $[b] = [b']$. Entonces $n|a-a'$ y $n|b-b'$ lo que implica $n|(a-a')+(b-b') = (a+b)-(a'+b')$. Así que $[a+b] = [a'+b']$.

9. Para cada entero $n > 1$ se define $U(n)$ como el conjunto de todos los enteros positivos menores que n y que son primos relativos con n. Entonces $U(n)$ es grupo con la multiplicación módulo n. Por ejemplo $U(12) = \{1, 5, 7, 11\}$. Para probar la cerradura de la operación se debe verificar que si $\text{mcd}\{a, n\} = 1$ y $\text{mcd}\{b, n\} = 1$, entonces $\text{mcd}\{ab, n\} = 1$. Para la existencia de inverso se puede tener en cuenta que la *congruencia lineal* $ax \equiv 1 \pmod{n}$ tiene solución si a y n son primos relativos.

10. Si G y G' son grupos entonces $G \times G' = \{(x, x') \,|\, x \in G \,\text{y}\, x' \in G'\}$ es un grupo con la operación $(x, x') * (y, y') = (xy, x'y')$ llamado *producto directo* de G y G'. En general, para n grupos G_i, $i = 1, 2, \ldots, n$, se tiene que $\prod_{i=1}^{n} G_i$ es un grupo con la operación componente a componente.

1.1.4 Teorema. Sea G un grupo. Entonces:

1. El elemento identidad es único.

2. Cada elemento $a \in G$ tiene un único inverso.

3. $(a^{-1})^{-1} = a$ para todo $a \in G$.

4. $(ab)^{-1} = b^{-1}a^{-1}$ para todo $a, b \in G$.

5. Dados $a, b, c \in G$, $ab = ac$ implica $b = c$, y $ba = ca$ implica $b = c$.

La última propiedad corresponde a las **leyes de cancelación**.

Demostración. La demostración de 5 se deja al lector.

1. Si e y e' son identidades de G, entonces $e = ee' = e'$.

2. Suponga que z y w satisfacen $az = za = e$ y $aw = wa = e$. Entonces $z = ez = (wa)z = w(az) = we = w$.

3. Es claro puesto que $a^{-1}a = aa^{-1} = e$.

4. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Similarmente se verifica que $(b^{-1}a^{-1})(ab) = e$. □

1.1.5. Ejercicios

1. Determine cuáles de los siguientes conjuntos G son grupos con la operación indicada. En caso afirmativo, diga si el grupo es abeliano.

   · G es el conjunto de los enteros con la operación $a * b = a + b + ab$.

   · G es el conjunto de los irracionales y el uno junto con la multiplicación.

   · G es el conjunto de los racionales $\neq -1$ con la operación $a * b = a + b + ab$.

   · G es el conjunto $\{1, 2, 3\}$ con la multiplicación módulo 4.

   · G es el conjunto $\{1, 2, 3, 4\}$ con la multiplicación módulo 5.

   · G es el conjunto $\mathbb{R} - \{0\}$ con la operación $a * b = |a|b$.

   · G es el conjunto de todas las matrices singulares de $n \times n$ con la suma de matrices.

· G es el conjunto de todas las matrices ortogonales de $n \times n$ con la multiplicación de matrices.

· Si H es grupo y S es un conjunto no vacío, considere G el conjunto de todas las funciones $f : S \longrightarrow H$ con la operación $(f, g) \mapsto fg$ donde $fg(s) = f(s)g(s)$.

· Para cada $\mathbf{u} \in \mathbb{R}^n$ considere la translación $T_{\mathbf{u}} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ definida por $T(\mathbf{x}) = \mathbf{x} + \mathbf{u}$. Sea G_1 el conjunto de todas las translaciones con la suma de funciones y G_2 el conjunto de todas las translaciones con la composición de funciones.

· G es el conjunto de todas las matrices $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $a \in \mathbb{R}$ con la multiplicación de matrices.

2. Escriba y demuestre la propiedad $(ab)^{-1} = b^{-1}a^{-1}$ utilizando notación aditiva.

3. Pruebe que $(a_1 a_2 \cdots a_m)^{-1} = a_m^{-1} \cdots a_2^{-1} a_1^{-1}$.

4. Pruebe que G es un grupo abeliano si y sólo si $(ab)^{-1} = a^{-1}b^{-1}$ para todo $a, b \in G$.

5. Demuestre que en un grupo abeliano, $(ab)^n = a^n b^n$ para todo entero positivo n.

6. Encuentre el inverso de $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ en $GL(2, \mathbb{Z}_{11})$.

7. Proporcione un ejemplo de un grupo donde puede ocurrir $(ab)^{-2} \neq b^{-2}a^{-2}$.

8. Proporcione un ejemplo de un grupo no abeliano donde algunos elementos distintos de la identidad satisfacen $(ab)^{-1} = a^{-1}b^{-1}$.

9. Pruebe que si a es un elemento de un grupo finito G, entonces existe un entero positivo n tal que $a^n = e$.

10. Sea G un grupo para el cual $x^2 = e$ para todo $x \in G$. Muestre que G es abeliano.

11. Sea G un grupo para el cual $a = a^{-1}$ para todo $a \in G$. Muestre que G es abeliano.

12. Demuestre que un grupo tiene exactamente un elemento idempotente, esto es, un elemento x tal que $xx = x$.

13. Escriba la tabla del grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$.

14. Explique por qué en una tabla de grupo, cada elemento del grupo aparece exactamente una vez en cada fila y cada columna.

15. Escriba un programa que imprima todos los elementos de $U(n)$ indicando su inverso.

1.2. Subgrupos

1.2.1 Definición. Sea H un subconjunto no vacío de un grupo G. Diremos que H es un **subgrupo** de G si es en sí mismo un grupo respecto a la operación de G.

La notación $H \leq G$ indica que H es subgrupo de G. Observe que H es un subgrupo de G si se verifica

1. El elemento identidad e de G pertenece a H.
2. H es cerrado bajo la operación de G, es decir, $a, b \in H$ implica que $ab \in H$.
3. Si $a \in H$, entonces $a^{-1} \in H$.

1.2.2. Ejemplos

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
2. $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ es un subgrupo de $\mathbb{Z}$ para todo entero n.
3. Si G es un grupo, y $a \in G$, entonces $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ es un subgrupo de G llamado *subgrupo cíclico generado por* a. Por ejemplo, en $\mathbb{Z}_{10}$ se tiene $\langle [2] \rangle = \{[0], [2], [4], [6], [8]\}$ y en $\mathbb{Z}$ se tiene $\langle 2 \rangle = 2\mathbb{Z}$.
4. El conjunto $SL(n, \mathbb{R})$ de todas las matrices de $n \times n$ con determinante 1, es un subgrupo de $GL(n, \mathbb{R})$ llamado *grupo lineal especial*.
5. Si θ es un número real utilizamos la notación $\operatorname{cis}(\theta) = \cos\theta + i \operatorname{sen}\theta$. El conjunto $U = \{\operatorname{cis}(\theta) \mid \theta \in \mathbb{R}\}$ es un subgrupo de $\mathbb{C}^*$. Similarmente $H = \{\operatorname{cis}(2\pi k/n) \mid k = 0, 1, 2, \ldots, n-1\}$ es un subgrupo *finito* de $\mathbb{C}^*$, en particular si $n = 4$, se tiene $H = \{1, i, -1, -i\}$.
6. Sea G un grupo. Entonces $Z(G) = \{a \in G \mid ax = xa \text{ para todo } x \in G\}$ es un subgrupo de G llamado *centro* de G. Por ejemplo:

$$Z(GL(2, \mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \neq 0 \right\}$$

7. $C_G(b) = \{a \in G \mid ab = ba\}$ es el subgrupo *centralizador* de $b \in G$.

8. Si $H \leq G$, entonces $N_G(H) = \{g \in G \mid g^{-1}Hg = H\}$ es el subgrupo *normalizador* de H en G.

1.2.3 Proposición. Sea H un subconjunto no vacío de un grupo G. Entonces H es un subgrupo de G si y sólo si $ab^{-1} \in H$ para todo $a, b \in H$.

Demostración. Si H es subgrupo y $a, b \in H$, entonces por la definición de grupo se tiene que $ab^{-1} \in H$. Recíprocamente, como H es no vacío, dado $a \in H$, se tiene que $e = aa^{-1}, \in H$, $a^{-1} = ea^{-1} \in H$ y $ab = a(b^{-1})^{-1} \in H$ si $b \in H$. □

1.2.4 Definición. El **orden** de un grupo G es su número de elementos (finito o infinito) y se denota $|G|$.

El **orden de un elemento** $a \in G$, denotado $|a|$, es el menor entero positivo n tal que $a^n = e$. Si tal entero no existe, se dice que a tiene orden infinito.

1.2.5. Ejemplos

1. $\mathbb{Z}$ y $\mathbb{R}$ tienen orden infinito (aunque sus cardinales son distintos), $|\mathbb{Z}_n| = n$ y $|U(12)| = 4$.

2. $|[2]| = 5$ en $\mathbb{Z}_{10}$, $|3| = 4$ en $U(10)$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ tienen orden 2 en $GL(2, \mathbb{R})$ pero $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ es de orden infinito.

1.2.6 Proposición. Sea G un grupo y $a \in G$.

1. Si a tiene orden infinito, entonces $a^i = a^j$ si y sólo si $i = j$.

2. Si a tiene orden finito, entonces $a^i = a^j$ si y sólo si $|a|$ divide a $i - j$.

Demostración. 1. Si $|a|$ es infinito, entonces $a^i = a^j \leftrightarrow a^{i-j} = e \leftrightarrow i - j = 0 \leftrightarrow i = j$.

2. Supongamos que $|a|$ es finito e igual a n. Si $a^i = a^j$ entonces $a^{i-j} = e$ y por el algoritmo de la división existen $q, r \in \mathbb{Z}$ únicos tales que $i - j = qn + r$ con $0 \leq r < n$. Así que $e = a^{i-j} = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r$ y por la definición de n se tiene que $r = 0$ y $i - j = nq$, es decir, $|a|$ divide a $i - j$. Recíprocamente si $i - j = nk$, entonces $a^{i-j} = a^{nk} = (a^n)^k = e^k = e$ y en consecuencia $a^i = a^j$. □

1.2.7. Ejercicios

1. Determine si el subconjunto H es subgrupo del grupo G dado.

   · $G = \mathbb{Z}$ y H el conjunto de los enteros divisibles por 2 y 3.

   · $G = GL(n, \mathbb{R})$ y H matrices invertibles diagonales.

   · G es el grupo de todas las matrices de $n \times n$ con la suma, H_1 las matrices triagulares, H_2 las matrices triangulares superiores, H_3 matrices simétricas, H_4 matrices antisimétricas y H_5 matrices singulares.

   · $G = \mathbb{C}$ y $H = \{a + bi \,|\, ab \geq 0\}$.

   · $G = \mathbb{C}^*$ y $H = \{a + bi \,|\, a^2 + b^2 = 1\}$.

2. Encuentre el orden de cada elemento en los grupos $\mathbb{Z}_{12}$ y $U(12)$.

3. Si G y G' son grupos finitos de orden m y n, respectivamente, ¿cuál es el orden de $G \times G'$?

4. Si G es un grupo finito de orden par, demuestre que debe existir un $a \neq e$ tal que $a^{-1} = a$.

5. Pruebe que si H y K son subgrupos de un grupo G, entonces $H \cap K$ es un subgrupo de G. Generalice y demuestre este resultado para una familia arbitraria de subgrupos de G.

6. Encuentre todos los subgrupos de $\mathbb{Z}_{12}$ y $U(20)$.

7. Suponga que H es un subgrupo propio de $\mathbb{Z}$ que contiene a 12, 30 y 54. ¿Cuáles son las posibilidades para H?

8. Sea G un grupo abeliano. Muestre que $H = \{a \in G \,|\, a^2 = e\}$ es subgrupo de G.

9. Pruebe que $Z(G) = \bigcap_{a \in G} C(a)$.

10. Sea G un grupo y $a \in G$. Muestre que $C(a) = C(a^{-1})$.

11. Sean A y B subgrupos de un grupo abeliano G. Muestre que $AB = \{ab \,|\, a \in A \,\text{y}\, b \in B\}$ es un subgrupo de G. Proporcione un ejemplo de un grupo G y dos subgrupos A y B donde AB no sea subgrupo.

12. Sea G un grupo y H un subgrupo. Pruebe que si $x \in G$, entonces $x^{-1}Hx = \{x^{-1}yx \,|\, y \in H\}$ es subgrupo de G.

13. Encuentre el orden en su respectivo grupo lineal de

$$\begin{bmatrix} \cos(\pi/3) & -\operatorname{sen}(\pi/3) \\ \operatorname{sen}(\pi/3) & \cos(\pi/3) \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

14. Sean a y b elementos de un grupo G. Muestre que $|a| = |a^{-1}|$, $|ab| = |ba|$ y $|a| = |cac^{-1}|$.

15. Suponga que $A \in GL(n, \mathbb{R})$ tiene orden finito. Muestre que un valor propio λ de A es necesariamente una raíz de la unidad, es decir, $\lambda^n = 1$ para algún n.

16. Muestre que el conjunto H de matrices invertibles y triangulares superiores es un subgrupo de $GL(n, \mathbb{R})$. Encuentre dos subgrupos propios de H.

17. Encuentre el orden del grupo de matrices diagonales (resp. triangulares superiores) invertibles de $n \times n$ (respecto al producto) y con entradas en $\mathbb{Z}_p$, p primo.

18. Escriba un programa que calcule el orden de un elemento en $GL(2, \mathbb{Z}_p)$, donde p es primo.

1.3. Grupos cíclicos

1.3.1 Definición. Un grupo G es **cíclico** si existe $a \in G$ tal que

$$G = \{a^n \mid n \in \mathbb{Z}\}$$

Tal elemento a es un *generador* de G. Se dice que G es *generado* por a y se denota $G = \langle a \rangle$.

1.3.2 Observación. Los grupos cíclicos son abelianos porque $a^k a^l = a^{k+l} = a^l a^k$.

1.3.3. Ejemplos

1. $\mathbb{Z} = \langle 1 \rangle$ y $n\mathbb{Z} = \langle n \rangle$.
2. $\mathbb{Z}_n = \langle [1] \rangle$.
3. $H = \{\text{cis}(2\pi k/n) \,|\, k = 0, 1, 2, \ldots, n-1\} = \langle \text{cis}(2\pi/n) \rangle$. En particular $\{1, i, -1, -i\} = \langle i \rangle$.
4. $\mathbb{Z}_2 \times \mathbb{Z}_2$ y $U(12)$ *no* son cíclicos.
5. $\mathbb{R}$ *no* es cíclico, ni ningún grupo *no numerable*.
6. $\mathbb{Q}$ *no* es cíclico.

1.3.4 Proposición. Todo subgrupo de un grupo cíclico es cíclico.

Demostración. Suponga que G es un grupo cíclico generado por a y sea H un subgrupo de G. Si $H = \{e\}$, entonces H es cíclico. Si $H \neq \{e\}$, entonces existe $a^t \neq e$ en H donde t es un entero positivo. Sea m el menor entero positivo tal que $a^m \in H$. Por cerradura se tiene que $\langle a^m \rangle \subseteq H$. Ahora, si $b \in H$, entonces $b = a^k$ para algún entero k y existen enteros únicos q y r tales que $k = qm + r$ con $0 \leq r < m$. Luego $b = a^k = a^{qm+r} = a^{qm}a^r$ y $a^r = a^{-qm}a^k = (a^m)^{-q}b \in H$. Por la elección de m resulta que $r = 0$ y $b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle$. Así $H \subseteq \langle a^m \rangle$. □

1.3.5 Ejemplo. Los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para algún entero n.

1.3.6 Lema. Si G es un grupo cíclico de orden n generado por a, entonces $\langle a^s \rangle = \langle a^d \rangle$ donde $d = \text{mcd}\{n, s\}$.

Demostración. Puesto que $s = dk$ para algún entero k, entonces $a^s = a^{dk} = (a^d)^k$ y $\langle a^s \rangle = \langle a^d \rangle$. De otra parte, existen enteros z y w tales que $d = zn + ws$ de donde $a^d = a^{zn+ws} = (a^n)^z (a^s)^w = e^z (a^s)^w = (a^s)^w$. Por tanto $\langle a^d \rangle = \langle a^s \rangle$. □

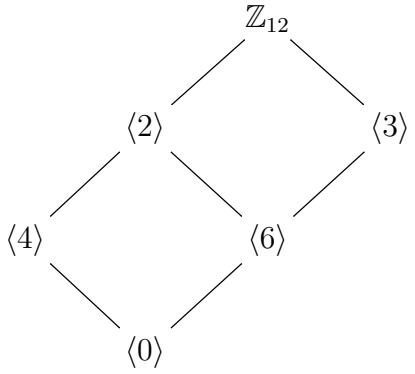
1.3.7 Teorema. Sea G un grupo cíclico de orden n generado por a. Si $b \in G$ y $b = a^s$, entonces b genera un subgrupo cíclico de orden n/d donde $d = \text{mcd}\{n, s\}$.

Demostración. Note que $|a^d| = n/d$ para cualquier divisor d de n. En efecto, $(a^d)^{n/d} = a^n = e$ implica que $|a^d| \leq n/d$ y si i es un entero positivo menor que n/d, entonces $(a^d)^i \neq e$ porque $di < n = |a|$. Teniendo en cuenta esto con $d = \text{mcd}\{n, s\}$ y el lema anterior, se concluye que $|a^s| = |\langle a^s \rangle| = |\langle a^d \rangle| = |a^d| = n/d$. □

Se deduce el siguiente resultado cuya demostración se propone como ejercicio.

1.3.8 Corolario. Si a es un generador de un grupo cíclico finito G de orden n, entonces los otros generadores de G son los elementos de la forma a^r donde r y n son primos relativos.

1.3.9 Ejemplo. Los generadores de $\mathbb{Z}_{12}$ son [1], [5], [7] y [11]. Luego el *diagrama reticular* de los subgrupos de $\mathbb{Z}_{12}$ es:



1.3.10. Ejercicios

1. ¿Cuál es el subgrupo cíclico de $\mathbb{Z}$ generado por -1?

2. Pruebe para cualquier elemento en un grupo, $|a| = |\langle a \rangle|$.

3. Liste los elementos de $\left\langle \frac{1}{3} \right\rangle$ como subgrupo de $\mathbb{Q}$ y como subgrupo de $\mathbb{Q}^*$.

4. Verifique que $U(14)$ es cíclico pero $U(20)$ no lo es.

5. Demuestre que en un grupo cíclico finito, el orden de un elemento divide al orden del grupo.

6. Muestre que un entero k tal que $1 \leq k < n$, $[k]$ es generador de $\mathbb{Z}_n$ si y sólo si n y k son primos relativos.

7. Encuentre todos los generadores de $\mathbb{Z}_{20}$.

8. Halle un generador de $\langle [20] \rangle \cap \langle [10] \rangle$ en $\mathbb{Z}_{24}$.

9. Para cualquier elemento a de un grupo, muestre que $\langle a \rangle$ es subgrupo de $C(a)$.

10. Demuestre que un grupo infinito debe tener un número infinito de subgrupos.

11. Describa el conjunto de las raíces n-ésimas de la unidad y pruebe que un grupo cíclico de orden n.

12. Suponga que G es un grupo cíclico de orden n y que a es un generador de G. Muestre que si un entero $r \neq 0$ es primo relativo con n, entonces a^r también es generador de G.

13. Sean G y G' grupos cíclicos de orden m y n, respectivamente, con m y n primos relativos. Muestre que $G \times G'$ es un grupo cíclico de orden mn.

14. Sea G un grupo abeliano finito y denote por a al producto de todos los elementos de G. Muestre que $a^2 = e$. Si en adición G es cíclico muestre que $a = e$ si $|G|$ es impar y $a \neq e$ si $|G|$ es par.

15. Escriba un programa que determine todos los generadores y subgrupos de $\mathbb{Z}_n$.

1.4. Permutaciones

1.4.1 Definición. Una **permutación** de un conjunto no vacío A es una función biyectiva de A en A.

1.4.2 Teorema. El conjunto de todas la permutaciones en A es un grupo respecto a la composición de funciones.

Demostración. Por las propiedades generales de las funciones se sabe que la función compuesta de funciones biyectivas es biyectiva, además la composición es asociativa. La función $x \mapsto x$ para todo $x \in A$ es la permutación identidad y dada una permutación $x \mapsto y$, su inverso es la permutación $y \mapsto x$. □

1.4.3 Definición. El grupo de todas las permutaciones de $\{1, 2, \ldots, n\}$ se llama **grupo simétrico de grado** n y se denota por S_n.

Observe que S_n tiene $n!$ elementos y es grupo *no* abeliano para $n \geq 3$. Utilizamos la notación:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

para la permutación en S_n tal que $\sigma(1) = i_1$, $\sigma(2) = i_2$, $\ldots$, $\sigma(n) = i_n$.

1.4.4. Ejemplos

1. Acordamos operar *de derecha a izquierda*. Así por ejemplo en S_4, si

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \quad \text{y} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix},$$

entonces

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad \text{y} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

2. El elemento identidad de S_4 es $\iota = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ y el inverso de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \quad \text{es} \quad \sigma^{-1} = \begin{pmatrix} 3 & 2 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

3. Los elementos de S_3 (utilizamos la notación de [1]) son:

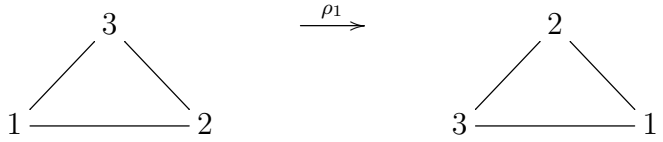
$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

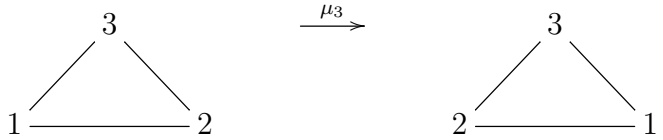
y la tabla de grupo es:

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	ρ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Geométricamente S_3 es el grupo D_3 de *simetrías de un triángulo equilátero*, donde las ρ_i son *rotaciones* y las μ_i son *reflexiones*. Por ejemplo



y



4. El grupo S_4 tiene 24 elementos y D_4, el grupo de simetrías de un cuadrado, tiene 8 elementos (4 rotaciones y 4 reflexiones). Así que $S_4 \neq D_4$.

La notación $\sigma = (i_1\, i_2\, \cdots\, i_k)$ indica la permutación $\sigma \in S_n$ tal que $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$ y $\sigma(j) = j$ para todo $j \neq i_1, i_2, \ldots, i_k$.

$\sigma = (i_1\, i_2\, \cdots\, i_k)$ se denomina **ciclo** de longitud k o k-ciclo.

Dos ciclos son **ajenos** si no tienen elementos comunes en la notación cíclica.

1.4.5 Ejemplos. Nos ubicamos en S_6.

1. $(1\,2\,4\,6)$ es un ciclo de longitud 4 que representa la permutación
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}.$$
Observe que $(1\,2\,4\,6) = (4\,6\,1\,2)$.
2. $(2\,3\,5\,6)(3\,1\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 4 & 5 & 2 \end{pmatrix}$ mientras que $(3\,1\,5)(2\,3\,5\,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 4 & 6 & 2 \end{pmatrix}$.
3. $(1\,3\,5)(4\,2\,6) = (4\,2\,6)(1\,3\,5)$. En general si σ y τ son ciclos ajenos, entonces $\sigma\tau = \tau\sigma$.
4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix} = (1\,5\,2\,3)(4\,6)$.

El último ejemplo ilustra el siguiente resultado general.

1.4.6 Teorema. Toda permutación en S_n es producto de ciclos ajenos.

Demostración. Sea $\sigma \in S_n$. Para cada $i \in S$, existe un entero positivo k_i tal que $\sigma(i)$, $\sigma^2(i)$, ..., $\sigma^{k_i}(i)$ son diferentes y $\sigma^{k_i+1}(i) = i$. Es suficiente considerar el producto de ciclos de la forma $(\sigma(i)\,\sigma^2(i)\,\ldots\,\sigma^{k_i}(i))$ que no tengan elementos comunes. □

Una **transposición** es un ciclo de longitud 2. Note que $(i_1\,i_2\,\cdots\,i_k) = (i_1\,i_k)(i_1\,i_{k-1})\cdots(i_1\,i_2)$. Como consecuencia se tiene el siguiente resultado.

1.4.7 Corolario. Toda permutación en S_n es producto de transposiciones.

1.4.8 Teorema. Ninguna permutación en S_n puede expresarse como producto de un número par de transposiciones y como producto de un número impar de transposiciones.

Se invita al lector a consultar la demostración del teorema anterior en [1] o [2]. Este hecho permite introducir la siguiente definición.

Una permutación en S_n es **par** o **impar** según pueda expresarse como producto de un número par o impar de transposiciones.

1.4.9 Ejemplo. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1\,6)(2\,3)(2\,5)$ es una permutación impar y $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1\,2)(1\,2)$ es una permutación par.

1.4.10 Teorema. Si $n \geq 2$, entonces el subconjunto A_n de S_n formado por todas las permutaciones pares es un subgrupo de S_n y tiene orden $n!/2$.

Demostración. A_n es no vacío porque contiene la permutación identidad, además es cerrado bajo el producto de permutaciones porque la suma de dos enteros pares en un entero par. Ahora, si $\sigma \in A_n$, entonces $\sigma = \tau_1\tau_2\cdots\tau_k$

donde cada τ_i es una transposición y k es par. Como $\sigma^{-1} = \tau_k^{-1} \cdots \tau_2^{-1}\tau_1^{-1} = \tau_k \cdots \tau_2\tau_1$ entonces $\sigma^{-1} \in A_n$. Así que A_n es subgrupo de S_n. Para terminar, si B_n es el conjunto de transposiciones impares de S_n, entonces la función $\lambda : A_n \longrightarrow B_n$ definida por $\lambda(\sigma) = (1\,2)\sigma$ es biyectiva y en consecuencia el orden de A_n es $n!/2$. □

El subgrupo A_n de S_n se denomina **grupo alternante**. Por ejemplo, $A_3 = \{\rho_0, \rho_1, \rho_2\}$.

1.4.11. Ejercicios

1. Sea $\sigma = (1\,2\,3\,4\,5)(1\,2\,3\,4\,6)(1\,2\,3\,4\,7)$ en S_7. Determine σ, σ^{-1} y $|\sigma|$.
2. Escriba la tabla del grupo D_4, el grupo de simetrías de un cuadrado.
3. Encuentre el orden de cada elemento en S_3 y en D_4.
4. Encuentre todos los subgrupos de S_3 y D_4. Dibuje los respectivos diagramas reticulares.
5. Demuestre que S_n no es abeliano para $n \geq 3$.
6. Hallar $C(a)$ para cada $a \in S_3$ y cada $a \in D_4$.
7. Halle el centro de S_3 y de D_4.
8. Determine el grupo alternante A_4.
9. Muestre que un k-ciclo tiene orden k.
10. Pruebe que el orden de una permutación, escrita como producto de ciclos ajenos, es el mínimo común múltiplo de los órdenes de los ciclos.

11. Sea $i \in \{1, 2, \ldots, n\}$ y $G(i) = \{\sigma \in S_n \,|\, \sigma(i) = i\}$. Muestre que $G(i)$ es subgrupo de S_n.

12. Escriba un programa que determine el orden de una permutación en S_n.

1.5. Homomorfismos

1.5.1 Definición. Sean G y G' grupos. Una función $\varphi : G \longrightarrow G'$ es un **homomorfismo** si $\varphi(ab) = \varphi(a)\varphi(b)$ para todo $a, b \in G$.

1.5.2 Ejemplos. Cada una de las siguientes funciones es un homomorfismo de grupos.

1. $\varphi : \mathbb{R} \longrightarrow \mathbb{R}^+$, $\varphi(x) = e^x$.

2. $\varphi : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$, $\varphi(A) = \det(A)$.

3. $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\varphi(a) = [a]$.

4. $\varphi : S_n \longrightarrow \mathbb{R}^*$ dada por

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

5. $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$, $\varphi(z) = \overline{z}$.

6. Sea A una matriz de $m \times n$ y $L : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ definida $L(\mathbf{x}) = A\mathbf{x}$. En general, cualquier función lineal entre espacios vectoriales es un homomorfismo de grupos.

1.5.3 Proposición. Sea $\varphi : G \longrightarrow G'$ un homomorfismo. Entonces:

1. $\varphi(e) = e'$.
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ para cada elemento $a \in G$.
3. $\ker(\varphi) = \{a \in G \,|\, \varphi(a) = e'\}$ es un subgrupo de G llamado **kernel** o **núcleo** de φ.
4. $\varphi(G) = \{\varphi(a) \,|\, a \in G\}$ es un subgrupo de G' llamado **imagen** de φ.

Demostración. La demostración de 4 se deja al lector.

1. Aplique la propiedad cancelativa a $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$.
2. Por la unicidad de los inversos y $e' = \varphi(e) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a)$.
3. $\ker(\varphi)$ es no vacío porque contiene a e. Ahora, $a, b \in \ker(\varphi)$ implica $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e'$ y por tanto $ab^{-1} \in \ker(\varphi)$. □

1.5.4 Ejemplos. Los siguientes subgrupos corresponden a los núcleos e imágenes de los homomorfismos dados en el ejemplo anterior.

1. $\ker(\varphi) = \{0\}$ y $\varphi(\mathbb{R}) = \mathbb{R}^+$.
2. $\ker(\varphi) = SL(n, \mathbb{R})$ y $\varphi(GL(n, \mathbb{R})) = \mathbb{R}^*$.
3. $\ker(\varphi) = n\mathbb{Z}$ y $\varphi(\mathbb{Z}) = \mathbb{Z}_n$.
4. $\ker(\varphi) = A_n$ y $\varphi(S_n) = \{1, -1\}$.
5. $\ker(\varphi) = \{0\}$ y $\varphi(\mathbb{C}) = \mathbb{C}$.

6. $\ker(\varphi)$ es el espacio nulo de A y $\varphi(\mathbb{R}^n)$ es el espacio columna de A.

A los homomorfismos inyectivos se les llama **monomorfismos** y a los sobreyectivos se les llama **epimorfismos**. Note que si $\varphi : G \longrightarrow G'$ es un homomorfismo, entonces φ es uno a uno si y sólo si $\text{Ker}(\varphi) = \{e\}$ y φ es sobre si y sólo si $\varphi(G) = G'$.

1.5.5 Definición. Un **isomorfismo** es un homomorfismo biyectivo. Dos grupos G y G' son **isomorfos** si existe un isomorfismo $\varphi : G \longrightarrow G'$.

¿Qué significa que dos grupos sean isomorfos? Empecemos considerando las tablas de grupo para $\mathbb{Z}_4$ con la adición y $G = \{1, i, -1, -i\}$ con la multiplicación.

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Observe que con las identificaciones $[0] \leftrightarrow 1$, $[1] \leftrightarrow i$, $[2] \leftrightarrow -1$ y $[3] \leftrightarrow -i$, las dos tablas son *indistinguibles* excepto por el nombre de los elementos y de la operación, es decir, los dos grupos son *estructuralmente el mismo*, son isomorfos. La función biyectiva $\varphi : \mathbb{Z}_4 \longrightarrow G$ definida por las anteriores identificaciones es un isomorfismo y se puede pensar como un *renombramiento* de los elementos preservando la estructura del grupo.

Ahora considere el 4-*grupo de Klein*, $V_4 = \{e, a, b, c\}$, dado por la tabla

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note que aunque se pueden definir funciones biyectivas entre $\mathbb{Z}_4$ y V_4, ninguna de ellas preserva todas las *propiedades estructurales*. Por ejemplo $\mathbb{Z}_4$ es cíclico pero V_4 no lo es, o $\mathbb{Z}_4$ tiene un único subgrupo no trivial y V_4 tiene tres subgrupos no triviales. Luego $\mathbb{Z}_4$ y V_4 *no* son isomorfos.

1.5.6. Ejemplos

1. $\varphi : \mathbb{R} \longrightarrow \mathbb{R}^+$ dada por $\varphi(x) = e^x$ es un isomorfismo.

2. $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$, $\varphi(z) = |z|$, es un *automorfismo* (isomorfismo en sí mismo) diferente de la función identidad.

3. Si $G = \langle a \rangle$ es un grupo cíclico infinito, entonces $\varphi : \mathbb{Z} \longrightarrow G$, $\varphi(k) = a^k$, es un isomorfismo. Luego $\mathbb{Z}$ es el *único* grupo cíclico infinito *salvo isomorfismo*. ¿Cuál es el análogo en el caso en que G sea cíclico finito?

4. Si S es una base de un espacio vectorial V de dimensión n, entonces $\varphi : V \longrightarrow \mathbb{R}^n$ definida por $\varphi(\mathbf{x}) = [\mathbf{x}]_S$ (vector de coordenadas de $\mathbf{x}$ en la base S) es un isomorfismo.

1.5.7 Teorema de Caley. Todo grupo es isomorfo a algún subgrupo de un grupo de permutaciones.

Demostración. Sea G un grupo. Para cada $a \in G$ se considera la permutación $T_a : G \longrightarrow G$, $T_a(x) = ax$. Estas permutaciones cumplen $T_{ab} = T_a \circ T_b$. Si $A(G)$ es el grupo de permutaciones de G, entonces la función $\varphi : G \longrightarrow A(G)$ definida por $\varphi(a) = T_a$ es un monomorfismo y en consecuencia G es isomorfo al grupo de permutaciones $\varphi(G)$. □

1.5.8. Ejercicios

1. Determine cuáles de las siguientes funciones son homomorfismos. En este ejercicio G y G' son grupos arbitrarios.

   · Sea $n \in \mathbb{Z}$ fijo y sea $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $\varphi(k) = nk$ para todo $k \in \mathbb{Z}$.

   · $\varphi : G \longrightarrow G$ definida por $\varphi(a) = a^{-1}$ para todo $a \in G$.

   · $\varphi : G \longrightarrow G'$ definida por $\varphi(a) = e'$ para todo $a \in G$.

   · $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$ definida por $\varphi(z) = |z|$ para todo $z \in \mathbb{C}$.

   · $\varphi : \mathbb{C}^* \longrightarrow \mathbb{C}^*$ definida por $\varphi(z) = |z|$ para todo $z \in \mathbb{C}^*$.

   · $\varphi : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ definida por $\varphi(x) = \sqrt{x}$ para todo $x \in \mathbb{R}^+$.

   · $\varphi : GL(n, \mathbb{R}) \longrightarrow GL(n, \mathbb{R})$ definida por $\varphi(A) = A^T$ para todo $A \in GL(n, \mathbb{R})$.

   · Sea $\mathbf{a} \in \mathbb{R}^3$ fijo y sea $\varphi : \mathbb{R}^3 \longrightarrow \mathbb{R}$ definida por $\varphi(\mathbf{x}) = \mathbf{a} \times \mathbf{x}$ para todo $\mathbf{x} \in \mathbb{R}^3$.

2. Determine el núcleo y la imagen de cada homomorfismo del problema anterior.

3. Sea G un grupo y $a \in G$. Muestre que la función $\varphi : G \longrightarrow G$ definida por $\varphi(x) = a^{-1}xa$ es un automorfismo.

4. Sea G un grupo. Determine una condición para que la función $\varphi : G \longrightarrow G$ definida por $\varphi(a) = a^2$ sea un homomorfismo.

5. Demuestre que todo grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}_n$.

6. Muestre que $n\mathbb{Z}$ y $m\mathbb{Z}$ son isomorfos para todo $n, m \in \mathbb{Z}$.

7. Sea M el conjunto de todas las matrices de la forma $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, $a, b \in \mathbb{R}$. Pruebe que M es un grupo con la suma isomorfo a $\mathbb{C}$ y M^* es un grupo con la multiplicación isomorfo a $\mathbb{C}^*$.

8. Pruebe que el conjunto $G = \mathbb{R} - \{-1\}$ con la operación $a * b = a + b + ab$ es un grupo isomorfo a $\mathbb{R}^*$.

9. Muestre que no existe un isomorfismo entre $\mathbb{Q}$ y $\mathbb{Q}^*$.

10. Muestre que si G y G' son grupos, entonces $G \times G'$ y $G' \times G$ son isomorfos.

11. Pruebe que la relación $G \simeq G'$ si G es isomorfo a G' es una relación de equivalencia.

12. Sea $\varphi : G \longrightarrow G'$ un isomorfismo. Demuestre que

    a) G es abeliano si y sólo si G' es abeliano.

    b) G es cíclico si y sólo si G' es cíclico.

    c) Si H es subgrupo de G, entonces $\varphi(H)$ es subgrupo de G'.

1.6. Clases laterales

Recuerde que en $\mathbb{Z}$ se estableció la relación de equivalencia $a \equiv b \pmod{n}$ si n divide a $a - b$ lo cual es igual que $a - b \in n\mathbb{Z}$. Las clases de equivalencia forman el grupo $\mathbb{Z}_n$.

El siguiente resultado general se verifica fácilmente.

1.6.1 Proposición. Sea H un subgrupo de un grupo G. La relación en G definida por $a \sim b$ si $ab^{-1} \in H$ es una relación de equivalencia y las clases de equivalencia son de la forma $[a] = Ha = \{ha \,|\, h \in H\}$.

1.6.2 Definición. El conjunto $Ha = \{ha \,|\, h \in H\}$ se denomina **clase lateral derecha** de H en G.

De manera análoga se definen las clases laterales *izquierdas*. Note que si G es abeliano se puede decir simplemente clase lateral.

1.6.3. Ejemplos

1. Las clases laterales derechas de $H = \{\rho_0, \mu_1\}$ en S_3 son H, $H\rho_1 = \{\rho_1, \mu_3\}$ y $H\rho_2 = \{\rho_2, \mu_2\}$.

2. Las clases laterales de $4\mathbb{Z}$ en $\mathbb{Z}$ son los elementos de $\mathbb{Z}_4$.

1.6.4 Teorema de Lagrange. Si G es un grupo finito y H es un subgrupo de G, entonces el orden de H divide al orden de G.

Demostración. Como G es finito, la relación de equivalencia $a \sim b$ si $ab^{-1} \in H$ produce la partición $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$ donde $Ha_i \cap Ha_j = \emptyset$ para $i \neq j$. La función $\lambda_i : H \longrightarrow Ha_i$ definida por $\lambda_i(h) = ha_i$ es biyectiva

y por tanto $|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_k| = k|H|$. Luego $|H|$ divide a $|G|$. □

1.6.5 Corolario. Todo grupo de orden primo es cíclico.

Demostración. Sea $a \in G$ con $a \neq e$. Entonces $\langle a \rangle \neq \{e\}$ y $|\langle a \rangle|$ divide a $|G|$. Así que $|\langle a \rangle| = |G|$ y $G = \langle a \rangle$. □

1.6.6 Ejemplo. Si p es primo, entonces $\mathbb{Z}_p$ es el único grupo de orden p salvo isomorfismo.

1.6.7. Ejercicios

1. Sea G un grupo. Defina en G una relación de equivalencia cuyas clases de equivalencia sean las clases laterales izquierdas.

2. ¿Una clase lateral derecha es también una clase lateral izquierda?

3. Muestre que aH es subgrupo de G si y sólo si $a \in H$.

4. Pruebe que en un grupo finito, el número de clases laterales izquierdas es igual al número de clases laterales derechas.

5. Sea H un subgrupo de S_3. Halle todas las clases laterales derechas e izquierdas de H en G. Repita el ejercicio para el grupo D_4.

6. Sea H un plano en $\mathbb{R}^3$ que pasa por el origen. Describa las clases laterales de H en $\mathbb{R}^3$.

7. Describa las clases laterales de $SL(n, \mathbb{R})$ en $GL(n, \mathbb{R})$.

8. Muestre que en un grupo finito, el orden de cada elemento divide al orden del grupo.

9. Pruebe que si G es un grupo finito de orden n, entonces $a^n = e$ para todo $a \in G$.

10. Sea H un subgrupo de un grupo G. El número de clases laterales derechas de H en G es el **índice** de H en G y se denota $(G : H)$. Muestre que si G es finito, entonces $(G : H) = |G|/|H|$.

11. Encuentre el número de clases laterales de $\langle 0\rangle \times \langle 1\rangle \times \langle 2\rangle$ en $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.

12. Demuestre que si $K \leq H \leq G$ son tales que $(H : K)$ y $(G : H)$ son ambos finitos, entonces $(G : K)$ es finito y $(G : K) = (G : H)(H : K)$.

1.7. Subgrupos normales y grupo cociente

Sea H un subgrupo de G. Se define $a^{-1}Ha = \{a^{-1}xa \,|\, x \in H\}$.

1.7.1 Definición. Un subgrupo N de un grupo G es un subgrupo **normal** si $a^{-1}Na \subseteq N$ para todo $a \in G$.

La notación $N \lhd G$ indica que N es un subgrupo normal de G.

1.7.2. Ejemplos

1. Si $\varphi : G \longrightarrow G'$ es un homomorfismo, entonces $\mathrm{Ker}(\varphi) \lhd G$.

2. $Z(G) \lhd G$ para todo grupo G.

3. El grupo alternante A_n es un subgrupo normal de S_n.

4. $SL(n\mathbb{R}) \lhd GL(n, \mathbb{R})$.

5. Todo subgrupo de un grupo abeliano es normal.

6. $H = \{\rho_0, \mu_1\}$ *no* es un subgrupo normal de S_3.

1.7.3. Observaciones

1. $a^{-1}Na \subseteq N$ para todo $a \in G$ si y sólo si $a^{-1}Na = N$ para todo $a \in G$. En efecto, $N = a(a^{-1}Na)a^{-1} \subseteq aNa^{-1} = (a^{-1})^{-1}Na^{-1} \subseteq N$.

2. $a^{-1}Na = N$ significa que son iguales como conjuntos y *no* que $a^{-1}na = n$ para todo $n \in N$.

1.7.4 Teorema. N es un subgrupo normal de G si y sólo si $aN = Na$ para todo $a \in G$.

Demostración. $a^{-1}Na = a$ para todo $a \in G$ si y sólo si $Na = aN$ para todo $a \in G$. Es decir, toda clase lateral derecha es una clase lateral izquierda y viceversa. □

Recuerde que si H es subgrupo de G entonces $a \sim b$ si $ab^{-1} \in H$ es una relación de equivalencia en G tal que $[a] = Ha = \{ha \,|\, h \in H\}$.

1.7.5 Teorema. Si N es un subgrupo normal de G entonces $G/N = \{[a] \,|\, a \in G\} = \{Na \,|a \in G\}$ es un grupo respecto a la operación $[a][b] = [ab]$.

Demostración. Si $[a] = [a']$ y $[b] = [b']$, entonces $a' = na$ y $b' = mb$ con $n, m \in N$. Entonces $a'b' = namb = n(ama)^{-1}ab = n_1ab$ donde $n_1 \in N$ porque $n, ama^{-1} \in N$. Luego $[ab] = [a'b']$ y la operación está bien definida. La asociatividad se sigue de la asociatividad de G, $[e]$ es la identidad de G/N y $[a^{-1}]$ es el inverso de $[a]$ en G/N. □

El grupo G/N del teorema anterior se denomina **grupo cociente**. Observe que si G es finito, entonces $|G/N| = |G|/|N|$.

1.7.6. Ejemplos

1. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Note que si inicialmente hubiéramos definido $\mathbb{Z}_n$ como el conjunto $\{0, 1, \ldots, n-1\}$ con la suma módulo n, se tendría que $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

2. $\mathbb{R}/\mathbb{Z} = \{r + \mathbb{Z} \,|\, 0 \leq r < 1\}$.

3. S_n/A_n es un grupo de dos elementos, por tanto es isomorfo a $\mathbb{Z}_2$.

1.7.7 Teorema. Si N es un subgrupo normal de G, entonces $\pi : G \longrightarrow G/N$ definida por $\pi(a) = [a]$ es un epimorfismo tal que $\ker(\pi) = N$.

Demostración. Es claro que π es un epimorfismo. Ahora $a \in \ker(\pi) \leftrightarrow \pi(a) = [a] = [e] \leftrightarrow ae^{-1} = a \in N$. □

El homomorfismo π anterior se denomina **epimorfismo canónico** o **natural**.

1.7.8 Ejemplo. El epimorfismo canónico $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ le asigna a cada $a \in \mathbb{Z}$ el conjunto de todos los enteros que dejan el mismo residuo que a cuando se divide entre n.

1.7.9. Ejercicios

1. Sea $N \triangleleft G$ y $\varphi : G \longrightarrow G'$ un homomorfismo. Muestre que $\varphi(N) \triangleleft \varphi(G)$.

2. Sean A y B subgrupos normales de un grupo G. Muestre que AB y $A \cap B$ son subgrupos normales de G.

3. Considere el grupo $G = \{(x, y) \,|\, x, y \in \mathbb{R}\,,\, x \neq 0\}$ con la operación $(a, b) * (c, d) = (ac, ad + b)$. Muestre que $N = \{(1, y) \,|\, y \in \mathbb{R}\}$ es un subgrupo normal de G. ¿Podría identificar G/N con un grupo conocido?

4. Muestre que $N = \{\rho_0, \rho_2\}$ es un subgrupo normal de D_4 y escriba la tabla de grupo para D_4/N.

5. Determine a qué grupos son isomorfos los grupos $\mathbb{Z}_2 \times \mathbb{Z}_4/\langle(1, 0)\rangle$, $\mathbb{Z}_2 \times \mathbb{Z}_4/\langle(0, 2)\rangle$ y $\mathbb{Z}_2 \times \mathbb{Z}_4/\langle(1, 2)\rangle$.

6. Muestre que $\mathbb{C}^*/N$ donde $N = \{z \in \mathbb{C}^* \,|\, |z| = 1\}$ es un grupo isomorfo a $\mathbb{R}^+$.

7. Si G es un grupo abeliano y H es subgrupo de G, demuestre que G/H es abeliano.

8. Si G es un grupo cíclico y H es subgrupo de G, demuestre que G/H es cíclico.

9. Demuestre que si $G/Z(G)$ es cíclico, entonces G es abeliano.

10. Sea G un grupo y $a \in G$. El automorfismo $\varphi : G \longrightarrow G$ definido por $\varphi(x) = a^{-1}xa$ se denomina **automorfismo interno de G inducido por a.**

    a) Muestre que el conjunto $\mathrm{Int}(G)$ de todos los automorfimos internos es un subgrupo de $\mathrm{Aut}(G)$, el grupo de todos los automorfismos de G.

    b) Pruebe que $G/Z(G)$ es isomorfo a $\mathrm{Int}(G)$.

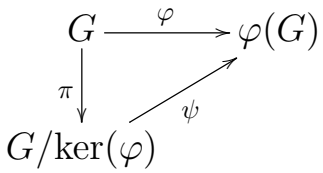
1.8. Teoremas de homomorfismos

1.8.1 Primer teorema de homomorfismos. Si $\varphi : G \longrightarrow G'$ es un homomorfismo, entonces $G/\ker(\varphi) \simeq \varphi(G)$.

Demostración. La función $\psi : G/\ker(\varphi) \longrightarrow \varphi(G)$ definida por $\psi(Ka) = \varphi(a)$ donde $K = \ker(\varphi)$, es un isomorfismo. □

1.8.2 Corolario. Si $\varphi : G \longrightarrow G'$ es un epimorfismo, entonces $G/\ker(\varphi) \simeq G'$.

1.8.3 Observación. Sea $\varphi : G \longrightarrow G'$ un homomorfismo y $\pi : G \longrightarrow G/\ker(\varphi)$ el epimorfismo canónico. Entonces el siguiente diagrama conmuta



es decir, $\psi \circ \pi(a) = \varphi(a)$ para todo $a \in G$.

1.8.4. Ejemplos

1. $\varphi : \mathbb{C}^* \longrightarrow \mathbb{R}^*$ definida por $\varphi(z) = |z|$ es un homomorfismo tal que $\mathrm{Ker}(\varphi) = \{z \in \mathbb{C}^* \,|\, |z| = 1\}$ y por tanto $\mathbb{C}^*/\ker(\varphi) \simeq \mathbb{R}^+$.

2. La función $\varphi : S_n \longrightarrow \mathbb{R}^*$ dada por

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

es un homomorfismo con $\mathrm{Ker}(\varphi) = A_n$ y $\varphi(S_n) = \{1, -1\}$. Entonces $S_n/A_n \simeq \{1, -1\} \simeq \mathbb{Z}_2$. Esta es otra perspectiva del tercer ejemplo en 1.7.6.

3. $\mathbb{R}/\mathbb{Z} \simeq \{z \in \mathbb{C}^* \,|\, |z| = 1\}$ porque $\varphi : \mathbb{R} \longrightarrow \mathbb{C}^*$ definida por $\varphi(x) = \text{cis}(2\pi x)$ es un homomorfismo cuyo núcleo es $\mathbb{Z}$.

4. $\varphi : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ definida por $\varphi(A) = \det(A)$ es un epimorfismo con $\text{Ker}(\varphi) = SL(n, \mathbb{R})$. Entonces $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*$.

1.8.5 Segundo teorema de homomorfismos. Sea $\varphi : G \longrightarrow G'$ un epimorfismo y H' un subgrupo de G'.

1. $\varphi^{-1}(H')$ es un subgrupo de G y contiene a $\ker(\varphi)$.

2. $\varphi^{-1}(H')/\ker(\varphi) \simeq H'$.

3. Si $H' \triangleleft G'$, entonces $\varphi^{-1}(H') \triangleleft G$.

Demostración. Las demostraciones de 1 y 3 se dejan como ejercicio al lector. Para 2, considere la restricción de φ a $\varphi^{-1}(H')$ que resulta un epimorfismo sobre H y aplique el primer teorema del isomorfismo. □

1.8.6 Tercer teorema de homomorfismos. Si $\varphi : G \longrightarrow G'$ es un epimorfismo y $N' \triangleleft G'$, entonces

$$G/\varphi^{-1}(N') \simeq G'/N' \,.$$

Demostración. La función $\psi : G \longrightarrow G'/N'$ dada por $\psi(a) = N'\varphi(a)$ para todo $a \in G$ es un epimorfismo tal que $\ker(\psi) = \varphi^{-1}(N')$. □

1.8.7 Ejemplo. La función $\varphi : \mathbb{Z} \longrightarrow 4\mathbb{Z}$ dada por $\varphi(a) = 4a$ es un epimorfismo, $12\mathbb{Z} \triangleleft 4\mathbb{Z}$ y $\varphi^{-1}(12\mathbb{Z}) = 3\mathbb{Z}$, entonces $\mathbb{Z}/3\mathbb{Z} \simeq 4\mathbb{Z}/12\mathbb{Z}$. ¿Qué puede observar?

1.8.8. Ejercicios

1. Sea G un grupo. Verifique que $G/\{e\} \simeq G$ y $G/G \simeq \{e\}$.

2. Sea G el grupo de todas las funciones $f : [0,1] \longrightarrow \mathbb{R}$ con la suma de funciones y $N = \{f \in G \,|\, f(1/2) = 0\}$. Pruebe que $G/N \simeq \mathbb{R}$.

3. Considere el subgrupo $N = \{1, -1\}$ de $\mathbb{R}^*$. Muestre que $\mathbb{R}^*/N$ es isomorfo a $\mathbb{R}^+$.

4. Pruebe que $\mathbb{Z} \oplus \mathbb{Z} \,/\, n\mathbb{Z} \times m\mathbb{Z} \simeq \mathbb{Z}_n \oplus \mathbb{Z}_m$.

5. Sean G y G' grupos. Muestre que $N = \{(a, e') \,|\, a \in G\} \triangleleft G \times G'$, $N \simeq G$ y $G \times G' \,/\, N \simeq G'$.

6. Sea H un subgrupo de G y $N \triangleleft G$. Muestre que $H \cap N \triangleleft H$, $HN \leq G$, $N \triangleleft HN$ y $(HN)/N \simeq H/(H \cap N)$.

7. Pruebe que si N es un subgrupo normal de G y a tiene orden finito en G, entonces Na tiene orden finito en G/N y $|Na|$ divide a $|a|$.

8. Si $\varphi : G \longrightarrow G'$ es un homomorfismo entre grupos finitos, muestre que $|\varphi(G)|$ divide a $|G|$ y a $|G'|$.

9. Sea H un subgrupo de G, $N(H) = \{x \in G \,|\, x^{-1}Hx = H\}$ (el **normalizador** de H en G) y $C(H) = \{x \in G \,|\, x^{-1}hx = h \,\text{para todo}\, h \in H\}$ (el **centralizador** de H en G). Pruebe que $C(H) \triangleleft N(H)$ y que $N(H)/C(H)$ es isomorfo a un subgrupo de $\mathrm{Aut}(G)$.

Capítulo 2

Anillos

Es usual que una estructura algebraica tenga más de una operación. En este capítulo estudiamos los anillos, los cuales son conjuntos en los que hay definidas dos operaciones. Nuestro desarrollo se enfoca, primero, en realizar un estudio general análogo al hecho para grupos, y después, nos ocupamos del caso especial de anillos de polinomios que tienen propiedades especiales similares a las del dominio de los números enteros.

2.1. Definición y propiedades básicas

2.1.1 Definición. Un **anillo** es un conjunto no vacío R junto con dos operaciones binarias $+$ y $\cdot$ (adición y multiplicación), tales que

1. R es un grupo abeliano con la operación $+$.
2. $(ab)c = a(bc)$ para todo $a, b, c \in R$.
3. $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$ para todo $a, b, c \in R$.

2.1.2. Ejemplos

1. $\mathbb{Z}$ con la adición y multiplicación de enteros es un anillo. Similarmente, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos con las operaciones usuales.

2. $\mathbb{Z}_n$ es un anillo con la suma y producto módulo n, esto es, $[a+b] = [a] + [b]$ y $[a][b] = [ab]$.

3. $M_{n\times n}(\mathbb{R})$ es el anillo de matrices de $n \times n$ respecto a la suma y multiplicación de matrices.

4. $C[0,1] = \{f : [0,1] \to \mathbb{R} \mid f \text{ es continua}\}$ es un anillo con la suma y multiplicación de funciones.

5. Si R_1 y R_2 son anillos, entonces $R_1 \times R_2$ es un anillo con las operaciones $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$ y $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$.

A continuación introducimos una terminología que se utiliza frecuentemente.

Un **anillo conmutativo** es un anillo R en el que se cumple la propiedad conmutativa del producto, es decir $xy = yx$ para todo $x, y \in R$.

Cuando exista un elemento $1 \in R$ tal que $a1 = 1a = a$ para todo $a \in R$, diremos que R es un **anillo con unitario**.

Si R es un anillo con unitario y a es un elemento invertible, respecto a la multiplicación, se dice que a es una **unidad**.

Observe que si existe un elemento unitario, es único. También cada unidad tiene un único inverso multiplicativo.

2.1.3. Ejemplos

1. Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ y $C[0,1]$ son anillos conmutativos pero $M_{n\times n}(\mathbb{R})$ *no* es conmutativo.

2. El número 1 es el unitario de los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, $[1]$ es el unitario de $\mathbb{Z}_n$, la matriz identidad I_n es el unitario de $M_{n\times n}(\mathbb{R})$ y la función constante $f(x) = 1$ es el unitario de $C[0,1]$. Note que $2\mathbb{Z}$ es un anillo con la suma y producto de enteros que *no* tiene unitario.

3. Las unidades de $\mathbb{Z}$ son 1 y -1, todo elemento distinto de cero en $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es una unidad, las unidades de $M_{n\times n}(\mathbb{R})$ son las matrices no singulares, $f \in C[0,1]$ es una unidad si $f(x) \neq 0$ para todo $x \in [0,1]$ y $[2]$ *no* es unidad en $\mathbb{Z}_4$.

2.1.4 Teorema. Sea R un anillo y $a, b, c \in R$. Entonces:

1. $a0 = 0a = 0$.

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

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

4. $a(b-c) = ab - ac$ y $(a-b)c = ac - bc$.

Si además R tiene un elemento unitario 1, se tiene que:

5. $(-1)a = -a$.

6. $(-1)(-1) = 1$.

Demostración. Se prueban las tres primeras propiedades, se dejan como ejercicio el resto.

1. Como $a0 = a(0+0) = a0+a0$ y $a0 = a0+0$, entonces $a0+a0 = a0+0$ y $a0 = 0$. Similarmente se prueba $0a = 0$.

2. Note que $-(ab) + ab = 0$ y $(-a)b + ab = (-a + a)b = 0b = 0$. Por la unicidad del inverso aditivo se tiene que $-(ab) = (-a)b$. Análogamente $-(ab) = a(-b)$.

3. $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$. ¿Qué se ha utilizado en cada paso? □

2.1.5 Definición. Sea S un subconjunto no vacío de un anillo R. Diremos que S es un **subanillo** de R si S es un anillo con a las operaciones de R.

Directamente de la definición se tiene el siguiente criterio.

2.1.6 Proposición. Sea S un subconjunto no vacío de un anillo R. Entonces S es un subanillo de R si y sólo si $a - b \in S$ y $ab \in S$ para todo $a, b \in S$.

2.1.7. Ejemplos

1. $n\mathbb{Z}$ es un subanillo de $\mathbb{Z}$ para todo entero n.

2. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{R}$.

3. $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{C}$.

4. El conjunto S de las matrices diagonales de $n \times n$ es un subanillo de $M_{n\times n}(\mathbb{R})$.

5. El conjunto de todas las funciones constantes es un subanilllo de $C[0,1]$.

6. El conjunto de las matrices simétricas de $n \times n$ *no* es un subanillo de $M_{n\times n}(\mathbb{R})$ porque no es cerrado bajo la multiplicación.

2.1.8. Ejercicios

1. Determine cuáles de los siguientes conjuntos R son anillos con las operaciones indicadas. En caso afirmativo, diga si el anillo es conmutativo y si tiene unitario y unidades.

   · $2\mathbb{Z} \times \mathbb{Z}$ con la suma y multiplicación componente a componente.

   · $R = \{0, 2, 4, 6, 8\}$ con la suma y multiplicación módulo 10.

   · Sea A un anillo y S un conjunto no vacío. Considere el conjunto R de todas las funciones $f : S \longrightarrow A$ con las operaciones $(f, g) \mapsto f + g$ dada por $(f + g)(s) = f(s) + g(s)$ y $(f, g) \mapsto fg$ dada por $(fg)(s) = f(s)g(s)$.

   · $\mathbb{R}^3$ con la suma y producto cruz usuales.

   · R es el conjunto de complejos imaginarios puros con la suma y multiplicación de complejos.

   · Sea G un grupo abeliano. Considere $R = G$ con la suma de G y la mulptiplicación definida por $ab = 0$ para todo $a, b \in R$.

   · Sea G un grupo abeliano. Considere R el conjunto de todos los homomorfismos de G en G con la suma y composiciones de funciones.

   · R es el conjunto de todas las matrices 2×2 con entradas enteras junto con la suma y multiplicación de matrices.

   · Sea A un anillo conmutativo con unitario y R el conjunto de todas las unidades de A con las operaciones de A.

2. Sean a y b elementos de un anillo R y $m, n \in \mathbb{Z}$. Muestre que $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$, $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$ y $n \cdot (-a) = -(n \cdot a)$.

3. Pruebe que si un anillo es cíclico respecto a la adición, entonces es conmutativo.

4. De ejemplos de un anillo R para cada caso.

   a) $a, b \in R$ distintos de 0 tales que $ax = b$ tiene más de una solución.

   b) $a^2 - b^2 \neq (a - b)(a + b)$

   c) S es subgrupo de R con la adición pero no es subanillo.

   d) Un subanillo con unitario distinto del unitario del anillo.

5. Un elemento a en un anillo R es *nilpotente* si $a^n = 0$ para algún entero positivo n. Muestre que si a y b son elementos nilpotentes de un anillo conmutativo, entonces $a + b$ también es nilpotente.

6. Muestre que un anillo R no tiene elementos nilpotentes distintos de cero si y sólo si 0 es la única solución de $x^2 = 0$ en R.

7. Demuestre que si x es un elemento nilpotente de un anillo con unitario R, entonces $1 + x$ y $1 - x$ son nilpotentes.

8. Suponga que a y b son elementos de un anillo conmutativo con unitario R. Pruebe que si a es una unidad de R y $b^2 = 0$, entonces $a + b$ es una también una unidad.

9. Un anillo R es *booleano* si $x^2 = x$ para todo $x \in R$. Demuestre que todo anillo booleano es conmutativo.

10. Halle todos los subanillos de $\mathbb{Z}_{24}$.

11. Determine tres subanillos de $M_{n\times n}(\mathbb{R})$ y tres de $C([0,1])$.

12. Sea R un anillo. Pruebe:

    a) Si $a \in R$, entonces $S = \{x \in R \,|\, ax = 0\}$ es un subanillo de R.

    b) El conjunto $\{x \in R \,|\, ax = xa \,\text{para todo}\, a \in R\}$ es un subanillo de R llamado el *centro* de R.

    c) La intersección de subanillos de R es de nuevo un subanillo de R.

    d) Si R tiene unitario, entonces $S = \{n \cdot 1 \,|\, n \in \mathbb{Z}\}$ es un subanillo de R.

2.2. Dominios enteros y definición de campo

2.2.1 Definición. Si a y b son elementos distintos de cero de un anillo R y $ab = 0$, entonces a y b se denominan **divisores de cero**. Más exactamente a es un divisor *izquierdo* de cero y b es un divisor *derecho* de cero.

2.2.2. Ejemplos

1. En $\mathbb{Z}_{12}$ se tiene que $[2][6] = [0]$ y $[3][4] = [0]$, así que $[2]$, $[3]$, $[4]$ y $[6]$ son divisores de cero.

2. Las matrices
$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \qquad \text{y} \qquad \begin{bmatrix} 4 & -6 \\ -2 & 3 \end{bmatrix}$$
son divisores de cero (izquierdo y derecho, respectivamente) de $M_{2\times 2}(\mathbb{R})$.

3. Las funciones

$$f(x) = \begin{cases} 1-2x & 0 \le x \le 1/2 \\ 0 & 1/2 < x \le 1 \end{cases} \quad \text{y} \quad g(x) = \begin{cases} 0 & 0 \le x \le 1/2 \\ 2x-1 & 1/2 < x \le 1 \end{cases}$$

son divisores de cero en $C[0,1]$.

4. $\mathbb{Z}_n$ no tiene divisores de cero si y sólo si n es primo.

2.2.3 Definición. Un **dominio entero** D es un anillo conmutativo con unitario y sin divisores de cero.

2.2.4. Ejemplos

1. $\mathbb{Z}$, $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[i]$ son dominios enteros.

2. $\mathbb{Z}_n$ es un domino entero si y sólo si n es primo.

3. $M_{n\times n}(\mathbb{R})$, $C[0,1]$ y $\mathbb{Z}\times\mathbb{Z}$ *no* son dominios enteros.

2.2.5 Definición. Un **campo** F es un anillo conmutativo con unitario en el que todo elemento distinto de cero es una unidad.

2.2.6. Ejemplos

1. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son campos.

2. $\mathbb{Z}_p$ es campo si y sólo si p es primo. Recuerde que la congruencia lineal $ax \equiv 1 \pmod p$ con $a \neq 0$, siempre tiene solución cuando p es primo.

3. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es campo. Note que si $a + b\sqrt{2} \neq 0$, entonces $a - b\sqrt{2} \neq 0$ y $(a + b\sqrt{2})^{-1} = (a - b\sqrt{2})/(a^2 - 2b^2)$.

4. $\mathbb{Z}$ *no* es campo.

2.2.7 Definición. La **característica** de un anillo R es el menor entero positivo n tal que $nx = 0$ para todo $x \in R$. Si tal entero no existe se dice que R tiene característica 0.

2.2.8 Ejemplo. $\mathbb{Z}_n$ tiene característica n, mientras $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tienen característica 0.

2.2.9. Cuaterniones

Considere el conjunto

$$\mathcal{C} = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \mid z, w \in \mathbb{C} \right\}.$$

Entonces $\mathcal{C}$ es un anillo (es subanillo de $M_{2\times 2}(\mathbb{C})$) *no* conmutativo con unitario $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ y cada $\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ tiene inverso multiplicativo

$$\frac{1}{|z|^2 + |w|^2} \begin{bmatrix} \overline{z} & -w \\ \overline{w} & z \end{bmatrix}.$$

Al anillo $\mathcal{C}$ lo llamamos el anillo de los **cuaterniones**. Otra manera de representarlo es

$$\mathcal{C} = \left\{ \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

donde

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad , \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad , \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{y} \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Note que los cuaterniones *no* forman un campo, sin embargo tiene subconjuntos que son campos.

2.2.10. Ejercicios

1. Determine si $\mathbb{Z}[x]$, el conjunto de todos los polinomios con coeficientes enteros, es un dominio entero.

2. Sea D un dominio entero y $a, b, c \in D$. Muestre que si $a \neq 0$ y $ab = ac$, entonces $b = c$.

3. Pruebe que todo dominio entero finito es un campo.

4. Pruebe que todo campo es un dominio entero.

5. Suponga que R es un anillo con unitario 1. Pruebe que R tiene característica $n > 0$ si y sólo si n es el menor entero positivo tal que $n \cdot 1 = 0$.

6. Pruebe que la característica de un dominio entero es 0 o primo.

7. Sean x y y elementos de un anillo conmutativo de característica p con p primo. Muestre que $(x + y)^p = x^p + y^p$. De un ejemplo de un anillo de característica finita donde lo anterior no ocurra.

8. Muestre que $\mathbb{Z}_3[i] = \{a+bi \mid a, b \in \mathbb{Z}_3\}$ es un campo de nueve elementos.

9. Muestre que los únicos cuaterniones que conmutan con i son de la forma $a + bi$.

10. Considere el subconjunto de cuaterniones $G = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$.

a) Demuestre G es un grupo no abeliano con la multiplicación.

b) Halle $Z(G)$.

c) Encuentre todos los subgrupos de G y verifique que todos son normales.

11. Para cada cuaternión $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ defina $x^* = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. Pruebe

    a) $(x^*)^* = x$, $(x+y)^* = x^* + y^*$, $(xy)^* = y^*x^*$ y $xx^* = x^*x$ es real y no negativo.

    b) Si se define $|x| = \sqrt{xx^*}$, entonces $|xy| = |x||y|$.

12. Demuestre que hay una infinidad de cuaterniones que satisfacen $x^2 = -1$.

2.3. Ideales y anillo cociente

2.3.1 Definición. Sea I un subconjunto no vacío de un anillo R. Diremos que I es un **ideal** de R si

1. I es un subgrupo aditivo de R.
2. $Ir \subseteq I$ y $rI \subseteq I$ para todo $r \in R$.

2.3.2. Ejemplos

1. $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$ para todo entero n.
2. Si S es un subgrupo aditivo de $\mathbb{Z}_n$, entonces S es un ideal.

3. $\mathbb{Z} \times \{0\}$ es un ideal de $\mathbb{Z} \times \mathbb{Z}$.

4. $I = \{f \in C[0,1] \,|\, f(a) = 0\}$ es un ideal de $C[0,1]$ para cada $a \in [0,1]$.

5. Si R es un anillo conmutativo con unidad y $a \in R$, entonces $\langle a \rangle = \{ra \,|\, r \in R\}$ es un ideal de R llamado *ideal principal generado por* a.

6. $\mathbb{Q}$ no es un ideal de $\mathbb{R}$ porque $\sqrt{2}\mathbb{Q}$ *no* está contenido en $\mathbb{Q}$.

Sea I un ideal de un anillo R. Como I es subgrupo normal de R, entonces podemos formar el grupo cociente $R/I = \{a + I \,|\, a \in R\}$ con la operación $(a + I) + (b + I) = (a + b) + I$.

Adicionalmente, se verifica que la operación $(a + I)(b + I) = ab + I$ esté bien definida, sea asociativa y distribuya sobre la suma.

2.3.3 Definición. Si I es un ideal del anillo R, entonces el **anillo cociente** es

$$R/I = \{a + I \,|\, a \in R\}$$

con las operaciones $(a + I) + (b + I) = (a + b) + I$ y $(a + I)(b + I) = ab + I$.

2.3.4. Ejemplos

1. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ es un anillo cociente.

2. $I = \{[0], [3]\}$ es un ideal de $\mathbb{Z}_6$ y $\mathbb{Z}_6/I = \{I, [1] + I, [2] + I\}$ es un anillo que se puede *identificar* con $\mathbb{Z}_3$.

3. Si $I = \mathbb{Z} \times \{0\}$, entonces $\mathbb{Z}/I = \{(0, n) + I \,|\, n \in \mathbb{Z}\}$ el cual se identifica con $\mathbb{Z}$.

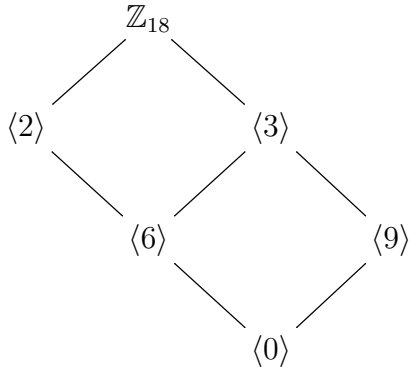
4. Si $I = \{f \in C[0,1] \mid f(1/2) = 0\}$, entonces $C[0,1]/I = \{r + I \mid r \in \mathbb{R}\}$ se identifica con $\mathbb{R}$.

2.3.5 Definición. Sea M un ideal propio de un anillo R. Diremos que M es un **ideal maximal** si para todo ideal B tal que $M \subseteq B \subseteq R$ se tiene que $M = B$ o bien $B = R$.

2.3.6. Ejemplos

1. $n\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ si y sólo si n es primo.

2. Del diagrama reticular se observa que $\langle 2\rangle$ y $\langle 3\rangle$ son ideales maximales de $\mathbb{Z}_{18}$.



2.3.7 Teorema. Sea R un anillo conmutativo con unitario y sea M un ideal de R. Entonces R/M es un campo si y sólo si M es un ideal maximal.

Demostración. Suponga que R/M es un campo y sea B un ideal de R tal que $M \subseteq B \subseteq R$. Si $M \subset B$ estrictamente, entonces se verifica que B contiene al unitario de R. En efecto, existe $b \in B - M$ y $b + M \neq M$, luego para $c + M = (b + M)^{-1}$ se tiene que $1 + M = (b + M)(c + M) = bc + M$ y por tanto $1 - bd \in M \subset B$ y $1 = (1 - bc) + bc \in B$. Así que $B = R$ y M es maximal.

Recíprocamente, sea M un ideal maximal de R. Si $a \in R - M$, entonces $a + M$ tiene inverso multiplicativo en R/M. Para ver esto, note que $B = \{ra + m \,|\, r \in R\,,\, m \in M\}$ es un ideal de R que contiene a M y por tanto $B = R$. Así que existen $r \in R$ y $m \in M$ tales que $1 + M = (ra + m) + M = ra + M = (r + M)(a + M)$. □

2.3.8 Ejemplo. $I = \{f \in C[0,1] \,|\, f(1/2) = 0\}$ es un ideal de maximal de $C[0,1]$ puesto que $C[0,1]/I$ se identifica con el campo $\mathbb{R}$.

2.3.9. Ejercicios

1. Muestre que en cualquier anillo R se tiene que $I = \{0\}$ e $I = R$ son ideales de R.

2. Sea R un anillo conmutativo con unitario. Pruebe que R es un campo si y sólo si los únicos ideales son $\{0\}$ y R.

3. Pruebe que si A y B son ideales de un anillo R, entonces $A \cap B$ y $A + B$ son ideales de R

4. Determine los ideales de $\mathbb{Z}_{24}$ y diga cuáles son maximales.

5. Sea R un anillo conmutativo con unitario y $a_1, a_2, \ldots, a_n \in R$. Muestre que $I = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \,|\, r_i \in R\}$ es un ideal de R llamado *ideal generado por* $a_1, a_2, \ldots, a_n$.

6. Describa el ideal $I = \langle x, 2 \rangle$ de $\mathbb{Z}[x]$.

7. Escriba las tablas para la adición y multiplicación del anillo $2\mathbb{Z}/6\mathbb{Z}$.

8. Muestre que $M = \{a + bi \in \mathbb{Z}[i] \,:\, 3|a \text{ y } 3|b\}$ es un ideal maximal de $\mathbb{Z}[i]$.

9. Muestre que $R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$ es un anillo y que el conjunto $I = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in \mathbb{R} \right\}$ es un ideal de R. Describa el anillo R/I.

10. Sea $R = M_{2\times 2}(\mathbb{Z})$ e I el subconjunto de R formado por todas las matrices con entradas pares. Muestre que I es un ideal de R y determine el número de elementos de R/I.

11. Sea N un ideal *propio* de un anillo conmutativo R. Diremos que N es un **ideal primo** de R si $ab \in N$ implica que $a \in N$ o $b \in N$ para todo $a, b \in R$.

    a) Muestre que $n\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ si y sólo si n es primo.

    b) Sea R un anillo conmutativo con unitario y N un ideal de R. Demuestre que R/N es un dominio entero si y sólo si N es un ideal primo.

    c) Pruebe que todo ideal maximal en un anillo conmutativo con unitario, es un ideal primo.

    d) Verifique que $\langle x \rangle$ es un ideal primo de $\mathbb{Z}[x]$ pero no es maximal.

2.4. Homomorfismos de anillos

2.4.1 Definición. Sean R y R' anillos. Una función $\varphi : R \to R'$ es un **homomorfismo** de anillos si para todo $a, b \in R$ se cumple

$$\varphi(a + b) = \varphi(a) + \varphi(b) \qquad \text{y} \qquad \varphi(ab) = \varphi(a)\varphi(b)\,.$$

Un homomorfismo biyectivo es un **isomorfismo** de anillos.

2.4.2. Ejemplos

1. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ definida por $\varphi(a) = [a]$ es un *epimorfismo* (homomorfismo sobreyectivo) de anillos.

2. Generalizando el ejemplo anterior, si I es un ideal de R, entonces la función $\pi : R \to R/I$ definida por $\pi(a) = a + I$ es un epimorfismo de anillos llamado epimorfismo *canónico* o *natural*.

3. $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_{10}$ definida por $\varphi([a]) = [5a]$ es un homomorfismo de anillos.

4. $\varphi : C[0,1] \to \mathbb{R}$ dada por $\varphi(f) = f(1/2)$ es un epimorfismo de anillos.

5. $\varphi : \mathbb{C} \to \mathbb{C}$ definida por $\varphi(z) = \overline{z}$ es un isomorfismo de anillos.

6. Si R y R' son anillos, entonces las *proyecciones* $\varphi_1 : R \times R' \to R$ dada por $\varphi(a, a') = a$, y $\varphi_2 : R \times R' \to R'$ definida por $\varphi(a, a') = a'$, son epimorfismos de anillos.

7. La función $\varphi : \mathbb{Z} \to 2\mathbb{Z}$, $\varphi(n) = 2n$, es un isomorfismo de grupos pero *no* es homomorfismo de anillos porque no preserva el producto.

A continuación, se enuncian algunas propiedades de los homomorfismos de anillos que el lector puede comprobar fácilmente de manera análoga al caso de grupos.

2.4.3 Proposición. Sea $\varphi : R \longrightarrow R'$ un homomorfismo de anillos.

1. $\mathrm{Ker}(\varphi) = \{a \in R \,|\, \varphi(a) = 0'\}$ es un ideal de R.

2. $\varphi(R) = \{\varphi(a) \,|\, a \in R\}$ es un subanillo de R'.

3. Si R es conmutativo, entonces $\varphi(R)$ es conmutativo.

4. Si R tiene unitario 1, $R' \neq \{0'\}$ y φ es sobreyectiva, entonces $\varphi(1)$ es el unitario de R'.

5. Si B es un ideal en R', entonces $\varphi^{-1}(B) = \{a \in R \,|\, \varphi(a) \in B\}$ es un ideal en R.

Note que por la propiedad 4, resulta que $\mathbb{Z}$ y $2\mathbb{Z}$ *no* son anillos isomorfos.

2.4.4 Primer teorema de homomorfismos para anillos. Si la función $\varphi : R \longrightarrow R'$ es un homomorfismo de anillos, entonces

$$R/\ker(\varphi) \simeq \varphi(R)\,.$$

Demostración. La función $\psi : R/\ker(\varphi) \longrightarrow \varphi(R)$ definida por

$$\psi(a + \ker(\varphi)) = \phi(a)$$

es un isomorfismo de anillos. □

2.4.5 Corolario. Si $\varphi : R \longrightarrow R'$ es un epimorfismo de anillos, entonces $R/\ker(\varphi) \simeq R'$.

2.4.6. Ejemplos

1. Desde este punto de vista, si consideramos el epimorfismo canónico $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\pi(a) = [a]$, se tiene que $\ker(\pi) = n\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. De hecho esta isomorfía es una igualdad.

2. Con el epimorfismo $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\varphi(m, n) = n$, resulta $\ker(\varphi) = \mathbb{Z} \times \{0\}$ y $\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \{0\} \simeq \mathbb{Z}$. Esta es la identificación de la que se habló en el tercer ejemplo de 2.3.4.

3. Dado el epimorfismo de anillos $\varphi : C[0,1] \longrightarrow \mathbb{R}$, $\varphi(f) = f(1/2)$, se tiene que $\ker(\varphi) = \{f \in C[0,1] \,|\, f(1/2) = 0\}$ y $C[0,1]/\ker(\varphi) \simeq \mathbb{R}$.

2.4.7. Campo de cocientes de un dominio entero

Sea D un dominio entero y $S = \{(a, b) \,|\, a, b \in D \,\text{y}\, b \neq 0\}$. Se define en S la relación $\sim$ dada por $(a, b) \sim (c, d)$ si y sólo si $ad = bc$, la cual es una relación de equivalencia. Denotamos por $[a, b]$ la clase de equivalencia de (a, b) y definimos $F = \{[a, b] \,|\, (a, b) \in S\}$ junto con las operaciones

$$[a, b] + [c, d] = [ad + bc, bd] \qquad \text{y} \qquad [a, b][c, d] = [ac, bd]\,.$$

Es ejercicio verificar que estas operaciones estén bien definidas y que F resulta ser un campo llamado *campo de cocientes del dominio entero* D. Por último, la función $\varphi : D \longrightarrow F$ definida por $\varphi(a) = [a, 1]$ es un homomorfismo inyectivo y en consecuencia F contiene a $\varphi(D)$ que es una copia isomorfa de D. Se suele utilizar la notación $[a, b] = a/b$ para los elementos de F.

2.4.8 Ejemplo. $\mathbb{Q}$ es el campo de cocientes de $\mathbb{Z}$.

2.4.9. Ejercicios

1. Sea $\varphi : R \to R'$ un homomorfismo de anillos. Muestre que:

   a) Si $r \in R$ y $n \in \mathbb{Z}^+$, entonces $\varphi(n \cdot r) = n \cdot \varphi(r)$ y $\varphi(r^n) = (\varphi(r))^n$.

   b) Si A es un ideal de R y φ es sobre, entonces $\varphi(A)$ es un ideal de R'.

c) φ es uno a uno si y sólo si $\text{Ker}(\varphi) = \{0\}$.

d) φ es un isomorfismo si y sólo si φ^{-1} es un isomorfismo.

2. Muestre que los anillos $2\mathbb{Z}$ y $3\mathbb{Z}$ no son isomorfos y que los campos $\mathbb{R}$ y $\mathbb{C}$ no son isomorfos.

3. Pruebe que si $\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ es un homomorfismo, entonces $\varphi(x) = ax$ para todo $x \in \mathbb{Z}_n$ donde a cumple $a^2 = a$.

4. Determine todos los homomorfismos de $\mathbb{Z}$ en sí mismo.

5. Sea R un anillo con unitario 1. Muestre que la función $\varphi : \mathbb{Z} \longrightarrow R$ definida por $\varphi(n) = n \cdot 1$ es un homomorfimo.

6. Sea R un anillo con unitario. Pruebe que si la característica de R es 0, entonces R tiene un subanillo isomormorfo a $\mathbb{Z}$ y si la característica es $n > 0$, entonces R tiene un subanillo isomormorfo a $\mathbb{Z}_n$.

7. Sea F un campo. Pruebe que si la característica de F es 0, entonces F tiene un subcampo isomormorfo a $\mathbb{Q}$ y si la característica es p, entonces F tiene un subcampo isomormorfo a $\mathbb{Z}_p$.

8. Use un isomorfismo de anillos para probar que $R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$ con las operaciones usuales es un campo.

9. Enuncie y demuestre el segundo y tercer teoremas de homomorfismos para anillos.

10. Sea A un subanillo de R e I un ideal de R. Pruebe que

a) $A + I$ es un subanillo de R que contiene a I.

b) $(A + I)/I \simeq A/(A \cap I)$.

11. Verifique todos los detalles en la construcción del campo de cocientes de un dominio entero.

2.5. Anillos de polinomios

Formalmente un **polinomio** con coeficentes en un anillo R es una sucesión infinita

$$a_0,\, a_1,\, a_2,\, \ldots$$

de elementos de R con $a_i = 0$ excepto un número finito de valores de i.

Dos polinomios

$$a_0,\, a_1,\, a_2,\, \ldots \qquad \text{y} \qquad b_0,\, b_1,\, b_2,\, \ldots$$

son iguales si $a_i = b_i$ para todo i.

Se suele escribir

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

si $a_n \neq 0$ y $a_i = 0$ para todo $i > n$.

El símbolo x se denomina **indeterminada** y *no* representa una variable o elemento desconocido de R.

Los a_i son los **coeficientes** del polinomio, a_n es el coeficiente **principal** y n es el **grado** del polinomio.

Note que $p(x) = 0$ no tiene grado y los polinomios de grado cero son los polinomios *constantes* de la forma $p(x) = a_0$ con $a_0 \neq 0$.

2.5.1 Ejemplo. Considere los polinomios $p(x) = x^3 + x$ y $q(x) = 2x$ con coeficientes en $\mathbb{Z}_3$. Por simplicidad denotamos por i a $[i]$. El polinomio $p(x)$ tiene grado 3 y el coeficiente principal de $q(x)$ es 2. No se debe confundir un polinomio con una función, por ejemplo $p(x)$ y $q(x)$ son distintos porque corresponden a las sucesiones $0, 1, 0, 1, 0, 0, \ldots$ y $0, 2, 0, 0, \ldots$, sin embargo las funciones $x \mapsto x^3 + x$ y $x \mapsto 2x$ de $\mathbb{Z}_3$ en sí mismo son iguales.

Sea $R[x]$ el conjunto de polinomios en una indeterminada x y con coeficientes en un anillo R. Para dos elementos de $R[x]$,

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{y} \quad q(x) = b_m x^m + \cdots + b_1 x + b_0$$

se define de la forma usual, la suma

$$p(x) + q(x) = c_s x^s + \cdots + c_1 x + c_0$$

donde $c_i = a_i + b_i$, aquí $a_i = 0$ si $i > n$ y $b_i = 0$ si $i > m$.

El producto es

$$p(x)q(x) = c_t x^t + \cdots + c_1 x + c_0$$

donde $c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$ para $0 \leq k \leq m + n$.

Con estas operaciones se construye un nuevo e importante ejemplo de anillo.

2.5.2 Teorema. El conjunto $R[x]$ de todos los polinomios en una indeterminada x y con valores en un anillo R es un anillo con la suma y multiplicación de polinomios.

2.5.3 Ejemplo. Dados $p(x) = 2x^3+x^2+2x+2, q(x) = 2x^2+2x+1 \in \mathbb{Z}_3[x]$, se tiene $p(x) + q(x) = 2x^3 + x$ y $p(x)q(x) = x^5 + 2x^3 + 2$.

2.5.4 Observación. Si R es un anillo conmutativo, entonces $R[x]$ es conmutativo, si R tiene unitario 1, entonces $p(x) = 1$ es el unitaro de $R[x]$ y si D es un dominio entero, entonces $D[x]$ es un dominio entero.

2.5.5. Ejercicios

1. Escriba dos polinomios de grado 7 y grado 6 en $\mathbb{Z}_5[x]$, cada uno con almenos cuatro coeficientes distintos, y halle su suma y su producto.

2. Muestre que $2x + 1 \in \mathbb{Z}_4[x]$ tiene un inverso multiplicativo en $\mathbb{Z}_4[x]$.

3. Muestre que los polinomios x^4+x y x^2+x determinan la misma función de $\mathbb{Z}_3$ en $\mathbb{Z}_3$.

4. Verifique que si D es un dominio entero, entonces para $f(x), g(x) \in D[x]$ se tiene que $\operatorname{grd}(f(x)g(x)) = \operatorname{grd} f(x) + \operatorname{grd} g(x)$. Muestre que para un anillo R puede ocurrir $\operatorname{grd}(p(x)q(x)) < \operatorname{grd} p(x) + \operatorname{grd} q(x)$ para algunos elementos no cero de $R[x]$.

5. Sea R un anillo conmutativo. Pruebe que la característica de $R[x]$ es la misma que la de R.

6. Sea $\varphi : R \longrightarrow R'$ un homomorfismo de anillos. Muestre que la función ψ de $R[x]$ en $R'[x]$ definida por $\psi(a_nx^n + \cdots + a_1x + a_0) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0)$ es un homomorfismo de anillos.

7. Muestre que si R y R' son anillos isomorfos, entonces $R[x]$ y $R'[x]$ son isomorfos.

8. Sea F un subcampo de un campo E y $\alpha \in E$. Demuestre que la transformación $\varphi_\alpha : F[x] \longrightarrow E$ definida por $\varphi_\alpha(a_n x^n + + \cdots + a_1 x + a_0) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$ es un homomorfismo de anillos (φ_α es el *homomorfismo de evaluación en* α).

9. Sea F campo y $\mathcal{D} : F[x] \longrightarrow F[x]$ la transformación de *diferenciación formal* de polinomios definida por $\mathcal{D}(a_n x^n + + \cdots + a_1 x + a_0) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$. Demuestre que $\mathcal{D}$ es un automorfismo de *grupos* (explique por qué no es de anillos) y encuentre el núcleo y la imagen.

10. Sea F un campo. Muestre que todos los polinomios con término constante $a_0 = 0$ es un ideal *principal* de $F[x]$.

2.6. Algoritmo de la división

El siguiente teorema es el análogo para polinomios del algoritmo de la división de enteros.

2.6.1 Algoritmo de la división. Sea F un campo. Si $a(x), b(x) \in F[x]$ con $b(x) \neq 0$, entonces existen polinomios únicos $q(x)$ y $r(x)$ en $F[x]$ tales que

$$a(x) = q(x)b(x) + r(x)$$

donde $r(x) = 0$ o $\operatorname{grd} r(x) < \operatorname{grd} b(x)$.

Demostración. Para la prueba se utiliza inducción fuerte sobre el grado de $a(x)$. Si $a(x) = 0$ o $\operatorname{grd} a(x) < \operatorname{grd} b(x)$, entonces se toma $q(x) = 0$ y $r(x) = a(x)$. Luego podemos considerar que $\operatorname{grd} a(x) \geq \operatorname{grd} b(x)$. Haciendo

$a(x) = a_n x^n + \cdots + a_0$ y $b(x) = b_m x^m + \cdots + b_0$, note que $a_n b_m^{-1} x^{n-m} b(x)$ y $a(x)$ tienen el mismo grado y el mismo coeficiente principal y por tanto $f(x) = a(x) - a_n b_m^{-1} x^{n-m} b(x)$ es cero o tiene grado menor que $\operatorname{grd} a(x)$. En el primer caso hemos acabado, y en el segundo caso, por la hipótesis inductiva, existen $q_1(x), r_1(x) \in F[x]$ tales que $f(x) = q_1(x)g(x) + r_1(x)$ con $r_1(x) = 0$ o $\operatorname{grd} r_1(x) < \operatorname{grd} b(x)$. Entonces $a(x) = a_n b_m^{-1} x^{n-m} b(x) + f(x) = q(x)b(x) + r(x)$ donde $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ y $r(x) = r_1(x)$ cumplen las condiciones.
Para mostrar la unicidad suponga que $a(x) = q(x)b(x) + r(x) = q^*(x)g(x) + r^*(x)$ donde $r(x) = 0$ o $\operatorname{grd} r(x) < \operatorname{grd} b(x)$ y también $r^*(x) = 0$ o $\operatorname{grd} r^*(x) < \operatorname{grd} b(x)$. Entonces $r^*(x) - r(x) = [q(x) - q^*(x)]b(x)$ y como $\operatorname{grd} r^*(x) - r(x) = \operatorname{grd} [q(x) - q^*(x)]b(x) \geq \operatorname{grd} b(x)$ no puede ser, entonces $r^*(x) - r(x) = 0$ y $q(x) - q^*(x) = 0$. □

El polinomio $f(x) \in F[x]$ es **mónico** si su coeficiente principal es 1.

Sean $f(x), g(x) \in F[x]$ con $g(x) \neq 0$. Diremos que $g(x)$ **divide a** $f(x)$ si existe $a(x) \in F[x]$ tal que $f(x) = a(x)g(x)$. En tal caso se denota $g(x)|f(x)$,

Un elemento $a \in F$ es un **cero** de $p(x) \in F[x]$ si $p(a) = 0$, aquí $p(a)$ es el elemento de F que resulta de sustituir a en la expresión de $p(x)$.

Un cero a de $p(x)$ es un cero de **multiplicidad** k si $(x - a)^k$ divide a $p(x)$ pero $(x - a)^{k+1}$ no lo divide.

2.6.2 Teorema del residuo. Si $a \in F$ y $p(x) \in F[x]$, entonces $p(a)$ es el residuo de dividir $p(x)$ por $x - a$.

Demostración. Existen $q(x), r(x) \in F[x]$ tales que $p(x) = q(x)(x-a) + r(x)$ donde $r(x) = 0$ o $\operatorname{grd} r(x) < \operatorname{grd} x - a = 1$. Entonces $r(x)$ es constante y $p(a) = r(a)$. □

2.6.3 Teorema del factor. Sea $a \in F$ y $p(x) \in F[x]$. Entonces a es cero de $p(x)$ si y sólo si $x - a$ es factor de $p(x)$.

Demostración. a es cero de $p(x)$ si y sólo si 0 es el residuo de dividir $p(x)$ entre $x - a$. □

2.6.4 Proposición. Un polinomio $p(x) \in F[x]$ de grado n tiene a lo más n ceros contando multiplicidad.

Demostración. Se utiliza inducción fuerte sobre n. Un polinomio de grado uno tiene exactamente un cero. Sea $p(x) \in F[x]$ de grado n y $a \in F$ un cero de $p(x)$ de multiplicidad k. Entonces $p(x) = (x-a)^k q(x)$ y $n = \text{grd}p(x) = k + \text{grd}q(x)$ y por tanto $k \leq n$. Si $p(x)$ no tiene otros ceros distintos de a, hemos terminado. Si $b \neq a$ es cero de $p(x)$, entonces $0 = p(b) = (b-a)^k q(b)$ implica $q(b) = 0$ y por la hipótesis de inducción $q(x)$ tiene a lo más $n - k$ ceros contando multiplicidades. Luego $p(x)$ tiene a los más $k + (n - k) = n$ ceros contando multiplicidades. □

2.6.5 Ejemplo. Considere $x^n - 1 \in \mathbb{C}[x]$. Por el teorema de Moivre se tiene que $\omega = \text{cis}(2\pi/n)$ satisface $\omega^n = 1$ y $\omega^k \neq 1$ si $1 \leq k < n$. Entonces $1, \omega, \omega^2, \ldots, \omega^{n-1}$ son ceros diferentes de $x^n - 1$ y no hay otros. El complejo ω se denomina *raíz n-ésima primitiva de la unidad*.

2.6.6 Definición. Un dominio entero D es un **dominio de ideales principales** si todo ideal de D es principal, es decir, de la forma

$$\langle a \rangle = \{xa \,|\, x \in D\}$$

para algún $a \in D$.

2.6.7 Ejemplo. $\mathbb{Z}$ es un dominio de ideales principales porque sus ideales son de la forma $n\mathbb{Z}$ con $n \in \mathbb{Z}$.

2.6.8 Teorema. Si F es un campo, entonces $F[x]$ es un dominio de ideales principales.

Demostración. Sabemos que $F[x]$ es un dominio entero. Si $I = \{0\}$, entonces $I = \langle 0 \rangle$ es principal. Si $I \neq \{0\}$ escogemos un elemento $g(x) \neq 0$ en I de grado mínimo y mostremos que $I = \langle g(x) \rangle$. Sea $f(x) \in I$. Existen $q(x)$ y $r(x)$ tales que $f(x) = q(x)g(x) + r(x)$ con $r(x) = 0$ o $\operatorname{grd} r(x) < \operatorname{grd} g(x)$. Pero $\operatorname{grd} r(x) < \operatorname{grd} g(x)$ no puede ocurrir pues $r(x) = f(x) - q(x)g(x) \in I$ y $g(x)$ es de grado mínimo. Así que $r(x) = 0$ y $f(x) \in \langle g(x) \rangle$. □

2.6.9 Observación. Si I es un ideal no trivial de $F[x]$, entonces $I = \langle g(x) \rangle$ donde $g(x)$ es un polinomio no nulo de grado mínimo en I. Tal polinomio no es único porque si $a \in F$ y $a \neq 0$, entonces $ag(x)$ tiene el mismo grado que $g(x)$ y genera el mismo ideal.

2.6.10. Ejercicios

1. Encuentre todos los ceros de $x^2 + 3x + 2 \in \mathbb{Z}_6[x]$.
2. Encuentre el cociente y el residuo de dividir $5x^4 + 3x^3 + 1$ entre $3x^2 + 2x + 1$ en $\mathbb{Z}_7[x]$
3. Pruebe que $\langle x \rangle$ es un ideal maximal de $\mathbb{Q}[x]$.
4. Muestre que $\mathbb{Z}[x]$ no es un dominio de ideales principales.
5. Sea F un campo. Muestre que $x - 1$ es factor de $f(x) = a_n x^n + \cdots + a_1 x + a_0$ si y sólo si $a_n + \cdots + a_1 + a_0 = 0$.

6. Encuentre infinitos polinomios $f(x)$ en $\mathbb{Z}_3[x]$ tales que $f(a) = 0$ para todo $a \in \mathbb{Z}_3$.

7. Sea $f(x) \in \mathbb{R}[x]$ y a un real tal que $f(a) = 0$ y $f'(a) \neq 0$ ($f'(x)$ es la derivada de $f(x)$). Muestre que a es cero de $f(x)$ de multiplicidad 1.

8. Muestre que si $f(x), g(x) \in F[x]$ y $g(x)|f(x)$, entonces $\langle f(x)\rangle \subseteq \langle g(x)\rangle$.

9. Exprese el polinomio $x^4 + 4 \in \mathbb{Z}_5[x]$ como producto de factores lineales.

10. Calcule los ceros de $x^6 - 1$ en $\mathbb{C}[x]$ y ubíquelos en el plano complejo.

2.7. Polinomios irreducibles

2.7.1 Definición. Sean $f(x), g(x) \in F[x]$, no ambos iguales a cero. Diremos que un polinomio *mónico* $d(x) \in F[x]$ es el **máximo común divisor** de $f(x)$ y $g(x)$ si

1. $d(x)|f(x)$ y $d(x)|g(x)$.

2. $h(x)|f(x)$ y $h(x)|g(x)$ implica $h(x)|d(x)$

Note que si $p(x)|q(x)$ en $F[x]$, entonces $ap(x)|q(x)$ para todo $a \in F$ con $a \neq 0$. Por ello se exige en la definición anterior que el polinomio sea mónico. El siguiente teorema nos dice la forma de dicho polinomio.

2.7.2 Teorema. Si $f(x), g(x) \in F[x]$ con $g(x) \neq 0$, entonces su máximo común divisor $d(x)$ existe y además

$$d(x) = a(x)f(x) + b(x)g(x)$$

para ciertos $a(x), b(x) \in F[x]$.

Demostración. El conjunto $I = \{s(x)f(x) + t(x)g(x) : s(x), t(x) \in F[x]\}$ es un ideal no trivial. Entonces existe un único polinomio mónico $d(x)$ que genera a I. Luego $d(x)|f(x)$, $d(x)|g(x)$ y $d(x) = a(x)f(x) + b(x)g(x)$ para ciertos $a(x), b(x) \in F[x]$. Adicionalmente, si $h(x)$ divide a $f(x)$ y a $g(x)$, entonces divide a $a(x)f(x) + b(x)g(x) = d(x)$. □

2.7.3 Ejemplo. $x + 1 \in \mathbb{Q}[x]$ es el mcd de $2x^3 + 2x^2 - 3x - 3$ y $x^2 + 1$, además $x - 1 = (-1)(2x^3 + 2x^2 - 3x - 3) + (2x + 2)(x^2 + 1)$.

2.7.4 Definición. $f(x), g(x) \in F[x]$ son **primos relativos** si su máximo común divisor es 1.

2.7.5 Ejemplo. $x^2 - 1$ y $x + 2$ son primos relativos en $\mathbb{Q}[x]$ y $1 = -\frac{1}{3}(x^2 - 1) + (\frac{1}{3}x - \frac{2}{3})(x + 2)$.

2.7.6 Proposición. Si $q(x)$ y $f(x)$ son primos relativos y $q(x)|f(x)g(x)$, entonces $q(x)|g(x)$.

Demostración. Existen $a(x), b(x) \in F[x]$ tales que $a(x)q(x)+b(x)f(x) = 1$ de donde $a(x)q(x)g(x)+b(x)f(x)g(x) = g(x)$. Como $q(x)$ divide a $a(x)q(x)g(x)$ y a $f(x)g(x)$, entonces divide a $g(x)$. □

2.7.7 Definición. Un polinomio $p(x) \in F[x]$ de grado *positivo* es **irreducible** en $F[x]$ si para cualquier $f(x) \in F[x]$ se tiene que $p(x)|f(x)$ o $p(x)$ es primo relativo con $f(x)$.

Observe que si $p(x)$ es irreducible en $F[x]$ y $p(x) = a(x)b(x)$, entonces $a(x)$ o $b(x)$ es constante, es decir, $p(x)$ no se puede factorizar de manera no trivial.

2.7.8 Ejemplo. $x^2 - 2$ es irreducible en $\mathbb{Q}[x]$ pero es *reducible* en $\mathbb{R}[x]$.

2.7.9 Teorema. Sea $p(x) \in F[x]$ y $\langle p(x)\rangle = \{f(x)p(x) \,|\, f(x) \in F[x]\}$ el ideal generado por $p(x)$. Entonces $\langle p(x)\rangle$ es un ideal maximal de $F[x]$ si y sólo si $p(x)$ es irreducible.

Demostración. Supongamos que $\langle p(x)\rangle$ es un ideal maximal de $F[x]$ y que $p(x)$ no es irreducible. Entonces $p(x) = a(x)b(x)$ donde $\operatorname{grd} a(x)$ y $\operatorname{grd} b(x)$ son ≥ 1. Puesto que todo ideal maximal es un *ideal primo* (ejercicio 11 de la sección 2.4), se tiene que $a(x) \in \langle p(x)\rangle$ o $b(x) \in \langle p(x)\rangle$. Esto es una contradicción porque $p(x)$ es de grado mínimo en $\langle p(x)\rangle$.
De otra parte, sea $p(x)$ irreducible en $F[x]$ y $\langle p(x)\rangle \subseteq \langle f(x)\rangle \subseteq F[x]$. Entonces $p(x) = a(x)f(x)$ para algún $a(x) \in F[x]$ y por irreducibilidad se tiene que $a(x)$ o $f(x)$ es una constante distinta de cero. En el primer caso $\langle p(x)\rangle = \langle f(x)\rangle$ y en el segundo caso $\langle f(x)\rangle = F[x]$. □

2.7.10 Observación. Si $p(x)$ es irreducible en $F[x]$, entonces $F[x]/\langle p(x)\rangle$ es un campo.

2.7.11. Ejemplos

1. El polinomio x^2+1 es irreducible en $\mathbb{Z}_3[x]$ porque es de grado dos y no tiene ceros en $\mathbb{Z}_3$ (ver ejercicio 3). Así que $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ es un campo. Ahora si $f(x) \in \mathbb{Z}_3[x]$, existen $q(x)$ y $r(x)$ tales que $f(x) = q(x)(x^2+1) + r(x)$ donde $r(x) = 0$ o $\operatorname{grd} r(x) < 2$. Como $f(x) + \langle x^2+1\rangle = r(x) + \langle x^2+1\rangle$ entonces $\mathbb{Z}_3[x]/\langle x^2+1\rangle = \{ax+b+\langle x^2+1\rangle \;|a,b \in \mathbb{Z}_3\}$ es un campo de nueve elementos.

2. $x^2+1 \in \mathbb{R}[x]$ es irreducible y $\mathbb{R}[x]/\langle x^2+1\rangle = \{ax+b+\langle x^2+1\rangle \;|a,b \in \mathbb{R}\}$ es un campo isomorfo a $\mathbb{C}$. Este ejemplo muestra otra forma de construir los números complejos.

El siguiente resultado es el análogo para polinomios del teorema fundamental de la Aritmética. La demostración puede ser consultada en [2].

2.7.12 Teorema de factorización única. Sea $f(x) \in F[x]$ de grado positivo. Entonces $f(x)$ es irreducible en $F[x]$ o bien es el producto de polinomios irreducibles. La escritura es única excepto el orden de los factores y factores que sean unidades.

2.7.13 Ejemplo. En $\mathbb{Z}_5[x]$ se tiene que $x^2 + 4 = (x + 4)(x + 1) = (2x + 3)(3x + 3)$, pero $3(2x + 3) = x + 4$ y 3 es una unidad de $\mathbb{Z}_5$.

Existen varios test de irreducibilidad para polinomios con coeficientes racionales, a continuación enunciamos e ilustramos uno de ellos.

2.7.14 Criterio de Eisenstein. Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Si existe un primo p tal que $p \not| a_n$, $p|a_{n-1}$, $\ldots$, $p|a_1$, $p|a_0$ y $p^2 \not| a_0$, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

2.7.15 Ejemplo. Si p es primo, entonces $x^n - p$ es irreducible sobre $\mathbb{Q}$ ya que $p \not| 1$, $p| - p$ y $p^2 \not| p$.

2.7.16. Ejercicios

1. Pruebe que si $f(x), g(x) \in F[x]$ son distintos de cero tales que $f(x)|g(x)$ y $g(x)|f(x)$, entonces $f(x) = ag(x)$ para algún $a \in F$

2. Muestre que si $p(x)$ es irreducible en $F[x]$ y $p(x)|a_1(x)a_2(x)\cdots a_k(x)$ donde $a_1(x)$, $a_2(x)$, $\ldots$, $a_k(x) \in F[x]$, entonces $p(x)|a_i(x)$ para algún i.

3. Sea $f(x) \in F[x]$ de grado 2 o 3. Pruebe que $f(x)$ es reducible en $F[x]$ si y sólo si $f(x)$ tiene un cero en F.

4. Encuentre todos los polinomios irreducibles de grado 2 o 3 en $\mathbb{Z}_2[x]$ y $\mathbb{Z}_3[x]$.

5. Escriba el polinomio $x^3 + 6$ de $\mathbb{Z}_7[x]$ como producto de factores irreducibles en $\mathbb{Z}_7$.

6. Un polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ es un polinomio **primitivo** si el mcd de sus coeficientes es 1. Pruebe:

   a) El producto de dos polinomios primitivos es primitivo.

   b) Si $f(x) \in \mathbb{Z}[x]$ es reducible sobre $\mathbb{Q}$, entonces es reducible sobre $\mathbb{Z}$.

7. Sea p primo. Muestre que el número de polinomios irreducibles sobre $\mathbb{Z}_p$ de la forma $x^2 + ax + b$ es $p(p+1)/2$.

8. Sea $f(x) \in \mathbb{Z}[x]$ de grado positivo y p un primo. Denote por $\overline{f}(x)$ el polinomio en $\mathbb{Z}_p[x]$ que se obtiene de $f(x)$ tomando los coeficientes módulo p. Demuestre que si $\overline{f}(x)$ es irreducible sobre $\mathbb{Z}_p$ y $grd\,\overline{f}(x) = grd\,f(x)$, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

9. Sea $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $a_0 \neq 0$. Demuestre que si $f(x)$ tiene un cero en $\mathbb{Q}$, entonces tiene un cero m en $\mathbb{Z}$ y m divide a a_0.

10. Sea $f(x)$ in $F[x]$ y a un elemento de F distinto de cero. Pruebe que si $af(x)$, $f(ax)$ o $f(x + a)$ es irreducible sobre F, entonces $f(x)$ es irreducible sobre F.

11. Pruebe que si p es primo, entonces el polinomio $x^{p-1} + x^{p-2} + \cdots + x + 1$ es irreducible sobre $\mathbb{Q}$.

12. Sea p primo y suponga que $f(x) \in \mathbb{Z}_p[x]$ es irreducible sobre $\mathbb{Z}_p$ de grado n. Muestre que $\mathbb{Z}_p[x]/\langle f(x)\rangle$ es un campo de p^n elementos.

13. Construya un campo con 25 elementos y un campo con 27 elementos.

14. Sea F un campo y φ un automorfismo de $F[x]$ tal que $\varphi(a) = a$ para todo $a \in F$. Si $f(x) \in F[x]$, pruebe que $f(x)$ es irreducible en $F[x]$ si y sólo si $\varphi(f(x))$ es irreducible en $F[x]$.

15. Determine tres automorfismos φ de $\mathbb{Q}[x]$ tales que $\varphi(a) = a$ para todo $a \in \mathbb{Q}$.

Capítulo 3

Campos

Adicionalmente a los grupos y anillos, hay una tercera estructura clásica del Álgebra, el campo, el cual definimos anteriormente y usamos en la teoría de anillos de polinomios. Los campos juegan un papel primordial en la definición de espacio vectorial en Álgebra Lineal. En este capítulo orientamos un estudio más detallado de esta estructura hacia los campos de extensión.

3.1. Introducción

Recuerde que un campo F es un anillo conmutativo con unitario en el que todo elemento distinto de cero es una unidad. Hasta ahora hemos visto los siguientes ejemplos de campos:

1. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.
2. $\mathbb{Z}_p$ con p primo.
3. $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(i)$.

4. R/M es un campo si R es un anillo conmutativo con unitario y M es un ideal maximal de R. En particular $F[x]/\langle p(x)\rangle$ donde $p(x)$ es un polinomio irreducible sobre un campo F.

5. Campo de cocientes de un dominio entero.

3.2. Espacio vectorial sobre un campo

En esta sección repasamos algunas ideas fundamentales de espacios vectoriales usando las estructuras vistas aquí. En particular, lo referente a base y dimensión lo utilizaremos más adelante.

3.2.1 Definición. Un **espacio vectorial** V **sobre un campo** F es un grupo abeliano $(V,+)$ tal que para todo $a \in F$ y todo $\mathbf{v} \in V$ existe un elemento $a\mathbf{v} \in V$ y se satisface

1. $a(\mathbf{u}+\mathbf{v}) = a\mathbf{u} + a\mathbf{v}$

2. $(a+b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$

3. $a(b\mathbf{u}) = (ab)\mathbf{u}$

4. $1\mathbf{u} = \mathbf{u}$

para todo $a, b \in F$ y $\mathbf{u}, \mathbf{v} \in V$.

A los elementos de V se les llama *vectores* y a los de F se les denomina *escalares*. Observe que se cumplen propiedades generales como la unicidad del vector cero y $0\mathbf{v} = \mathbf{0}$.

3.2.2 Ejemplos. Si F es un campo, los siguientes conjuntos son espacios vectoriales sobre F.

1. $F^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in F\}$ con la suma componente a componente y multiplicación por escalar usual.

2. Más generalmente, el conjunto $M_{m\times n}(F)$ de matrices de $m \times n$ con entradas en F con las operaciones usuales de matrices. ¿Cuántos elementos tiene $M_{m\times n}(\mathbb{Z}_p)$?

3. $F[x]$ con la suma de polinomios y la multiplicación de un escalar por un polinomio.

4. Si F es un subcampo de un campo E, entonces E es un espacio vectorial sobre F. Por ejemplo, $\mathbb{C}$ es un espacio vectorial sobre $\mathbb{R}$.

5. Sea A un conjunto no vacío. El conjunto $\mathcal{F}(A, F)$ de todas las funciones $f : A \longrightarrow F$ con las operaciones usuales de funciones definidas por $(f + g)(x) = f(x) + g(x)$ y $(rf)(x) = rf(x)$. Como casos particulares importantes se tienen el conjunto suc($\mathbb{R}$) de sucesiones con valores en $\mathbb{R}$ y el conjunto $\mathcal{C}(I, \mathbb{R})$ de funciones continuas definidas en $I \subseteq \mathbb{R}$.

3.2.3 Definición. Sea V un espacio vectorial sobre un campo F y W un subconjunto no vacío de V. Se dice que W es un **subespacio** de V si W es un espacio vectorial sobre F con las operaciones de V.

En el ejercicio 1, se encuentra un criterio para probar rápidamente que un subconjunto de un espacio vectorial es un subespacio.

3.2.4. Ejemplos

1. Los subespacios de $\mathbb{R}^3$ son rectas y planos que pasan por el origen.

2. Sea A una matriz de $m \times n$. Entonces $W = \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} = \mathbf{0}_{\mathbb{R}^m}\}$ es un subespacio de $\mathbb{R}^n$.

3. Si I es un intervalo abierto de números reales, entonces el conjunto $\mathcal{D}(I, \mathbb{R})$ de funciones diferenciables es un subespacio de $\mathcal{C}(I, \mathbb{R})$. También si J es un intervalo cerrado, entonces $\mathcal{C}(J, \mathbb{R})$ es un subespacio del espacio vectorial $\mathcal{I}(J, \mathbb{R})$ de funciones integrables.

3.2.5 Definición. Sea V un espacio vectorial sobre un campo F. Una **combinación lineal** de $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$ es un vector de la forma $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$ donde $a_i \in F$.

Se obtiene directamente el siguiente resultado.

3.2.6 Teorema. Si S es un subconjunto no vacío de V, entonces el conjunto $\operatorname{gen} S$ de todas las combinaciones lineales de elementos de S es un subespacio de V.

3.2.7 Observación. El subespacio $\operatorname{gen} S$ del teorema anterior se denomina **subespacio generado por** S y es el subespacio más pequeño de V que contiene a S.

3.2.8. Ejemplos

1. En $\mathbb{R}^3$, una recta que pasa por el origen es generada por un vector no nulo, y un plano que pasa por el origen es generado por dos vectores no paralelos.

2. gen $\{x^n, x^{n-1}, \ldots, x, 1\}$ es el subespacio P_n de $F[x]$ de todos los polinomios de grado menor e igual que n.

3. Las matrices $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ y $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ generan el subespacio de *matrices simétricas* de 2×2.

4. El conjunto $\{e_n \mid n \in \mathbb{N}\}$ donde $e_{nk} = \begin{cases} 1 & \text{si } k = n \\ 0 & \text{si } k \neq n \end{cases}$ *no* genera a $\text{suc}(\mathbb{R})$.

5. F^n, $M_{m\times n}(F)$ y P_n son espacios vectoriales *finitamente generados* pero $\text{suc}(\mathbb{R})$, $F[x]$ y $\mathcal{C}(I, \mathbb{R})$ *no* son finitamente generados.

3.2.9 Definición. Sea V un espacio vectorial sobre un campo F. Un subconjunto finito de vectores $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$ es **linealmente independiente** si $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{0}$ implica que $a_1 = a_2 = \cdots = a_k = 0$. En caso contrario se dice que el subconjunto es **linealmente dependiente**.

3.2.10 Ejemplos. Sea V un espacio vectorial sobre un campo F.

1. Un conjunto $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\} \subset V$ es linealmente dependiente si y sólo si existen escalares $a_1, a_2, \ldots, a_k$, no todos nulos, tales que $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k = \mathbf{0}$.

2. Todo conjunto de vectores que contenga al vector cero es linealmente dependiente.

3. Dos vectores no nulos $\mathbf{u}$ y $\mathbf{v}$ son linealmente dependientes si y sólo si son *paralelos*, esto es, $\mathbf{u} = t\mathbf{v}$ para algún $t \in F$.

4. Si S es un subconjunto linealmente independiente y $\mathbf{u} \notin \operatorname{gen} S$, entonces $S \cup \{\mathbf{u}\}$ es linealmente independiente.

5. En $\mathbb{R}^n$ se tiene que $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ son linealmente independientes si y sólo si el sistema lineal $A\mathbf{x} = \mathbf{0}$ admite únicamente la solución trivial $\mathbf{x} = \mathbf{0}$ donde A es la matriz cuyas columnas son los $\mathbf{v}_j$.

3.2.11 Definición. Sea V un espacio vectorial sobre F. Un subconjunto B de V es una **base** para V si es linealmente independiente y todo vector de V es una combinación lineal de elementos de B.

3.2.12. Ejemplos

1. Sea A_{ij} la matriz de $m \times n$ donde la entrada ij-ésima es 1 y el resto son 0. Entonces el conjunto $\{A_{ij} \mid i = 1, 2, \ldots, m \,\text{y}\, j = 1, 2, \ldots, n\}$ es una base de $M_{m\times n}(F)$.

2. $\{1, x, x^2, x^3, \ldots\}$ es base de $F[x]$.

3. $\{e_n \mid n \in \mathbb{N}\}$ *no* es base de $\operatorname{suc}(\mathbb{R})$.

La demostración del siguiente resultado se deja para el lector.

3.2.13 Teorema. Si $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\}$ y $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ son bases de un espacio vectorial V, entonces $m = n$.

Esta propiedad que comparten todas las bases de un mismo espacio vectorial nos permite definir el concepto de dimensión. Aunque el resultado anterior es el caso *finito dimensional*, también se cumple en el caso infinito. Note que no hemos demostrado la existencia de una base para un espacio vectorial,

el lector puede encontrar en los ejercicios de esta sección algunas ideas al respecto.

3.2.14 Definición. Si un espacio vectorial V tiene una base de n elementos, se dice que V tiene **dimensión** n. Un espacio vectorial es *finito dimensional* si tiene una base finita, en caso contrario es de *dimensión infinita*.

3.2.15. Ejemplos

1. Las dimensiones de F^n, $M_{m\times n}$ y P_n son, respectivamente, n, mn y $n+1$.

2. $F[x]$, suc$(\mathbb{R})$ y $\mathcal{C}(I,\mathbb{R})$ tienen dimensión infinita.

3. La dimensión de $\mathbb{C}$ sobre $\mathbb{C}$ es 1 mientras que la dimensión de $\mathbb{C}$ sobre $\mathbb{R}$ es 2.

4. La dimensión de $\mathbb{R}$ sobre $\mathbb{Q}$ es infinita.

3.2.16. Ejercicios

Sea V un espacio vectorial sobre un campo F.

1. Pruebe que un subconjunto no vacío W de V es un subespacio de V si y sólo si $a\mathbf{u}+b\mathbf{u}\in W$ para todo $\mathbf{u},\mathbf{v}\in W$ y todo $a,b\in F$.

2. Muestre que si $\mathbf{u},\mathbf{v},\mathbf{w}\in V$ son linealmente independientes, entonces $\mathbf{u}$, $\mathbf{u}+\mathbf{v}$ y $\mathbf{u}+\mathbf{v}+\mathbf{w}$ son linealmente independientes.

3. Suponga que $\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_k\in V$ son linealmente dependientes. Muestre que uno de los vectores es combinación lineal de los otros.

4. Pruebe que si $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ genera a V, entonces un subconjunto de S es base para V.

5. Suponga que V tiene dimensión finita y que $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\} \subset V$ es linealmente independiente. Pruebe que existen vectores $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m$ tales que el conjunto $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k, \mathbf{w}_1, \ldots, \mathbf{w}_m\}$ es base para V.

6. Sean U y W subespacios de V. Se define $U + W = \{\mathbf{u} + \mathbf{w} \ : \ \mathbf{u} \in U \, , \, \mathbf{w} \in W\}$.

   a) Muestre que $U + W$ es un subespacio de V.

   b) Pruebe que $U \cap W = \{\mathbf{0}\}$ si y sólo si $\mathbf{u} + \mathbf{w} = \mathbf{u}' + \mathbf{w}'$ implica $\mathbf{u} = \mathbf{u}'$ y $\mathbf{w} = \mathbf{w}'$ para $\mathbf{u}, \mathbf{u}' \in U$ y $\mathbf{w}, \mathbf{w}' \in W$.

   c) U y W son *linealmente complementarios* si $U \cap W = \{\mathbf{0}\}$ y $U + W = V$. En tal caso W es el complemento lineal de U. Pruebe que U y W son linealmente complementarios si todo $\mathbf{x} \in V$ se puede escribir de manera única como $x = \mathbf{u} + \mathbf{w}$ con $\mathbf{u} \in U$ y $\mathbf{w} \in W$.

   Si además V es n-dimensional muestre que:

   d) Todo subespacio de V tiene un complemento lineal.

   e) $\dim(U + W) = \dim U + \dim W$ si $U \cap W = \{\mathbf{0}\}$. Adicionalmente, $U + W = V$ si y sólo si $\dim U + \dim W = n$

   f) $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$.

7. Sean V y W espacios vectoriales sobre un campo F. Diremos que $L : V \longrightarrow W$ es una *trasformación lineal* si $L(\mathbf{u} + \mathbf{v}) = L(\mathbf{u}) + L(\mathbf{v})$ y $L(k\mathbf{u}) = kL(\mathbf{u})$ pata todo $\mathbf{u}, \mathbf{v} \in V$ y todo $k \in F$.

a) Pruebe que la suma de funciones lineales, la multiplicación de una función lineal por un escalar y la composición de funciones lineales resultan ser también funciones lineales.

b) Demuestre que si $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ es una base de V y $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ es un subconjunto de W, entonces existe una y sólo una transformación lineal $L : V \longrightarrow W$ tal que $L(\mathbf{u}_i) = \mathbf{v}_i$ para $i = 1, 2, \ldots, n$.

c) Defina el núcleo e imagen de una transformación lineal y pruebe que son subespacios.

d) U y V se llaman *isomorfos* si existe una función $L : V \longrightarrow W$ lineal y biyectiva. En tal caso L es un *isomorfismo*. Pruebe que los isomorfismos transforman bases en bases (asuma dimensión finita).

e) Pruebe que si V es n-dimensional, entonces V es isomorfo a F^n.

8. Una función $P : V \longrightarrow V$ es una *proyección lineal* si es lineal y $P^2 = P \circ P = P$.

   a) Sea W un subespacio de V. Muestre que existe una proyección lineal P tal que $P(V) = W$.

   b) Si V y U son espacios vectoriales sobre un campo F y W un subespacio de V. Pruebe que toda función lineal $L : W \longrightarrow U$ admite una extensión lineal $\widehat{L} : V \longrightarrow U$.

9. Para probar la existencia de una base en un espacio vectorial se utiliza el *Lema de Zorn* de la teoría de conjuntos, el cual dice que si S es un conjunto no vacío *parcialmente ordenado*, tal que toda *cadena* no vacía tiene una *cota superior*, entonces S tiene un *elemento maximal*.

Un ejercicio más simple para aplicar este lema es probar que todo anillo con unitario contiene un ideal maximal.

3.3. Extensiones de campos

3.3.1 Definición. Un campo E es una **extensión** (o campo de extensión) del campo F si F es un subcampo de E.

3.3.2 Ejemplo. $\mathbb{C}$ es una extensión de $\mathbb{R}$ y $\mathbb{Q}(\sqrt{2})$ es una extensión de $\mathbb{Q}$.

3.3.3. Observaciones

1. E es un campo de extensión de F si $F \subseteq E$ y las operaciones de F son las de E restringidas a F.

2. Si E es una extensión de F, entonces E es un espacio vectorial sobre F.

3. $x^2 + 1 \in \mathbb{R}[x]$ no tiene ceros en $\mathbb{R}$ pero $\mathbb{C}$ es una extensión de $\mathbb{R}$ que tiene a i como cero de $x^2 + 1$.

4. $\mathbb{R}/\langle x^2 + 1\rangle$ y $\mathbb{C}$ son campos isomorfos.

3.3.4 Teorema de Kronecker. Sea F un campo y $f(x)$ un polinomio no constante en $F[x]$. Entonces existe una extensión E de F y un $\alpha \in E$ tal que $f(\alpha) = 0$.

Demostración. Sea $p(x)$ un factor irreducible de $f(x)$. Entonces $\langle p(x)\rangle$ es un ideal maximal y $F[x]/\langle p(x)\rangle$ es un campo. La función $\varphi : F \longrightarrow$

$F[x]/\langle p(x)\rangle$ definida por $\varphi(a) = a + \langle p(x)\rangle$ es un homomorfismo inyectivo de campos y en consecuencia F es isomorfo a $\varphi(F)$. Luego, podemos considerar $E = F[x]/\langle p(x)\rangle$ como una extensión de F con la identificación $a \leftrightarrow a + \langle p(x)\rangle$. Adicionalmente, si $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ entonces $\alpha = x + \langle p(x)\rangle$ satisface

$$\begin{aligned} p(\alpha) &= p(x + \langle p(x)\rangle) \\ &= a_n(x + \langle p(x)\rangle)^n + a_{n-1}(x + \langle p(x)\rangle)^{n-1} + \cdots + a_1(x + \langle p(x)\rangle) + a_0 \\ &= a_n(x^n + \langle p(x)\rangle) + a_{n-1}(x^{n-1} + \langle p(x)\rangle) + \cdots + a_1(x + \langle p(x)\rangle) + a_0 \\ &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle \\ &= 0 + \langle p(x)\rangle \end{aligned}$$

□

3.3.5. Ejemplos

1. $E = \mathbb{R}/\langle x^2 + 1\rangle$ es una extensión de $\mathbb{R}$ identificando $r \leftrightarrow r + \langle x^2 + 1\rangle$ y $x + \langle x^2 + 1\rangle \in E$ es un cero de $x^2 + 1 \in E[x]$.

2. Dado el polinomio $f(x) = (x^2 - 5)(x^2 - 7) \in \mathbb{Q}$, existe una extensión E de $\mathbb{Q}$ y un $\lambda \in E$ tal que $f(\lambda) = 0$, por ejemplo, $\mathbb{Q}[x]/\langle x^2 - 5\rangle$ es un campo de extensión de $\mathbb{Q}$ que contiene un cero de $f(x)$.

3. $\mathbb{Z}_3/\langle x^3 + 2x + 2\rangle$ es una extensión de $\mathbb{Z}_3$ que tiene 27 elementos y $x^3 + 2x + 2$ tiene un cero allí.

El teorema de Kronecker garantiza la existencia de una extensión de $\mathbb{Q}$, donde $x^2 - 2$ tiene una raíz y, por tanto, cabe preguntarse cuál es la menor extensión

de $\mathbb{Q}$ que cumple con ello. Es el momento de justificar las definiciones de campos como $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ y $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

3.3.6 Definición. Si F es un campo y $a_1, a_2, \ldots, a_n$ son elementos de una extensión E de F, se denota por $F(a_1, a_2, \ldots, a_n)$ el subcampo más pequeño de E que contiene a F y al conjunto $\{a_1, a_2, \ldots, a_n\}$.

Es ejercicio verificar que $F(a_1, a_2, \ldots, a_n)$ es la intersección de todos los subcampos de E que contienen a F y a $\{a_1, a_2, \ldots, a_n\}$

3.3.7. Ejemplos

1. $\mathbb{R}(i) = \mathbb{C}$.
2. $\mathbb{Q}(\sqrt{2})$ es el menor campo que contiene a $\mathbb{Q}$ y a $\sqrt{2}$.

Por el teorema de Kronecker, el polinomio $p(x) = x^2 + 1 \in \mathbb{Q}[x]$ tiene un cero α en una extensión E de $\mathbb{Q}$. Puesto que $-\alpha$ es también cero de $p(x)$, entonces $p(x) = (x - \alpha)(x + \alpha)$, es decir, $p(x)$ se *descompone* en la extensión E.

3.3.8 Definición. Sea E una extensión de un campo F y sea $f(x) \in F[x]$. Diremos que $f(x)$ **se descompone en** E si $f(x)$ se puede factorizar como producto de factores lineales en $E[x]$. Adicionalmente, E es un **campo de descomposición para** $f(x)$ **sobre** F si $f(x)$ se descompone en E pero no se descompone en un subcampo propio de E.

3.3.9 Ejemplo. Los ceros de $f(x) = (x^2 - 3)(x^2 + 1) \in \mathbb{Q}[x]$ son $\pm\sqrt{3}$ y $\pm i$. Luego un campo de descomposición para $f(x)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3})(i) = \{\alpha + \beta i \,|\, \alpha, \beta \in \mathbb{Q}(\sqrt{3})\} = \{a + b\sqrt{3} + ci + d\sqrt{3}i \,|\, a, b, c, d \in \mathbb{Q}\}$.

Para terminar esta sección, probamos la existencia de campos de descomposición.

3.3.10 Teorema. Si F es un campo y $f(x)$ es un polinomio no constante de $F[x]$, entonces existe un campo de descomposición E para $f(x)$ sobre F.

Demostración. Se aplica inducción fuerte sobre $\operatorname{grd} f(x)$. Si $\operatorname{grd} f(x) = 1$, entonces el resultado es cierto por ser $f(x)$ un polinomio lineal. Suponga que el resultado es cierto para todos los polinomios de grado menor que $\operatorname{grd} f(x)$. Por el teorema de Kronecker existe una extensión E de F en la que $f(x)$ tiene un cero a_1. Entonces $f(x) = (x - a_1)g(x)$ donde $g(x) \in E[x]$ y puesto que $\operatorname{grd} g(x) < \operatorname{grd} f(x)$, existe un campo K que contiene a E y todos los ceros $a_2, a_3, \ldots, a_n$ de $g(x)$. Luego $F(a_1, a_2, \ldots, a_n)$ es un campo de descomposición de $f(x)$ sobre F. □

3.3.11. Ejercicios

1. Sea E una extensión de F y $a_1, a_2, \ldots, a_n \in E$. Pruebe que el campo $F(a_1, a_2, \ldots, a_n)$ es la intersección de todos los subcampos de E que contienen a F y a $\{a_1, a_2, \ldots, a_n\}$.

2. Demuestre que $\mathbb{R}(i) = \mathbb{C}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ y $\mathbb{Q}(4 - i) = \mathbb{Q}(1 + i)$.

3. Sean $f(x) = x^3 - 1$ y $g(x) = x^4 + x^2 + 1$ en $\mathbb{Q}[x]$. Pruebe que $\mathbb{Q}(3i)$ es una extensión de $\mathbb{Q}$ que contiene los ceros de $f(x)$ y de $g(x)$.

4. Muestre que $\mathbb{R}[x]/\langle x^2 + 1\rangle$ es isomorfo a $\mathbb{C}$.

5. Sean F un campo, $p(x) \in F[x]$ un polinomio irreducible sobre F y a un cero de $p(x)$ en alguna extensión E de F. Demuestre:

   a) $F(a)$ es isomorfo a $F[x]/\langle p(x)\rangle$.

   b) Si $\operatorname{grd} p(x) = n$, entonces todo elemento de $F(a)$ puede escribirse de manera única como $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0$, donde $c_0, c_1, \ldots, c_{n-2}, c_{n-1} \in F$.

   c) Si b es un cero de $p(x)$ en alguna extensión E' de F, entonces $F(a)$ y $F(b)$ son isomorfos.

6. Encuentre un polinomio $p(x) \in \mathbb{Q}[x]$ tal que $\mathbb{Q}(\sqrt{1+\sqrt{5}})$ es isomorfo a $\mathbb{Q}[x]/\langle p(x)\rangle$.

7. Muestre que $\mathbb{Q}(\sqrt[6]{2})$ es un espacio vectorial sobre $\mathbb{Q}$ y encuentre una base.

8. Sean F un campo, $p(x) \in F[x]$ un polinomio irreducible sobre F y a un cero de $p(x)$ en alguna extensión de F. Demuestre que si $\varphi : F \longrightarrow F'$ es un isomorfismo de campos y b es un cero de $\varphi(p(x))$ en alguna extensión de F', entonces existe un isomorfismo $\psi : F(a) \longrightarrow F'(b)$ que coincide con φ en F y $\psi(a) = b$.

9. Sea $\varphi : F \longrightarrow F'$ un isomorfismo de campos y $f(x) \in F[x]$. Pruebe que si E es un campo de descomposición para $f(x)$ sobre F y E' es un campo de descomposición para $\varphi(f(x))$ sobre F', entonces existe un isomorfismo de E en E' que coincide con φ en F.

10. Sea F un campo y $f(x) \in F[x]$. Muestre que cualquier par de campos de descomposición de $f(x)$ sobre F son isomorfos.

11. Determine el campo de descomposición de $x^6 - 2 \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$.

12. Determine el campo de descomposición de $x^n - a \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$, donde a es un número racional positivo.

3.4. Elementos algebraicos y trascendentes

3.4.1 Definición. Sea E un campo de extensión del campo F. Un elemento $\alpha \in E$ es **algebraico sobre** F si existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. En caso contrario α es **trascendente sobre** F.

3.4.2. Ejemplos

1. $i \in \mathbb{C}$ es algebraico sobre $\mathbb{R}$.

2. $\sqrt{1+\sqrt{7}} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, porque es cero de $x^4 - 2x^2 - 6$.

3. π y e son trascendentes sobre $\mathbb{Q}$, pero no es fácil probarlo.

4. Todo elemento de un campo F es algebraico sobre F.

3.4.3 Proposición. Sea E una extensión de F y $\alpha \in E$. Si α es algebraico sobre F, entonces existe un único polinomio mónico $p(x) \in F[x]$ y de grado mínimo tal que $p(\alpha) = 0$. Además $p(x)$ es irreducible.

Demostración. Existe un polinomio no nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Podemos suponer $f(x)$ mónico multiplicándolo por el recíproco del coeficiente principal. Sea $p(x)$ un polinomio mónico de grado mínimo tal que $p(\alpha) = 0$. Si $p(x) = a(x)b(x)$ con $0 < \operatorname{grd} a(x)\,, \operatorname{grd} b(x) < \operatorname{grd} p(x)$, entonces $0 = p(\alpha) = a(\alpha)b(\alpha)$ y $a(\alpha) = 0$ o $b(\alpha) = 0$ que contradice la minimalidad del grado. □

3.4.4 Definición. El polinomio $p(x)$ de la proposición anterior se llama **polinomio mínimo irreducible de** α **sobre** F y se denota $\text{irr}(\alpha, F)$. El **grado de** α **sobre** F es $\text{grd}(\alpha, F) = \text{grd}\,\text{irr}(\alpha, F)$.

3.4.5 Ejemplo. $\text{irr}(\sqrt{5}, \mathbb{Q}) = x^2 - 5$ y $\text{grad}(\sqrt{1+\sqrt{7}}, \mathbb{Q}) = 4$

3.4.6 Teorema. Si E es un campo de extensión de F y $\alpha \in E$ es un elemento algebraico sobre F, entonces $F(\alpha) = \{f(\alpha) \,:\, f(x) \in F[x]\}$ y $\dim(F(\alpha), F) = \text{grd}(\alpha, F)$.

Demostración. Sea $\alpha \in E$ algebraico sobre F, $p(x) = \text{irr}(\alpha, F)$ y $n = \text{grd}(\alpha, F)$. Dado $f(x) \in F[x]$, existen $q(x), r(x) \in F[x]$ únicos tales que $f(x) = q(x)p(x) + r(x)$ y $0 < \text{grd}\, r(x) < n$ o $r(x) = 0$. Entonces $f(\alpha) = r(\alpha)$ y cualquier expresión polinómica en α se puede expresar como un polinomio de grado a lo más $n-1$. Así que $K = \{f(\alpha) \,:\, f(x) \in F[x]\}$ es un dominio entero que resulta ser un espacio vectorial sobre F con base $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Por tanto K es campo (ver ejercicio 1) y $\dim(K, F) = n = \text{grd}(\alpha, F)$. Note que si M es cualquier campo que contiene a F y α entonces contiene a K y $K = F(\alpha)$, el campo de extensión de F que se obtiene al agregar α. □

3.4.7 Observación. Si $\alpha \in E$ es un elemento algebraico sobre F, entonces $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F donde $n = \text{grd}(\alpha, F)$.

3.4.8. Ejemplos

1. $\mathbb{R}(i) = \{a + bi \,|\, a, b \in \mathbb{R}\} = \mathbb{C}$ porque i es algebraico sobre $\mathbb{R}$ y $\text{grd}(i, \mathbb{R}) = 2$.

2. $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,|\, a, b, c \in \mathbb{Q}\}$.

3. El polinomio $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible. Por el teorema de Kronecker existe una extensión E de $\mathbb{Z}_2$ que contiene un cero α de $p(x)$ y por el teorema anterior $\mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\}$ es un campo de cuatro elementos. El lector puede escribir las tablas de las operaciones para este campo.

3.4.9. Ejercicios

1. Sea D un dominio entero tal que es un espacio vectorial finito dimensional sobre un campo F. Demuestre que D es un campo.

2. Sea E una extensión de F y $\alpha \in E$ un elemento algebraico sobre F. Determine el núcleo y la imagen del homomorfismo de evaluación $\psi : F[x] \longrightarrow E$ definido por $\psi(f(x)) = f(\alpha)$.

3. Sea E un campo de extensión de F y $\alpha \in E$. Pruebe que α es trascendente sobre F si y sólo si el homomorfismo de evaluación $\psi : F[x] \longrightarrow E$, $\psi(f(x)) = f(\alpha)$, es uno a uno.

4. Sea $\alpha \in E$ un elemento algebraico sobre F. Pruebe que todo elemento $\beta \in F(\alpha)$ es algebraico sobre F y $\text{gra}(\beta, F) \leq \text{gra}(\alpha, F)$.

5. Describa el campo $\mathbb{Q}(\pi)$.

6. Pruebe por dos métodos distintos que $\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ es un subcampo de $\mathbb{R}$.

7. Demuestre que los siguientes números complejos son algebraicos y encuentre el grado de cada uno sobre $\mathbb{Q}$: $\sqrt{2} + \sqrt{3}$, $\sqrt{7} + \sqrt[3]{12}$, $2 + i\sqrt{3}$ y $\cos(2\pi/p) + i\,\text{sen}(2\pi/p)$ donde p es un primo.

8. Sea F un subcampo de E y $a \in E$ tal que a^2 es algebraico sobre F. Muestre que a es algebraico sobre F.

9. Para el polinomio irreducible $f(x) = x^3 + x + 1$ sobre $\mathbb{Z}_2$ realice un desarrollo análogo al último ejemplo de esta sección.

3.5. Extensiones algebraicas y extensiones finitas

3.5.1 Definición. Sea E un campo de extensión del campo F.

1. E es una **extensión algebraica** de F si todo elemento de E es algebraico sobre F.

2. E es una **extensión finita** de F si E es un espacio vectorial sobre F de dimensión finita. En tal caso, $\dim(E, F)$ se llama **grado de E sobre F** y se denota $[E : F]$.

3.5.2. Ejemplos

1. Si $\alpha \in E$ es algebraico sobre F, entonces $F(\alpha)$ es una extensión finita de F y $[F(\alpha) : F] = \text{grad}(\alpha, F)$. En particular $\mathbb{C} = \mathbb{R}(i)$ es una extensión finita de $\mathbb{R}$ y $[\mathbb{C} : \mathbb{R}] = 2$. Similarmente $\mathbb{Q}(\sqrt[6]{2})$ es una extensión finita de $\mathbb{Q}$ y $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$.

2. Por el ejercicio 4 de la sección anterior, todo $\beta \in F(\alpha)$ es algebraico sobre F y por tanto $F(\alpha)$ es una extensión algebraica de F. Así, $\mathbb{C}$ es una extensión algebraica de $\mathbb{R}$ y $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{1+\sqrt{7}})$ y $\mathbb{Q}(\sqrt[6]{2})$ son extensiones algebraicas de $\mathbb{Q}$.

3. $\mathbb{C}$ *no* es una extensión algebraica de $\mathbb{Q}$ porque π es trascendente sobre $\mathbb{Q}$.

4. $\mathbb{R}$ *no* es una extensión finita de $\mathbb{Q}$ porque $\dim(\mathbb{R}, \mathbb{Q})$ es infinito.

3.5.3 Teorema. Si E es una extensión finita de F, entonces E es una extensión algebraica de F.

Demostración. Sea E una extensión finita de F tal que $[E : F] = n$ y $a \in E$. El conjunto $\{1, a, a^2, \ldots, a^n\}$ es linealmente dependiente y existen escalares $c_0, c_1, \ldots, c_n \in F$, no todos nulos, tales que $c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n = 0$. Entonces $p(x) = c_n x^n + \cdots + c_1 x + c_0 \in F[x]$ y $p(a) = 0$. □

3.5.4 Observación. El recíproco del teorema anterior *no* es cierto. Por ejemplo, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ es una extensión algebraica de $\mathbb{Q}$ pero no es finita porque contiene elementos de todo grado sobre $\mathbb{Q}$.

El siguiente resultado es muy importante y se asemeja al teorema de Lagrange para grupos finitos.

3.5.5 Teorema. Si K es una extensión finita de E y E es una extensión finita de F, entonces K es una extensión finita de F y

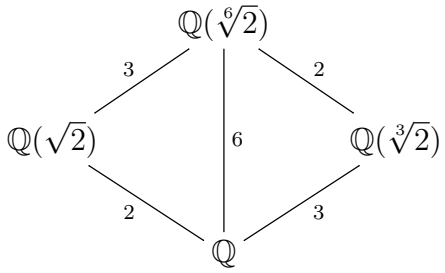
$$[K : F] = [K : E][E : F] .$$

Demostración. Si $\{a_i \mid i = 1, 2, \ldots, m\}$ es una base de K sobre E y $\{b_j \mid j = 1, 2, \ldots, n\}$ es una base de E sobre F, entonces los mn elementos $a_i b_j$ forman una base de K sobre F. □

3.5.6. Ejemplos

1. $\{1, \sqrt{5}\}$ es base de $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ sobre $\mathbb{Q}(\sqrt{7})$ y $\{1, \sqrt{7}\}$ es base de $\mathbb{Q}(\sqrt{7})$ sobre $\mathbb{Q}$, así que $\{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$ es base de $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ sobre $\mathbb{Q}$ y $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = 4$. El lector puede verificar que $\mathbb{Q}(\sqrt{5} + \sqrt{7}) = \mathbb{Q}(\sqrt{5}, \sqrt{7})$ mostrando las dos contenencias.

2. Para probar que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$, note primero que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[6]{2})$ implica $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$. Por otro lado, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ implica que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ y $[\mathbb{Q}\sqrt[3]{2}) : \mathbb{Q}] = 3$ dividen a $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ y por ser primos relativos $6 \leq [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. En resumen, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6 = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}]$ y $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.



3.5.7 Teorema. Sea E un campo de extensión de F. El conjunto de todos los elementos de E que son algebraicos sobre F es un subcampo de E.

Demostración. Sea $A = \{\alpha \in E : \alpha \text{ es algebraico sobre } F\}$. Si $\alpha, \beta \in A$, entonces $F(\alpha)$ es una extensión finita de F y $[F(\alpha) : F] = \text{grd}(\alpha, F)$. Como $F \subseteq F(\alpha)$ y β es algebraico sobre F, entonces β es algebraico sobre $F(\alpha)$. Así que $F(\alpha, \beta) = (F(\alpha))(\beta)$ es una extensión finita de $F(\alpha)$, y por el teorema anterior, $F(\alpha, \beta)$ es una extesión finita de F. Esto significa que $F(\alpha, \beta) \subseteq A$ y por tanto $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$ y α/β si $\beta \neq 0$ son elementos de A. $\square$

El campo de todos los elementos de E que son algebraicos sobre F se denomina **clausura algebraica de F en E.**

3.5.8 Ejemplo. El conjunto $A = \{z \in \mathbb{C} : z \text{ es algebraico sobre } \mathbb{Q}\}$ de *números algebraicos* es un subcampo de $\mathbb{C}$.

3.5.9. Ejercicios

1. Demuestre que si K es una extensión algebraica de E y E es una extensión algebraica de F, entonces K es una extensión algebraica de F.

2. Sea K una extensión finita de F tal que $[K : F] = n$. Muestre que K y F^n son espacios vectoriales sobre F isomorfos.

3. Sea F un campo y E un campo de descomposición para un polinomio no constante de $F[x]$. Pruebe que E es una extensión finita de F.

4. Verifique que $f(x) = 15x^4 - 10x^2 + 9x + 21$ es irreducible sobre $\mathbb{Q}$ y pruebe que si α es un cero de $f(x)$ en alguna extensión de $\mathbb{Q}$, entonces $\sqrt[3]{2}$ no pertenece a $\mathbb{Q}(\alpha)$.

5. Muestre que $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{2}) : \mathbb{Q}] = 12$.

6. Pruebe que $\text{grd}(\sqrt{3} + \sqrt{5}, \mathbb{Q}) = 4$.

7. Sean $a, b \in \mathbb{Q}^+$. Demuestre que $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

8. Halle el grado y una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}$.

9. Sea E una extensión de F y A la clausura algebraica de F en E.

a) Muestre que si $\alpha \in E$ es algebraico sobre A, entonces α es algebraico sobre F.

b) Pruebe que todo polinomio de $F[x]$ se descompone en A.

10. Un campo F es *algebraicamente cerrado* si todo polinomio no constante en $F[x]$ tiene algún cero en F. Por ejemplo, $\mathbb{C}$ es algebraicamente cerrado por el teorema fundamental del Álgebra. Demuestre:

    a) F es algebraicamente cerrado si y sólo si todo polinomio no constante en $F[x]$ se descompone en F.

    b) Si F es algebraicamente cerrado, entonces F no tiene extensiones algebraicas propias.

    c) Si E es una extensión finita de $\mathbb{R}$, entonces $E = \mathbb{R}$ o $E = \mathbb{C}$.

11. Suponga que $f(x)$ y $g(x)$ son irreducibles sobre F tales que $\operatorname{grd} f(x)$ y $\operatorname{grd} g(x)$ son primos relativos. Pruebe que si α es un cero de $f(x)$ en alguna extensión de F, entonces $g(x)$ es irreducible sobre $F(\alpha)$.

12. Sean $a, b \in \mathbb{Q}^+$. Muestre que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ si y sólo si existe $c \in \mathbb{Q}$ tal que $a = bc^2$.

13. Sea E un campo de extensión de F tal que $[E : F]$ es primo. Muestre que para todo $a \in E$, $F(a) = F$ o $F(a) = E$.

14. Suponga que E es una extensión de F y que $a, b \in E$ son algebraicos sobre F. Muestre que si $\operatorname{grd}(a, F) = m$ y $\operatorname{grd}(b, F) = n$ son primos relativos, entonces $[F(a, b) : F] = mn$.

15. Sean K, E y G extensiones de F tales que $E, G \subseteq K$. Pruebe que si $[E : F]$ y $[G : F]$ son primos, entonces $E = G$ o $E \cap G = F$.

3.6. Campos fijos y el grupo de Galois

3.6.1 Definición. Sea E un campo de extensión de F.

1. $a \in E$ **queda fijo bajo** el automorfismo φ de E si $\varphi(a) = a$.

2. Una colección $\mathcal{A}$ de automorfismos de E **deja fijo al subcampo** F si cada $a \in F$ queda fijo bajo toda $\varphi \in \mathcal{A}$.

3.6.2. Ejemplos

1. $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$ definida por $\varphi(z) = \overline{z}$ es un automorfismo de $\mathbb{C}$ que deja fijo a $\mathbb{R}$.

2. El automorfismo $\varphi : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ dado por $\varphi(a+b\sqrt{2}) = a - b\sqrt{2}$ deja fijo a $\mathbb{Q}(\sqrt{3})$.

3. $\varphi : \mathbb{Z}_2(\alpha) \longrightarrow \mathbb{Z}_2(\alpha)$ definida por $\varphi(a) = a^2$ (ver ejemplo 3.4.8.3) es un automorfismo que deja fijo a $\mathbb{Z}_2$.

3.6.3 Proposición. Si E es un campo y $\mathcal{A}$ es una colección de automorfismos de E, entonces $E_{\mathcal{A}} = \{x \in E \,|\varphi(x) = x \,\text{para todo}\, \varphi \in \mathcal{A}\}$ es un subcampo de E llamado **campo fijo** de $\mathcal{A}$.

Demostración. $0, 1 \in E_{\mathcal{A}}$ porque todo automorfismo deja fijo los neutros. Sean $a, b \in E$ y $\varphi \in \mathcal{A}$. Entonces $\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = a \pm b$, $\varphi(ab) = \varphi(a)\varphi(b) = ab$ y $\varphi(ab^{-1}) = \varphi(a) \pm \varphi(b)^{-1} = a \pm b^{-1}$ si $b \neq 0$. Así que $a \pm b, ab, a/b \in E_{\mathcal{A}}$ y $E_{\mathcal{A}}$ es subcampo de E. □

3.6.4 Ejemplo. Considere la extensión $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} : a, b, c, d \in \mathbb{Q}\}$ de $\mathbb{Q}$. Cualquier automorfismo de $\mathbb{Q}(\sqrt{3},\sqrt{5})$ deja fijo a los racionales (ver ejercicio 1) y por tanto queda completamente determinado por sus valores en $\sqrt{3}$ y $\sqrt{5}$. Así que hay cuatro automorfismos $\iota : \sqrt{3} \mapsto \sqrt{3}, \sqrt{5} \mapsto \sqrt{5}$; $\sigma : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto \sqrt{5}$; $\tau : \sqrt{3} \mapsto \sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}$ y $\gamma : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}$. Note que $E_{\{\iota,\sigma\}} = \mathbb{Q}(\sqrt{5})$, $E_{\{\iota,\tau\}} = \mathbb{Q}(\sqrt{3})$, $E_{\{\iota,\gamma\}} = \mathbb{Q}(\sqrt{3},\sqrt{5})$ y $E_{\{\iota,\sigma,\tau,\gamma\}} = \mathbb{Q}$.

Recuerde que si E es un campo, entonces el conjunto de todos los automorfismos de E es un grupo con la composición de funciones.

3.6.5 Teorema. Sea E un campo de extensión de F. El conjunto $\mathrm{Gal}(E, F)$ de todos los automorfismos de E que dejan fijo a F es un grupo con la composición de funciones.

Demostración. $\mathrm{Gal}(E, F)$ es no vacío porque la identidad es un automorfismo de E que deja fijo a F. Si $\varphi, \phi \in \mathrm{Gal}(E, F)$, entonces $\varphi\phi \in \mathrm{Gal}(E, F)$ porque $\varphi\phi(a) = \varphi(\phi(a)) = \varphi(a) = a$ para todo $a \in F$. Por último, si $\varphi \in \mathrm{Gal}(E, F)$, entonces $a = \varphi^{-1}(a)$ para todo $a \in F$. □

3.6.6 Definición. El grupo $\mathrm{Gal}(E, F)$ se denomina **grupo de Galois de E sobre F**.

3.6.7. Ejemplos

1. Según el ejemplo anterior $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}), \mathbb{Q}) = \{\iota, \sigma, \tau, \gamma\}$ y la tabla de grupo es

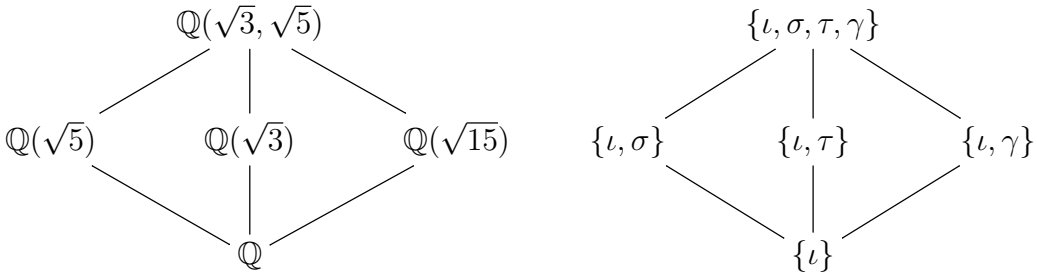
	ι	σ	τ	γ
ι	ι	σ	τ	γ
σ	σ	ι	γ	τ
τ	τ	γ	ι	σ
γ	γ	τ	σ	ι

Note que este grupo es isomorfo al 4-grupo de Klein o $\mathbb{Z}_2 \times \mathbb{Z}_2$.

2. Cualquier automorfismo φ de $\mathbb{Q}(\sqrt{2})$ deja fijo los racionales y queda determinado por su valor en $\sqrt{2}$. Puesto que $2 = \varphi(2) = \varphi(\sqrt{2}\sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = [\varphi(\sqrt{2})]^2$, entonces $\varphi(\sqrt{2}) = \pm\sqrt{2}$ y $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ tiene sólo los dos elementos $a + b\sqrt{2} \mapsto a + b\sqrt{2}$ y $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Es decir, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ es $\mathbb{Z}_2$.

3. Considere la extensión $\mathbb{Q}(\sqrt[3]{2})$ de $\mathbb{Q}$. Puesto que $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ y $\sqrt[3]{2}$ es la única raíz cúbica real de 2, entonces $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. Así que el automorfismo identidad es el único elemento de $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \mathbb{Q}))$. Observe que el campo fijo de $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$ es $\mathbb{Q}(\sqrt[3]{2})$.

3.6.8 Observación. Existe una correspondencia entre los subgrupos de $\mathrm{Gal}(E, F)$ y los subcampos de E que contienen a F, hecho que se enuncia en el teorema fundamental de la teoría de Galois, el cual se encuentra fuera del alcance de este libro. Para más información sobre este aspecto, se invita al lector a consultar [3] y [5]. A continuación, se ilustra el caso particular de $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q})$.



3.6.9. Ejercicios

1. Sea E un campo de extensión de $\mathbb{Q}$. Muestre que todo automorfismo de E deja fijo a $\mathbb{Q}$. ¿Cuáles son los automorfismos de $\mathbb{Q}$?

2. Si $\alpha^2 \in \mathbb{Q}$ y $\alpha \notin \mathbb{Q}$, halle todos los automorfimos de $\mathbb{Q}(\alpha)$ que dejan fijo a $\mathbb{Q}$.

3. Suponga que F es un campo finito de característica p. Pruebe que la función $\varphi : E \longrightarrow E$ definida por $\varphi(a) = a^p$, es un automorfismo y $F_{\{\varphi\}}$ es isomorfo a $\mathbb{Z}_p$.

4. Sea E un campo de característica cero y $\sigma_1, \sigma_2, \ldots, \sigma_n$ automorfismos distintos de E. Demuestre que no existen c_1, c_2, $\ldots$, $c_n \in E$, no todos cero, tales que $c_1\sigma_1(a) + c_2\sigma_2(a) + \cdots + c_n\sigma_n(a) = 0$ para todo $a \in E$.

5. Pruebe que si E es una extensión finita de F, entonces $G(E, F)$ es un grupo finito y $|G(E, F)| \leq [E : F]$.

6. Determine $\mathrm{Gal}(\mathbb{C}, \mathbb{R})$ y $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}(i))$.

7. Verifique que $\omega = \mathrm{cis}(2\pi/5)$ satisface $\omega^5 = 1$ y es cero de $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Encuentre $\mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q})$.

8. Sea $f(x) \in F[x]$ con ceros $a_1, a_2, \ldots, a_n$. Si $K = F(a_1, a_2, \ldots, a_n)$, muestre que cada elemento de $\mathrm{Gal}(K, F)$ define una permutación de los a_i.

9. Dibuje los diagramas reticulares para los subgrupos de $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q})$ y los subcampos de $\mathbb{Q}(\sqrt[4]{2}, i)$.

10. Sea E un campo de extensión de F, $\mathcal{F}$ la colección de todos los subcampos de E que contienen a F y $\mathcal{G}$ la colección de todos los subgrupos de $\mathrm{Gal}(E, F)$. Defina $g : \mathcal{F} \longrightarrow \mathcal{G}$ por $g(K) = \mathrm{Gal}(E, K)$ y $f : \mathcal{G} \longrightarrow \mathcal{F}$ por $f(H) = E_H$. Demuestre:

    a) Si $K, L \in \mathcal{F}$ y $K \subseteq L$, entonces $g(K) \supseteq g(L)$.

    b) Si $G, H \in \mathcal{G}$ y $G \subseteq H$, entonces $f(G) \supseteq f(H)$.

    c) $(fg)(K) \supseteq K$ para todo $K \in \mathcal{F}$ y $(gf)(G) \supseteq G$ para todo $G \in \mathcal{G}$.

Bibliografía

[1] Fraleigh, J. B., *A First Course in Abstract Algebra*, 7th ed., Pearson, 2002.

[2] Herstein, I. N., *Abstract Algebra*, 3rd ed., John Wiley & Sons, Inc., 1999.

[3] Hungerford, T. W., *Algebra*, Springer, 2003.

[4] Kostrikin, A. I., *Introduction to Algebra*, Springer-Verlag, 1982.

[5] Lang, S., *Undergraduate Algebra*, 3rd ed., Springer, 2005.

Índice alfabético