Una Introducción al Álgebra Abstracta

Luciano J. González

2025

FACULTAD DE CIENCIAS
EXACTAS Y NATURALES
Universidad Nacional de La Pampa

Facultad de Ciencias Exactas y Naturales
Universidad Nacional de La Pampa
CONICET
`lucianogonzalez@exactas.unlpam.edu.ar`
`https://gonzalezluciano.github.io/`

Índice general

Capítulo 1

Grupos

En este capítulo presentamos los conceptos básicos en teoría de grupo y una serie de ejemplos importantes tendientes a que el lector se familiarice con las nociones introducidas. En la última sección probaremos uno de los resultados más importantes en la teoría de grupos.

1.1. Definiciones y ejemplos

Dado un conjunto no vacío A, una **operación binaria** $*$ sobre A es una función que asigna a cada par (a, b) de elementos de A un elemento $a * b$ de A. Esto es, $*\colon A \times A \to A$ es una función. También se dice que A es cerrado bajo $*$.

Definición 1.1.1. Un **grupo** es un par $\langle G, * \rangle$ donde G es un conjunto no vacío y $*$ es un operación binaria sobre G que verifica las siguientes condiciones:

(G1) *Asociativa*: $a * (b * c) = (a * b) * c$, para cualesquiera $a, b, c \in G$;

(G2) *Elemento neutro*: existe un elemento $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$;

(G3) *Inverso*: para cada elemento $a \in G$ existe un elemento $b \in G$ tal que $a * b = b * a = e$.

A menudo, cuando no haya peligro de confusión, nos referiremos a un grupo $\langle G, * \rangle$ simplemente con G y además, para elementos a y b en G, escribiremos ab en lugar de $a * b$.

Ejemplo 1.1.2.

(1) Sea $\mathbb{Z}$ el conjunto de los números enteros y sea $+$ la suma ordinaria entre enteros. Entonces $\langle \mathbb{Z}, + \rangle$ es un grupo.

(2) Sea $\mathbb{Q}' = \mathbb{Q} \setminus \{0\}$ el conjunto de los números racionales distintos de cero. Sea $*$ la multiplicación ordinario entre racionales. Entonces, $\langle \mathbb{Q}', * \rangle$ es un grupo. ¿es $\langle \mathbb{Q}, * \rangle$ un grupo ?

(3) Sea $G = M_{nm}(\mathbb{R})$ la familia de todas las matrices de orden $n \times m$ con entradas en los números reales y considere la suma usual entre matrices. Entonces, G es un grupo.

(4) Sea S un conjunto no vacío y $\mathrm{Sym}(S) = \{f : S \to S : \ f \text{ es biyectiva}\}$. Sea $\circ$ la composición usual de funciones. Por lo tanto, $\langle \mathrm{Sym}(S), \circ \rangle$ es un grupo. Cuando S es un conjunto finito de n elementos, $\mathrm{Sym}(S)$ es llamado **el grupo simétrico de grado** n y es denotado por S_n (véase §1.5).

(5) Dado $n \geq 2$ consideremos el conjunto U_n de todas las raíces n-esimas de la unidad, esto es,

$$U_n = \{z \in \mathbb{C} : z^n = 1\}.$$

Usando el producto usual de números complejos podemos probar que U_n es un grupo con respecto a él.

(6) Sea $\mathbb{R}$ el conjunto de los números reales y sea G el conjunto de todas las funciones $T_a : \mathbb{R} \to \mathbb{R}$ definidas por $T_a(x) = x + a$ para cualquier $x \in \mathbb{R}$ y con $a \in \mathbb{R}$. La operación $\circ$ es la composición usual de funciones. Entonces, $\langle G, \circ \rangle$ es un grupo. ■

Diremos que un grupo G es **finito** si G tiene un número finito de elementos. El número de elementos de un grupo finito G es llamado el **orden** de G y lo denotaremos por $|G|$ y también por $o(G)$, según nos convega. En general para un conjunto X, denotaremos por $\#(X)$ el cardinal de X. Es decir, si G es un grupo, entonces $|G| = \#(G)$.

Definición 1.1.3. Un grupo G es llamado **abeliano** si la operación $*$ es conmutativa. Esto es, si $a * b = b * a$ para todos $a, b \in G$.

Cuando G sea un grupo abeliano, usaremos el símbolo $+$ en lugar de $*$ para representar a la operación de G y también denotaremos al elemento neutro de G por 0 (el cual no deberá confundirse con el entero 0) en lugar de e. Los grupos en (1)-(3), (5) y (6) del Ejemplo 1.1.2 son todos abelianos. Veamos algunos ejemplos de grupos no abelianos.

Ejemplo 1.1.4.

(1) Sea $\mathbb{R}$ el conjunto de todos los números reales y sea G el conjunto de todas las funciones $T_{a,b} : \mathbb{R} \to \mathbb{R}$ definidas por $T_{a,b}(x) = ax + b$ para cualesquiera $x \in \mathbb{R}$, donde a, b son reales y $a \neq 0$. La operación $\circ$ es la composición usual entre funciones. Comprobar que $(T_{a,b} \circ T_{c,d})(x) = T_{ac,ad+b}(x)$ y que $\langle G, \circ \rangle$ es un grupo no abeliano.

(2) Sea $S = \{(x, y) : \ x, y \in \mathbb{R}\}$ el plano y considere las funciones $f, g : \mathbb{R}^2 \to \mathbb{R}^2$ definidas por $f(x, y) = (-x, y)$ y $g(x, y) = (-y, x)$ respectivamente. Observemos que f es la reflexión con respecto al eje y y g es la rotación de $90^{\underline{o}}$ en sentido contrario a las manecillas del reloj con respecto al origen. Definimos el conjunto $G = \{f^i g^j : \ i = 0, 1; \ j = 0, 1, 2, 3\}$ y $\circ$ es la composición usual de funciones. Por lo tanto, $\langle G, \circ \rangle$ es un grupo no abeliano de orden 8.

(3) Sea $GL_2(\mathbb{R})$ el conjunto de todas la matrices cuadradas de orden 2 que son invertibles. Esto es, todas las matrices de la forma

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con $a, b, c, d \in \mathbb{R}$ tal que $ad - bc \neq 0$. Entonces, $GL_2(\mathbb{R})$ con el producto usual de matrices es un grupo no abeliano, llamado el **grupo lineal general de grado** 2. ■

Antes de continuar con el estudio de grupos y sus propiedades veamos dos ejemplos más de grupo que merecen una atención especial.

Ejemplo 1.1.5 (Grupos Dihedrales)**.** Tomemos en $\mathbb{C}$ el círculo unidad (el círculo centrado en el origen y radio 1) $U = \{z \in \mathbb{C} : \ |z| = 1\} = \{z = e^{i\alpha} : \ \alpha \in \mathbb{R}\}$. Para cada argumento α, vamos a denotar el complejo $z \in U$ con argumento α por z_α, esto es, $z_\alpha = e^{i\alpha}$. Por propiedades usuales del producto de complejos tenemos que

$$z_\alpha z_\beta = z_{\alpha+\beta} \quad \text{y} \quad z_\alpha^{-1} = z_{-\alpha}.$$

Luego, tenemos que U es cerrado bajo el producto usual de números complejos.

La rotación en un ángulo α del círculo unidad es la función $R_\alpha \colon U \to U$ definida simplemente por

$$R_\alpha(z_\beta) = z_{\alpha+\beta}$$

para cada $z_\beta \in U$. Además, se cumple que $R_{\alpha+2k\pi} = R_\alpha$ para todo $k \in \mathbb{Z}$. Si L_α es la recta que pasa por 0 y el punto $z_\alpha \in U$, entonces la simetría con respecto a la recta L_α es la función $S_\alpha \colon U \to U$ definida por

$$S_\alpha(z_\beta) = z_{2\alpha-\beta} = z_{2\alpha}(z_\beta)^{-1}$$

para cada $z_\beta \in U$. Además, $S_{\alpha+\pi}(z_\beta) = z_{2\alpha+2\pi-\beta} = z_{2\alpha-\beta} = S_\alpha(z_\beta)$, esto es, $S_{\alpha+\pi} = S_\alpha$. Luego, podemos considerar el conjunto

$$D = \{R_\alpha, S_\beta : \ 0 \leq \alpha < 2\pi \text{ y } 0 \leq \beta < \pi\}$$

de todas las rotaciones y simetrías del círculo unidad. Sea $\circ$ la composición usual de funciones y sean $0 \leq \alpha, \alpha_1, \alpha_2 < 2\pi$ y $0 \leq \beta, \beta_1, \beta_2 < \pi$. Entonces, no es difícil verificar que

$$\begin{aligned} R_{\alpha_1} \circ R_{\alpha_2} &= R_{\alpha_1+\alpha_2} \\ R_\alpha \circ S_\beta &= S_{\beta+\frac{\alpha}{2}} \\ S_\beta \circ R_\alpha &= S_{\beta-\frac{\alpha}{2}} \\ S_{\beta_1} \circ S_{\beta_2} &= S_{2(\beta_1-\beta_2)}. \end{aligned}$$

También tenemos que $R_0 = \mathrm{id}_U \in D$ y las funciones inversas de R_α y S_β son $R_{-\alpha}$ y S_β. Por lo tanto $\langle D, \circ\rangle$ es un grupo.

Consideremos ahora el grupo U_n de las raíces n-esimas de la unidad con $n > 2$. Entonces como ya sabemos U_n es un polígono regular de n lados centrado en el origen y con n ejes de simetría. Sea D_n el subconjunto de D formado por todas las rotaciones y simetrías Δ tales que $\Delta(U_n) = U_n$. De una manera similar al caso de D, se puede comprobar que D_n con $\circ$ es un grupo. Además, un simple análisis muestra que las rotaciones en D_n son de la forma $R_{\frac{2k\pi}{n}}$ con $k = 0, 1, 2, \ldots, n-1$ y las simetrías en D_n corresponden a los n ejes de simetría de U_n. Entonces, $o(D_n) = 2n$ y el grupo D_n es llamado el **n-ésimo grupo Dihedral**. Este es otro ejemplo de grupo no abeliano (¿podría mostrar un ejemplo donde no se cumple la ley conmutativa?). Observe que si $R = R_{\frac{2\pi}{n}}$ (rotación de ángulo $\frac{2\pi}{n}$) y $S = S_0$ (simetría respecto del eje x) entonces para cada $z_\beta \in U$, $(S \circ R \circ S)(z_\beta) = S(R(S(z_\beta)) = S(R(z_{-\beta})) = S(z_{-\beta+\frac{2\pi}{n}}) = z_{\beta-\frac{2\pi}{n}} = R^{-1}(z_\beta)$,

.	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Cuadro 1.1: El grupo $\mathcal{Q}_8$.

Esto es, $S \circ R \circ S = R^{-1}$. Por otra parte, como $R^i(z_\beta) = z_{\beta + \frac{2i\pi}{n}} = R_{\frac{2i\pi}{n}}(z_\beta)$, $R^0, R^1, R^2, \ldots, R^{n-1}$ son las n rotaciones distintas de D_n. Dado que $(R^i \circ S)(z_\beta) = z_{-\beta + \frac{2i\pi}{n}} = S_{\frac{i\pi}{n}}(z_\beta)$, entonces las composiciones $R^i \circ S$ con $0 \leq i < n$ son n simetrías distintas de D_n y por lo tanto son todas las simetrías de D_n. Luego,

$$D_n = \{R^0, R^1, R^2, \ldots, R^{n-1}, S, R \circ S, R^2 \circ S, \ldots, R^{n-1} \circ S\}. \quad \blacksquare$$

Ejemplo 1.1.6 (Grupos Cuaterniones)**.** El **grupo de cuaterniones**, $\mathcal{Q}_8$, es definido por

$$\mathcal{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

con el producto . definido por medio del Cuadro 1.1.

El único punto tedioso para probar que $\langle \mathcal{Q}_8, . \rangle$ es un grupo, es chequear la ley asociativa, las restantes leyes se prueban sin dificultad. Para esto podemos realizar la siguiente identificación. Consideremos en $M_2(\mathbb{C})$ las siguientes cuatro matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad k = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$$

Luego, se puede comprobar que el producto de estas matrices corresponde exactamente con el producto dado en el Cuadro 1.1. Entonces, como ya sabemos que el producto de matrices es asociativo, podemos concluir que el producto . en $\mathcal{Q}_8$ es asociativo y por lo tanto $\mathcal{Q}_8$ es un grupo. $\blacksquare$

Terminamos esta sección mostrando algunas propiedades básicas y sencillas que cumplen los grupos en general. Dejamos las demostraciones a cargo del lector.

Proposición 1.1.7. *Sea G un grupo. Entonces,*

(1) *El elemento neutro e de G es único.*

(2) *Cada elemento $a \in G$ tiene un único inverso $a^{-1} \in G$.*

(3) *Si* $a \in G$, *entonces* $(a^{-1})^{-1} = a$.

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

Proposición 1.1.8. *Sea* G *un grupo y sean* $a, b, c \in G$. *Entonces,*

(1) *Si* $ab = ac$, *entonces* $b = c$.

(2) *Si* $ba = ca$, *entonces* $b = c$.

Sea G un grupo. Vamos a definir qué se entiende por a^n con $a \in G$ y $n \in \mathbb{Z}$. Para cada $a \in G$ y cada entero no negativo n, se define la potencia n-ésima de a por

$$\begin{cases} a^0 = e \\ a^n = a^{n-1} * a \quad \text{para cada } n \geq 1. \end{cases}$$

Y dado n un entero positivo se define

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

Compruebe que las reglas usuales de exponentes se satisfacen: para cualesquiera m y n enteros

(P1) $a^m * a^n = a^{m+n}$;

(P2) $(a^n)^{-1} = a^{-n}$;

(P3) $(a^{-1})^n = a^{-n}$;

(P4) $(a^m)^n = a^{mn}$;

Si G es un grupo abeliano, la definición anterior se expresa como sigue. Para cada $a \in G$ y cada entero no negativo n:

$$\begin{cases} 0.a = e \\ n.a = (n-1).a + a \quad \text{para cada } n \geq 1 \end{cases}$$

y para cada entero positivo n

$$(-n).a = n.(-a).$$

Observe que en la última ecuación $-n$ es el opuesto del entero (positivo) n en $\mathbb{Z}$ y $-a$ es el opuesto del elemento a en el grupo G.

1.2. Subgrupos

Definición 1.2.1. Sea G un grupo. Un subconjunto H de G es dicho a ser un **subgrupo** de G si cumple las siguientes condiciones:

(1) $e \in H$, esto es, el elemento neutro de G pertenece a H;

(2) si $a, b \in H$, entonces $ab \in H$;

(3) si $a \in H$, entonces $a^{-1} \in H$.

Escribiremos $H \leq G$ para indicar que H es un subgrupo de G.

Para cada grupo G existen dos subgrupos especiales llamados los **subgrupos triviales** y ellos son: G y $\{e\}$. Diremos que un subgrupo H de un grupo G es **propio** si $H \neq G$. Dado que todo subgrupo H de G debe contener al elemento neutro de G, resulta sencillo en algunos casos identificar cuales subconjuntos de G no pueden ser subgrupos. Es decir, si $A \subseteq G$ tal que $e \notin A$, entonces A no puede ser un subgrupo de G.

Proposición 1.2.2. *Sea G un grupo y H un subconjunto no vacío de G. H es un subgrupo de G si y sólo si para cualesquiera $a, b \in H$, $ab^{-1} \in H$.*

Ejemplo 1.2.3.

(1) $\mathbb{Z}$ es un subgrupo de $\mathbb{Q}$ y $\mathbb{Q}$ es un subgrupo de $\mathbb{R}$, con la operación suma.

(2) Sea $G = \mathbb{Q} \setminus \{0\}$ el grupo con la multiplicación usual. Entonces, $H = \{u^2 : u \in \mathbb{Q} \setminus \{0\}\}$ es un subgrupo de G.

(3) Sea G un grupo.

(a) Sea $a \in G$. Entonces, por las propiedades de los exponentes, tenemos que $A = \{a^n : n \text{ es un entero}\}$ es un subgrupo de G, llamado el **subgrupo cíclico de G generado por** a y es denotado por $\langle a \rangle$.

(b) Sea $a \in G$ y sea $Z(a) = \{x \in G : \ xa = ax\}$. Luego, $Z(a)$ es un subgrupo de G.

(c) Sea H un subgrupo de G y $a \in G$. Definimos

$$a^{-1}Ha = \{a^{-1}ha : \ h \in H\}.$$

Veamos que $a^{-1}Ha$ es un subgrupo de G usando la caracterización de la Proposición 1.2.2. Sean $x, y \in a^{-1}Ha$. Así, existen $h_1, h_2 \in H$ tal que $x = a^{-1}h_1a$ e $y = a^{-1}h_2a$. Entonces, $xy^{-1} = (a^{-1}h_1a)(a^{-1}h_2a)^{-1} = (a^{-1}h_1a)(a^{-1}h_2^{-1}a) = a^{-1}(h_1h_2^{-1})a$. Dado que $h_1, h_2 \in H$ y H es un subgrupo de G, tenemos que $h := h_1h_2^{-1} \in H$. En consecuencia, $xy^{-1} = a^{-1}ha \in a^{-1}Ha$. Por lo tanto, $a^{-1}Ha$ es un subgrupo de G.

(4) El n-enésimo grupo dihedral $\langle D_n, \circ \rangle$ es un subgrupo de $\langle D, \circ \rangle$ (véase en pag. 3). ■

Proposición 1.2.4. *Sea G un grupo y sean H_1 y H_2 dos subgrupos de G. Entonces, $H_1 \cap H_2$ es un subgrupo de G.*

Demostración. Sean H_1 y H_2 dos subgrupos del grupo G. Notemos primero que $e \in H_1 \cap H_2$, ya que H_1 y H_2 son subgrupos. Sean $a, b \in H_1 \cap H_2$. Esto es, $a, b \in H_1$ y $a, b \in H_2$. Entonces, como H_1 y H_2 son subgrupos, $ab^{-1} \in H_1$ y $ab^{-1} \in H_2$. Luego, $ab^{-1} \in H_1 \cap H_2$. Por lo tanto, $H_1 \cap H_2$ es un subgrupo de G. ■

1.3. Subgrupos generados

Para describir un subgrupo a veces no es necesario especificar todos sus elementos. Será suficiente indicar ciertos elementos claves del subgrupo para tener un descripción completa del subgrupo. Por ejemplo, si H es el subgrupo de números pares del grupo aditivo $\langle \mathbb{Z}, + \rangle$, entonces podemos representar cada elemento de H usando el elemento $2 \in H$. En efecto, si $k \in H$, entonces podemos escribir $k = 2n$ para un $n \in \mathbb{Z}$ y además cada número de la forma $2n$ con $n \in \mathbb{Z}$ pertenece a H. Esto es, $H = \{2n : n \in \mathbb{Z}\}$ y así tenemos generado el subgrupo H usando el elemento 2. También, hemos visto en la página 4 que el n-enésimo grupo dihedral D_n puede ser construido usando solo la rotación $R_{\frac{2\pi}{n}}$ y la simetría S_0.

La siguiente proposición es una generalización de la Proposición 1.2.4 y dejamos la demostración a cargo del lector.

Proposición 1.3.1. *Sea G un grupo y sea $\{H_i\}_{i \in I}$ una familia de subgrupos de G. Entonces, $\bigcap_{i \in I} H_i$ es un subgrupo de G.*

Consideremos un grupo G y $A \subseteq G$. Por la proposición anterior podemos concluir que

$$\langle A \rangle := \bigcap \{H : \ H \text{ es un subgrupo de } G \text{ y } A \subseteq H\} \tag{1.1}$$

es un subgrupo de G. Note que siempre hay un subgrupo de G que contiene a A, de hecho es el mismo G. El subgrupo $\langle A \rangle$ es llamado el **subgrupo generado por** A. Si $H = \langle A \rangle$ diremos que A **genera** H o que A es un **conjunto generador para** H. Cuando A es finito, digamos $A = \{a_1, \ldots, a_n\}$, denotaremos $\langle A \rangle = \langle a_1, \ldots, a_n \rangle$. Si $G = \langle a_1, \ldots, a_n \rangle$, diremos que G es un grupo **finitamente generado**.

Proposición 1.3.2. *Sea G un grupo y A un subconjunto de G. Entonces, $\langle A \rangle$ es el menor subgrupo de G que contiene a A. Esto es,*

(1) *$\langle A \rangle$ es un subgrupo de G;*

(2) *$A \subseteq \langle A \rangle$;*

(3) *si H es un subgrupo de G tal que $A \subseteq H$, entonces $\langle A \rangle \subseteq H$.*

Demostración. Sea G un grupo y $A \subseteq G$. Es claro de (1.1) que $A \subseteq \langle A \rangle$. Para probar 2, sea H un subgrupo de G tal que $A \subseteq H$. Entonces, por (1.1) de nuevo, tenemos que $\langle A \rangle \subseteq H$. ■

La proposición anterior es muy útil para demostrar que un subgrupo H es generado por un conjunto A. Es decir, si H es un subgrupo de G y queremos probar que es generado por un conjunto A es suficiente con probar que:

(i) $A \subseteq H$;

(ii) si H' es un subgrupo de G tal que $A \subseteq H'$, entonces $H \subseteq H'$.

Observación 1.3.3.

(1) Sea G un grupo. Entonces $\langle\emptyset\rangle = \{e\}$.

(2) Si H es un subgrupo de un grupo G, entonces $\langle H\rangle = H$.

(3) Sea H un subgrupo de un grupo G. Para probar que $\langle A\rangle \subseteq H$ es suficiente mostrar que $A \subseteq H$.

Ejemplo 1.3.4.

(1) Consideremos el grupo aditivo $\mathbb{Z}$. Entonces $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$.

(2) Sea G un grupo y $a \in G$. Entonces el subgrupo cíclico $\langle a\rangle$, es el subgrupo generado por a. ■

Proposición 1.3.5. *Sea G un grupo y sea $A \subseteq G$ no vacío. Entonces,*

$$\langle A\rangle = \{a_1^{k_1}a_2^{k_2}\dots a_n^{k_n} :\ n \in \mathbb{N},\ a_1,\dots,a_n \in A \text{ y } k_1,\dots,k_n \in \mathbb{Z}\}.$$

Esta proposición nos dice que un elemento está en el subgrupo generado por A si y sólo si es un producto de potencias de elementos o de inversos de elementos de A.

Demostración. Escribimos

$$H := \{a_1^{k_1}a_2^{k_2}\dots a_n^{k_n} :\ n \in \mathbb{N},\ a_1,\dots,a_n \in A \text{ y } k_1,\dots,k_n \in \mathbb{Z}\}.$$

Vamos a probar que H es el menor subgrupo de G que contiene a A. Veamos primero que es un subgrupo. Como A es no vacío, sea $a \in A$. Entonces $e = a^0 \in H$. Ahora sean $x, y \in H$. Entonces, $x = a_1^{k_1}a_2^{k_2}\dots a_n^{k_n}$ e $y = b_1^{l_1}b_2^{l_2}\dots b_m^{l_m}$ donde $n, m \in \mathbb{N}$, $a_1,\dots,a_n, b_1,\dots,b_m \in A$ y $k_1,\dots,k_n, l_1,\dots,l_m \in \mathbb{Z}$. Así,

$$xy = (a_1^{k_1}a_2^{k_2}\dots a_n^{k_n})(b_1^{l_1}b_2^{l_2}\dots b_m^{l_m}).$$

Por asociatividad nos queda que

$$xy = a_1^{k_1}a_2^{k_2}\dots a_n^{k_n}b_1^{l_1}b_2^{l_2}\dots b_m^{l_m} \in H.$$

Ahora, $x^{-1} = (a_1^{k_1}a_2^{k_2}\dots a_n^{k_n})^{-1} = (a_n^{k_n})^{-1}\dots(a_1^{k_1})^{-1} = a_n^{-k_n}\dots a_1^{-k_1} \in H$. Por lo tanto, H es un subgrupo de G. Sea $a \in A$. Entonces, $a = a^1 \in H$. En consecuencia, $A \subseteq H$. Ahora sea H' un subgrupo de G tal que $A \subseteq H'$. Queremos probar que $H \subseteq H'$. Sea $x = a_1^{k_1}a_2^{k_2}\dots a_n^{k_n} \in H$. Entonces, $a_1,\dots,a_n \in A$. Como $A \subseteq H'$, $a_1,\dots,a_n \in H'$. Dado que H' es un subgrupo, $x = a_1^{k_1}a_2^{k_2}\dots a_n^{k_n} \in H'$. Con lo cual $H \subseteq H'$. Por lo tanto, de la Proposición 1.3.2, $\langle A\rangle = H$. ■

Corolario 1.3.6. *Sea G un grupo abeliano y $a_1,\dots,a_n \in G$. Entonces,*

$$\langle a_1,\dots,a_n\rangle = \{k_1.a_1 + \dots + k_n.a_n :\ k_1,\dots,k_n \in \mathbb{Z}\}.$$

Ejemplo 1.3.7. Por el Ejemplo 1.1.5 tenemos que el n-ésimo grupo dihedral es

$$D_n = \{R^0, R^1, R^2,\dots, R^{n-1}, S, R\circ S, R^2\circ S,\dots, R^{n-1}\circ S\}.$$

Así podemos observar que todo elemento de D_n es el producto de potencias de R y S. Entonces D_n es generado por R y S. ■

1.4. Congruencias de Enteros

En esta breve sección presentaremos algunos ejemplos de grupos, los cuales serán importantes a lo largo del libro para ejemplificar ciertos conceptos. Además, estos grupos serán de utilidad para dar contraejemplos de algunas afirmaciones.

Sea n un entero positivo. Dos enteros a y b se dicen **congruentes módulo** n, denotado por $a \equiv_n b$, si y sólo si $n | a - b$. En otras palabras,

$$a \equiv_n b \Longleftrightarrow (\exists q \in \mathbb{Z})(a - b = nq).$$

El siguiente resultado es una caracterización de la congruencia módulo n que resulta de utilidad en muchas situaciones.

Proposición 1.4.1. *Sea n un entero positivo y sean $a, b \in \mathbb{Z}$. Entonces, $a \equiv_n b$ si y sólo si a y b tienen el mismo resto cuando son divididos por n.*

No es difícil mostrar que la relación $\equiv_n$ es de equivalencia sobre los enteros. Esto es, $\equiv_n$ es reflexiva, simétrica y transitiva. Así, para cada entero a se define la clase de equivalencia de a por $[a] := \{m \in \mathbb{Z} : \ m \equiv_n a\}$, y $\mathbb{Z}_n := \mathbb{Z}/ \equiv_n$ siendo el conjunto de las clases de equivalencias. Recuerde que cada entero pertenece exactamente a una clase de equivalencia. Entonces, por la proposición anterior, los elementos de $\mathbb{Z}_n$ pueden ser representados por los restos posibles de dividir por n,

$$\begin{array}{rcl} [0] & = & \{m \in \mathbb{Z} : \ m \equiv_n 0\} \\ [1] & = & \{m \in \mathbb{Z} : \ m \equiv_n 1\} \\ [2] & = & \{m \in \mathbb{Z} : \ m \equiv_n 2\} \\ \vdots & \vdots & \vdots \\ [n-1] & = & \{m \in \mathbb{Z} : \ m \equiv_n n-1\}. \end{array}$$

Para simplificar un poco la notación en el trabajo con enteros módulo n, denotaremos también a la clase de equivalencia de un entero a por $\overline{a}$. Así, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ y lo llamaremos **conjunto de enteros módulo** n.

La siguiente proposición nos muestra que la relación congruencia módulo n se comporta bien con las operaciones de suma y producto de enteros. Además, bajo cierta condición hay una ley de cancelación.

Proposición 1.4.2. *Sea n un entero positivo.*

(1) *Si $a \equiv_n b$ y $c \equiv_n d$, entonces*

$$a + c \equiv_n b + d \quad y \quad ac \equiv_n bd.$$

(2) *Si $ab \equiv_n ac$ y a es relativamente primo a n, entonces $b \equiv_n c$.*

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Cuadro 1.2: Tablas de suma y multiplicación para $\mathbb{Z}_5$

Demostración. (1) Es un buen ejercicio para que realice el lector. Probemos (2). Ya que a es relativamente primo a n, existen enteros x e y tales que $1 = ax + ny$. Así, $1 \equiv_n ax$. Luego, por (1) tenemos que $b \equiv_n abx$ y $c \equiv_n acx$. También, ya que $ab \equiv_n ac$ y por (1) nuevamente, $abx \equiv_n acx$. Entonces, por simetría y transitividad obtenemos que $b \equiv_n c$. ■

Sea n un entero positivo. Ahora podemos dotar al conjunto $\mathbb{Z}_n$ con dos operaciones, suma y multiplicación. Sean $a, b \in \mathbb{Z}$. Definimos

$$\overline{a} + \overline{b} := \overline{a+b} \quad \text{y} \quad \overline{a}.\overline{b} := \overline{ab}. \tag{1.2}$$

Observemos que las definiciones de las operaciones suma $+$ y producto $\cdot$ que recién definimos sobre $\mathbb{Z}_n$ dependen de los representantes que elijamos para cada clase. Por ejemplo, pensemos en $\mathbb{Z}_5$. Tenemos que

$$\overline{3} = \overline{8} \quad \text{y} \quad \overline{2} = \overline{12}$$

entonces debería pasar que $\overline{3} + \overline{2} = \overline{8} + \overline{12}$. Lo cual, haciendo las cuentas, es verdad porque $\overline{3} + \overline{2} = \overline{0} = \overline{8} + \overline{12}$. Se debe probar que esto vale siempre. Esto significa que las operaciones están bien definidas. La proposición anterior nos permite probar que ambas operaciones, suma y multiplicación, en $\mathbb{Z}_n$ están bien definidas. Esto es,

$$\text{si } \overline{a} = \overline{a'} \text{ y } \overline{b} = \overline{b'}, \text{ entonces } \overline{a} + \overline{b} = \overline{a'} + \overline{b'} \text{ y } \overline{a}.\overline{b} = \overline{a'}.\overline{b'}.$$

En las tablas del Cuadro 1.2 se muestran las operaciones de suma y multiplicación en $\mathbb{Z}_5$. Las siguientes dos proposiciones son consecuencias inmediatas de las propiedades conocidas de los números enteros.

Proposición 1.4.3. *Sea n un entero positivo. Entonces, $\langle \mathbb{Z}_n, + \rangle$ es un grupo abeliano.*

Demostración. A cargo del lector. ■

Proposición 1.4.4. *Sea n un entero positivo. Entonces, la multiplicación para $\mathbb{Z}_n$ es asociativa, conmutativa y $\overline{1}$ es el elemento neutro.*

Demostración. A cargo del lector. ■

Observe que en $\mathbb{Z}_n$ el $\overline{0}$ no tiene inverso multiplicativo. También pueden existir otros elementos en $\mathbb{Z}_n$ que no posean inverso multiplicativo. Por ejemplo, en $\mathbb{Z}_4$ el $\overline{2}$ no tiene inverso multiplicativo. Así, nos surge la siguiente pregunta:¿cuándo un elemento de $\mathbb{Z}_n$ tiene un inverso multiplicativo? La siguiente proposición responde a esta pregunta.

Proposición 1.4.5. *Sea n un entero positivo y sea $a \in \mathbb{Z}$. Entonces, $\overline{a}$ tiene un inverso multiplicativo en $\mathbb{Z}_n$ si y sólo si a y n son relativamente primos.*

Demostración. Sea n un entero positivo y sea $a \in \mathbb{Z}$. Entonces,

$$\begin{aligned} \overline{a} \text{ tiene un inverso multiplicativo} &\iff \text{existe } \overline{b} \in \mathbb{Z}_n \text{ tal que } \overline{a}.\overline{b} = \overline{1} \\ &\iff \text{existe } \overline{b} \in \mathbb{Z}_n \text{ tal que } \overline{ab} = \overline{1} \\ &\iff ab \equiv_n 1 \\ &\iff ab - 1 = nq \text{ para algún } q \in \mathbb{Z} \\ &\iff 1 = ab - nq \text{ para algún } q \in \mathbb{Z} \\ &\iff a \text{ es relativamente primo a } n. \quad \blacksquare \end{aligned}$$

Observación 1.4.6. Se puede observar de la demostración anterior cómo puede obtenerse el inverso multiplicativo de un elemento $\overline{a}$ en $\mathbb{Z}_n$. Dado a un entero relativamente primo a n, por el Algoritmo de Euclides, se pueden hallar enteros x e y tales que $1 = ax + ny$. Entonces,

$$\overline{1} = \overline{ax + ny} = \overline{a}.\overline{x} + \overline{n}.\overline{y} = \overline{a}.\overline{x} + \overline{0}.\overline{y} = \overline{a}.\overline{x}.$$

Por lo tanto, $\overline{x}$ es el inverso de $\overline{a}$ en $\mathbb{Z}_n$.

Denotaremos por $U(\mathbb{Z}_n)$ al conjunto de todos los elementos de $\mathbb{Z}_n$ que tienen un inverso multiplicativo y llamaremos a sus elementos **unidades**.

Corolario 1.4.7. *Para cada entero positivo primo p, tenemos que $U(\mathbb{Z}_p) = \mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$.*

El conjunto $U(\mathbb{Z}_n)$ es cerrado bajo la multiplicación . definida en (1.2). En efecto, sean $\overline{a}, \overline{b} \in U(\mathbb{Z}_n)$ con $0 < a, b < n$. Por la proposición anterior, a y b son ambos relativamente primos a n. Entonces, ab es relativamente primo a n. Por lo tanto, $\overline{a}.\overline{b} \in U(\mathbb{Z}_n)$. Con lo cual, tenemos ahora que $U(\mathbb{Z}_n)$ es un conjunto con una operación binaria. Como $U(\mathbb{Z}_n) \subseteq \mathbb{Z}_n$, y ya sabemos que la operación producto en $\mathbb{Z}_n$ es asociativa y conmutativa, entonces el producto también es asociativo y conmutativo en $U(\mathbb{Z}_n)$. Además, es claro que el neutro multiplicativo $\overline{1} \in U(\mathbb{Z}_n)$. Por lo tanto, podemos concluir lo siguiente:

Proposición 1.4.8. *Para cada entero positivo n, $\langle U(\mathbb{Z}_n), .\rangle$, donde . es la multiplicación heredada de $\mathbb{Z}_n$, es un grupo abeliano.*

Ejemplo 1.4.9. Consideremos $\mathbb{Z}_5$. Entonces, $U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. El producto de los elementos de $U(\mathbb{Z}_n)$ es mostrado en el Cuadro 1.3. $\blacksquare$

La φ-**función Euler** es una función $\varphi\colon \mathbb{N} \to \mathbb{N}$ definida de la siguiente manera:

- $\varphi(1) = 1$
- para $n > 1$, $\varphi(n)$ es el número de enteros positivos menores que n que son relativamente primos a n. En otras palabras, $\varphi(n) = \#(\{m \in \mathbb{N} : \ m < n \text{ y } (m, n) = 1\})$.

.	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Cuadro 1.3: El producto en $U(\mathbb{Z}_n)$

Proposición 1.4.10. *Para cada entero positivo $n > 1$, $\varphi(n) = \#(U(\mathbb{Z}_n))$. Además, si p es un entero primo, entonces $\varphi(p) = p - 1$.*

Las siguientes propiedades de la función φ serán probadas más adelante.

Proposición 1.4.11.

(1) *Para cada primo p y $n \in \mathbb{N}$,*

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1).$$

(2) *Si m y n son enteros positivos relativamente primos, entonces*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

(3) *Si $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\dots.p_k^{\alpha_k}$, entonces*

$$\begin{aligned}
\varphi(n) &= p_1^{\alpha_1-1}(p_1-1).\dots.p_k^{\alpha_k-1}(p_k-1)\\
&= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right).\dots.p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)\\
&= n.\left(1-\frac{1}{p_1}\right).\dots.\left(1-\frac{1}{p_k}\right).
\end{aligned}$$

Finalizamos esta sección con dos resultados importantes de la teoría de números.

Teorema 1.4.12 (Generalización de Euler del Pequeño Teorema de Fermat)**.** *Sea n un entero positivo y sea a un entero tal que $(n, a) = 1$. Entonces,*

$$a^{\varphi(n)} \equiv_n 1.$$

Demostración. Recordemos que $\varphi(n) = \#(U(\mathbb{Z}_n))$. Teniendo en cuenta la Proposición 1.4.10 podemos suponer que

$$U(\mathbb{Z}_n) = \{\overline{j_1}, \overline{j_2}, \dots, \overline{j_{\varphi(n)}}\}$$

donde cada $\overline{j_i}$ con $i = 1, 2, \dots, \varphi(n)$ es tal que $1 \leq j_i < n$ y es relativamente primo a n. Ahora definimos la función $f\colon U(\mathbb{Z}_n) \to U(\mathbb{Z}_n)$ como sigue $f(\overline{j}) = \overline{aj}$. Es directo mostrar que f está bien definida. Veamos que es inyectiva. Supongamos que $f(\overline{j}) = f(\overline{k})$. Así, $\overline{aj} = \overline{ak}$ y con lo cual, $aj \equiv_n ak$. Como a es relativamente primo a n, nos queda $j \equiv_n k$ (ver Proposición 1.4.2). Entonces, $\overline{j} = \overline{k}$. Por lo tanto, f es una función inyectiva. Ahora, como $U(\mathbb{Z}_n)$ es finito, podemos concluir que f es una biyección. Esto nos da que $\{\overline{j_1}, \overline{j_2}, \ldots, \overline{j_{\varphi(n)}}\} = \{\overline{aj_1}, \overline{aj_2}, \ldots, \overline{aj_{\varphi(n)}}\}$. Con lo cual,

$$j_1 j_2 \ldots j_{\varphi(n)} \equiv_n aj_1 aj_2 \ldots aj_{\varphi(n)} \equiv_n a^{\varphi(n)} j_1 j_2 \ldots j_{\varphi(n)}.$$

Ya que $j_1, j_2, \ldots, j_{\varphi(n)}$ son todos relativamente primos a n, obtenemos que $1 \equiv_n a^{\varphi(n)}$, como queríamos demostrar. ■

Teorema 1.4.13 (Pequeño Teorema de Fermat). *Sea a un entero no divisible por el entero primo positivo p. Entonces,*

$$a^{p-1} \equiv_p 1.$$

1.5. Grupos Simétricos

Sea S un conjunto no vacío. Denotaremos por $\mathrm{Sym}(S)$ al conjunto de todas las funciones biyectivas de S sobre S y llamaremos **permutaciones** a los elementos de $\mathrm{Sym}(S)$. El símbolo $\circ$ denota la composición usual de funciones. Como ya hemos visto en el Ejemplo 1.1.2, $\langle \mathrm{Sym}(S), \circ \rangle$ es un grupo. Llamaremos a los subgrupos de $\mathrm{Sym}(S)$ **grupos de permutaciones sobre** S. Veremos en el Capítulo 2 que de hecho todos los grupos pueden ser considerados como grupos de permutaciones sobre algún conjunto (Teorema de Cayley).

Cuando S es un conjunto finito no vacío denotamos al conjunto $\mathrm{Sym}(S)$ por S_n y llamamos al grupo permutación $\langle S_n, \circ \rangle$ el **grupo simétrico de orden** n. Si S es un conjunto finito, digamos $S = \{a_1, a_2, \ldots, a_n\}$, de n elementos lo podemos identificar, sin pérdida de generalidad como $S = \{1, 2, \ldots, n\}$[1]. Observe que S_n tiene $n!$ elementos.

A cada permutación σ de S_n la vamos expresar como

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Una de las ventajas de considerar las permutaciones en esta manera es que la composición de dos permutaciones puede ser hecha gráficamente y así de una manera más sencilla. Veamos un ejemplo. Consideremos las permutaciones σ y τ de S_3 dadas abajo

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

la composición de σ por τ puede ser entonces realizada como sigue

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

donde

$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(2) = 3$$
$$(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(1) = 1$$
$$(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(3) = 2.$$

[1] El grupo permutación $\mathrm{Sym}(S)$ depende solo de la cardinalidad de S y no de los elementos que componen a S

Ahora introducimos otra notación para representar las permutaciones de S_n. Un **k-ciclo** de S_n es una expresión de la forma $(a_1\ a_2\ \dots\ a_k)$ donde todos los a_i son distintos. Este ciclo representa la permutación de S_n que envía a_1 a a_2, a_2 a $a_3, \dots,$ envía a_{k-1} a a_k y finalmente envía a_k a a_1, mientras deja fijos todos los otros elementos en $\{1, 2, \dots, n\}$ que no aparecen en el ciclo. Por ejemplo, sea

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

en S_5. Entonces esta permutación se puede escribir como el 3-ciclo (1 2 5). Y el 4-ciclo (3 2 5 4) representa la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}.$$

El producto de dos ciclos es simplemente la composición de las permutaciones que representan. Por ejemplo, el producto de los ciclos (1 3 2 4) y (3 2 5) en S_5 es

$$(1\ 3\ 2\ 4)(3\ 2\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Observemos también que si σ es un k-ciclo $(a_1\ \dots\ a_k)$ de S_n, entonces

$$\sigma(a_1) = a_2, \quad \sigma^2(a_1) = \sigma(a_2) = a_3, \quad \sigma^3(a_1) = \sigma(a_3) = a_4, \ \dots$$
$$\dots\ \sigma^{k-1}(a_1) = a_k, \quad \sigma^k(a_1) = a_1$$

Con lo cual, la permutación σ se puede expresar como el k-ciclo

$$(a_1\ \sigma(a_1)\ \sigma^2(a_1)\ \dots\ \sigma^{k-1}(a_1)).$$

Proposición 1.5.1. *Si σ es un k-ciclo, entonces k es el menor entero positivo tal que $\sigma^k = \mathrm{id}_{S_n}$.*

Demostración. Consideremos un k-ciclo $\sigma = (a_1\ a_2\ \dots\ a_k)$ de S_n. Debemos probar que

(i) $\sigma^k = \mathrm{id}_{S_n}$ (la permutación identidad de S_n);

(ii) si $\sigma^m = \mathrm{id}_{S_n}$, entonces $k \leq m$.

Sea $x \in \{1, 2, \dots, n\}$. Si x no aparece en el k-ciclo $(a_1\ a_2\ \dots\ a_k)$, entonces $\sigma(x) = x$, lo cual implica que $\sigma^k(x) = x$. Sea a_i con $1 \leq i < k$. Entonces,

$$\begin{aligned} \sigma^k(a_i) &= \sigma^{k-1}(a_{i+1}) \\ &= \sigma^{k-(k-i)}(a_k) \\ &= \sigma^i(a_k) \\ &= \sigma^{i-1}(a_1) \\ &= \sigma^{i-2}(a_2) \\ &= \sigma^{i-(i-1)}(a_{i-1}) \\ &= \sigma(a_{i-1}) \\ &= a_i. \end{aligned} \qquad \begin{aligned} \sigma^k(a_k) &= \sigma^{k-1}(a_1) \\ &= \sigma^{k-(k-1)}(a_{k-1}) \\ &= \sigma(a_{k-1}) \\ &= a_k. \end{aligned}$$

Luego, $\sigma^k = \mathrm{id}_{S_n}$. Ahora sea m tal que $\sigma^m = \mathrm{id}_{S_n}$. Supongamos que $m < k$. Con lo cual,

$$a_1 = \sigma^k(a_1) = \sigma^{k-m+m}(a_1) = \sigma^{k-m}(\sigma^m(a_1)) = \sigma^{k-m}(a_1) = a_{k-m+1}.$$

Esto es una contradicción. Luego, $k \leq m$. ■

Corolario 1.5.2. *Sea σ un k-ciclo. Si m es un entero tal que $\sigma^m = \mathrm{id}_{S_n}$, entonces k divide a m.*

Demostración. Sea m tal que $\sigma^m = \mathrm{id}_{S_n}$. Supongamos que m no es divisible por k. Entonces $m = k.q + r$ con $0 < r < k$. Luego, $\mathrm{id}_{S_n} = \sigma^m = \sigma^{k.q+r} = (\sigma^k)^q.\sigma^r = (\mathrm{id}_{S_n})^q.\sigma^r = \sigma^r$. Esto, por la proposición anterior, contradice que k es el menor entero positivo tal que $\sigma^k = \mathrm{id}_{S_n}$. Por lo tanto, m es divisible por k. ■

Diremos que dos ciclos son **disjuntos** si no tienen números en común. Por ejemplo, en S_5, los ciclos (1 3 4) y (2 5) son disjuntos, mientras los ciclos (1 3 4) y (3 1 5 2) no son disjuntos porque tienen en común los enteros 1 y 3.

Observemos que podemos comprobar fácilmente que la siguiente permutación se puede expresar como el producto de dos ciclos disjuntos y que además el producto de estos dos ciclos disjuntos es conmutativo:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} = (1\ 5)(2\ 4\ 3) = (2\ 4\ 3)(1\ 5).$$

Ahora veremos formalmente que estos dos hechos se cumplen siempre. Esto es, probaremos que el producto de dos ciclos disjuntos es conmutativo y que cada permutación de S_n se puede escribir como producto de ciclos disjuntos.

Proposición 1.5.3. *Sean α y β dos ciclos disjuntos. Entonces, $\alpha\beta = \beta\alpha$.*

Demostración. Sean $\alpha = (a_1\ a_2\ \dots\ a_k)$ y $\beta = (b_1\ b_2\ \dots\ b_l)$ dos ciclos disjuntos de S_n. Debemos probar que para cada entero $j \in \{1, 2, \dots, n\}$, $\alpha\beta(j) = \beta\alpha(j)$. Sea primero j tal que no aparece en ninguno de los dos ciclos. Entonces, $\alpha(j) = j$ y $\beta(j) = j$. Así, $\alpha\beta(j) = \alpha(j) = j$ y $\beta\alpha(j) = \beta(j) = j$. Con lo cual $\alpha\beta(j) = \beta\alpha(j)$. Ahora, sea $a_i \in \{a_1, a_2, \dots, a_{k-1}\}$. Ahora, tenemos que $\alpha\beta(a_i) = \alpha(a_i) = a_{i+1}$ y $\beta\alpha(a_i) = \beta(a_{i+1}) = a_{i+1}$. Entonces, $\alpha\beta(a_i) = \beta\alpha(a_i)$. También, $\alpha\beta(a_k) = \alpha(a_k) = a_1$ y $\beta\alpha(a_k) = \beta(a_1) = a_1$. Por lo tanto, $\alpha\beta(j) = \beta\alpha(j)$ para todos los enteros que aparecen en el ciclo α. Similarmente, podemos probar que $\alpha\beta(j) = \beta\alpha(j)$ para todos los enteros j que aparecen en el ciclo β. Por lo tanto, hemos probado que $\alpha\beta(j) = \beta\alpha(j)$ para todo $j \in \{1, 2, \dots, n\}$. ■

Teorema 1.5.4. *Cada permutación en S_n se puede escribir como un producto de ciclos disjuntos.*

Demostración. Sea $\sigma \in S_n$. Definimos primero el ciclo $\alpha_1 = (\sigma(1)\ \sigma^2(1)\ \dots\ \sigma^{k_1}(1))$. Observe que $\sigma^{k_1}(1) = 1$ y $k_1 \leq n$. Si $k_1 = n$, entonces la permutación σ se puede escribir con el único

n-ciclo $(\sigma(1)\ \sigma^2(1)\ \dots\ \sigma^n(1))$. Si $k_1 < n$, entonces hay un $i_1 \in \{1, 2, \dots, n\}$ que no aparece en el ciclo α_1. Consideremos el ciclo

$$\alpha_2 = (\sigma(i_1)\ \sigma^2(i_1)\ \dots\ \sigma^{k_2}(i_1)).$$

Observe que $\sigma^{k_2}(i_1) = i_1$ y $k_2 \leq n - k_1$. Los dos ciclos son disjuntos. Pues, si $\sigma^l(1) = \sigma^m(i_1)$ y $l \leq m$ (similarmente si $m \leq l$), entonces $1 = \sigma^{m-l}(i_1)$ lo que implica que los dos ciclos son iguales. Esto es una contradicción pues elegimos i_1 que no estuviera en el ciclo α_1. Ahora, si $k_2 = n - k_1$, entonces la permutación σ se puede escribir como $\alpha_1\alpha_2$. Si $k_2 < n - k_1$ entonces podemos elegir un entero $i_2 \in \{1, 2, \dots, n\}$ tal que no aparezca en los ciclos α_1 y α_2. Consideramos el ciclo $\alpha_3 = (\sigma(i_2)\ \sigma^2(i_2)\ \dots\ \sigma^{k_3}(i_2))$. Podemos observar que $\sigma^{k_3}(i_2) = i_2$ y $k_3 \leq n - k_1 - k_2$. De la misma manera que vimos antes podemos probar que los ciclos α_1, α_2 y α_3 son disjuntos dos a dos. Como el conjunto $\{1, 2, \dots, n\}$ es finito en algún momento este procedimiento debe detenerse. Esto es, para algún entero positivo r, hay un $i_r \in \{1, 2, \dots, n\}$ que no aparece en los ciclos disjuntos $\alpha_1, \alpha_2, \dots, \alpha_{r-1}$ y podemos formar el ciclo $\alpha_r = (\sigma(i_r)\ \sigma^2(i_r)\ \dots\ \sigma^{k_r}(i_r))$ con $k_r = n - (k_1 + k_2 + \cdots + k_{r-1})$. Por lo tanto, la permutación σ se puede escribir como $\alpha_1\alpha_2 \dots \alpha_r$. ■

Observe que la prueba anterior no sólo da la demostración de que se puede descomponer una permutación en un producto de ciclos disjuntos sino que también nos da un procedimiento para determinar la descomposición de un ciclo.

Ejemplo 1.5.5. Consideremos el grupo simétrico S_{10} y la siguiente permutación

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

Primero formamos el ciclo

$$\alpha_1 = (\sigma(1)\ \sigma^2(1)\ \sigma^3(1)\ \sigma^4(1)) = (3\ 10\ 4\ 1).$$

Luego, elegimos un entero que no aparece en α_1, por ejemplo 2, y formamos el ciclo

$$\alpha_2 = (\sigma(2)\ \sigma^2(2)\ \sigma^3(2)) = (8\ 7\ 2).$$

Ahora, elegimos un entero que no aparezca en α_1 ni en α_2, por ejemplo el 5, y formamos el ciclo

$$\alpha_3 = (\sigma(5)) = (5).$$

Como todavía quedan enteros en $\{1, 2, 4, 5, 6, 7, 8, 9, 10\}$ que no aparecen en los ciclos anteriores continuamos de la misma manera. Tomemos un entero que no aparece en los ciclos α_1, α_2 y α_3, por ejemplo el 6, y formamos

$$\alpha_4 = (\sigma(6)\ \sigma^2(6)) = (9\ 6).$$

Ahora, podemos ver que todos los enteros de $\{1, 2, 4, 5, 6, 7, 8, 9, 10\}$ aparecen exactamente en uno de los ciclos anteriores. Entonces,

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

Proposición 1.5.6. *Sea $\sigma \in S_n$. Si σ tiene la descomposición en ciclos disjuntos $\sigma = \sigma_1\sigma_2 \dots \sigma_k$ de longitudes $m_1, m_2, \dots, m_k$, respectivamente, entonces el mínimo común múltiplo M de los números $m_1, m_2, \dots, m_k$ es el menor entero positivo tal que $\sigma^M = \mathrm{id}_{S_n}$.*

Demostración. Sea M el mínimo común múltiplo de los números $m_1, m_2, \dots, m_k$. Como los ciclos $\sigma_1, \sigma_2, \dots, \sigma_k$ son disjuntos dos a dos, tenemos que $\sigma_i\sigma_j = \sigma_j\sigma_i$ para $1 \leq i, j \leq k$. Luego

$$\sigma^M = (\sigma_1.\sigma_2.\dots.\sigma_k)^M = \sigma_1^M.\sigma_2^M.\dots.\sigma_k^M = \mathrm{id}_{S_n},$$

porque $m_i \mid M$ para cada $i \in \{1, \dots, k\}$. Por otra parte, si $\sigma^N = \mathrm{id}_{S_n}$, entonces $\sigma_1^N.\sigma_2^N.\dots.\sigma_k^N = \mathrm{id}_{S_n}$. Luego, $\sigma_i^N = \mathrm{id}_{S_n}$ para todo $i \in \{1, \dots, k\}$. Entonces, por el Corolario 1.5.2, tenemos que $m_i \mid N$ para todo $i \in \{1, \dots, k\}$. Entonces, $M \mid N$ y por lo tanto, M es el menor entero positivo tal que $\sigma^M = \mathrm{id}_{S_n}$. ∎

Finalizamos esta sección con algunos resultados referidos a permutaciones pares e impares. Una **transposición** es un 2-ciclo $(a_1\ a_2)$. Observemos que todo k-ciclo $(a_1\ a_2\ \dots\ a_k)$ de S_n se puede escribir como producto de transposiciones:

$$(a_1\ a_2\ a_3\ \dots\ a_{k-1}\ a_k) = (a_1\ a_2)(a_2\ a_3)\dots(a_{k-1}\ a_k).$$

El lector debe notar que la manera de escribir un k-ciclo como producto de transposiciones no es única. ¿Puede hallar dos formas de escribir el siguiente 4-ciclo $\sigma = (1\ 2\ 3\ 4)$ de S_5 como producto de transposiciones?

Por el Teorema 1.5.4, tenemos que cada permutación se puede representar como producto de ciclos disjuntos y como hemos observado recién, cada ciclo se puede escribir como producto de transposiciones. Por lo tanto, podemos concluir que *toda permutación de S_n se puede escribir como producto de transposiciones.*

Si bien la representación en producto de transposiciones de una permutación no es única, tenemos el siguiente resultado. Una demostración del mismo puede verse en [5, Theorem 5.4 y 5.5], [8, Theorem 3.3.1] o en [1, Section 3.5].

Proposición 1.5.7. *Toda permutación de S_n es o bien el producto de un número impar de transposiciones o bien el producto de un número par de transposiciones y ningún producto de un número par de transposiciones puede ser el producto de un número impar de transposiciones.*

Ahora podemos realizar la siguiente definición.

Definición 1.5.8. Una permitación σ de S_n es llamada **par** si es el producto de un número par de transposiciones y es llamada **impar** si es el producto de un número impar de transposiciones.

Sea A_n el conjunto de todas las permutaciones pares de S_n. Afirmamos que A_n es de hecho un subgrupo de S_n (véase el Ejercicio 1.6). A_n es llamado el **grupo alternante de grado** n.

1.6. Grupos cíclicos

Los grupos cíclicos son los grupos que pueden ser generados por un solo elemento. Al final de la sección veremos que básicamente hay solo dos tipos de grupos cíclicos: $\mathbb{Z}$ y $\mathbb{Z}_n$. En esta sección estudiaremos las propiedades de los grupos cíclicos y los subgrupos cíclicos, los cuales juegan un rol fundamental en la clasificación de todos los grupos abelianos.

Definición 1.6.1. Un grupo G es llamado **cíclico** si existe un elemento $a \in G$ tal que $G = \langle a \rangle$.

Como ya hemos visto anteriormente, si G es un grupo cíclico generado a, tenemos que

$$G = \langle a \rangle = \{a^k : \ k \in \mathbb{Z}\}.$$

Y si sabemos que G es abeliano, escribimos

$$G = \langle a \rangle = \{ka : \ k \in \mathbb{Z}\}.$$

Ejemplo 1.6.2.

1. El grupo aditivo $\mathbb{Z} = \langle 1 \rangle$ es cíclico. También, $\mathbb{Z}_n = \langle \overline{1} \rangle$ es cíclico. ■

Observación 1.6.3. No todo grupo es un grupo cíclico. Veamos el siguiente ejemplo. Sea $S = \{1, 2, 3\}$ y consideremos el grupo simétrico de orden 3, S_3. Explicitamos los elementos de S_3:

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

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

La operación $\circ$ es dada en el cuadro 1.4. Para cada elemento de S_3 generamos el subgrupo cíclico generado por ese elemento. Tenemos que

$$\begin{aligned}
\langle \rho_1 \rangle &= \{id, \rho_1, \rho_1^2\} = \{id, \rho_1, \rho_2\} \\
\langle \rho_2 \rangle &= \{id, \rho_2, \rho_2^2\} = \{id, \rho_2, \rho_1\} \\
\langle \mu_1 \rangle &= \{id, \mu_1\} \\
\langle \mu_2 \rangle &= \{id, \mu_2\} \\
\langle \mu_3 \rangle &= \{id, \mu_3\}
\end{aligned}$$

Ninguno de los anteriores es S_3, por lo tanto S_3 no es cíclico. Los subgrupos de S_3 son mostrados en la Figura 1.1. Observe que todos los subgrupos propios de S_3 son cíclicos; sin embargo, ningún elemento genera al grupo entero.

Teorema 1.6.4. *Todo grupo cíclico es abeliano.*

Teorema 1.6.5. *Cada subgrupo de un grupo cíclico es cíclico.*

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Cuadro 1.4: La operación $\circ$ en S_3

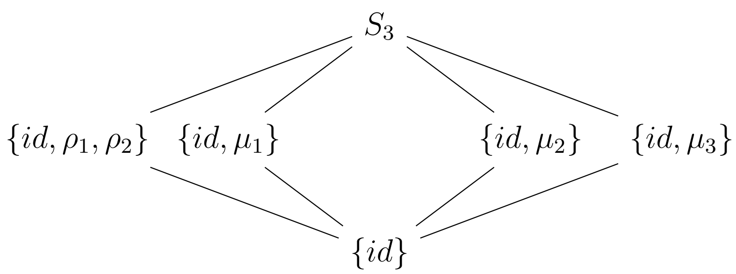

Figura 1.1: Los subgrupos de S_3

Demostración. Sea G un grupo cíclico generado por un elemento a, esto es, $G = \langle a \rangle$ y supongamos que H es un subgrupo de G. Si $H = \{e\}$, entonces claramente es cíclico. Supongamos que H contiene un elemento g distinto del neutro e. Así, $g = a^n$ para algún entero n (porque $g \in H \subseteq G = \langle a \rangle$). Podemos suponer sin perdida de generalidad que $n > 0$. Sea m el menor entero positivo tal que $a^m \in H$. Tal m existe por el Principio de Buena Ordenación. Vamos a mostrar que $h = a^m$ es un generador de H. Sea $h' \in H$. Luego, $h' \in G$ y entonces $h' = a^k$ para algún entero k. Por el algoritmo de la división, podemos encontrar enteros q y r tales que $k = mq + r$ con $0 \leq r < m$. En consecuencia, nos queda que

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

Así, $a^r = a^k h^{-q} = h' h^{-q}$. Ya que h' y h^{-q} están en H, a^r pertenece también a H. Pero, dijimos que m era el menor entero positivo tal que $a^m \in H$ y, obtuvimos que $a^r \in H$ y $0 \leq r < m$. Luego, $r = 0$ y así $k = mq$. Entonces,

$$h' = a^k = a^{mq} = h^q.$$

Por lo tanto, H es generado por h ■

Definición 1.6.6. Sea a un elemento de un grupo G. El **orden** de a, denotado por $o(a)$, es definido a ser $o(a) := \text{ínf}\{n \in \mathbb{N} : \; a^n = e\}$. En caso que el conjunto $\{n \in \mathbb{N} : \; a^n = e\}$ sea vacío, $o(a) = \infty$.

Claramente podemos ver que en cualquier grupo G, $o(e) = 1$ y e es el único elemento de orden 1.

Proposición 1.6.7. *Sea a un elemento de orden finito en un grupo.*

(1) *Si $a^n = e$ entonces $o(a)|n$.*

(2) *Si $a^i = a^j$ entonces $o(a)|i - j$.*

(3) $o(a) = o(a^{-1})$.

Demostración. Para probar (1), supongamos que $a^n = e$. Como sabemos existen $q, r \in \mathbb{Z}$ únicos tales que

$$n = o(a)q + r, \quad 0 \leq r < o(a).$$

Así, $a^r = a^{n-o(a)q} = a^n(a^{o(a)})^{-q} = e$. Como $o(a)$ es el menor entero positivo k tal que $a^k = e$, tenemos que $r = 0$. Entonces, $n = o(a)q$ y así $o(a)|n$.

El punto (2) es consecuencia de (1). Para probar (3), sea $o(a) = n$. Así, $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. Supongamos que t es un entero positivo tal que $(a^{-1})^t = e$. Con lo cual, $(a^t)^{-1} = e$ y entonces $a^t = e$. Luego, $n \leq t$. Por lo tanto, $o(a^{-1}) = n = o(a)$. ■

Proposición 1.6.8. *Sea G un grupo y $a \in G$.*

(1) *Si $o(a) = \infty$, entonces $a^i = a^j$ si y sólo si $i = j$.*

(2) *Si $o(a) = n \in \mathbb{N}$, entonces para cualquier $i \in \mathbb{Z}$, $a^i = a^k$ para un único $0 \leq k \leq n - 1$.*

Demostración. (1) Sea $a \in G$ tal que $o(a) = \infty$. Supongamos que $a^i = a^j$. Tenemos que $i \leq j$ o $j \leq i$. Si $i \leq j$, entonces $a^{j-i} = a^j(a^i)^{-1} = a^j(a^j)^{-1} = e$. Como $o(a) = \infty$, $j - i = 0$ y por lo tanto $i = j$. Similarmente si $j \leq i$. La reciproca es trivial.

(2) Supongamos que $o(a) = n \in \mathbb{N}$. Sea $i \in \mathbb{Z}$. Así, existen $q, r \in \mathbb{Z}$ tal que $i = nq + r$ con $0 \leq r \leq n - 1$. Luego,

$$a^i = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r.$$

Para ver que r es el único con tal propiedad, sea j tal que $a^i = a^j$ y $0 \leq j \leq n - 1$. Podemos suponer sin perdida de generalidad que $j \leq r$. Así, $a^r = a^i = a^j$. Por la proposición anterior tenemos que $n|r - j$ mientras $0 \leq r - j < n$. Esto implica que $r - j = 0$, esto es, $r = j$. ■

Los dos corolarios siguientes son consecuencia de las proposiciones anteriores y sus demostraciones se deja a cargo del lector.

Corolario 1.6.9. *Para cualquier elemento a en un grupo G, se cumple que:*

(1) Si $o(a) = \infty$, entonces $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$.

(2) Si $o(a) = n$, entonces $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

(3) $o(\langle a \rangle) = o(a)$.

Corolario 1.6.10. *Sea G un grupo finito.*

(1) *Un elemento a es un generador de G si y sólo si $o(a) = o(G)$.*

(2) *El grupo G es cíclico si y sólo si existe un $a \in G$ tal que $o(a) = o(G)$.*

Proposición 1.6.11. *Sea G un grupo abeliano y sean $a, b \in G$. Si $o(a)$ y $o(b)$ son relativamente primos, entonces $o(a + b) = o(a)a(b)$.*

Demostración. Llamemos $o(a) = n$ y $o(b) = m$. Así, $(n, m) = 1$ (n y m son relativamente primos). Tenemos que probar que mn es el orden del elemento $a + b$. Primero, como G es abeliano, tenemos que $mn.(a + b) = mn.a + mn.b = e + e = e$. Sea ahora t un entero positivo tal que $t.(a + b) = e$. Entonces, $t.a + t.b = e$ y así $t.a = t.(-b)$. Luego, $nt.a = nt.(-b)$. Como $n = o(a)$, $e = nt.a = nt.(-b)$. Entonces, $o(-b) \mid nt$. Ya que $o(-b) = o(b) = m$, $m \mid nt$. Y ahora, dado que m y n son relativamente primos, $m \mid t$. Análogamente, podemos obtener que $n \mid t$. Luego, como m y n son relativamente primos y $m \mid t$ y $n \mid t$, tenemos que $mn \mid t$. En consecuencia, $mn \leq t$. Por lo tanto $o(a + b) = nm = o(a)o(b)$. ∎

Proposición 1.6.12. *Sea G un grupo, y sea $a \in G$ de orden n. Entonces, para cada entero k, $o(a^k) = \dfrac{n}{mcd(n,k)}$.*

Demostración. Sea $d = mcd(n, k)$. Sean $n = \frac{n}{d}.d$ y $k = \frac{k}{d}.d$ Primero

$$\left(a^k\right)^{\frac{n}{d}} = a^{k.\frac{n}{d}} = a^{n.\frac{k}{d}} = (a^n)^{\frac{k}{d}} = e.$$

Ahora supongamos que $\left(a^k\right)^s = e$. Entonces $a^{ks} = e$. Luego $n \mid ks$. Sea $t \in \mathbb{Z}$ tal que

$$ks = nt \implies \tfrac{k}{d}ds = \tfrac{n}{d}dt \implies \tfrac{k}{d}s = \tfrac{n}{d}t.$$

Así obtenemos que $\frac{n}{d} \mid \frac{k}{d}s$. Como $mcd(n, k) = d$, tenemos que $mcd(\frac{n}{d}, \frac{k}{d}) = 1$. Con lo cual $\frac{n}{d} \mid s$. Por lo tanto, $o(a^k) = \frac{n}{d} = \dfrac{n}{(n,k)}$. ∎

Ejemplo 1.6.13. Sea $\mathbb{Z}_{30}$. Entonces podemos calcular los órdenes de cada uno de sus elementos. Por ejemplo:

$$\begin{aligned} o(\overline{4}) = o(4.\overline{1}) &= \frac{30}{mcd(30,4)} = \frac{30}{2} = 15. \\ o(\overline{18}) = o(18.\overline{1}) &= \frac{30}{mcd(30,18)} = \frac{30}{6} = 5. \\ o(\overline{21}) = o(21.\overline{1}) &= \frac{30}{mcd(30,21)} = \frac{30}{1} = 30. \quad \blacksquare \end{aligned}$$

Ejemplo 1.6.14. Sea $\mathbb{Z}_{90}$. Determinemos todos los elementos de $\mathbb{Z}_{90}$ de orden 15. Sea $\overline{a} \in \mathbb{Z}_{90}$. Entonces

$$o(\overline{a}) = o(a.\overline{1}) = \frac{90}{mcd(90,a)} = 15 \implies mcd(90, a) = 6.$$

Usando el Teorema Fundamental de la Aritmética tenemos que:

$$\begin{aligned} 90 &= 2.3^2.5 \\ a &= 2^{\alpha}.3^{\beta}.5^{\gamma} \\ 6 &= 2.3.5^0 \end{aligned} \quad \implies \quad \begin{aligned} 1 &= \min(1, \alpha) \\ 1 &= \min(2, \beta) \\ 0 &= \min(1, \gamma) \end{aligned}$$

Entonces, $\alpha \geq 1$, $\beta = 1$ y $\gamma = 0$. Entonces las posibilidades son:

$$2.3 \qquad 2^2.3 \qquad 2^3.3 \qquad 2^4.3$$

Entonces los elementos de $\mathbb{Z}_{90}$ de orden 15 son: $\overline{6}$, $\overline{12}$, $\overline{24}$, y $\overline{48}$. ■

Corolario 1.6.15. *Sea $G = \langle a \rangle$ un grupo cíclico de orden n. Entonces, $G = \langle a^k \rangle$ si y sólo si $mcd(n,k) = 1$.*

Demostración. Sea $k \in \mathbb{Z}$. Entonces,

$$\begin{aligned} G = \langle a^k \rangle &\iff o(a^k) = n \\ &\iff \frac{n}{mcd(n,k)} = n \\ &\iff mcd(n,k) = 1. \end{aligned}$$ ■

1.7. Teorema de Lagrange

En esta sección probaremos el Teorema de Lagrange, el cual afirma que el orden de todo subgrupo divide al orden del grupo, y mostraremos algunas de sus consecuencias.

Comenzamos con la siguiente construcción. Sea H un subgrupo de un grupo G. Definimos sobre G la siguiente relación binaria: para cada $a, b \in G$,

$$a \sim b \quad \text{si y sólo si} \quad ab^{-1} \in H.$$

Afirmamos que esta relación es de equivalencia sobre el grupo G. Dejamos los detalles al lector. Note que la clase de equivalencia $[a]$ de un elemento $a \in G$ es

$$Ha = \{ha : \ h \in H\}.$$

En efecto, sea $b \in [a]$. Entonces, $b \sim a$ y así, $ba^{-1} \in H$. Con lo cual, existe $h \in H$ tal que $ba^{-1} = h$. Luego, $b = ha \in Ha$. Esto prueba que $[a] \subseteq Ha$. Sea ahora $b \in Ha$. Esto es, existe $h \in H$ tal que $b = ha$. Así, $ba^{-1} = h \in H$. Entonces, $b \sim a$ y con lo cual, $b \in [a]$. Por lo tanto, $Ha \subseteq [a]$. Hemos demostrado que $[a] = Ha$.

El conjunto Ha es llamado la **clase lateral derecha** de H representada por a. Observemos que una clase lateral derecha puede estar representado por cualquiera de sus miembros.

Ejemplo 1.7.1. Considere el grupo $\mathbb{Z}_6$ y el subgrupo $H = \{\overline{0}, \overline{3}\}$ de $\mathbb{Z}_6$. Entonces, las clases laterales derechas son

$$\begin{aligned} H + \overline{0} &= \{\overline{b} \in \mathbb{Z}_6 : \ \overline{b} \sim \overline{0}\} = \{\overline{b} \in \mathbb{Z}_6 : \ \overline{b} - \overline{0} \in H\} = \{\overline{0}, \overline{3}\} = H + \overline{3} \\ H + \overline{1} &= \{\overline{b} \in \mathbb{Z}_6 : \ \overline{b} \sim \overline{1}\} = \{\overline{b} \in \mathbb{Z}_6 : \ \overline{b} - \overline{1} \in H\} = \{\overline{1}, \overline{4}\} = H + \overline{4} \\ H + \overline{2} &= \{\overline{b} \in \mathbb{Z}_6 : \ \overline{b} \sim \overline{2}\} = \{\overline{b} \in \mathbb{Z}_6 : \ \overline{b} - \overline{2} \in H\} = \{\overline{2}, \overline{5}\} = H + \overline{5}. \end{aligned}$$ ■

Como las clases laterales derechas son clases de equivalencias, ellas forman una partición del grupo. En particular, si G contiene solo un número finito de clases laterales derechas de H (particularmente cuando G es finito), entonces podemos encontrar representantes $a_1, \ldots, a_s \in G$ tales que

$$G = Ha_1 \uplus Ha_2 \uplus \cdots \uplus Ha_s.$$

Donde $\uplus$ denota la unión disjunta, esto es, $Ha_i \cap Ha_j = \emptyset$ si $i \neq j$. Llamaremos al número de clases laterales derehas distintas de H en G el **indice** de H en G, y lo denotaremos por $[G : H]$.

Ejemplo 1.7.2. Si $G = \mathbb{Z}_6$ y $H = \{\overline{0}, \overline{3}\}$, entonces por el Ejemplo 1.7.1 tenemos que $[G : H] = 3$. ■

Ejemplo 1.7.3. Sea S_3 el grupo simétrico de orden 3. Sea $\alpha = (1\ 2\ 3)$ y $\beta = (1\ 2)$. Tenemos que

$$S_3 = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\} = \{e, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}.$$

Sea $H = \langle\alpha\rangle = \{e, \alpha, \alpha^2\}$ el subgrupo generado por α. Entonces, el lector puede comprobar, calculando todas las clases laterales derechas, que

$$S_3 = H \uplus H\beta.$$

Con lo cual $[S_3 : H] = 2$. Sea $K = \langle\beta\rangle = \{e, \beta\}$. Entonces,

$$S_3 = K \uplus K\alpha \uplus K\alpha^2$$

y $[S_3 : K] = 3$. ■

Ya estamos listos para enunciar y probar el Teorema de Lagrange sobre grupos finitos. El Teorema de Lagrange asegura que el orden de un subgrupo de un grupo finito es un divisor del orden del grupo. Por ejemplo, si G es un grupo de orden 6, entonces los órdenes posibles de un subgrupo de G son 1, 2, 3 o 6.

Teorema 1.7.4 (Teorema de Lagrange)**.** *Sea G un grupo finito y sea H un subgrupo de G. Entonce, $|H|$ es un divisor de $|G|$. Además, $[G : H] = |G|/|H|$.*

Demostración. Por la discusión previa, tenemos que $G = Ha_1 \uplus Ha_2 \uplus \cdots \uplus Ha_s$ para alguna elección de representantes $a_1, \ldots, a_s \in G$. Entonces, tenemos que $|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_s|$. Ahora vamos a probar que cada clase lateral derecha Ha de H en G tiene el mismo número de elementos que H. Para esto vamos a construir una función biyectiva entre H y Ha.

Definimos $\varphi\colon H \to Ha$ por $\varphi(h) = ha$. La función φ es claramente sobreyectiva. Veamos que es inyectiva. Supongamos que $\varphi(h_1) = \varphi(h_2)$. Esto es, $h_1a = h_2a$. Por la ley de cancelación, tenemos que $h_1 = h_2$. Entonces, φ es inyectiva. Por lo tanto, φ es una biyección. Esto implica que $|H| = |Ha|$ para cada $a \in G$. Ahora, nos queda que

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_s| = s|H|.$$

Se sigue que $|H|$ es un divisor de $|G|$. Además, $[G : H] = s = |G|/|H|$. ■

Veamos algunas consecuencias inmediatas del Teorema de Lagrange. Entre ellas veremos otra manera de probar la generalización de Euler del Pequeño Teorema de Fermat.

Corolario 1.7.5. *Sean H y K subgrupos de un grupo finito G. Si $K \subseteq H \subseteq G$, entonces*

$$[G:K] = [G:H][H:K].$$

Demostración. Por el Teorema de Lagrange tenemos que

$$[G:K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}.\frac{|H|}{|K|} = [G:H][H:K]. \qquad \blacksquare$$

Corolario 1.7.6. *Sea G un grupo finito y $a \in G$. Entonces, $o(a)$ es un divisor de $|G|$ y en particular, $a^{|G|} = e$.*

Corolario 1.7.7 (La generalización de Euler del Pequeño Teorema de Fermat)**.** *Sean n y a enteros relativamente primos. Entonces, $a^{\varphi(n)} \equiv_n 1$.*

Demostración. Se sigue del hecho que el grupo $U(\mathbb{Z}_n)$ es de orden $\varphi(n)$. $\blacksquare$

Corolario 1.7.8. *Si G es un grupo de orden primo p, entonces G es cíclico.*

Demostración. Sea $x \in G$ tal que $x \neq e$. Luego, $|\langle x\rangle| > 1$. Ahora, por el Teorema de Lagrange, $|\langle x\rangle| \mid |G| = p$. Entonces, $|\langle x\rangle| = |G|$. Con lo cual, $\langle x\rangle = G$. $\blacksquare$

Es importante señalar que la recíproca del Teorema de Lagrange no es cierta. Esto es, si G es un grupo arbitrario de orden finito n y $d \mid n$, entonces no existe necesariamente un subgrupo de G de orden d. Veamos el siguiente ejemplo.

Ejemplo 1.7.9. Sea A_4 el grupo alternante de grado 4 (véase página 17). Explícitamente, observamos que

$$\begin{aligned} A_4 = \{&(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4),\\ &(1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}. \end{aligned}$$

Así vemos que el orden de A_4 es 12. El 6 es un divisor del orden de A_4, pero A_4 no posee ningún subgrupo de orden 6. En efecto, supongamos por absurdo que H es un subgrupo de A_4 de orden 6. Observemos que A_4 tiene 8 elementos de orden 3, ellos son los ocho 3-ciclos. También vemos claramente que el índice $[A_4 : H]$ es 2, esto es, A_4 tienen exactamente dos clases laterales derechas de H. Sea ahora a cualquier elemento de A_4 de orden 3. Como $[A_4 : H] = 2$ y H, Ha y Ha^2 son tres clases laterales derechas, tenemos que

$$H = Ha \quad \text{o} \quad H = Ha^2 \quad \text{o} \quad Ha = Ha^2.$$

En cualquiera de los tres casos anteriores, se tiene que $a \in H$. Hemos mostrado que H contiene los 8 elementos de A_4 de orden 3, lo cual es absurdo, pues H es de orden 6. Por lo tanto, A_4 no posee un subgrupo de orden 6. $\blacksquare$

Ahora veremos que algunas reciprocas parciales del Teorema de Lagrange son posibles.

Proposición 1.7.10. *Sea G un grupo cíclico de orden finito n. Si $d \mid n$, entonces existe un único subgrupo H_d de G de orden d.*

Demostración. Sea $G = \langle a \rangle$ de orden n y $d \mid n$. Por la Proposición 1.6.12 tenemos que elemento $a^{n/d}$ tiene orden $\dfrac{n}{mcd(n, n/d)} = \dfrac{n}{n/d} = d$. Entonces el subgrupo $H_d := \langle a^{n/d} \rangle$ tiene orden d.

Ahora, probemos que es el único subgrupo de G de orden d. Supongamos que H es un subgrupo de G de orden d. Con lo cual, $H = \langle a^k \rangle$ para algún entero positivo k. Como H es de orden d, $(a^k)^d = e$. En consecuencia, $a^{kd} = e$. Luego, $n \mid kd$, esto es, $kd = nq$ para algún entero positivo q. Entonces,

$$a^k = \left(a^{n/d}\right)^q .$$

Entonces, $a^k \in H_d$. Luego, $H \subseteq H_d$ y, como tienen mismo orden (finito), así $H = H_d$. ■

Observación 1.7.11. La proposición anterior nos permite determinar el número exacto de elementos de orden d de un grupo cíclico G. En efecto, sea $G = \langle a \rangle$ de orden n. Sea $d \mid n$. Queremos saber exactamente cuántos elementos de G tienen orden d. Por la proposición anterior sabemos que existe un único subgrupo $\langle a \rangle$ de G de orden d. Entonces, todo elemento de orden d genera a $\langle a \rangle$. Ahora por la Proposición 1.6.15, a^k genera a $\langle a \rangle$ si y sólo si $mcd(k, d) = 1$. Entonces, hay tantos elementos de orden d, como enteros positivos k menores que d tal que $mcd(k, d) = 1$. Entonces, el número de elementos de orden d es igual a $\varphi(d)$ (φ es la función de Euler, véase pag. 11).

Los siguientes teoremas importantes, que expresan una recíproca parcial del Teorema de Lagrange, serán probados en capítulos siguientes.

Teorema 1.7.12. *Si G es un grupo abeliano finito y d es un divisor del orden de G, entonces existe un subgrupo H de G de orden d.*

Teorema 1.7.13 (Teorema de Cauchy)**.** *Si G es un grupo finito y p es un primo que divide al orden de G, entonces G tiene un elemento de orden p.*

Teorema 1.7.14 (Teorema de Sylow)**.** *Si G es un grupo finito de orden $p^\alpha m$, donde p es un primo y $p \nmid m$, entonces G tiene un subgrupo de orden p^α.*

Ejercicios propuestos

Ejercicio 1.1. Sea G un grupo y sea A un subconjunto *finito no vacío* de G cerrado bajo la operación de G, esto es, si $a, b \in A$, entonces $ab \in A$. Probar que A es un subgrupo de G.

Ejercicio 1.2. Sea G un grupo y H un subgrupo de G. Probar que los siguientes son subgrupos de G.

(a) $N(H) = \{a \in G : aHa^{-1} = H\}$ ($N(H)$ es llamado el **normalizador de** H).

(b) $C(H) = \{a \in G : aha^{-1})h,\ \forall h \in H\}$ ($C(H)$ es llamado el **centralizador de** H).

Ejercicio 1.3. Sea $n \in \mathbb{N}$. Sean $\underline{a}, \underline{b}, \underline{a'}, \underline{b'} \in \mathbb{Z}_n$. Probar que si $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$, entonces $\overline{a} + \overline{b} = \overline{a'} + \overline{b'}$ y $\overline{a}.\overline{b} = \overline{a'}.\overline{b'}$.

Ejercicio 1.4. Determinar los elementos invertibles de $\mathbb{Z}_{15}$ y hallar sus inversos. (Véase el Ejercicio 1.30.)

Ejercicio 1.5. Sea $n \in \mathbb{N}$ y considerar el grupo multiplicativo $\mathrm{U}(\mathbb{Z}_n)$. Sea $d > 1$ y $d \mid n$. Probar que el conjunto $U_d(\mathbb{Z}_n) = \{\overline{a} \in \mathrm{U}(\mathbb{Z}_n) : a \equiv_d 1\}$ es un subgrupo de $\mathrm{U}(\mathbb{Z}_n)$. Para cada divisor positivo d de 12, hallar todos los subgrupos $\mathrm{U}_d(\mathbb{Z}_{12})$.

Ejercicio 1.6. Probar que el conjunto A_n de todas las permutaciones pares de S_n es de hecho un subgrupo de S_n y se cumple que $\sigma^{-1}\tau\sigma \in A_n$, para todo $\sigma \in S_n$ y todo $\tau \in A_n$.

Ejercicio 1.7. Determinar si los siguientes grupos son cíclicos o no: $\mathrm{U}(\mathbb{Z}_6)$, $\mathrm{U}(\mathbb{Z}_8)$, $\mathrm{U}(\mathbb{Z}_{10})$, y $\mathrm{U}(\mathbb{Z}_{12})$.

Ejercicio 1.8. Sea G un grupo finito y $a, b \in G$ tales que $ab = ba$. Probar que $o(ab)$ divide a $o(a) \cdot o(b)$.

Ejercicio 1.9. Hallar el grupo alternante A_4 de grado 4 (*Sug. Véase el Ejercicio 2.15 para saber cuántos elementos debe tener* A_4*.*). Determinar el orden de cada elemento de A_4. ¿Es A_4 cíclico?

Ejercicio 1.10. Determinar el orden de las siguientes permutaciones.

(a) $\sigma_1 = (2\ 1\ 5)(3\ 7)$.

(b) $\sigma_2 = (3\ 10\ 4\ 1)(8\ 7\ 2)(12\ 13)(11\ 5\ 8\ 6\ 9)$.

(c) $\sigma_3 = (a_1\ a_2\ \ldots\ a_k)$.

(d) $\sigma_4 = (a_1\ a_2)(a_3\ a_4)\ldots(a_{k-1}, a_k)$, donde $a_i \neq a_j$ para todo i y j.

Ejercicio 1.11. Sea G un grupo y $a \in G$ tal que $o(a) = 21$. Determinar los órdenes de los elementos $a^2, a^3, a^7, a^9, a^{12}, a^{15}$.

Ejercicio 1.12.

(a) Determinar el orden de los siguientes elementos de $\mathbb{Z}_{360}$: $\overline{5}$, $\overline{12}$, $\overline{30}$, $\overline{45}$, $\overline{120}$ y $\overline{358}$.

(b) Determinar todos los elementos de $\mathbb{Z}_{72}$ que tengan orden 3, 6, 8, 9, 12, 24.

(c) ¿Es posible encontrar un elemento de $\mathbb{Z}_{36}$ de orden 5? Justificar.

Ejercicio 1.13. Sea G un grupo y $a \in G$ de orden n. Probar que si $s = mcd(n, k)$, entonces $\langle a^k \rangle = \langle a^s \rangle$.

Ejercicio 1.14. Sea G un grupo y $a \in G$ tal que $o(a) = 1000$. Listar los elementos de los siguientes subgrupos: $\langle a^{30} \rangle$, $\langle a^{200} \rangle$, $\langle a^{340} \rangle$, $\langle a^{400} \rangle$ y $\langle a^{600} \rangle$.

Ejercicio 1.15. Sea G un grupo y $a \in G$ de orden n. Probar que $\langle a^i \rangle = \langle a^j \rangle$ si y sólo si $mcd(n, i) = mcd(n, j)$.

Ejercicio 1.16. Determinar todos los generadores de $\mathbb{Z}_{100}$.

Ejercicio 1.17.

(a) Hallar todos los generadores del grupo cíclico $\mathbb{Z}_{24}$.

(b) Sabiendo que $\overline{3}$ es un generador de $\mathrm{U}(\mathbb{Z}_{50})$, hallar todos los generadores de $\mathrm{U}(\mathbb{Z}_{50})$.

Ejercicio 1.18. Sea G un grupo y H un subgrupo de G. Probar que la relación binaria $\sim$ sobre G, definida por $a \sim b \iff ab^{-1} \in H$, es de equivalencia.

Ejercicio 1.19. Considere el grupo multiplicativo $U(\mathbb{Z}_{32})$ y sea $H = \langle \overline{15} \rangle$. Hallar todas las clase laterales derechas de H. Determinar el índice de H en $U(\mathbb{Z}_{32})$.

Ejercicio 1.20. Considere el grupo abeliano $\mathbb{Z}$ con la suma usual de enteros. Sea $H := \{4k : k \in \mathbb{Z}\}$. Hallar todas las clases laterales derechas de H en $\mathbb{Z}$. (*Sug. Utilice la notación aditiva, ya que $\mathbb{Z}$ es abeliano.*)

Ejercicio 1.21. Sea $G = \langle a \rangle$ un grupo cíclico de orden 15. Determinar las clases laterales derechas de $\langle a^5 \rangle$ en G. Listarlas a todas.

Ejercicio 1.22. Sea G un grupo. Sean H y K subgrupos de G. Probar que si existen elementos a y b de G tales que $aH = bK$, entonces $H = K$.

Ejercicio 1.23. Sea G un grupo, y sean H y K tales que $K \leq H \leq G$.Si $|G| = 420$ y $|K| = 42$. Determine los posibles órdenes del subgrupo H. Y si K debe ser un subgrupo propio de H, y H un subgrupo propio de G, ¿cuál o cuáles son los posibles órdenes de H?

Ejercicio 1.24. Sea G un grupo de orden pq, con p y q enteros primos distintos. Probar que todo subgrupo propio de G es cíclico. Dar un ejemplo de un grupo de orden 6 el cual no sea cíclico (a pesar que todos sus subgrupos).

Ejercicio 1.25. Sea G un grupo abeliano de orden impar. Probar que:

(a) Para todo $a \in G$, $a \neq -a$.

(b) La suma de todos los elementos de G da como resultado el neutro de G.

Ejercicio 1.26. Sea G un grupo de orden p^2, con p primo. Probar que G es cíclico o para todo $a \in G - \{e\}$ se tiene que $o(a) = p$.

Ejercicio 1.27. Sea p un entero primo. Si G un grupo que tiene exactamente un subgrupo de orden p, ¿cuál es el orden de G?.

Ejercicio 1.28.

(a) Hallar todos los subgrupos de $\mathbb{Z}_{42}$.

(b) Sea $G = \langle a \rangle$ un grupo cíclico. Hallar todos sus subgrupos.

(c) Hallar todos los subgrupos de $\mathrm{U}(\mathbb{Z}_{50})$.

Ejercicio 1.29. Dar un ejemplo de un grupo con exactamente 10 subgrupos (incluyendo los triviales). ¿Puede generalizarlo para cualquier n?

Ejercicios con GAP

Ejercicio 1.30. Para cada $n = 15, 26, 50, 100$, hallar los inversos de los elementos invertibles de $\mathbb{Z}_n$.

Ejercicio 1.31. Generar el grupo simétrico $G = S_3$ de orden 3.

(a) Use el comando `ai:=Elements(G)[i]` con `i=1,2,3,4,5,6` para obtener cada uno de los elementos del grupo `G`.

(b) Compruebe que en G no se cumple que para todos $a, b, c, d, x \in G$, si $axb = cxd$, entonces $ab = cd$.

Ejercicio 1.32. (a) Generar los grupos dihedrales D_4, D_6, D_8, D_{10} y D_{12}.

(b) Hallar un conjunto de generadores para cada uno de los grupos anteriores.

(c) Listar los elementos de D_4, D_6, D_8, D_{10} y D_{12}.

(d) Comprobar que el orden de cada uno de los grupos dihedrales D_n del inciso (a) es $2n$.

(e) Compruebe que los grupos D_4, D_6, D_8, D_{10} y D_{12} no son abelianos.

Ejercicio 1.33. (a) Generar el grupo simétrico S_5 y determinar su orden.

(b) Considerar los siguientes elementos de S_5:

$$a = (3\ 2\ 1) \qquad b = (1\ 5)(2\ 3) \qquad c = (2\ 5)(4\ 1).$$

Generar los subgrupos generados

$$\langle a \rangle \quad \langle a, b \rangle \quad \langle a, c \rangle \quad \langle b, c \rangle \quad \langle a, b, c \rangle.$$

(c) Determinar el orden de cada uno de los subgrupos del inciso anterior.

(d) ¿Qué relación encuentra entre el orden del grupo S_5 y los subgrupos del inciso (b)? Haga una conjetura y compruebe para el grupo simétrico S_6 y algunos subgrupos generados.

Ejercicio 1.34. Generar el grupo Dihedral D_{24}. Llamar `a` y `b` a los dos generadores de D_{24}.

(a) Generar los subgrupos: $H_1 = \langle a \rangle$, $H_2 = \langle a^2, b \rangle$ y $H_3 = \langle a, b^2 \rangle$.

(b) Determinar el orden de los subgrupos H_1, H_2 y H_3.

(c) Determinar si $H_1 = H_2$, $H_1 = H_3$ o $H_2 = H_3$.

(d) Determinar si H_1 y H_2 son cíclicos.

(e) Determinar si H_3 es cíclico.

Ejercicio 1.35. Utilizar la función `ulist` que se encuentra en el archivo ulist.txt.

(a) Determinar el orden (cantidad de elementos) de $U(n)$ para $n = 9, 27, 81, 243, 5, 25, 125, 625$. Haga una conjetura acerca del tamaño del grupo $U(p^k)$ siendo p un primo distinto de 2 y k un entero positivo. Compare su conjetura con (1) de la Proposición 1.4.11.

(b) Hallar el orden de $U(n)$ para $n = 18, 54, 162, 486, 50, 250, 98, 242$. Proponer una conjetura acerca de la relación entre el orden de $U(2p^k)$ y el orden de $U(p^k)$, donde p es un primo distinto de 2.

(c) Sean m y n relativamente primos. Establecer un conjetura acerca del orden de $U(m.n)$ en términos de los órdenes de $U(m)$ y $U(n)$. Luego véase la Proposición 1.6.11.

Ejercicio 1.36. Utilizar la función `ulist` para generar el grupo $U(n)$.

(a) Hallar los inversos de los elementos de $U(20)$ (véase la Observación 1.4.6).

(b) Hallar los órdenes de cada uno de los elementos de $U(20)$.

(c) ¿Es $U(20)$ cíclico? Justificar. En caso afirmativo hallar dos generados distintos.

(d) ¿Es $U(11)$ cíclico? Justificar. En caso afirmativo hallar dos generados distintos.

Ejercicio 1.37. Generar el grupo simétrico S_{36} de orden 36.

(a) Determinar el orden de las siguientes permutaciones:

  (i) $a = (2, 5, 1)(3, 7)$
  (ii) $b = (5, 2, 7, 3)(1, 4, 8, 11, 10, 6)$
  (iii) $c = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)(13, 17, 11, 19, 20, 12)$
  (iv) $d = (5, 2, 7, 3)(1, 4, 8, 11, 10, 6)(9, 12, 17, 13, 21, 30, 36, 29)$
  (v) $e = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)(13, 14, 15, 16, 17, 18, 19, 20, 21)(22, 23, 24, 25, 26, 27)$.

(b) Formular una conjetura acerca del orden de una permutación σ que puede escribirse como un producto de permutaciones disjuntas $\sigma = \sigma_1\sigma_2 \dots \sigma_k$. Compruebe su conjetura con algunos ejemplos más. Luego compare con la Proposición 1.5.6.

Ejercicio 1.38. Generar el grupo simétrico S_{36} de orden 36.

(a) Hallar un elemento a de S_{36} de orden 24.

(b) Hallar la lista de los divisores (positivos) de 24.

(c) Para cada divisor (positivo) d de 24, determinar el orden del elemento a^d.

(d) Formular una conjetura acerca del orden de un elemento a^d siendo d un divisor del orden de a. Compruebe su conjetura con otros ejemplos.

(e) Ahora hallar los órdenes de los elementos a^5, a^7, a^9, a^{10}, a^{11}, a^{13}, a^{14} y a^{15}.

(f) Formular una conjetura acerca del orden del elemento a^k, siendo k cualquier entero positivo menor que 24. Compruebe su conjetura con otros ejemplos.

Ejercicio 1.39. Utilizar la función `cyclic(n,a)`.

(a) Generar los subgrupos cíclicos de $U(100)$ generados por $a = 3, 7, 9, 21, 49$.

(b) Determinar si el grupo $U(n)$ es cíclico para $n = 3, 9, 27, 5, 25, 125, 7, 49, 343$. (*Ayuda:* Utilice el comando `Size(ulist(n))=Size(cyclic(n,a))`) para preguntarle a GAP si $U(n)$ está generado por a.) Haga una conjetura, y pruebe para otros valores de n.

(c) Determinar si el grupo $U(n)$ es cíclico para $n = 6, 18, 54, 10, 50, 250, 14, 98, 686$. Haga una conjetura.

(d) Determinar si el grupo $U(n)$ es cíclico para $n = 8, 16, 32$. Haga una conjetura.

(e) Determinar si el grupo $U(n)$ es cíclico para $n = 12, 20, 28, 44, 52, 15, 21, 33, 39, 51, 57, 69, 35, 55, 65, 85$. Haga una conjetura.

(f) Realice un resumen de sus conjeturas anteriores.

Ejercicio 1.40. Utilizar la función `orderFrequency` que se encuentra en el archivo orderFrequency.txt.

(a) Determinar la cantidad de elementos de cada orden en los grupos cíclicos de orden 4,7,10,15,30,75,100.

(b) Determinar la cantidad de elementos de cada orden en los grupos Dihedrales D_5, D_{21}, D_{33}, D_{49}. Hacer una conjetura acerca de la cantidad de elementos de orden 2 en D_n.

(c) Determinar la cantidad de elementos de cada orden en los grupos Dihedrales D_{12}, D_{24}, D_{36}, D_{50}. Hacer una conjetura acerca de la cantidad de elementos de orden 2 en D_n.

(d) Hacer una conjetura acerca de la cantidad de elementos de orden 2 en D_n para cada n.

(e) ¿Puede observar alguna relación entre los órdenes de los elementos de un grupo y el orden del grupo?

Ejercicio 1.41. Calcular el orden de los grupos $GL(2, \mathbb{Z}_p)$ y $SL(2, \mathbb{Z}_p)$ para $p = 3, 5, 7$. ¿Puede establecer una relación entre los órdenes de $GL(2, \mathbb{Z}_p)$ y $SL(2, \mathbb{Z}_p)$ junto con $p - 1$? Basados en estos ejemplos, ¿p siempre divide al orden de $SL(2, \mathbb{Z}_p)$? ¿Y qué pasa con $p - 1$ y $p + 1$? Tratar de conjeturar una fórmula para el orden de $GL(2, \mathbb{Z}_p)$ y $SL(2, \mathbb{Z}_p)$. Compruebe las fórmulas obtenidas para $p = 11, 13, 17, 19$.

Ejercicio 1.42. Generar cada uno de los siguientes grupos, y algunos de sus subgrupos. Obtenga el orden de cada grupo y de cada uno de los subgrupos generados. Formule una conjetura con respecto al orden de un grupo G y el orden de un subgrupo H de G.

(a) S_3. (b) S_4. (c) D_4. (d) D_6.

Ejercicio 1.43. (a) Generar el grupo alternante A_4 de orden 4.

(b) Determinar el orden de A_4.

(c) Determinar el orden de cada uno de sus elementos.

(d) Generar todos los subgrupos de A_4.

(e) Determinar el orden de cada uno de los subgrupos de A_4.

(f) Utilice los resultados anteriores para probar que la recíproca del Teorema de Lagrange no es cierta.

Ejercicio 1.44. (a) Generar el grupo $G = \langle a \rangle$ cíclico de orden 36.

(b) Para cada divisor d de 36, generar el único subgrupo del grupo cíclico de orden 36 (véase la Proposición 1.7.10).

(c) Generar el menor subgrupo de G conteniendo:

(i) a^6 y a^4; (ii) a^{10} y a^2; (iii) a^{12} y a^8; (iv) a^{15} y a^2; (v) a^9 y a^{12}.

(d) Determinar el orden de cada uno de los subgrupos del inciso anterior. Luego, para cada subgrupo, proponer el menor valor t tal que dicho subgrupo es $\langle a^t \rangle$.

(e) Dados s y r enteros positivos, conjeturar quien es el menor valor t tal que $\langle a^s, a^t \rangle = \langle a^t \rangle$.

Ejercicio 1.45. (a) Generar el grupo $G = \langle a \rangle$ cíclico de orden 60.

(b) Hallar el orden de cada uno de los siguientes subgrupos de G:

(i) $\langle a^4 \rangle \cap \langle a^6 \rangle$ (iii) $\langle a^{12} \rangle \cap \langle a^8 \rangle$ (v) $\langle a^9 \rangle \cap \langle a^{12} \rangle$.

(ii) $\langle a^{10} \rangle \cap \langle a^2 \rangle$ (iv) $\langle a^{15} \rangle \cap \langle a^2 \rangle$

(c) Para cada uno de los subgrupos anteriores, hallar el menor valor t tal que $\langle a^s, a^r \rangle = \langle a^t \rangle$.

(d) Formular una conjetura acerca de quien es el menor valor t para el cual $\langle a^s \rangle \cap \langle a^r \rangle = \langle a^t \rangle$. Compruebe su conjetura con otros ejemplos.

Capítulo 2

Homomorfismos y Grupo Cocientes

En este capítulo introducimos dos conceptos importantes para estudiar las estructuras de grupos y estos son la de **homomorfismos** entre grupos y la de **grupos cocientes** de un grupo. Un grupo cociente de un grupo es otra manera de obtener un grupo más "chico" a partir del grupo original y así, como con los subgrupos, la estructura de un grupo es reflejada en la estructura de sus grupos cocientes. Un homomorfismo entre dos grupos es una función que preserva las operaciones de los grupos y los vincula entre si. El estudio de grupos cocientes es esencialmente equivalente al estudio de los homomorfismos sobreyectivos.

2.1. Homomorfismos

En esta sección estudiaremos las nociones de homomorfismo e isomorfismo. El concepto de isomorfismo entre dos grupos establece que ambos grupos son "algebraicamente iguales", esto es, tienen exactamente la misma estructura de grupo. La noción de homomorfismo es más débil que la de isomorfismo pero igualmente importante dentro de la Teoría de Grupo (y dentro de cualquier teoría sobre estructuras algebraicas) como veremos a lo largo de todo el curso.

Definición 2.1.1. Sean $\langle G_1, *_1\rangle$ y $\langle G_2, *_2\rangle$ dos grupos. Una función $\varphi\colon G_1 \to G_2$ es llamada un **homomorfismo de grupo** si

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$$

para todos $a, b \in G_1$.

Ejemplo 2.1.2.

(1) Consideremos los grupos $\langle \mathbb{R}_+, .\rangle$ y $\langle \mathbb{R}, +\rangle$ de los números reales positivos con el producto usual y el conjunto de todos los números reales con la suma usual, respectivamente. Sea $\varphi\colon \mathbb{R} \to \mathbb{R}_+$ la función definida por

$$\varphi(x) = e^x.$$

Entonces, φ es un homomorfismo del grupo $\langle \mathbb{R}, +\rangle$ al grupo $\langle \mathbb{R}_+, .\rangle$. En efecto, sean $x, y \in \mathbb{R}$. Entonces,

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

(2) Sea n un entero positivo. Se define $\pi_n \colon \mathbb{Z} \to \mathbb{Z}_n$ como sigue

$$\pi_n(i) = \bar{i}.$$

Verifiquemos que es un homomorfismo. Sean i y j dos enteros. Entonces, $\pi_n(i+j) = \overline{i+j} = \bar{i} + \bar{j} = \pi_n(i) + \pi_n(j)$. Por lo tanto, π_n es un homomorfismo. Además, π_n es una función sobreyectiva.

(3) Sea $GL_2(\mathbb{R})$ el grupo lineal general de grado 2 y sea $\mathbb{R}^* = \mathbb{R} - \{0\}$ el grupo de los números reales no nulos con el producto habitual. Definimos $\varphi \colon GL_2 \to \mathbb{R}^*$ como sigue $\varphi(A) = \det(A)$. Verifique que φ es un homomorfismo. ■

Veamos algunas propiedades básicas que cumplen los homomorfismos.

Proposición 2.1.3. *Sean G_1 y G_2 dos grupos y $\varphi \colon G_1 \to G_2$ un homomorfismo.*

(1) *Sea e_1 el elemento neutro de G_1 y sea e_2 el elemento neutro de G_2. Entonces, $\varphi(e_1) = e_2$.*

(2) *Para cada elemento $a \in G_1$, $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

(3) *Para cada elemento $a \in G_1$ y cada $n \in \mathbb{Z}$, $\varphi(a^n) = \varphi(a)^n$.*

(4) *Si H_1 es un subgrupo de G_1, entonces $\varphi(H_1)$ es un subgrupo de G_2.*

(5) *Si H_2 es un subgrupo de G_2, entonces, $\varphi^{-1}(H_2)$ es un subgrupo de G_1.*

(6) *Si $a \in G_1$ es tal que $o(a) < \infty$, entonces $o(\varphi(a)) < \infty$ y $o(\varphi(a)) | o(a)$.*

Demostración. Los puntos $(1) - (3)$ son sencillos de verificar y quedan a cargo del lector. Para probar (4) sea H_1 un subgrupo de G_1. Sean $a, b \in H_1$. Debemos probar que $\varphi(a)\varphi(b)^{-1} \in \varphi(H_1)$. Por el punto (2) y del hecho que φ es un homomorfismo, tenemos que $\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$. Como H_1 es un subgrupo, $ab^{-1} \in H_1$. Entonces, $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(H_1)$. Por lo tanto, $\varphi(H_1)$ es un subgrupo de G_2. Ahora probamos (5). Sea H_2 un subgrupo de G_2. Sean $a, b \in \varphi^{-1}(H_2)$. Entonces, $\varphi(a), \varphi(b) \in H_2$. Dado que H_2 es un subgrupo, $\varphi(a)\varphi(b)^{-1} \in H_2$. Como φ es un homomorfismo, tenemos que $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1})$. Con lo cual, $ab^{-1} \in \varphi^{-1}(H_2)$. Entonces, $\varphi^{-1}(H_2)$ es un subgrupo de G_1. Siendo $o(a) = n$, la propiedad (6) es consecuencia de que $\varphi(a)^n = \varphi(a^n) = \varphi(e_1) = e_2$ y de la Proposición 1.6.7. ■

Observación 2.1.4. Sea $\varphi \colon G_1 \to G_2$ un homomorfismo. Entonces, la imagen de G_1 por φ, $\operatorname{Im}(\varphi)$ es un subgrupo de G_2.

Proposición 2.1.5. *Sea G un grupo y sea a un elemento arbitrario de G. Entonces, hay un único homomorfismo de $\mathbb{Z}$ a G que envía el 1 a a.*

Demostración. Primero probemos la existencia. Definimos la función $\varphi \colon \mathbb{Z} \to G$ como $\varphi(n) = a^n$. Es claro que esta función cumple que $\varphi(1) = a$. Veamos que es un homomorfismo. Para n y m dos enteros cualesquiera, tenemos que $\varphi(n+m) = a^{n+m} = a^n a^m = \varphi(n)\varphi(m)$. Entonces, φ es un homomorfismo. Ahora probemos que es única. Supongamos que $\psi \colon \mathbb{Z} \to G$ es un homomorfismo tal que $\psi(1) = a$. Sea $n \in \mathbb{Z}$. Entonces, $\varphi(n) = a^n = \psi(1)^n = \psi(n.1) = \psi(n)$. Por lo tanto, $\varphi = \psi$. ■

Proposición 2.1.6. *Sean G_1, G_2 y G_3 grupos y sean $\varphi\colon G_1 \to G_2$ y $\psi\colon G_2 \to G_3$ homomorfismos. Entonces, $\psi \circ \varphi\colon G_1 \to G_3$ es un homomorfismo.*

Demostración. A cargo del lector. ■

Definición 2.1.7. Sea $\varphi\colon G_1 \to G_2$ un homomorfismo. El siguiente subconjunto de G_1

$$\mathrm{Nu}(\varphi) = \{a \in G_1 : \ \varphi(a) = e_2\}$$

es llamado el **núcleo** de φ.

Proposición 2.1.8. *Si $\varphi\colon G_1 \to G_2$ es un homomorfismo, entonces $\mathrm{Nu}(\varphi)$ es un subgrupo de G_1. Además, para cada $g \in G_1$ y cada $a \in \mathrm{Nu}(\varphi)$, $gag^{-1} \in \mathrm{Nu}(\varphi)$.*

Demostración. A cargo del lector. ■

Ejemplo 2.1.9. Consideremos el homomorfismo $\pi_n\colon \mathbb{Z} \to \mathbb{Z}_n$ definido por $\pi_n(i) = \overline{i}$ (véase el Ejemplo 2.1.2). Calculemos el núcleo de π_n. Sea $i \in \mathbb{Z}$. Entonces

$$i \in \mathrm{Nu}(\pi_n) \iff \pi_n(i) = \overline{0} \iff \overline{i} = \overline{0} \iff n \mid i \iff i = nk \text{ para algún } k \in \mathbb{Z}.$$

Entonces $\mathrm{Nu}(\pi_n) = \{nk : k \in \mathbb{Z}\} = \langle n \rangle$. ■

Ejemplo 2.1.10. Sea $\mathbb{R}^* = \mathbb{R} - \{0\}$ con el producto usual de números reales. Sea $\psi\colon \mathbb{R}^* \to \mathbb{R}^*$ definida por $\psi(x) = |x|$. Usando las propiedades del valor absoluto de números reales, es sencillo probar que ψ es un homomorfismo sobreyectivo. Calculemos su núcleo: sea $x \in \mathbb{R}^*$. Teniendo en cuenta que $1 \in \mathbb{R}^*$ es el neutro, tenemos que

$$x \in \mathrm{Nu}(\psi) \iff \psi(x) = 1 \iff |x| = 1 \iff x = 1 \text{ o } x = -1.$$

Entonces, $\mathrm{Nu}(\psi) = \{-1, 1\}$. ■

Definición 2.1.11. Diremos que un homomorfismo $\varphi\colon G_1 \to G_2$ es un **monomorfismo** si φ es una función inyectiva y diremos a φ un **epimorfismo!de grupo** si φ es sobreyectiva. Un homomorfismo que es monomorfismo y epimorfismo es llamado **isomorfismo**. Si $\varphi\colon G_1 \to G_2$ es un isomorfismo diremos que G_1 es **isomorfo a** G_2 y lo denotaremos por $G_1 \cong G_2$.

Se puede probar sin dificultad que la relación "ser isomorfo a" sobre la clase de todos los grupos es una relación de equivalencia. Esto es, para cada grupo G, $G \cong G$; si $G_1 \cong G_2$, entonces $G_2 \cong G_1$ y; si $G_1 \cong G_2$ y $G_2 \cong G_3$, entonces $G_1 \cong G_3$.

Proposición 2.1.12. *Sea $G = \langle a \rangle$ un grupo cíclico.*

- *Si $o(G) = o(a) = n < \infty$, entonces $G \cong \mathbb{Z}_n$.*
- *Si $o(G) = o(a) = \infty$, entonces $G \cong \mathbb{Z}$.*

Demostración. • Supongamos que $o(a) = n$ es finito. Consideramos la aplicación $\beta\colon G \to \mathbb{Z}_n$ definida por $\beta(a^i) = \overline{i}$, para todo $i \in \mathbb{Z}$.

- β está bien definida: Como $G = \langle a \rangle$ es de orden finito, debemos probar primero que β está bien definida. Es decir, debemos probar que si $a^i = a^j$, entonces $\beta(a^i) = \beta(a^j)$. Supongamos que $a^i = a^j$. Entonces, $a^{i-j} = e$. Como $o(a) = n$, tenemos que $n \mid i - j$. Con lo cual $\bar{i} = \bar{j}$. Por lo tanto, $\beta(a^i) = \beta(a^j)$.

- β es inyectiva: Supongamos que $\beta(a^i) = \beta(a^j)$. Entonces $\bar{i} = \bar{j}$. Entonces $i - j = nq$. Ahora
$$a^i = a^{nq+j} = (a^n)^q a^j = ea^j = a^j.$$
Por lo tanto, β es inyectiva.

- β es sobreyectiva: Sea $\bar{i} \in \mathbb{Z}_n$. Entonces $\beta(a^i) = \bar{i}$.

- β es homomorfismo: Sean $a^i, a^j \in G$.
$$\beta(a^i a^j) = \beta(a^{i+j}) = \overline{i+j} = \bar{i} + \bar{j} = \beta(a^i) + \beta(a^j).$$

• Supongamos que $o(a) = \infty$. Definimos la función $\alpha\colon \mathbb{Z} \to G$ de la siguiente manera: para cada $i \in \mathbb{Z}$,
$$\alpha(i) = a^i.$$
Entonces, por la Proposición 1.6.8, podemos probar sin dificultad que α es una función biyectiva y verifica la siguiente identidad
$$\alpha(i + j) = \alpha(i)\alpha(j). \tag{2.1}$$
Por lo tanto, α es un isomorfismo. ■

La proposición anterior nos dice de alguna manera que existen, salvo isomorfismo, sólo tipos de grupos cíclicos: los finitos $\mathbb{Z}_n$, y el infinito $\mathbb{Z}$. Esto significa que si queremos probar que una propiedad algebraica se cumple para un grupo cíclico G, es suficiente con probarla para $\mathbb{Z}_n$ o $\mathbb{Z}$, según corresponda. El siguiente corolario es directo de la proposición anterior.

Corolario 2.1.13. *Dos grupos cíclicos son isomorfos syss ellos tienen el mismo orden.*

Demostración. Es claro que si dos grupos son isomorfos, entonces tienen el mismo orden. Sean G_1 y G_2 dos grupos cíclicos con el mismo orden. Si $o(G_1) = o(G_2) = \infty$, entonces por lo visto en el Ejemplo **??** tenemos que $G_1 \cong \mathbb{Z}$ y $G_2 \cong \mathbb{Z}$. Entonces $G_1 \cong G_2$. Por otro lado, si $o(G_1) = o(G_2) = n < \infty$, entonces también por Ejemplo **??** tenemos que $G_1 \cong \mathbb{Z}_n$ y $G_2 \cong \mathbb{Z}_n$. Por lo tanto $G_1 \cong G_2$. ■

Proposición 2.1.14. *Sea $\varphi\colon G_1 \to G_2$ un homomorfismo. Entonces, φ es un monomorfismo si y sólo si* $\mathrm{Nu}(\varphi) = \{e_1\}$.

Demostración. ($\Rightarrow$) Supongamos que φ es un monomorfismo. Es claro que $\{e_1\} \subseteq \mathrm{Nu}(\varphi)$. Sea $x \in \mathrm{Nu}(\varphi)$. Entonces $\varphi(x) = e_2$. Como φ es un homomorfismo, $\varphi(e_1) = e_2$. Entonces $\varphi(x) = \varphi(e_1)$. Ahora por ser φ inyectiva, tenemos que $x = e_1$. Por lo tanto, $\mathrm{Nu}(\varphi) = \{e_1\}$.

($\Leftarrow$) Supongamos que $\mathrm{Nu}(\varphi) = \{e_1\}$. Probemos que φ es inyectiva. Sean $a, b \in G_1$ y supongamos que $\varphi(a) = \varphi(b)$. Entonces, por propiedades de homomorfismo tenemos que $\varphi(ab^{-1}) = e_2$.

Con lo cual, $ab^{-1} \in \mathrm{Nu}(\varphi)$. Entonces $ab^{-1} = e_1$. Lo cual implica que $a = b$. Por lo tanto, φ es inyectiva. ■

Ejemplo 2.1.15. Suponga que queremos determinar todos los homomorfismos posibles φ de $\mathbb{Z}_7$ a $\mathbb{Z}_{12}$. Dado que el núcleo de φ es un subgrupo de $\mathbb{Z}_7$, tenemos por el Teorema de Lagrange que el orden de $\mathrm{Nu}(\varphi)$ divide al orden de $\mathbb{Z}_7$, es decir, divide a 7. Con lo cual el orden de $\mathrm{Nu}(\varphi)$ es 1 o 7. Entonces, tenemos que $\mathrm{Nu}(\varphi) = \{e\}$ o $\mathrm{Nu}(\varphi) = \mathbb{Z}_7$. Si $\mathrm{Nu}(\varphi) = \{e\}$ entonces φ es un monomorfismo y así el orden de $\mathrm{Im}(\varphi)$ es 7. Como $\mathrm{Im}(\varphi)$ es un subgrupo de $\mathbb{Z}_{12}$, nos queda que 7 divide al 12. Lo cual es una contradicción. Entones nos queda que $\mathrm{Nu}(\varphi) = \mathbb{Z}_7$. Por lo tanto, el único homomorfismo posible φ de $\mathbb{Z}_7$ a $\mathbb{Z}_{12}$ es el que envía todos los elementos de $\mathbb{Z}_7$ al elemento neutro de $\mathbb{Z}_{12}$. ■

Proposición 2.1.16. *Sea $\varphi\colon G_1 \to G_2$ un isomorfismo. Entonces,*

(1) *$o(a) = o(\varphi(a))$, para todo $a \in G_1$;*

(2) *G_1 es abeliano syss G_2 es abeliano;*

(3) *G_1 es cíclico syss G_2 es cíclico.*

Demostración. Como $\varphi\colon G_1 \to G_2$ es un isomorfismo, tenemos que $\varphi^{-1}\colon G_2 \to G_1$ es también un isomorfismo.

Ahora para probar (1), sea $a \in G_1$. Supongamos primero que $o(a) < \infty$. Entonces, usando la propiedad (6) de la Proposición 2.1.3 para φ y φ^{-1}, tenemos que

$$o(\varphi(a))|o(a) \quad \text{y} \quad o(a) = o(\varphi^{-1}(\varphi(a)))|o(\varphi(a)).$$

Entonces, $o(a) = o(\varphi(a))$. Supongamos ahora que $o(a) = \infty$. Debemos probar que $o(\varphi(a)) = \infty$. Supongamos que $o(\varphi(a)) = k < \infty$. Entonces

$$\varphi(a^k) = \varphi(a)^k = e_2 = \varphi(e_1).$$

Dado que φ es isomorfismo, en particular es inyectiva, tenemos que $a^k = e_1$. Entonces $o(a) \leq k < \infty$, lo cual es una contradicción. Por lo tanto, $o(\varphi(a)) = \infty$.

Es directo probar (2).

Para (3), supongamos que G_1 es cíclico y esta generado por el elemento a, esto es, $G_1 = \langle a \rangle$. Veremos que G_2 esta generado por el elemento $\varphi(a)$. Sea $g \in G_2$. Como φ es un isomorfismo, existe $n \in \mathbb{Z}$ tal que $\varphi(a^n) = g$. Así, $\varphi(a)^n = \varphi(a^n) = g$. Entonces, $G_2 = \langle \varphi(a) \rangle$. Si ahora suponemos que G_2 es cíclico, entonces usamos que $\varphi^{-1}\colon G_2 \to G_1$ es un isomorfismo para probar que G_1 es cíclico. ■

Ahora consideraremos homomorfismos sobre grupos cíclicos.

Proposición 2.1.17. *Sea $G = \langle a \rangle$ un grupo cíclico y sea H un grupo arbitrario. Si $\varphi, \psi\colon G \to H$ son homomorfismos tales que $\varphi(a) = \psi(a)$, entonces $\varphi = \psi$.*

La proposición anterior nos dice que los homomorfismos desde un grupo cíclio $G = \langle a \rangle$ a un grupo arbitrario H están determinados por su valor en el generador a.

Proposición 2.1.18. *Sea $G = \langle a \rangle$ un grupo cíclico infinito y sea b un elemento de un grupo H. Entonces, existe un único homomorfismo $\varphi\colon G \to H$ tal que $\varphi(a) = b$.*

Ahora, si $G = \langle a \rangle$ es un grupo cíclico de orden finito, ya no es más verdad que para cada elemento b de un grupo H existe un homomorfismo $\varphi\colon G \to H$ tal que $\varphi(a) = b$. Por ejemplo, sea $G = \mathbb{Z}_5 = \langle \overline{1} \rangle$ y sea $1 \in H = \mathbb{Z}$. Supongamos que $\varphi : \mathbb{Z}_5 \to \mathbb{Z}$ es un homomorfismo tal que $\varphi(\overline{1}) = 1$. Luego, $0 = \varphi(\overline{0}) = \varphi(5.\overline{1}) = 5.\varphi(\overline{1}) = 5.1 = 5$, lo cual es imposible. De manera más general, si $G = \langle a \rangle$ es de orden finito y $\varphi\colon G \to H$ es un homomorfismo, entonces por la Proposición 2.1.3 (6) tenemos que $\varphi(a)$ es de orden finito y divide al orden de a.

Ahora, veremos una condición necesaria y suficiente para que tales homomorfismos existan.

Proposición 2.1.19. *Sea $G = \langle a \rangle$ un grupo cíclico de orden finito n y sea b un elemento de orden finito de un grupo H. Entonces, existe un único homomorfismo $\varphi\colon G \to H$ tal que $\varphi(a) = b$ si y sólo si $o(b)$ divide al orden de G.*

Demostración. Supongamos primero que existe un homomorfismo $\varphi\colon G \to H$ tal que $\varphi(a) = b$ (el cual sabemos que es único por la Proposición 2.1.17). Por la Proposición 2.1.3, tenemos que $o(\varphi(a)) \mid o(a) = n$. Recíprocamente, supongamos que $o(b)$ divide al orden de G, esto es, $o(b) \mid n$. Como $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$, definimos $\varphi\colon G \to H$ como $\varphi(a^i) = b^i$ para cada $i = 0, 1, \ldots, n-1$. Es claro que φ está bien definida. Veamos que es un homomorfismo. Sean $i, j \in \{0, 1, \ldots, n-1\}$. Si $i + j < n$, entonces $\varphi(a^{i+j}) = b^{i+j}$, y con lo cual $\varphi(a^i a^j) = \varphi(a^{i+j}) = b^{i+j} = b^i b^j = \varphi(a^i)\varphi(a^j)$. Ahora, si $i + j \geq n$, entonces $i + j - n < n$ y $a^i a^j = a^{i+j-n}$. Entonces, $\varphi(a^i a^j) = \varphi(a^{i+j-n}) = b^{i+j-n} = b^{i+j} b^{-n}$. Como $o(b) \mid n$, tenemos que $b^{-n} = (b^n)^{-1} = e^{-1} = e$. Luego, $\varphi(a^i a^j) = b^{i+j} = b^i b^j = \varphi(a^i)\varphi(a^j)$. Así, φ es un homomorfismo y, por la Proposición 2.1.17, es único. ∎

Por lo tanto, con la proposición anterior, hemos reducido la determinación de la existencia de homomorfismos $\varphi\colon \langle a \rangle \to H$ a la determinación de la existencia de elementos en H cuyo orden es un divisor de $n = o(a)$. En particular, si H es un grupo finito de orden m, como todo elemento de H tiene orden que divide a m, se trata de determinar los elementos de H cuyos órdenes son divisores de $d = mcd(n, m)$. Como consecuencia, podemos ver que si n y m son relativamente primos, esto es, $d = mcd(n, m) = 1$, existe un único homomorfismo $\varphi\colon \langle a \rangle \to H$ y es el que $\varphi(x) = e_H$ para todo $x \in \langle a \rangle$ (pues, el único elemento de H de orden 1 es e_H).

Ejemplo 2.1.20. Determinemos todos los homomorfismos posibles de $\mathbb{Z}_{30}$ en $\mathbb{Z}_{42}$. Ya que $mcd(30, 42) = 6$, buscamos los elementos de $\mathbb{Z}_{42}$ que tienen orden un divisor de 6, esto es, elementos de $\mathbb{Z}_{42}$ que tienen órdenes 1, 2, 3 o 6 (podemos usar el procedimiento del Ejemplo 1.6.14 para hallar los elementos de un orden dado):

<u>Orden 1:</u> El único elemento de $\mathbb{Z}_{42}$ de orden 1 es el $\overline{0}$ y el homomorfismo φ_0 es el trivial.

<u>Orden 2:</u> El elemento de $\mathbb{Z}_{42}$ de orden 2 es: $\overline{21}$. Entonces, el homomorfismo es definido por:

- $\varphi_{21}(i.\overline{1}) = i.\overline{21}$ con $i \in \{0, 1, 2, \ldots, 29\}$.

Orden 3: Los elementos de $\mathbb{Z}_{42}$ de orden 3 son: $\overline{14}$ y $\overline{28}$. Entonces, los homomorfismos posibles son definidos por:

- $\varphi_{14}(i.\overline{1}) = i.\overline{14}$ con $i \in \{0, 1, 2, \ldots, 29\}$.
- $\varphi_{28}(i.\overline{1}) = i.\overline{28}$ con $i \in \{0, 1, 2, \ldots, 29\}$.

Orden 6: Los elementos de $\mathbb{Z}_{42}$ de orden 6 son: $\overline{7}$ y $\overline{35}$. Entonces, los homomorfismos posibles son definidos por:

- $\varphi_{7}(i.\overline{1}) = i.\overline{7}$ con $i \in \{0, 1, 2, \ldots, 29\}$.
- $\varphi_{35}(i.\overline{1}) = i.\overline{35}$ con $i \in \{0, 1, 2, \ldots, 29\}$. ■

Observación 2.1.21. Sean $G = \langle a \rangle$ y $H = \langle b \rangle$ grupos cíclicos finitos de órdenes n y m, respectivamente. Sea $d = mcd(n, m)$. Sea H_d el único subgrupo de H de orden d. Ahora bien, cada elemento de H_d tiene un orden que divide a d, y así para cada elemento de H_d hay un homomorfismo de G en H. Y estos son todos, pues si $b' \in H$ es tal que $o(b')$ divide a n, y como $o(b')$ divide a m (pues, $m = |H|$), entonces $o(b')$ divide a d. Con lo cual $b' \in H_d$[1].

Finalizamos esta sección probando el Teorema de Cayley, el cual afirma que todo grupo es isomorfo a un grupo permutación.

Sea G un grupo y a un elemento de G. Se define la función $L_a \colon G \to G$ como sigue $L_a(x) = ax$. Veamos que L_a es una biyección. Supongamos que $L_a(x) = L_a(y)$. Así, por definición de L_a, $ax = ay$. En consecuencia, $x = y$. Entonces, L_a es inyectiva. Sea $y \in G$. Considere el elemento $x = a^{-1}y$. Así, $L_a(x) = ax = aa^{-1}y = y$. Entonces, L_a es sobreyectiva. Por lo tanto, $L_a \in \mathrm{Sym}(G)$.

Teorema 2.1.22 (Teorema de Cayley)**.** *Cada grupo G es isomorfo a un subgrupo de* $\mathrm{Sym}(G)$*.*

Demostración. Definimos la función $\varphi \colon G \to \mathrm{Sym}(G)$ como $\varphi(a) = L_a$. Observemos que para todo $x \in G$, tenemos que

$$(L_a \circ L_b)(x) = L_a(L_b(x)) = L_a(bx) = abx = L_{ab}(x).$$

Entonces, $\varphi(ab) = L_{ab} = L_a \circ L_b = \varphi(a) \circ \varphi(b)$. Lo que prueba que φ es un homomorfismo. Ahora probamos que φ es inyectiva. Supongamos que $\varphi(a) = \varphi(b)$. Así, $L_a = L_b$. Con lo cual, $a = ae = L_a(e) = L_b(e) = be = b$. Entonces, φ es un monomorfismo. Por lo tanto, G es isomorfo al subgrupo $\mathrm{Im}(\varphi)$ de $\mathrm{Sym}(G)$. ■

Ejemplo 2.1.23. Consideremos el grupo $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ de enteros módulo 3. Entonces,

$$L_{\overline{0}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{0} & \overline{1} & \overline{2} \end{pmatrix} \quad L_{\overline{1}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{2} & \overline{0} \end{pmatrix} \quad L_{\overline{2}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{2} & \overline{0} & \overline{1} \end{pmatrix}$$

[1]Sea $G = \langle a \rangle$ con $o(a) = n$. Sea $d \mid n$ y H_d el único subgrupo de G de orden d. Si $b \in G$ es tal que $o(b) \mid d$, entonces $b \in H_d$. En efecto, por un lado tenemos que $\langle b \rangle$ es un subgrupo de G de orden $o(b)$. Por otro lado, como $o(b) \mid d$, existe un único subgrupo K de H_d de orden $o(b)$. Pero K es también subgrupo de G. Entonces, por unicidad $\langle b \rangle = K \subseteq H_d$.

Si identificamos $\overline{0}, \overline{1}, \overline{2}$ con 1, 2, y 3 respectivamente, entonces obtenemos que

$$L_{\overline{0}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{0} & \overline{1} & \overline{2} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad L_{\overline{1}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{2} & \overline{0} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$L_{\overline{2}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{2} & \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Por lo tanto, tenemos que $\mathbb{Z}_3$ es isomorfo al grupo permutación $G = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. ■

Ejemplo 2.1.24. Sea $G_4 = \{e, a, a^2, a^3 :\ a^4 = e\}$ el grupo cíclico de orden 4. Entonces,

$$L_a = \begin{pmatrix} e & a & a^2 & a^3 \\ a & a^2 & a^3 & e \end{pmatrix}$$

Si denotamos e, a, a^2, a^3 por 1,2,3,4 respectivamente, L_a es identificable con la permutación $\sigma = (1\ 2\ 3\ 4)$. Entonces,

$$\begin{aligned} e &\mapsto \mathrm{id} = (1) \\ a &\mapsto L_a = (1\ 2\ 3\ 4) = \sigma \\ a^2 &\mapsto L_{a^2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4) = \sigma^2 \\ a^3 &\mapsto L_{a^3} = (1\ 4\ 3\ 2) = \sigma^3. \end{aligned}$$

Por lo tanto, G_4 es isomorfo al subgrupo $H = \{e, \sigma, \sigma^2, \sigma^3\}$ de S_4. ■

2.2. Grupos Cocientes

En este sección estudiaremos la noción de grupo cociente. Esta es otra manera de obtener un grupo a partir de un grupo original G. Como en el caso de subgrupos, los grupos cocientes nos permiten obtener un mayor entendimiento de la estructura de un grupo G. También veremos que el estudio de los grupos cocientes es esencialmente equivalente al estudio de los homomorfismos sobreyectivos (epimorfismos) de G. Comenzamos considerando una clase especial de subgrupos de un grupo G.

Definición 2.2.1. Un subgrupo H de un grupo G es llamado **normal** si $ghg^{-1} \in H$ para todo $g \in G$ y todo $h \in H$. Cuando H sea un subgrupo normal de G lo denotaremos por $H \lhd G$.

Ejemplo 2.2.2. Sea G un grupo.

1. Ambos G y el subgrupo trivial $\{e\}$ son normales en G.

2. Sea $\varphi\colon G \to G'$ un homomorfismo. Entonces, por la Proposición 2.1.8, el núcleo de φ, $\mathrm{Nu}(\varphi)$, es un subgrupo normal de G. ■

Proposición 2.2.3. *Sea G un grupo y H un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

(1) $H \lhd G$;

(2) $aHa^{-1} \subseteq H$ *para todo* $a \in G$;

(3) $aHa^{-1} = H$ *para todo* $a \in G$;

(4) $aH = Ha$ *para todo* $a \in G$.

Proposición 2.2.4. *Sea G un grupo abeliano. Entonces, todo subgrupo de G es normal.*

El producto de dos subgrupos H y K de un grupo G dado por

$$HK = \{hk : \; h \in H \text{ y } k \in K\}$$

no es en general un subgrupo de G. Consideremos el ejemplo abajo.

Ejemplo 2.2.5. Tomemos el grupo simétrico de orden 3, S_3. Sean $H = \{(1), \; (1\;2)\}$ y $K = \{(1), \; (1\;3)\}$. Compruebe que son subgrupos de S_3. Ahora el producto de H por K es

$$HK = \{(1), \; (1\;2), \; (1\;3), \; (1\;3\;2)\}.$$

Si HK fuera un subgrupo de S_3 se debería cumplir que $(1\;3)(1\;2) \in HK$. Verificar que esto no se cumple. Por lo tanto HK no es un subgrupo de S_3. ■

Proposición 2.2.6. *Sea G un grupo y sean H y K subgrupos de G. Entonces, HK es un subgrupo de G si y sólo si $HK = KH$.*

Demostración. $\Rightarrow$) Supongamos que HK es un subgrupo de G. Sea $hk \in HK$. Luego, $(hk)^{-1} \in HK$. Así, $(hk)^{-1} = h_1k_1$. Es claro que $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$. Por lo tanto, hemos mostrado que $HK \subseteq KH$. Un argumento similar prueba que $KH \subseteq HK$. Entonces, $HK = KH$.

$\Leftarrow$) Asumamos que $HK = KH$. Sean $hk, h_1k_1 \in HK$. Queremos probar que $(hk)(h_1k_1)^{-1} \in HK$. Observemos que $(hk)(h_1k_1)^{-1} = hkk_1^{-1}h_1^{-1} = h(kk_1^{-1})h_1^{-1} = hh_2k_2$ para algunos $h_2 \in H$ y $k_2 \in K$. Entonces, $(hk)(h_1k_1)^{-1} \in HK$. Por lo tanto, HK es un subgrupo de G. ■

Proposición 2.2.7. *Sean H y K dos subgrupos de un grupo G. Si K es un subgrupo normal de G, entonces KH es un subgrupo de G.*

Demostración. Es claro que $e \in KH$. Sean $kh, k_1h_1 \in KH$. Entonces,

$$(kh)(k_1h_1) = [k(hk_1h^{-1})](hh_1) \in KH$$

porque $hk_1h^{-1} \in K$ por ser K un subgrupo normal. También, tenemos que

$$(kh)^{-1} = h^{-1}k^{-1} = (h^{-1}k^{-1}h)h^{-1} \in KH$$

pues, $h^{-1}k^{-1}h \in K$. ■

Como hemos visto en la Proposición 2.1.8, todo homomorfismo da lugar a un subgrupo normal, a saber el núcleo del homomorfismo. El ejemplo siguiente muestra un caso donde un subgrupo normal es el núcleo de un homomorfismo. En la sección siguiente veremos que esta relación se cumple, de hecho, en general.

Ejemplo 2.2.8. El **grupo lineal especial** $SL_2(\mathbb{R})$ de grado 2 de todas las matrices cuadradas de orden 2 tal que el determinante es igual 1 es un subgrupo normal del grupo $GL_2(\mathbb{R})$ de todas las matrices cuadradas de orden 2 invertibles ya que el determinante $\det\colon GL_2(\mathbb{R}) \to \mathbb{R}^*$ es un homomorfismo y su núcleo es $SL_2(\mathbb{R})$. ■

Definición 2.2.9. Un grupo G es llamado **simple** si G no tiene subgrupos normales no triviales.

Ejemplo 2.2.10. Todo grupo G de orden primo p es simple. ■

Sea G un grupo y sea H un subgrupo normal de G. Recordemos la definición de la relación $\sim$ dada en §1.7: sean $a, b \in G$,

$$a \sim_H b \quad \text{syss} \quad ab^{-1} \in H.$$

Como hemos dicho allí, la relación $\sim_H$ es de equivalencia. Para cada elemento $a \in G$ denotaremos a su clase de equivalencia por $[a]_H$ o por $a/\sim_H$. Y cuando no haya peligro de confusión, simplemente denotaremos la clase de equivalencia del elemento a por la relación $\sim_H$ por $[a]$ o $a/\sim$.

Como ya hemos visto, la clase de equivalencia de un elemento a de G es la clase lateral derecha, esto es, $[a] = Ha$. Dado que H es un subgrupo normal de G tenemos, por la Proposición 2.2.3, que $[a] = Ha = aH$ para todo $a \in G$. Denotaremos al conjunto cociente por G/H.

Ahora veremos que la relación de equivalencia $\sim_H$ sobre un grupo G dada por un subgrupo normal H de G se comporta bien con las operaciones del grupo G.

Proposición 2.2.11. *Sea G un grupo y sea H un subgrupo normal de G. Sean $a, b, c, d \in G$.*

(1) *Si $a \sim b$ y $c \sim d$, entonces $ac \sim bd$.*

(2) *Si $a \sim b$, entonces $a^{-1} \sim b^{-1}$.*

Demostración. (1) Supongamos que $a \sim b$ y $c \sim d$. Por definición $ab^{-1}, cd^{-1} \in H$. Ahora, $ac(bd)^{-1} = acd^{-1}b^{-1}$. Denotemos $h := cd^{-1} \in H$. Así, $ac(bd)^{-1} = ahb^{-1} = a(b^{-1}b)hb^{-1} = (ab^{-1})(bhb^{-1})$. Como H es un subgrupo normal, $bhb^{-1} \in H$. Entonces, nos queda que $ac(bd)^{-1} \in H$. Por lo tanto, $ac \sim bd$.

(2) Supongamos que $a \sim b$. Entonces, $ab^{-1} \in H$. Esto es, $ab^{-1} = h$ para algún $h \in H$. Esto es, $a = hb$. Como H es un subgrupo normal de G, $a = hb = bh'$ para algún $h' \in H$. Así, $a^{-1} = h'^{-1}b^{-1}$. Luego, $a^{-1}b = h'^{-1} \in H$. Con lo cual, $a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$. Entonces, $a^{-1} \sim b^{-1}$. ■

Ahora estamos en condiciones de definir una operación binaria sobre el conjunto cociente G/H de la siguiente manera. Sean $a, b \in G$,

$$[a][b] := [ab] \quad \text{o en términos de clases laterales} \quad (Ha)(Hb) := H(ab).$$

Tenemos que probar que esta operación está bien definida sobre G/H. En otras palabras, debemos chequear que esta operación sobre G/H no depende de los representantes tomados en las clases $[a]$ y $[b]$. Supongamos que se cumple que $[a] = [a']$ y $[b] = [b']$. Entonces, $a \sim a'$ y $b \sim b'$. Por la proposición anterior, tenemos que $ab \sim a'b'$. Así, $[a][b] = [ab] = [a'b'] = [a'][b']$.

Teorema 2.2.12. *Sea H un subgrupo normal de un grupo G. Entonces, G/H forma un grupo con respecto a la operación $[a][b] = [ab]$.*

Demostración. Como vimos en el párrafo anterior la operación $[a][b] = [ab]$ está bien definida. Veamos que es asociativa. Sean $a, b, c \in G$. Entonces,

$$[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c].$$

El elemento neutro en G/H es $[e]$. En efecto, $[a][e] = [ae] = [a]$. Análogamente, $[e][a] = [a]$. Dado $a \in G$, el inverso de $[a]$ es $[a^{-1}]$. Pues, $[a][a^{-1}] = [aa^{-1}] = [e]$ y también (con el mismo argumento) $[a^{-1}][a] = [e]$. Luego, $[a]^{-1} = [a^{-1}]$. El teorema queda demostrado. ■

El grupo G/H recién obtenido es llamado el **grupo cociente de G por H** o, a veces también es llamado el **grupo factor de G por H**. Es usual denotar la operación del grupo cociente G/H por el mismo símbolo que es usado para la operación del grupo original G. Por ejemplo, en el caso de un grupo aditivo $\langle G, +\rangle$, uno debería escribir la operación del grupo cociente como $[a] + [b] = [a + b]$.

Note que la condición de que el subgrupo H de G sea normal para definir el grupo cociente G/H es fundamental.

Observación 2.2.13. Sea G un grupo finito y sea $H \lhd G$. Por el Teorema de Lagrange (Teorema 1.7.4) tenemos que

$$\left|\frac{G}{H}\right| = [G : H] = \frac{|G|}{|H|}.$$

Ejemplo 2.2.14. Consideremos el grupo aditivo de los enteros $\mathbb{Z}$. Como $\mathbb{Z}$ es abeliano, todos los subgrupos de $\mathbb{Z}$ son normales. También, ya sabemos que los subgrupos de $\mathbb{Z}$ son los subgrupos cíclicos $\langle n\rangle$ donde n es un entero positivo. Sea $n > 1$. Entonces, las clases laterales (o clases de equivalencia) del grupo cociente $\mathbb{Z}/\langle n\rangle$ son de la forma

$$[a] = a + \langle n\rangle = \{a + kn : \ k \in \mathbb{Z}\}.$$

Así, podemos ver que las clases laterales del subgrupo $\langle n\rangle$ son las clases de equivalencia de la relación congruencia módulo n en $\mathbb{Z}$. Esto es $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$. El punto que queremos señalar aquí es que el grupo de enteros módulo n es un disfraz perfecto para el grupo cociente de $\mathbb{Z}$ por $\langle n\rangle$:

$$\langle \mathbb{Z}_n, +_n\rangle = \langle \mathbb{Z}/\langle n\rangle, +\rangle. \quad ■$$

Ejemplo 2.2.15. Sean $G = \langle 3\rangle = \{3k : k \in \mathbb{Z}\}$ y $H = \langle 12\rangle = \{12k : k \in \mathbb{Z}\}$ subgrupos de $\mathbb{Z}$. En particular, son dos grupos. También es director ver que H es subgrupo de G. Ahora probaremos que el grupo cociente $G/H = \langle 3\rangle/\langle 12\rangle$ es isomorfico a $\mathbb{Z}_4$. Sabemos que

$$\langle 3\rangle/\langle 12\rangle = \{x + \langle 12\rangle : x \in \langle 3\rangle\}.$$

Sea $x \in \langle 3 \rangle$. Entonces $3 \mid x$. Dividimos x por 12: $x = 12q + r$ con $0 \leq r < 12$. Como $r = 12q - x$ y $3 \mid x$, tenemos que $3 \mid r$. Entonces $r \neq 1, 2, 4, 5, 7, 8, 10, 11$. Por lo tanto, tenemos que $x + \langle 12 \rangle = r + \langle 12 \rangle$ siendo r tal que $x = 12q + r$ con $r = 0, 3, 6, 9$. Por lo tanto,

$$\langle 3 \rangle / \langle 12 \rangle = \{0 + \langle 12 \rangle, 3 + \langle 12 \rangle, 6 + \langle 12 \rangle, 9 + \langle 12 \rangle\}.$$

Observamos que el grupo cociente $\langle 3 \rangle / \langle 12 \rangle$ tiene orden 4. Se puede probar, por comprobación directa, que $3 + \langle 12 \rangle$ tiene orden 4. Por lo tanto, el grupo cociente $\langle 3 \rangle / \langle 12 \rangle$ está generado por elemento $3 + \langle 12 \rangle$. Esto es, estamos diciendo que $\langle 3 \rangle / \langle 12 \rangle$ es un grupo cíclico de orden 4. Por lo tanto, por el Teorema 2.1.13, tenemos que $\langle 3 \rangle / \langle 12 \rangle \cong \mathbb{Z}_4$. ■

Teorema 2.2.16. *Sea H un subgrupo normal de un grupo G. Entonces, la aplicación $\pi \colon G \to G/H$ definida por $\pi(a) = [a]$ para cada $a \in G$ es un epimorfismo. Además,* $\mathrm{Nu}(\pi) = H$.

Demostración. Veamos que π es un homomorfismo. Sean $a, b \in G$. Entonces, $\pi(ab) = [ab] = [a][b] = \pi(a)\pi(b)$. Es claro que π es una aplicación sobreyectiva. Por lo tanto, π es un epimorfismo del grupo G sobre el grupo cociente G/H. Sea $a \in G$. Entonces,

$$a \in \mathrm{Nu}(\pi) \iff \pi(a) = [e] \iff ae^{-1} \in H \iff a \in H.$$

Por lo tanto, $\mathrm{Nu}(\pi) = H$. ■

2.3. Teoremas de Homomorfismos

En esta sección veremos varios resultados los cuales expresan la relación existente entre homomorfismos de grupos y grupos cocientes. Entre ellos, el Primer Teorema de Isomorfismo afirma que la imagen homomórfica de un grupo es isomorfico al grupo cociente del grupo por el correspondiente núcleo. También analizaremos diferentes ejemplos y aplicaciones de estos resultados.

Teorema 2.3.1. *Sea $f \colon G \to G'$ un homomorfismo. Sea H un subgrupo normal de G tal que $H \subseteq \mathrm{Nu}(f)$. Entonces, existe un único homomorfismo $\varphi \colon G/H \to G'$ tal que $f = \varphi \circ \pi$ donde π es el epimorfismo canónico. Además, si $H = \mathrm{Nu}(f)$, entonces φ es un monomorfismo.*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/H \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

Demostración. Vamos a definir $\varphi \colon G/H \to G'$, como es natural, por $\varphi([a]) = f(a)$ para cada $[a] \in G/H$. Veamos que φ está bien definida. Supongamos que $[a] = [b]$. Así, $ab^{-1} \in H$ y, por hipótesis, $ab^{-1} \in \mathrm{Nu}(f)$. Esto es, $f(ab^{-1}) = e'$. Con lo cual, $f(a)f(b)^{-1} = e'$ y, entonces

$f(a) = f(b)$. Entonces, $\varphi([a]) = f(a) = f(b) = \varphi([b])$. Con lo que φ está bien definida. Ahora veamos que es un homomorfismo. Sean $[a], [b] \in G/H$. Entonces,

$$\varphi([a][b]) = \varphi([ab]) = f(ab) = f(a)f(b) = \varphi([a])\varphi([b]).$$

Sea $a \in G$. Por definición de φ, tenemos que $f(a) = \varphi([a]) = \varphi(\pi(a)) = (\varphi \circ \pi)(a)$. Entonces, se cumple que $f = \varphi \circ \pi$. Ahora probamos que φ es el único homomorfismo con esas propiedades. Supongamos que $\psi \colon G/H \to G'$ es un homomorfismo tal que $f = \psi \circ \pi$. Entonces, para cada $[a] \in G/H$, $\varphi([a]) = f(a) = (\psi \circ \pi)(a) = \psi([a])$. Por lo tanto, $\varphi = \psi$. Finalmente, supongamos que $H = \mathrm{Nu}(f)$. Sea $[a] \in \mathrm{Nu}(\varphi)$. Así, $\varphi([a]) = e'$. Con lo cual, $f(a) = e'$. Entonces, $a \in \mathrm{Nu}(f) = H$. Esto es, $[a] = [e]$. Hemos probado que $\mathrm{Nu}(\varphi) = \{[e]\}$. Por lo tanto, φ es inyectivo. ■

Teorema 2.3.2 (Primer Teorema de Isomorfismo)**.** *Sea $f \colon G \to G'$ un epimorfismo de G sobre G'. Entonces,*

$$G/\mathrm{Nu}(f) \cong G'.$$

Demostración. Por el teorema anterior sabemos que existe el monomorfismo $\varphi \colon G/\mathrm{Nu}(f) \to G'$ tal que $f = \varphi \circ \pi$. Solo nos resta probar que φ es sobreyectivo. Sea $g' \in G'$. Como f es sobreyectivo, existe $a \in G$ tal que $f(a) = g'$. Entonces, $(\varphi \circ \pi)(a) = g'$. Con lo cual, $\varphi([a]) = g'$. Luego, φ es sobreyectivo. Por lo tanto, $\varphi \colon G/\mathrm{Nu}(f) \to G'$ es un isomorfismo. ■

Si $G' = f(G)$ para algún homomorfismo f, decimos que G' es **imagen homomórfica** de G. El Primer Teorema de Isomorfismo nos dice que los subgrupos normales están en correspondencia con las imágenes homomórficas de G (ver la Figura 2.1).

$$\begin{aligned} H \text{ subgrupo normal de } G &\Longrightarrow \pi \colon G \to G/H \text{ es un epimorfismo y} \\ & \mathrm{Nu}(\pi) = H \\[2em] f \colon G \to G' \text{ es epimorfismo } &\Longrightarrow \mathrm{Nu}(f) \text{ es un subgrupo normal y} \\ & G' \cong G/\mathrm{Nu}(f) \end{aligned}$$

Figura 2.1: Correspondencia entre subgrupos normales y epimorfismos.

Ejemplo 2.3.3. Consideremos $\mathbb{Z}$ como un subgrupo aditivo de los números reales $\mathbb{R}$. Es de hecho un subgrupo normal ya que $\mathbb{R}$ es abeliano. Entonces,

$$\mathbb{R}/\mathbb{Z} = \{r + \mathbb{Z} : \ r \in \mathbb{R}\}.$$

Note que $r_1 + \mathbb{Z} = r_2 + \mathbb{Z}$ syss $r_1 - r_2 \in \mathbb{Z}$. Entonces, se puede mostrar que

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

Consideremos el círculo unidad $S^1 = \{e^{2\pi ix} : \ 0 \leq x < 1\} = \{\cos\theta + i\sin\theta : \ 0 \leq \theta < 2\pi\}$ con el producto usual de complejos, esto es,

$$e^{2\pi ix}e^{2\pi iy} = e^{2\pi i(x+y)}$$

donde $0 \leq x, y < 1$. Definimos la función $f\colon \mathbb{R} \to S^1$ como $f(x) = e^{2\pi ix}$. Entonces, f es un epimorfismo y $\mathrm{Nu}(f) = \mathbb{Z}$. Por lo tanto, por el Primer Teorema de Isomorfismo,

$$\mathbb{R}/\mathbb{Z} \cong S^1. \quad \blacksquare$$

Ejemplo 2.3.4. Sea $\mathbb{Q}[X]$ el grupo aditivo de los polinomios con coeficiente racionales y sea

$$H = \{p(X) \in \mathbb{Q}[X] : \ p(0) = 0\}.$$

Entonces, H es el núcleo del epimorfismo $f\colon \mathbb{Q}[X] \to \mathbb{Q}$ definido por

$$f(p(X)) = p(0).$$

Por lo tanto, tenemos que $\mathbb{Q}[X]/H \cong \mathbb{Q}$. ■

Teorema 2.3.5 (Segundo Teorema de Isomorfismo)**.** *Sea H un subgrupo de un grupo G y sea K un subgrupo normal de G. Entonces,*

$$HK = \{hk : \ h \in H \ y \ k \in K\}$$

es un subgrupo de G, $H \cap K$ es un subgrupo normal de H y

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

Demostración. Como K es un subgrupo normal de G, ya sabemos que HK es un subgrupo de G. Es fácil mostrar que $H \cap K$ es un subgrupo normal de H. También es claro que K es un subgrupo normal de HK. Así, podemos definir $\varphi\colon H \to (HK)/K$ como $\varphi(h) = [h]_K$. La función φ es un homomorfismo dado que es la composición del homomorfismo inclusión $i\colon H \to HK$ y el homomorfismo canónico $HK \to (HK)/K$. Además, verifica que

$$h \in \mathrm{Nu}(\varphi) \iff [h]_K = [e]_K \iff h \in H \cap K.$$

Con lo cual, $\mathrm{Nu}(\varphi) = H \cap K$. Ahora queremos ver que φ es sobreyectiva. Sea $[hk]_K \in (HK)/K$. Entonces, $\varphi(h) = [h]_K = [hk]_K$ (pues, $h(hk)^{-1} = hk^{-1}h^{-1} \in K$ dado que K es un subgrupo normal de G). Ahora, aplicando el Primer Teorema de Isomorfismo obtenemos el resultado buscado. ■

Introducimos a continuación algunas notaciones que nos permitirán entender un poco más fácilmente el teorema de correspondencia. Sea G un grupo y sea N un subgrupo de G. Denotamos los siguientes conjuntos:

- $\mathrm{Sub}(G) = \{H : \ H \text{ es un subgrupo de } G\}$;

- $\mathrm{Sub}^N(G) = \{H : \ H \text{ es un subgrupo de } G \text{ y } N \subseteq H\}$;
- $\mathrm{Sub}_{Nor}(G) = \{H : \ H \text{ es un subgrupo normal de } G\}$;
- $\mathrm{Sub}^N_{Nor}(G) = \{H : \ H \text{ es un subgrupo normal de } G \text{ y } N \subseteq H\}$.

Teorema 2.3.6 (Teorema de Correspondencia)**.** *Sea N un subgrupo normal del grupo G. Entonces hay una correspondencia biyectiva entre los conjuntos $\mathrm{Sub}^N(G)$ y $\mathrm{Sub}(G/N)$. También, los conjuntos $\mathrm{Sub}^N_{Nor}(G)$ y $\mathrm{Sub}_{Nor}(G/N)$ están en correspondencia biyectiva.*

Demostración. Definimos la función

$$\varphi \colon \mathrm{Sub}^N(G) \to \mathrm{Sub}(G/N)$$

por

$$\varphi(H) = \pi_N(H) = H/N.$$

Sea $H \in \mathrm{Sub}^N(G)$. Dado que N es también un subgrupo normal de H, H/N tiene sentido. Como H es un subgrupo de G, tenemos que $\varphi(H) = H/N$ es un subgrupo de G/N. Así, φ está bien definida.

Sea S un subgrupo de G/N. Sea $H := \pi_N^{-1}(S) = \{g \in G : \ \pi_N(g) \in S\} = \{g \in G : \ [g] \in S\}$ donde $\pi_N \colon G \to G/N$ es el epimorfismo canónico. Por la Proposición 2.1.3 tenemos que H es un subgrupo de G. Claramente, $N \subseteq H$. Dado que π_N es una función sobreyectiva, $\varphi(H) = \pi_N(H) = \pi_N(\pi_N^{-1}(S)) = S$. Luego, hemos probado que φ es sobreyectiva.

Supongamos que $H_1, H_1 \in \mathrm{Sub}^N(G)$ son tales que $\varphi(H_1) = \varphi(H_2)$. Esto es, $H_1/N = H_2/N$. Sea $h \in H_1$. Así, $[h] \in H_1/N$ y, con lo cual, $[h] \in H_2/N$. Luego, $h \in H_2$. Entonces, $H_1 \subseteq H_2$. De la misma manera podemos mostrar que $H_2 \subseteq H_1$. Entonces, $H_1 = H_2$ y por lo tanto, φ es inyectiva.

Sea $H \in \mathrm{Sub}^N_{Nor}(G)$. Veamos que H/N es un subgrupo normal de G/N. Sean $[h] \in H/N$ y $[g] \in G/N$. Ahora, $[g][h][g]^{-1} = [ghg^{-1}]$ y, como H es normal, $ghg^{-1} \in H$. Entonces, $[g][h][g]^{-1} \in H/N$. Finalmente, probemos que si S es un subgrupo normal de G/N, entonces $H = \pi_N^{-1}(S)$ es un subgrupo normal de G. Sean $h \in H$ y $g \in G$. Así, $[h] \in S$. Como S es normal, tenemos que $[ghg^{-1}] = [g][h][g]^{-1} \in S$. Esto es, $ghg^{-1} \in H$. ■

Teorema 2.3.7 (Tercer Teorema de Isomorfismo)**.** *Sea $f \colon G \to G'$ un epimorfismo del grupo G sobre el grupo G'. Suponga que H' es un subgrupo normal de G' y sea $H := f^{-1}(H')$. Entonces, H es un subgrupo normal de G y*

$$\frac{G}{H} \cong \frac{G'}{H'}.$$

Demostración. Definimos $\varphi \colon G \to G'/H'$ como $\varphi(g) = [f(g)]_{H'}$. Observemos que φ es un epimorfismo por ser composición del epimorfismo $f \colon G \to G'$ y del epimorfismo canónico $G' \to G'/H'$. Es directo chequear que $H := f^{-1}(H')$ es un subgrupo normal de G. Ahora queremos probar que el núcleo de φ es H. Esto es así ya que

$$\begin{aligned} h \in \mathrm{Nu}(\varphi) &\iff \varphi(h) = [f(h)]_{H'} = [e]_{H'} \\ &\iff f(h) \in H' \\ &\iff h \in f^{-1}(H') = H. \end{aligned}$$

Por el Primer Teorema de Isomorfismo, tenemos que $G/H \cong G'/H'$. ■

Ejemplo 2.3.8. Sea $\mathbb{C}$ el grupo aditivo de todos los números complejos y sea $\mathbb{C}^*$ el grupo multiplicativo de todos los números complejos no nulos. La función exponencial $\exp\colon \mathbb{C} \to \mathbb{C}^*$ es un epimorfismo. Sea $S^1 = \{z \in \mathbb{C} : \ |z| = 1\}$. Se puede comprobar sin dificultad que S^1 es un subgrupo de $\mathbb{C}^*$ y que $\exp^{-1}(S^1) = \mathrm{Im}(\mathbb{C}) = \{ib : \ b \in \mathbb{R}\}$. Entonces, por el Tercer Teorema de Isomorfismo, tenemos que

$$\mathbb{C}/\mathrm{Im}(\mathbb{C}) \cong \mathbb{C}^*/S^1 \cong {}^2\langle \mathbb{R}^+, .\rangle.$$

Por el Primer Teorema de Isomorfismo podemos probar que $\mathbb{C}/\mathrm{Im}(\mathbb{C}) \cong \langle \mathbb{R}, +\rangle$[3]. Por lo tanto, concluimos que la función exponencial induce un isomorfismo entre $\langle \mathbb{R}, +\rangle$ y $\langle \mathbb{R}^+, .\rangle$. ■

Corolario 2.3.9. *Sea G un grupo y $H \lhd G$. Si $\widehat{K} \lhd G/H$, entonces*

$$\frac{G/H}{\widehat{K}} \cong \frac{G}{K}$$

donde $K = \pi_H^{-1}\left(\widehat{K}\right)$.

Demostración. Sea $H \lhd G$ y $\widehat{K} \lhd G/H$. Sea $\pi_H\colon G \to G/H$ el epimorfismo canónico. Entonces $K = \pi_H^{-1}\left(\widehat{K}\right)$ es un subgrupo normal de G. Entonces, aplicando el Tercer Teorema de Isomorfismo obtenemos que

$$\frac{G}{K} \cong \frac{G/H}{\widehat{K}}$$ ■

Este corolario (que es una consecuencia del Tercer Teorema de Isomorfismo) junto con el Teorema de Correspondencia nos está diciendo que no obtendremos información nueva al tomar cocientes de un grupo cociente.

2.4. Teorema de Cauchy

En esta sección veremos un ejemplo de la utilidad de la noción de grupo cociente. Esto se hará evidente en la demostración del Teorema de Cauchy.

El **centro** de un grupo G es definido a ser el subgrupo normal

$$Z(G) := \{a \in G : \ ax = xa \text{ para todo } x \in G\}.$$

Si $a \in G$, consideramos también el subgrupo (no necesariamente normal)

$$Z(a) := \{x \in G : \ ax = xa\}$$

llamado el **centralizador** de a en G.

[2] Considere la función $\varphi\colon \mathbb{C}^* \to \langle \mathbb{R}^+, .\rangle$ definida por $\varphi(z) = |z|$. Es claro que φ es un epimorfismo. Además, $z \in \mathrm{Nu}(\varphi) \iff |z| = 1 \iff z \in S^1$. Entonces, por el Primer Teorema de Isomorfismo, $\mathbb{C}^*/S^1 \cong \langle \mathbb{R}^+, .\rangle$.

[3] Es directo ya que, $\varphi\colon \mathbb{C} \to \langle \mathbb{R}, +\rangle$ dada por $\varphi(x + iy) = x$ is un epimorfismo y $\mathrm{Nu}(\varphi) = \mathrm{Im}(\mathbb{C})$.

Sea G un grupo finito. Si $a, b \in G$, definimos la relación binaria

$$a \sim b \iff \text{existe } x \in G \text{ tal que } b = xax^{-1}$$

Es inmediato verificar que la relación $\sim$ es de equivalencia y que para cada $a \in G$, $[a] = \{xax^{-1} : \ x \in G\}$. Queremos determinar el cardinal de $[a]$. Para esto definimos una función $f\colon [a] \to \{xZ(a) : \ x \in G\}$ como sigue: para cada $x \in G$, $f(xax^{-1}) = xZ(a)$. Primero veamos que f está bien definida: supongamos que $xax^{-1} = yay^{-1}$. Entonces

$$\begin{aligned} xax^{-1} = yay^{-1} \implies y^{-1}xa = ay^{-1}x \implies y^{-1}x \in Z(a) \implies \\ \implies xZ(a) = yZ(a) \implies f(xax^{-1}) = f(yay^{-1}). \end{aligned}$$

Recuerde que $\{xZ(a) : \ x \in G\}$ es el conjunto de todas clases laterales de $Z(a)$. Vamos a mostrar que la función f es inyectiva. Sean $x, y \in G$ y supongamos que $f(xax^{-1}) = f(yay^{-1})$. Entonces, tenemos que

$$xZ(a) = yZ(a) \implies y^{-1}x \in Z(a) \implies y^{-1}xa = ay^{-1}x \implies xax^{-1} = yay^{-1}.$$

En consecuencia, f es inyectiva. Además es trivial observar que f es sobreyectiva, por lo tanto podemos concluir que f es biyectiva. Por lo tanto, $\#([a]) = \#(\{xZ(a) : \ x \in G\}) = [G : Z(a)]$. Además, si $a \in Z(G)$, entonces $[a] = \{a\}$, pues $xax^{-1} = axx^{-1} = a$. Luego en la descomposición de G en clases de equivalencia bajo la relación $\sim$,

$$G = [a_1] \uplus \cdots \uplus [a_t],$$

tendremos que algunas de estas clases serán las correspondientes a elementos $a \in Z(G)$. Con lo cual, tenemos que

$$G = Z(G) \uplus [a_1] \uplus \cdots \uplus [a_s]$$

y por lo tanto

$$|G| = |Z(G)| + [G : Z(a_1)] + \cdots + [G : Z(a_s)]. \tag{2.2}$$

Teorema 2.4.1 (Teorema de Cauchy). *Sea G un grupo finito y p un divisor primo de $|G|$. Entonces, G contiene un elemento de orden p.*

Demostración. Supongamos primero G es abeliano. Sea $a \in G$. Si $o(a) = pm$ sabemos que $o(a^m) = p$. Supongamos que $p \nmid o(a)$. Sea $H = \langle a \rangle$, que es un subgrupo normal de G (pues estamos asumiendo que G es abeliano), con lo cual $|G/H| < |G|$. Por inducción completa sobre el orden de grupo[4], podemos suponer que G/H contiene un elemento b_1 de orden p[5]. Sea $\pi\colon G \to G/H$ y $b \in G$ tal que $\pi(b) = b_1$. Si $b^t = e$, entonces $b_1^t = \pi(b^t) = e$ y por lo tanto $p \mid t$. Luego, $b^{t/p}$ tiene orden p.

Pasemos ahora al caso general. Si $p \mid |Z(G)|$, como $Z(G)$ es abeliano, por lo anterior $Z(G)$ contiene un elemento de orden p y por lo tanto G contiene un elemento de orden p. Supongamos que $p \nmid |Z(G)|$. Como $p \mid |G|$, de la ecuación (2.2) tenemos que $p \nmid [G : Z(a_i)]$ para algún i. Como $|G| = |Z(a_i)|[G : Z(a_i)]$ y p es primo, necesariamente $p \mid \#(Z(a_i))$. Como $\#(Z(a_i)) < |G|$, por inducción podemos suponer que $Z(a_i)$ (y por lo tanto G) contiene un elemento de orden p. ■

[4]Para todo $n \in \mathbb{N}$, si G' es un grupo de orden n y $p \mid n$, entonces G' contiene un elemento de orden p.

[5]Observemos que $|G/H| = \dfrac{|G|}{|H|} = \dfrac{|G|}{\langle a \rangle}$. Como $p \mid |G|$ y $p \nmid o(a)$, $p \mid |G/H|$, por ser p primo.

Ejercicios propuestos

Ejercicio 2.1. Sean $\langle G_1, +\rangle$ y $\langle G_2, +\rangle$ dos grupos abelianos. Sea $\varphi\colon G_1 \to G_2$ un homomorfismo. Expresar las propiedades (2) y (3) de la Proposición 2.1.3 con la notación aditiva.

Ejercicio 2.2. Sean G_1, G_2 y G_3 grupos y sean $\varphi\colon G_1 \to G_2$ y $\psi\colon G_2 \to G_3$ homomorfismos. Probar que $\psi \circ \varphi\colon G_1 \to G_3$ es un homomorfismo.

Ejercicio 2.3. Sea $\varphi\colon G_1 \to G_2$ un homomorfismo. Probar que $\mathrm{Nu}(\varphi)$ es un subgrupo de G_1. Además, probar que para cada $g \in G_1$ y cada $a \in \mathrm{Nu}(\varphi)$, $gag^{-1} \in \mathrm{Nu}(\varphi)$.

Ejercicio 2.4. Sea D_n el n-ésimo grupo Dihedral. Para cada $a \in D_n$ se define

$$\varphi(a) = \begin{cases} 1 & \text{si } a \text{ es una rotación} \\ -1 & \text{si } a \text{ es una simetría} \end{cases}$$

Probar que φ es un homomorfismo de D_n al grupo multiplicativo $\{-1, 1\}$. Determinar el núcleo de φ.

Ejercicio 2.5. Para cada uno de las siguientes funciones, probar que es un homomorfismo, determinar su núcleo, su imagen, y determinar si es monomorfismo, epimorfismo o isomorfismo.

(a) $f_1\colon \mathbb{R} \to \mathbb{R}_+$, donde $\langle \mathbb{R}, +\rangle$ y $\langle \mathbb{R}_+, .\rangle$.

(b) $f_2\colon GL_2(\mathbb{R}) \to \mathbb{R}^*$, donde $\mathbb{R}^* = \mathbb{R} - \{0\}$ con el producto usual de números reales.

(c) Sea $\mathbb{R}[X]$ el grupo formado por todos los polinomios con coeficientes reales con la suma usual de polinomios. Sea $f_3\colon \mathbb{R}[X] \to \mathbb{R}[X]$ definida por $f_3(p(X)) = p'(X)$, donde $p'(X)$ es el polinomio derivado de $p(X)$.

(d) Sea $\mathbb{C}^* = \mathbb{C} - \{0\}$ con el producto usual de números complejos. Sea $f_4\colon \mathbb{C}^* \to \mathbb{C}^*$ definida por $f_4(z) = z^4$.

(e) $f_5\colon \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ definida por $f_5(\overline{a}) = 3\overline{a}$.

(f) $f_6\colon \mathrm{U}(\mathbb{Z}_{16}) \to \mathrm{U}(\mathbb{Z}_{16})$ definida por $f_6(\overline{a}) = \overline{a}^3$.

Ejercicio 2.6. Sea $\varphi\colon G_1 \to G_2$ un homomorfismo del grupo G_1 al grupo G_2. Sea H un subgrupo de G_1. Probar que:

(a) Si H es cíclico, entonces $\varphi(H)$ es un subgrupo cíclico de G_1.

(b) Si H es abeliano, entonces $\varphi(H)$ es abeliano.

Ejercicio 2.7.

(a) Probar que $\mathrm{U}(\mathbb{Z}_8)$ no es isomorfico a $\mathrm{U}(\mathbb{Z}_{10})$.

(b) Probar que $\mathrm{U}(\mathbb{Z}_8)$ es isomorfico a $\mathrm{U}(\mathbb{Z}_{12})$.

Ejercicio 2.8.

(a) Determinar el grupo permutación al cual es isomorfo $\mathbb{Z}_5$.

(b) Determinar el grupo permutación al cual es isomorfo $\mathrm{U}(\mathbb{Z}_{10})$.

Ejercicio 2.9. Sea G un grupo. Sea $\mathrm{Aut}(G) = \{f : f\colon G \to G \text{ es un isomorfismo}\}$. A los elementos de $\mathrm{Aut}(G)$ se lo llama **Automorfismos de** G. Probar que $\mathrm{Aut}(G)$ con la composición usual de funciones forma un grupo. (*Sug. Es suficiente con probar que* $\mathrm{Aut}(G)$ *es un subgrupo de* $\mathrm{Sym}(G)$.)

Ejercicio 2.10. Sea G un grupo y sea a un elemento de G. Sea $f_a\colon G \to G$ definida por $f_a(x) = axa^{-1}$. Probar que f_a es un automorfismo de G. El automorfismo f_a es llamado el **automorfismo interior de** G **inducido por** a.

Ejercicio 2.11. Sea G un grupo. Sea $\mathrm{Inn}(G) = \{f_a : a \in G\}$ donde para cada $a \in G$, f_a es el automorfismo interior de G inducido por a. Probar que $\mathrm{Inn}(G)$ es un subgrupo de $\mathrm{Aut}(G)$.

Ejercicio 2.12. Determinar los siguientes grupos de automorfismos y automorfismos interiores.

(a) $\mathrm{Aut}(\mathbb{Z})$ y $\mathrm{Inn}(\mathbb{Z})$.

(b) $\mathrm{Aut}(\mathbb{Z}_8)$ y $\mathrm{Inn}(\mathbb{Z}_8)$.

Ejercicio 2.13. Probar que para todo entero positivo n, $\mathrm{Aut}(\mathbb{Z}_n)$ es isomorfo a $\mathrm{U}(\mathbb{Z}_n)$. Seguir los siguientes pasos.

1. Probar que si $\langle \overline{a} \rangle = \mathbb{Z}_n$, entonces $\overline{a} \in \mathrm{U}(\mathbb{Z}_n)$.

2. Probar que si $f\colon G_1 \to G_2$ es un isomorfismo, entonces para todo $a \in G_1$ se tiene que $o(f(a)) = o(a)$.

3. Probar que si $\alpha\colon \mathbb{Z}_n \to \mathbb{Z}_n$ es un isomorfismo, entonces $\alpha(\overline{1}) \in \mathrm{U}(\mathbb{Z}_n)$.

4. Probar que $\varphi\colon \mathrm{Aut}(\mathbb{Z}_n) \to \mathrm{U}(\mathbb{Z}_n)$ definida por $\varphi(\alpha) = \alpha(\overline{1})$ es un isomorfismo.

Ejercicio 2.14. Sea G un grupo y $H \leq G$. Recordemos que $N(H) = \{a \in G : aHa^{-1} = H\}$ es un subgrupo de G, y $C(H) = \{a \in G : aha^{-1} = h, \ \forall h \in H\}$ es un subgrupo de $N(H)$ (véase el Ejercicio 1.2). Probar que la función $\varphi\colon N(H) \to \mathrm{Aut}(H)$ definida por: para cada $a \in N(H)$, sea $\varphi(a) = f_a\colon H \to H$ es dada por $f_a(h) = aha^{-1}$, es un homomorfismo cuyo núcleo es $C(H)$.

Ejercicio 2.15. Considere el grupo alternante A_n de grado (ver 17) el cual sabemos que es un subgrupo normal de S_n (véase el Ejercicio 1.6). Sea $\alpha\colon S_n \to \mathbb{Z}_2$ definida por

$$\alpha(\sigma) = \begin{cases} 0 & \text{si } \sigma \text{ es una permutación par} \\ 1 & \text{si } \sigma \text{ es una permutación impar.} \end{cases}$$

Probar que α es un homomorfismo y su núcleo es A_n. Luego, probar que $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.

Ejercicio 2.16. Sea $\varphi\colon G_1 \to G_2$ un homomorfismo. Probar que si $K \triangleleft G_2$, entonces $\varphi^{-1}(K) \triangleleft G_1$.

Ejercicio 2.17. Sea U_n el conjunto de las raíces n-ésimas de la unidad. Probar que U_n es un subgrupo normal de $\mathbb{C}^*$ y es el núcleo de un homomorphismo

Ejercicio 2.18.

(a) Viendo a $\langle 8\rangle$ y $\langle 48\rangle$ como subgrupos de $\mathbb{Z}$, probar que el grupo cociente $\langle 8\rangle/\langle 48\rangle$ es isomorfico a $\mathbb{Z}_6$.

(b) Probar de forma general que para $n, k \in \mathbb{N}$ tales que $k \mid n$, tenemos que $\langle k\rangle/\langle n\rangle \cong \mathbb{Z}_{(\frac{n}{k})}$.

Ejercicio 2.19. Sea G un grupo cíclico y sea H un subgrupo de G. Probar que el grupo cociente G/H es cíclico.

Ejercicio 2.20. Considere el grupo lineal general de grado 2, $GL_2(\mathbb{R})$. Sea $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) : \det(A) = 1\}$ y $H = \{A \in GL_2(\mathbb{R}) : \det(A) \in \{-1, 1\}\}$. Probar que

$$GL_2(\mathbb{R})/SL_2(\mathbb{R}) \cong \mathbb{R}^* \qquad \text{y} \qquad GL_2(\mathbb{R})/H \cong \mathbb{R}^+.$$

Ejercicios con GAP

Ejercicio 2.21.

(a) Generar los grupos Z_{30} y $\mathbb{Z}_{42}$ como grupos de permutaciones.

(b) Hallar todos los elementos de $\mathbb{Z}_{42}$ de orden 2, 3 y 6.
(*Ayuda:* Defina la siguiente función:
`gap>f:=i -> Order(Elements(Z42)[i]);;)`
Genere la siguiente lista:
```
gap>List([1..42], f);
[ 1, 42, 21, 14, 21, 42, 7, 6, 21, 14, 21, 42, 7, 42, 3, 14, 21, 42, 7, 42,
21, 2, 21, 42, 7, 42, 21, 14, 3, 42, 7, 42, 21, 14, 21, 6, 7, 42, 21, 14, 21,
42 ]
```
Entonces, por ejemplo, `Elements(Z42)[8]` es un elemento de orden 6 y `Elements(Z42)[15]` es un elemento de orden 3.

(c) Para cada elemento a del inciso anterior, generar el homomorfismo $f_a\colon \mathbb{Z}_{30} \to \mathbb{Z}_{42}$ dado por $f_a(\overline{1}) = a$.

(d) Para cada uno de los homomorfismos anteriores, hallar su núcleo e imagen. Indicar cuáles son monomorfismos y cuáles epimorfismos.

Ejercicio 2.22. Sea $G = \langle a\rangle$ un grupo cíclico de orden n. Se definen las funciones $f_k\colon G \to G$ por $f_k(a^i) = a^{ki}$ para $i = 1, 2, \ldots, n-1$, las cuales son homomorfismos (endomorfismos).

Notar que la imagen de cada f_k es $f_k(G) = \langle f_k(a) \rangle$. Tomar $n = 10$ y determinar cuáles de los homomorfismos f_k, con $k = 1, 2, \ldots, 10$, son isomorfismos[6] (autoisomorfismos). Formule una conjetura y compruebe para otros valores de n y k.

Ejercicio 2.23. Generar los grupos dihedrales D_n para $n = 6, 8, 10, 12$.

(a) Para cada D_n, hallar su centro $Zn = Z(D_n)$.

(b) Preguntarle a GAP is Zn es normal en D_n, para cada n.

(c) Determinar el orden de cada centro Zn.

(d) Para cada n, hallar las clases laterales derechas de Zn en D_n.

(e) Generar el grupo cociente D_n/Zn.

(f) Para cada n, comprobar que $\dfrac{|D_n|}{|Zn|} = \left|\dfrac{D_n}{Zn}\right|$.

Ejercicio 2.24. Generar cada grupo, y comprobar el Teorema de Cauchy. Esto es, para cada divisor primo p del orden del grupo hallar un elemento de orden p.

(a) $G_1 = S_4$. (b) $G_2 = S_5$. (c) $G_3 = D_4$. (d) $G_4 = Z_{10}$. (e) $G_5 = U(15)$.

[6]Recuerde que si los conjuntos A y B son finitos y tienen la misma cantidad de elementos, entonces una función $f\colon A \to B$ es biyectiva sí y solo si f es sobreyectiva. También recuerde que f es sobreyectiva si $f(A) = B$.

Capítulo 3

Grupos Abelianos Finitos

En este capítulo veremos dos nuevos métodos de construir grupos a partir de unos dados, a saber producto directo de grupos y suma directa de subgrupos. A diferencia de considerar subgrupos y grupos cocientes, estos dos métodos nuevos permiten obtener grupos mayores que los originales. Esto nos permitirá establecer el Teorema Fundamental de los Grupos Abelianos Finitos.

3.1. Producto Directo de Grupos

Sean G_1 y G_2 dos grupos arbitrarios. Consideremos el producto cartesiano de G_1 por G_2:

$$G_1 \times G_2 = \{(a_1, a_2) : \ a_1 \in G_1 \text{ y } a_2 \in G_2\}.$$

Podemos definir de manera natural una operación binaria sobre $G_1 \times G_2$ de la siguiente forma: dados $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$,

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Como G_1 y G_2 son grupos, esta operación está bien definida.

Proposición 3.1.1. *Si G_1 y G_2 son dos grupos, entonces $G_1 \times G_2$ con la operación arriba definida es un grupo. Si G_1 y G_2 son abelianos, entonces $G_1 \times G_2$ es abeliano.*

Llamaremos al grupo $G_1 \times G_2$ el **producto directo de** G_1 por G_2. En realidad, llamaremos a $G_1 \times G_2$ el **producto directo de** G_1 y G_2, porque es sencillo comprobar que $G_1 \times G_2$ es isomorfico a $G_2 \times G_1$.

Dados dos grupos G_1 y G_2, tenemos dos funciones naturales del producto directo sobre una de las componentes del producto. Esto es, se definen

$$\pi_1 : G_1 \times G_2 \to G_1 \quad \text{y} \quad \pi_2 : G_1 \times G_2 \to G_2$$

como sigue:

$$\pi_1(a_1, a_2) = a_1 \quad \text{y} \quad \pi_2(a_1, a_2) = a_2$$

para todo $(a_1, a_2) \in G_1 \times G_2$.

Proposición 3.1.2. *Las funciones π_1 y π_2 son epimorfismos.*

Los epimorfismos π_1 y π_2 son llamados las **proyecciones canónicas** de la primera y segunda coordenada (argumento), respectivamente.

Observación 3.1.3. Para cualesquiera dos grupos G_1 y G_2, el producto directo $G_1 \times G_2$ contiene dos subgrupos normales particulares (aparte de los triviales), a saber

$$\widehat{G_1} = \{(a, e_2) : \ a \in G_1\} \quad \text{y} \quad \widehat{G_2} = \{(e_1, b) : \ b \in G_2\}.$$

Además, $G_1 \cong \widehat{G_1}$ y $G_2 \cong \widehat{G_2}$.

Proposición 3.1.4. *Sean G_1 y G_2 dos grupos. Si $G = G_1 \times G_2$, entonces*

$$G/\widehat{G_1} \cong G_2 \quad y \quad G/\widehat{G_2} \cong G_1.$$

Así como hemos definido el producto directo de dos grupos, podemos definir el producto directo de un número finito de grupos (y aún más, se puede definir el producto directo de una familia arbitraria de grupos). Sean $G_1, \ldots, G_n$ grupos, con $n > 1$, y consideramos sobre el producto cartesiano $G_1 \times \cdots \times G_n$ la operación binaria definida (de manara análoga al caso de $n = 2$) por

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

para todos $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \cdots \times G_n$. También, para cada $i = 1, \ldots, n$, tenemos la **i-ésima proyección canónica**

$$\pi_i : G_1 \times \cdots \times G_n \to G_i$$

definida por

$$\pi_i(a_1, \ldots, a_i, \ldots, a_n) = a_i.$$

Ejemplo 3.1.5. Sea C_2 un grupo cíclico de orden dos y sea C_3 un grupo cíclico de orden 3. Esto es, $C_2 = \langle a \rangle = \{e, a : \ a^2 = e\}$ y $C_3 = \langle b \rangle = \{e, b, b^2 : \ b^3 = e\}$. Entonces, el producto directo de C_2 y C_3 es

$$C_2 \times C_3 = \{(e, e), (e, b), (e, b^2), (a, e), (a, b), (a, b^2)\}.$$

El producto directo $C_2 \times C_3$ es un grupo de orden 6. No es difícil comprobar que el elemento (a, b) de $C_2 \times C_3$ es de orden 6. Entonces, $C_2 \times C_3$ es un grupo cíclico generado por el elemento (a, b), esto es, $C_2 \times C_3 = \langle (a, b) \rangle$. En otras palabras

$$C_2 \times C_3 = C_6 = \{e, c, c^2, c^3, c^4, c^5 : \ c^6 = e\}.$$

con $c = (a, b)$. ■

Proposición 3.1.6. *Sean G_1 y G_2 grupos finitos. Entonces, para todo $(a_1, a_2) \in G_1 \times G_2$, tenemos que*

$$o(a_1, a_2) = mcm(o(a_1), o(a_2)).$$

Demostración. Sea $(a_1, a_2) \in G_1 \times G_2$. Supongamos que $n = o(a_1)$, $m = o(a_2)$ y $k = o(a_1, a_2)$. Como $(e_1, e_2) = (a_1, a_2)^k = (a_1^k, a_2^k)$, resulta que $a_1^k = e_1$ y $a_2^k = e_2$ y por tanto $n \mid k$ y $m \mid k$. Luego, si $t = mcm(n, m)$, entonces $t \mid k$. Por otra parte, como $n \mid t$ y $m \mid t$, $(a_1, a_2)^t = (a_1^t, a_2^t) = (e_1, e_2)$. Entonces, $k \mid t$. Con lo cual, $mcm(n, m) = t = k = o(a_1, a_2)$. ■

Ejemplo 3.1.7. Determinemos el número de elementos del grupo $\mathbb{Z}_{100} \times \mathbb{Z}_{25}$ de orden 10. Por la Proposición 3.1.6 debemos determinar el número de elementos $(a, b) \in \mathbb{Z}_{100} \times \mathbb{Z}_{25}$ tal que $o(a, b) = mcm(o(a), o(b)) = 10$. Entonces, las posibilidades para $o(a)$ y $o(b)$ son (tener en cuenta que $o(a) \mid 100$ y $o(b) \mid 25$): $o(a) = 10$ y $o(b) = 5$ o 1, o $o(a) = 2$ y $o(b) = 5$.

Caso 1: $o(a) = 10$ y $o(b) = 1$ o 5. Para a: Como $\mathbb{Z}_{100}$ tiene un único subgrupo cíclico de orden 10, y en un grupo cíclico de orden 10 hay 4 generadores, entonces en $\mathbb{Z}_{100}$ hay 4 elementos de orden 10. Para b: el único elemento de orden 1 es $\overline{0}$; en $\mathbb{Z}_{25}$ hay un único subgrupo cíclico de orden 5, y todo grupo cíclico de orden 5 tiene 4 generadores. Con lo cual en $\mathbb{Z}_{25}$ hay un elemento de orden 1 y 4 de orden 5. Por lo tanto, en este caso tenemos 4.5=20 elementos de orden 10 en $\mathbb{Z}_{100} \times \mathbb{Z}_{25}$.

Caso 2: $o(a) = 2$ y $o(b) = 5$. Para a: Todo grupo cíclico de orden par tiene tiene un único subgrupo de orden 2. Así hay un sólo elemento de $\mathbb{Z}_{100}$ de orden 2. Para b: Igual que en el caso anterior, tenemos que hay 4 elementos de orden 5 en $\mathbb{Z}_{25}$. Entonces, en este caso tenemos 4 elementos de orden 10.

Por lo tanto, $\mathbb{Z}_{100} \times \mathbb{Z}_{25}$ tiene en total 24 elementos de orden 10. ■

Por la Proposición 2.1.12 sabemos que los grupos cíclicos de orden n finitos son exactamente, salvo isomorfismo, todos los $\mathbb{Z}_n$ con $n \geq 1$. Con lo cual, podemos generalizar y abstraer el Ejemplo 3.1.5 de una manera más general.

Proposición 3.1.8. *Sean n y m enteros positivos. Entonces, m y n son relativamente primos si y sólo si $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.*

Demostración. Supongamos primero que m y n son relativamente primos. El producto directo de $\mathbb{Z}_m$ y $\mathbb{Z}_n$ es

$$\mathbb{Z}_m \times \mathbb{Z}_n = \{(a, b) : \ a \in \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}, \quad b \in \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}\}$$

y es un grupo de orden mn. Ahora, por la Proposición 3.1.6, tenemos que

$$o((\overline{1}, \overline{1})) = mcm(o(\overline{1}), o(\overline{1})) = mcm(m, n) = mn.$$

Luego, $\mathbb{Z}_m \times \mathbb{Z}_n$ es un grupo cíclico de orden mn generado por el par $(\overline{1}, \overline{1})$. Por lo tanto, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Ahora supongamos que $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ y probemos que $(m, n) = 1$. Como $\mathbb{Z}_m \times \mathbb{Z}_n$ es cíclico, existe un par $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ tal que $o((a, b)) = mn$. Veamos que $o(a) = m$ y $o(b) = n$. Como $o(a)n.(a, b) = (0, 0)$, tenemos que $mn \mid o(a)n$. Así $m \mid o(a)$. Además, ya que $a \in \mathbb{Z}_m$, $o(a) \mid m$. Con lo cual, hemos mostrado que $o(a) = m$. Análogamente, $o(b) = n$. Entonces tenemos que

$$mn = o((a, b)) = mcm(o(a), o(b)) = mcm(m, n)$$

y esto implica que m y n son relativamente primos. ■

El resultado de la proposición anterior se puede generalizar de la siguiente forma: $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ es un grupo cíclico si y sólo si los enteros positivos $m_1, \ldots, m_k$ son relativamente primos dos a dos[1] (ver Ejercicio 3.3). Esta afirmación se puede probar por inducción sobre el número de factores en $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ y utilizando la proposición anterior.

Ejemplo 3.1.9. Considere el grupo $G = \mathbb{Z}_{24} \times \mathbb{Z}_{36} \times \mathbb{Z}_{60}$. Como 24, 36 y 60 no son relativamente primos, tenemos que G no es cíclico, en otras palabras, G no contiene un elemento de orden $51840 = 24 \cdot 36 \cdot 60$. Pero podemos afirmar que el mayor orden posible de los elementos de G es el mínimo común múltiplo (mcm) de 24, 36 y 60, el cual es 360. Para probar esto, primero notemos que el elemento $(\overline{1}, \overline{1}, \overline{1})$ es de orden 360, pues $o(\overline{1}, \overline{1}, \overline{1}) = mcm(o(\overline{1}), o(\overline{1}), o(\overline{1})) = mcm(24, 36, 60) = 360$. Además, ya que 360 es múltiplo de 24, 36 y 60, tenemos que $360.a = 0$ para todo $a \in G$. Entonces, $o(a) \mid 360$. Así, $o(a) \leq 360$ para todo $a \in G$. ■

3.2. Grupos Abelianos Finitos

Dado que en esta sección todos los grupos son abelianos, denotaremos *al elemento neutro de dichos grupos por* 0. Cuando haya peligro de confusión, usaremos subíndice: 0_G denota el elemento neutro del grupo abeliano G.

Sea G un grupo abeliano. Sean H_1 y H_2 dos subgrupos de G. Consideramos la función $s\colon H_1 \times H_2 \to G$ definida por

$$s(a_1, a_2) = a_1 + a_2$$

para todos $a_1 \in H_1$ y $a_2 \in H_2$. Es sencillo verificar que la función s es un homomorfismo. Recordemos que tenemos definida la suma de dos subgrupos de un grupo. Esto es,

$$H_1 + H_2 = \{a_1 + a_2 : \ a_1 \in H_1 \text{ y } a_2 \in H_2\}$$

es un subgrupo de G, pues G es abeliano y así todo subgrupo es normal. Con lo cual, la función s tiene como imagen al subgrupo $H_1 + H_2$. Esto es, $s\colon H_1 \times H_2 \to H_1 + H_2$ es un epimorfismo. La siguiente proposición nos dice cuándo s es un isomorfismo. En otras palabras, la proposición da condiciones necesarias y suficientes para que los grupos $H_1 \times H_2$ y $H_1 + H_2$ sean isomorfos.

Proposición 3.2.1. *Sea G un grupo abeliano y sean H_1 y H_2 dos subgrupos de G. Entonces, las siguientes condiciones son equivalentes:*

(1) *$s\colon H_1 \times H_2 \to H_1 + H_2$ es un isomorfismo;*

(2) *$H_1 \cap H_2 = \{0\}$;*

(3) *los elementos de $H_1 + H_2$ se escriben de manera única como $a_1 + a_2$ con $a_1 \in H_1$ y $a_2 \in H_2$.*

Demostración. (1) $\Rightarrow$ (2) Sea $a \in H_1 \cap H_2$. Así, $-a \in H_2$. Luego, $s(a, -a) = a + (-a) = 0 = 0 + 0 = s(0, 0)$. Como s es un isomorfismo, $(a, -a) = (0, 0)$. Entonces, $a = 0$. Por lo tanto, $H_1 \cap H_2 = \{0\}$.

[1]Son relativamente primos dos a dos si m_i y m_j son relativamente primos para todos i y j distintos.

(2) $\Rightarrow$ (3) Sea $x \in H_1 + H_2$ y supongamos que $x = a_1 + a_2$ y $x = b_1 + b_2$ con $a_1, b_1 \in H_1$ y $a_2, b_2 \in H_2$. Entonces $H_1 \ni a_1 - b_1 = b_2 - a_2 \in H_2$. Luego $a_1 - b_1, b_2 - a_2 \in H_1 \cap H_2 = \{0\}$ y así tenemos que $a_1 = b_1$ y $a_2 = b_2$. Por lo tanto, todo elemento $x \in H_1 + H_2$ se escribe de forma única como $x = a_1 + a_2$ con $a_1 \in H_1$ y $a_2 \in H_2$.

(3) $\Rightarrow$ (1) Como hemos visto anteriormente, s es un epimorfismo. Así, solo resta probar que s es inyectiva. Supongamos que $s(a_1, a_2) = s(b_1, b_2)$. Esto es, $a_1 + a_2 = b_1 + b_2$. Por (3), tenemos que $a_1 = b_1$ y $a_2 = b_2$ y así $(a_1, a_2) = (b_1, b_2)$. Entonces s es inyectiva y por lo tanto es un isomorfismo. ■

Si alguna de las condiciones equivalentes de la proposición anterior se cumple, diremos que la suma $H_1 + H_2$ es **directa** y escribiremos $H_1 \oplus H_2$ en lugar de $H_1 + H_2$.

Ejemplo 3.2.2.

(1) Sea $G = G_1 \times G_2$. Entonces, como vimos $\widehat{G_1}$ y $\widehat{G_2}$ son subgrupos de G y se verifica que $G = \widehat{G_1} \oplus \widehat{G_2}$.

(2) Sea X un conjunto no vacío y consideremos el grupo $\mathcal{P}(X)$ de subconjuntos de X cuya operación es la diferencia simétrica, esto es, si $A, B \subseteq X$, entonces $A \triangle B = (A \cup B) - (A \cap B)$. Supongamos que $X = A \cup B$ para ciertos subconjuntos A y B de X tales que $A \cap B = \emptyset$. Entonces, $\mathcal{P}(A)$ y $\mathcal{P}(B)$ son subgrupos de $\mathcal{P}(X)$ tales que $\mathcal{P}(X) = \mathcal{P}(A) \oplus \mathcal{P}(B)$.

(3) Sea p un número primo y para $n \in \mathbb{Z}^+$ considere

$$E_{p^n} := \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \quad (n \text{ factores}).$$

Entonces, E_{p^n} es un grupo abeliano de orden p^n con la propiedad que $o(x) = p$ para todo $x \in E_{p^n}$. Este grupo es llamado el **grupo abeliano elemental de orden** p^n. Ahora vamos a mostrar que el grupo abeliano elemental de orden p^2 tiene exactamente $p + 1$ subgrupos de orden p. Ya que cada elemento no nulo de E_{p^2} tiene orden p, cada uno de estos genera un subgrupo cíclico de orden p de E_{p^2}. Por el Teorema de Lagrange, subgrupos distintos de orden p se intersecan trivialmente[2]. Así, los $p^2 - 1$ elementos no nulos de E_{p^2} son separados en subconjuntos (cuya intersecciones dos a dos solo contienen el 0) de tamaño $p - 1$. Entonces, debe haber

$$\frac{p^2 - 1}{p - 1} = p + 1$$

subgrupos distintos de orden p. ■

Podemos generalizar la noción de suma directa de subgrupos de la siguiente manera. Sea G un grupo abeliano y sean $H_1, \ldots, H_n$ subgrupos de G. Consideremos la suma de dichos subgrupos, $H_1 + \cdots + H_n = \{h_1 + \cdots + h_n : \ h_i \in H_i \text{ con } i = 1, \ldots, n\}$. Esta suma es un subgrupo de G. Diremos que la suma $H_1 + \cdots + H_n$ es directa y escribiremos $H_1 \oplus \cdots \oplus H_n$ si se verifica que:

$$h_1 + \cdots + h_n = h_1' + \cdots + h_n' \Longrightarrow h_i = h_i' \ \forall i = 1, \ldots, n$$

[2]Dos subgrupos H_1 y H_2 se intersecan trivialmente si $H_1 \cap H_2 = \{0\}$.

donde $h_i, h_i' \in H_i$ para $i = 1, \ldots, n$.

Sea G un grupo abeliano finito de orden n. Como hemos visto en el Capítulo 1 Sección 1.6, para cada $a \in G$, $o(a) \mid n$. Así, los órdenes de los elementos de G están acotados superiormente. Por lo tanto, podemos dar la siguiente definición.

Definición 3.2.3. Sea G un grupo abeliano finito de orden n. Llamaremos **exponente** de G al mayor de los órdenes de los elementos de G. Lo denotamos por $\exp(G)$. Esto es,

$$\exp(G) = \text{máx}\{o(a) : a \in G\}.$$

Notemos que si $m = \exp(G)$, entonces existe un elemento $a \in G$ tal que $o(a) = m$ y para todo $x \in G$, $o(x) \leq m$.

Proposición 3.2.4. *Sea G un grupo abeliano finito y sea $m = \exp(G)$. Entonces, para cada $a \in G$, $o(a) \mid m$.*

Demostración. Sea $a \in G$ tal que $o(a) = m$ y sea $x \in G$ con $o(x) = f$. Por definición de $m = \exp(G)$, $f \leq m$. Supongamos que $f \nmid m$. Entonces, algún divisor primo p de m debe figurar en f con mayor exponente que en m. Es decir, $m = p^u m_0$ y $f = p^v f_0$ con $p \nmid m_0$, $p \nmid f_0$ y $v > u \geq 0$. Entonces, el elemento $y = p^u.a$ tiene orden m_0[3] y el elemento $z = f_0.x$ tiene orden p^v[4]. Como m_0 y p^v son relativamente primos[5], el elemento $y + z$ tiene orden[6] $p^v m_0 > p^u m_0 = e$. Lo cual es una contradicción, pues $m = \exp(G)$. Luego, f divide a m. ■

Corolario 3.2.5. *Sea G un grupo abeliano finito y sea $e = \exp(G)$. Entonces, $e.a = 0$ para todo $a \in G$.*

Demostración. Sea $a \in G$. Por la proposición anterior, $o(a) \mid e$. Con lo cual, $e = o(a)q$ con $q \in \mathbb{Z}$. Así, $e.a = (o(a)q).a = q.(o(a).a)) = q.0 = 0$. ■

Ejemplo 3.2.6.

(1) Sea $\varphi \colon G \to G'$ un epimorfismo. Entonces, $\exp(G')$ *es un divisor de* $\exp(G)$. En efecto, si $a' \in G'$ es tal que $o(a') = \exp(G') = e'$, sea $a \in G$ tal que $\varphi(a) = a'$. Si $t = o(a)$, entonces $0' = \varphi(0) = \varphi(t.a) = t.\varphi(a) = t.a'$. Entonces, e' divide a t, que a su vez t divide a $\exp(G)$. Por lo tanto, $\exp(G') = e' \mid \exp(G)$.

(2) Sea G un grupo finito de orden n. Entonces, G es cíclico si y sólo si $\exp(G) = n$. ■

Proposición 3.2.7. *Sean G_1 y G_2 grupos abelianos finitos. Entonces,*

$$\exp(G_1 \times G_2) = mcm(\exp(G_1), \exp(G_2)).$$

[3] En efecto, $m_0.y = m_0 p^u.a = m.a = 0$. Si $t.y = 0 \Longrightarrow tp^u.a = 0 \Longrightarrow m \mid tp^u \Longrightarrow p^u m_0 \mid tp^u \Longrightarrow m_0 \mid t \Longrightarrow m_0 \leq t$. Por lo tanto, $o(y) = m_0$.

[4] Similar al caso anterior.

[5] Pues, si m_0 y p^v no son relativamente primos, entonces hay un primo p' tal que $p' \mid m_0$ y $p' \mid p^v \Longrightarrow p' = p \Longrightarrow p \mid m_0$. Lo cual es absurdo.

[6] Ver en el Capítulo 1 Sección 1.6.

Demostración. Sean $k = \exp(G_1 \times G_2)$, $n = \exp(G_1)$ y $m = \exp(G_2)$. Entonces, existen $a_1 \in G_1$ y $a_2 \in G_2$ tal que $o(a_1) = n$ y $o(a_2) = m$. Ahora, por el punto (2) del Ejemplo 3.1.5, obtenemos que

$$o(a_1, 0_2) = mcm(o(a_1), o(0_2)) = mcm(n, 1) = n \quad \text{y}$$

$$o(0_1, a_2) = mcm(o(0_1), o(a_2)) = mcm(1, m) = m.$$

Entonces, Por la Proposición 3.2.4, $n \mid k$ y $m \mid k$. Con lo cual, k es múltiplo de n y m. Sea d un múltiplo de n y m. Esto es, $n \mid d$ y $m \mid d$. Así , $d = nq_1$ y $d = mq_2$. Como $k = \exp(G_1 \times G_2)$, existe $(a, b) \in G_1 \times G_2$ tal que $o(a, b) = k$. Entonces, por el Corolario anterior,

$$d.(a, b) = (d.a, d.b) = (nq_1.a, mq_2.b) = (0_1, 0_2)$$

y por tanto, $k \mid d$. Hemos mostrado que $k = mcm(n, m)$. por lo tanto, $\exp(G_1 \times G_2) = mcm(\exp(G_1), \exp(G_2))$. ■

Proposición 3.2.8. *Sea G un grupo abeliano finito no cíclico y sea $a \in G$ tal que $o(a) = \exp(G)$. Entonces, $\langle a\rangle$ es un sumando directo de G, esto es, existe un subgrupo T de G tal que $G = \langle a\rangle \oplus T$.*

Demostración. Como G no es cíclico y $o(a) = \exp(G) = e > 1$, $\{0\} \subsetneq \langle a\rangle \subsetneq G$. Veamos en primer lugar la siguiente afirmación:
Afirmación: *Existe un primo p y existe un $x \notin \langle a\rangle$ tal que $p.x = 0$.*

Consideremos el conjunto $X = \{x \in G : \ x \notin \langle a\rangle\}$ que es no vacío. Podemos elegir en X un elemento x con el menor orden posible. Es decir, $o(x) \leq o(y)$ para todo $y \in X$. Sea $t = o(x)$. Entonces, $t > 1$ (pues, si $t = 1$, entonces $x = 1.x = 0 \in \langle a\rangle$ lo cual es absurdo). Así, podemos elegir un divisor primo p de t. Si $p = t$, no hay nada que probar. Supongamos que $t = p.s$. Como $s.(p.x) = (sp).x = t.x = 0$, $o(p.x) \leq s < t$. Con lo cual, $p.x \notin X$ y así $p.x \in \langle a\rangle$. Si $p.x = 0$, no hay nada que probar. Supongamos entonces que $p.x = i.a$ para algún $0 < i < o(a) = e$. Luego, como $t \mid e$ y por lo tanto $p \mid e$. Esto es, $e = pf$. Luego, $0 = e.x = f.(p.x) = f.(i.a)$ y entonces $e \mid fi$, esto es, $pf \mid fi$. Con lo cual, $p \mid i$. Si $i = pj$, entonces $p.x = i.a = (pj).a$. Si ponemos $y = x - j.a$ entonces $p.y = p.x - (pj).a = p.x - i.a = 0$. Por otra parte, $y \notin \langle a\rangle$, pues si $y \in \langle a\rangle$ tendríamos que $y, j.a \in \langle a\rangle$ y, así $x = y + j.a \in \langle a\rangle$, lo que es imposible. Esto prueba la afirmación.

Sea $x \notin \langle a\rangle$ y p un primo tal que $p.x = 0$. Afirmamos que $\langle a\rangle \cap \langle x\rangle = \{0\}$. Pues, si $i.x \in \langle a\rangle$ con $0 < i < p = o(x)$[7] y por lo tanto $\langle i.x\rangle \subseteq \langle a\rangle$. Como $(i, p) = 1$ tenemos que $\langle x\rangle = \langle i.x\rangle \subseteq A$[8]. Esto es, $x \in \langle a\rangle$, lo cual es absurdo.

Sea el grupo cociente $G' = G/\langle x\rangle$. Luego, $o(G') = \frac{o(G)}{p} < o(G)$. Si $\pi \colon G \to G'$ es el epimorfismo canónico, entonces de $e.a = 0$ resulta que $e.\pi(a) = 0$, es decir, $o(\pi(a)) \mid e$. Si $f.\pi(a) = 0$ entonces $\pi(f.a) = 0$, esto es, $f.a \in \mathrm{Nu}(\pi) = \langle x\rangle$. Y como $f.a \in \langle a\rangle$, tenemos que

[7] Por ser p primo.

[8] Supongamos que $(i, p) = 1$. Es claro que $\langle i.x\rangle \subseteq \langle x\rangle$. Sea n un entero. Como i y p son relativamente primos, $1 = iq + pk$ con q y k enteros. Así, $n = niq + npk$. Luego, $n.x = niq.x + npk.x$. Como $o(x) = p$, $npk.x = 0$. Entonces, $n.x = niq.x = (nq).(i.x) \in \langle i.x\rangle$. Entonces, $\langle x\rangle \subseteq \langle i.x\rangle$.

$f.a = 0$, así $e \mid f$. Luego, $o(\pi(a)) = e$. Como G' es imagen homomórfica de G sabemos que $\exp(G')$ divide a $\exp(G) = e$ y como $\pi(a) \in G'$ es tal que $o(\pi(a)) = e$ tenemos que e divide a $\exp(G')$. Luego concluimos que $\exp(G') = \exp(G) = e$. Ahora bien, como el orden de $\pi(a)$ es el exponente de G' y $o(G') < o(G)$ por inducción sobre el orden de G podemos suponer que $\langle \pi(a) \rangle$ es un sumando directo de G', esto es, que existe un subgrupo T' de G' tal que $G' = \langle \pi(a) \rangle \oplus T'$.

Sea $T := \pi^{-1}(T')$ que es un subgrupo de G tal que $\langle x \rangle \subseteq T$ (pues, $\langle x \rangle = \mathrm{Nu}(\pi)$, de donde $\pi(\langle x \rangle) = \{0\} \subseteq T'$). Ahora probaremos que $G = \langle a \rangle \oplus T$.

- Sea $u \in \langle a \rangle \cap T$. Así, $u = i.a$ y $\pi(u) = i.\pi(a) \in \langle \pi(a) \rangle$. Como $u \in T$, $\pi(u) \in T'$. Luego, $\pi(u) \in \langle \pi(a) \rangle \cap T' = \{0\}$, esto es, $\pi(u) = 0$ y por lo tanto, $u \in \mathrm{Nu}(\pi) = \langle x \rangle$ y como $u \in \langle a \rangle$ resulta que $u = 0$. Hemos probado que $\langle a \rangle \cap T = \{0\}$.

- Vamos a probar que $G = \langle a \rangle + T$. Sea $g \in G$. Entonces, $\pi(g) \in G' = \langle \pi(a) \rangle \oplus T'$. con lo cual, $\pi(g) = i.\pi(a) + t'$ con $t' \in T'$. Así, $t' = \pi(t)$ con $t \in T$, pues π es sobreyectiva. Luego $\pi(g) = \pi(i.a + t)$ y en consecuencia, $g - (i.a + t) \in \mathrm{Nu}(\pi) = \langle x \rangle \subseteq T$ y, por lo tanto $g = i.a + s$ con $s \in T$. ∎

Ejemplo 3.2.9. Sea $G = \mathbb{Z}_4 \times \mathbb{Z}_6$. Por (2) del Ejemplo 3.2.6 y por la Proposición 3.2.7, sabemos que $\exp(G) = 12$ y que el par $(1, 1)$ tiene orden 12. Entonces, por la proposición anterior, hay un subgrupo T de G tal que $G = \langle (1, 1) \rangle \oplus T$. De aquí observamos que T debe tener orden 2. Por ejemplo el par $(2, 3)$ tiene orden 2 y $(2, 3) \notin \langle (1, 1) \rangle$. Entonces, $G = \langle (1, 1) \rangle \oplus \langle (2, 3) \rangle$. ∎

Teorema 3.2.10 (Teorema Fundamental de los Grupos Abelianos Finitos)**.** *Sea G un grupo abeliano finito. Entonces,*

(1) $G = G_1 \oplus G_2 \oplus \cdots \oplus G_{s-1} \oplus G_s$
donde $G_1, \ldots, G_s$ son subgrupos cíclicos de G y cuyos órdenes $e_1, e_2, \ldots, e_s$ son tales que $e_s \mid e_{s-1} \mid \cdots \mid e_2 \mid e_1$.

(2) *El número s de subgrupos y los órdenes $e_1, \ldots, e_s$ en (1) están unívocamente determinados por G (es decir, si $G = H_1 \oplus \cdots \oplus H_r$ con $H_1, \ldots, H_r$ subgrupos cíclicos de G, de órdenes $f_1, \ldots, f_r$ tales que $f_r \mid f_{r-1} \mid \cdots \mid f_2 \mid f_1$, entonces $r = s$ y $e_1 = f_1, \ldots, e_s = f_s$).*

Demostración. Sean $e_1 = \exp(G)$ y $a_1 \in G$ tal que $o(a_1) = e_1$. Por la Proposición 3.2.8, tenemos que $G = \langle a_1 \rangle \oplus T$ para algún subgrupo T de G. Si $T = \{0\}$, entonces $G = \langle a_1 \rangle$ es cíclico y hemos terminado. Supongamos que $T \neq \{0\}$. Notemos que $o(T) < o(G)$ y los órdenes de los elementos de T son divisores de e_1[9], de donde $e_2 = \exp(T)$ es tal que $e_2 \mid e_1$. Aplicando el mismo razonamiento a T, si $a_2 \in T$ es tal que $o(a_2) = e_2$, entonces $T = \langle a_2 \rangle \oplus T_1$ para algún subgrupo T_1 de T. Con lo cual, $G = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus T_1$ y $o(T_1) < o(T) < o(G)$. Cada vez que aplicamos este procedimiento obtenemos un subgrupo de menor orden y por lo tanto luego de un número finito de pasos obtendremos la descomposición buscada.

Para probar la unicidad, vamos a probar primero por un lado que $r \leq s$ y que $o(H_j) \mid o(G_j)$ para todo $j = 1, \ldots, r$. Para esto, suponemos por contradicción que una de las siguientes afirmaciones se cumple:

[9] Esto es consecuencia de que $T \subseteq G$ y la Proposición 3.2.4

(1) Existe un índice j tal que $o(H_j) \nmid o(G_j)$;

(2) $r > s$.

Supongamos que la condición (1) se cumple. Recordemos que $o(G_j) = e_j$. Entonces, $e_j.G = e_j.G_1 \oplus \cdots \oplus e_j.G_{j-1}$ (pues, $e_j.G_i = \{0\}$ ya que $e_i \mid e_j$ para $i = j+1, j+2, \ldots, n$) y $e_j.H_j \neq \{0\}$ (pues, como $H_j = \langle b_j \rangle$ es cíclico, si $e_j H_j = \{0\}$ entonces $o(H_j) = o(b_j) \mid e_j = o(G_j)$ lo cual es absurdo). Sea $r_j = o(e_j.H_j) > 1$ y consideremos el subgrupo K_1 de $e_j.G$ cuyos elementos tienen orden un divisor de r_j, es decir, $K_1 = \{x \in e_j.G : \ r_j x = 0\}$. Si $x \in K_1$, entonces $x = e_j x_1 + \cdots + e_j x_{j-1}$, con $x_i \in G_i$[10] y $0 = r_j x = r_j e_j x_1 + \cdots + r_j e_j x_{j-1}$.

Como los $x_i \in G_i$ y los G_i forman una suma directa, entonces $r_j e_j x_i = 0$ para todo $i = 1, \ldots, j-1$. Esto implica que $e_j x_i \in K_1$ para todo $i = 1, \ldots, j-1$, entonces

$$x \in (K_1 \cap G_1) \oplus \cdots \oplus (K_1 \cap G_{j-1})^{11}.$$

Con lo cual $K_1 \subseteq (K_1 \cap G_1) \oplus \cdots \oplus (K_1 \cap G_{j-1})$. Además, se tiene que $K_1 \cap G_i$ con $i = 1, \ldots, j-1$ es cíclico de orden menor o igual que r_j, pues es un subgrupo del grupo cíclico G_i, y los elementos de K_1 tienen orden a lo más r_j.

De lo anterior podemos concluir que $o(K_1) \leq r_j^{j-1}$ Por otro lado se tiene que para cada $i = 1, \ldots, j$, H_i contiene un subgrupo T_i isomorfo a H_j (pues, $o(H_j)$ divide a $o(H_i)$ para $i = 1, \ldots, j$ y H_i es cíclico), entonces $e_j.T_i \cong e_j.H_j$ y de aquí $r_j e_j.T_i \cong r_j e_j.H_j = \{0\}$, por lo tanto $e_j.T_i \subseteq K_1$, para todo $i = 1, \ldots, j$. De esto

$$e_j T_1 \oplus \cdots \oplus e_j.T_j \subseteq K_1,^{12}$$

lo cual implica que $r_j^j \leq o(K_1) \leq r_j^{j-1}$[13], lo que es una contradicción, ya que $r_j > 1$.

Ahora, si suponemos que se cumple (2), esto es, $r > s$, entonces $r \geq s+1$. Tomemos $j = s+1$, $G_j = \{0\}$ y claramente se tiene que $o(H_j) \nmid o(G_j)$. Aplicando el argumento anterior, para este caso, se llega a una contradicción.

Por lo tanto, hemos demostrado que

$$r \leq s \quad \text{y} \quad o(H_j) \mid o(G_j) \ \text{ para todo } j = 1, \ldots, r.$$

De manera análoga, podemos probar que $s \leq r$ y $o(G_j) \mid o(H_j)$ para todo $j = 1, \ldots, s$. Por lo tanto el número s de subgrupos y los órdenes $e_1, \ldots, e_s$ están unívocamente determinados. ■

Los enteros $e_1, e_2, \ldots, e_s$ en el Teorema 3.2.10 son llamados los **factores invariantes** de G. La descripción de G en el Teorema 3.2.10 (1) es llamada la **descomposición en factores invariantes** de G. Notemos que si G es un grupo abeliano finito de orden n y $G = G_1 \oplus \cdots \oplus G_s$

[10] Pues, $x \in e_j.G = e_j.G_1 \oplus \cdots \oplus e_j.G_{j-1}$

[11] La suma $(K_1 \cap G_1) + \cdots + (K_1 \cap G_{j-1})$ es directa pues la suma $G_1 + \cdots + G_{j-1}$ es directa.

[12] Esta suma es directa porque $T_i \cong H_i$ y la suma $H_1 + \cdots + H_j$ es directa, con lo que la suma $T_1 + \cdots + T_j$ es directa.

[13] En efecto, tenemos que $e_j.T_i \cong e_j.H_j$ para todo $i = 1, \ldots, j$, entonces $o(e_j.T_i) = o(e_j.H_j) = r_j$ para cada $i = 1, \ldots, j$. Luego, $o(e_j.T_1 \oplus \cdots \oplus e_j.T_j) = r_j^j$.

es su descomposición en factores invariantes con órdenes $e_1, \ldots, e_s$ respectivamente, entonces $n = e_1 e_2 \ldots e_s$ y para cada $i \in \{1, 2, \ldots, s\}$

$$G_i \cong \mathbb{Z}_{e_i}$$

y por lo tanto

$$G \cong \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_s}.$$

El Teorema 3.2.10 nos da una manera efectiva de listar *todos* los grupos abelianos finitos de un orden dado. Para encontrar todos, salvo isomorfismo, los grupos abelianos finitos de orden n debemos encontrar todas las sucesiones de enteros $e_1, \ldots, e_s$ tales que

(FI1) $e_i \geq 2$ para todo $i = 1, 2, \ldots, s$;

(FI2) $e_{i+1} \mid e_i$;

(FI3) $n = e_1 e_2 \ldots e_s$.

Observación 3.2.11.

(1) Si $e_1, e_2, \ldots, e_s$ son los factores invariantes de G, entonces $e_i \mid e_1$ para todo $i = 1, 2, \ldots, s$. Si p es cualquier divisor primo de n, entonces por (FI3) tenemos que p debe dividir a algún e_i y con lo cual p divide a e_1. Por lo tanto, *cada divisor primo de n debe dividir al primer factor invariante e_1* de G.

(2) Sean $e_1, e_2, \ldots, e_s$ los factores invariantes de G. Si n es el producto de primos distintos (todos de primera potencia), digamos por ejemplo $n = p_1 p_2 \ldots p_k$, entonces por la observación anterior $p_j \mid e_1$ para cada $j = 1, 2, \ldots, k$. En consecuencia $n = p_1 p_2 \ldots p_k \mid e_1$[14] y por lo tanto $n = e_1$. Así, hemos probado que si n es el producto de primos distintos, entonces hay sólo una posible lista de factores invariantes para un grupo abeliano de orden n: La única lista consta de un sólo e_i: e_1.

Corolario 3.2.12. *Si n es el producto de primos distintos, todos de primera potencia, entonces salvo isomorfismo el único grupo abeliano de orden n es el grupo cíclico $\mathbb{Z}_n$.*

Ejemplo 3.2.13. Determinemos todos, salvo isomorfismo, los grupos abelianos de orden $n = 180$. Usando la factorización de n en producto de potencias de primos, tenemos que $n = 180 = 2^2.3^2.5$. Como hemos visto en la observación anterior, debemos tener que $2.3.5 \mid e_1$, así los posibles valores para e_1 son

$$e_1 = 2.3.5, \quad 2^2.3.5, \quad 2.3^2.5 \quad \text{o} \quad 2^2.3^2.5.$$

Para cada uno de estos valores debemos encontrar todos los posibles valores de e_2. Luego, para cada uno de los valores posibles de e_2, todos los posibles valores de e_3, y así continuando hasta que todas las listas satisfaciendo las condiciones (FI1)-(FI3) son obtenidas.

[14] Es consecuencia del hecho que los primos $p_1, p_2, \ldots, p_k$ son distintos.

Factores Invariantes	Grupos Abelianos
$2^2.3^2.5$	$\mathbb{Z}_{180}$
$2.3^2.5, \quad 2$	$\mathbb{Z}_{90} \times \mathbb{Z}_2$
$2^2.3.5, \quad 3$	$\mathbb{Z}_{60} \times \mathbb{Z}_3$
$2.3.5, \quad 2.3$	$\mathbb{Z}_{30} \times \mathbb{Z}_6$

Cuadro 3.1: Todos, salvo isomorfismo, los grupos abelianos de orden 180.

Por ejemplo, si $e_1 = 2.3^2.5$, el único número e_2 que divide a e_1 tal que e_1e_2 divida a $n = 180$ es $e_2 = 2$. En este caso, obtenemos que $e_1e_2 = 2^2.3^2.5 = 180 = n$, así esta lista está completa: $e_1 = 2.3^2.5$ y $e_2 = 2$. El grupo abeliano correspondiente a esta lista es $\mathbb{Z}_{90} \times \mathbb{Z}_2$.

Si $e_1 = 2.3.5$, los únicos candidatos para e_2 son $e_2 = 2, 3, 2.3$. Si $e_2 = 2$ or 3, entonces ya que $e_3 \mid e_2$ debemos tener necesariamente que $e_2 = e_3$. Pero esto es una contradicción porque $e_1e_2e_3$ sería divisible por 2^3 o 3^3 y $n = 180$ no es divisible por 2^3 ni 3^3. Con lo cual el único número posible para e_2 es $2.3 = 6$. Luego, la única lista de factores invariantes cuyo primer término es 2.3.5 es: $e_1 = 2 \cdot 3 \cdot 5$ y $e_2 = 2 \cdot 3$. El correspondiente grupo abeliano es $\mathbb{Z}_{30} \times \mathbb{Z}_6$.

Similarmente, todas las listas posibles de factores invariantes pueden ser obtenidas con sus correspondientes grupos abelianos, ver el Cuadro 3.1. ■

En el ejemplo anterior se puede observar que el proceso para determinar todas las listas posibles de factores invariantes de un orden dado n depende en gran medida de la factorización de n en producto de potencias de primos. Los resultados a continuación junto con el Teorema Fundamental de Grupos Abelianos Finitos nos permitirán obtener un proceso más sistemático y computacionalmente más rápido para determinar todos los grupos abelianos finitos de un orden dado.

Sea G es un grupo abeliano y $n \in \mathbb{Z}$. Definimos

$$G_n = \{x \in G : \ n.x = 0\}.$$

Se puede comprobar fácilmente que G_n es un subgrupo de G (véase Ejercicio **??**).

Proposición 3.2.14. *Sea G un grupo abeliano finito de orden $n = st$ con s y t relativamente primos. Entonces, $G = G_s \oplus G_t$ y $o(G_s) = s$, $o(G_t) = t$.*

Demostración. Tenemos que $1 = us + vt$ con $u, v \in \mathbb{Z}$. Si $x \in G_s \cap G_t$ entonces $x = 1.x = (us).x + (vt).x = u.(s.x) + v.(t.x) = u.0 + v.0 = 0$. Con lo cual, $G_s \cap G_t = \{0\}$. Sea $x \in G$. Luego, $x = (us).x + (vt).x$. Ahora, como $s.((vt).x) = (vst).x = (vn).x = 0$, $(vt).x \in G_s$. Similarmente, $(us).x \in G_t$. Entonces, $G = G_s + G_t$. Por lo tanto, $G = G_s \oplus G_t$.

Para probar que $o(G_s) = s$ y $o(G_t) = t$, vamos a ver que s y $o(G_s)$ tienen los mismos divisores primos e igual para $o(G_t)$ y t. Sea p un divisor primo de s. Entonces, p es un divisor primo de $n = o(G)$. Con lo cual, por el Teorema de Cauchy (ver Teorema 2.4.1), G contiene un elemento x de orden p. Como $p \mid s$ resulta $s.x = 0$, es decir, $x \in G_s$ y, por lo tanto $p \mid o(G_s)$.

Ahora supongamos que p es un divisor primo de $o(G_s)$. Por el Teorema de Cauchy, G_s contiene un elemento x de orden p. Como $s.x = 0$, $p \mid s$. Así, s y $o(G_s)$ tienen los mismo divisores primos. De manera similar, t y G_t tienen los mismos divisores primos. Como s y t son relativamente primos y $st = o(G_s)o(G_t)$, tenemos que $s = o(G_s)$ y $t = o(G_t)$. ■

Proposición 3.2.15. *Sea G un grupo abeliano de orden $n > 1$. Si $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ es su única descomposición en producto de potencias de primos distintos, entonces*

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$$

con $G_1, G_2, \dots, G_k$ subgrupos de G de órdenes $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, $\dots p_k^{\alpha_k}$, respectivamente. Además, esta descomposición es única, esto es, si $G = H_1 \oplus \cdots \oplus H_k$ con $o(H_i) = p_i^{\alpha_i}$ para $i = 1, \dots, k$, entonces $H_i = G_i$ para todo $i = 1, \dots, k$.

Demostración. Es consecuencia de la Proposición 3.2.14, ya que los primos $p_1, p_2, \dots, p_k$ son todos distintos (puede usar inducción sobre k). Veamos que la descomposición es única. Supongamos que $G_1 \oplus \cdots \oplus G_k = G = H_1 \oplus \cdots \oplus H_k$ con $o(G_i) = o(H_i) = p_i^{\alpha_i}$ para todo $i = 1, \dots, k$. Sea $i \in \{1, \dots, k\}$ y probemos que $G_i = H_i$. Sea $x \in G_i$. Sabemos que $x = h_1 + \cdots + h_k$ con $h_j \in H_j$ para todo $j \in \{1, \dots, k\}$. Luego, como $o(x) = mcm(o(h_1), \dots, o(h_k))$, tenemos que $o(h_j) \mid o(x)$ para todo $j \in \{1, \dots, n\}$. Además, $o(h_j) = p_j^{\gamma_j}$ para algún $\gamma_j \leq \alpha_j$. Entonces, para cada $j \in \{1, \dots, k\} - \{i\}$, $p_j^{\gamma_j} \mid o(x) \mid p_i^{\alpha_i}$. Así $\gamma_j = 0$ y $h_j = 0$. Luego $x = h_i \in H_i$. Hemos probado que $G_i \subseteq H_i$. Análogamente, $H_i \subseteq G_i$. Por lo tanto, $G_i = H_i$. ■

Proposición 3.2.16. *Sea p un número primo y sea α un entero positivo. Si G es un grupo abeliano de orden p^α, entonces existen únicos enteros positivos $\beta_1, \dots, \beta_s$ tal que*

$$G \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \cdots \times \mathbb{Z}_{p^{\beta_s}}$$

con $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_s$ y $\beta_1 + \beta_2 + \cdots + \beta_s = \alpha$.

Demostración. Por el Teorema Fundamental de los Grupos Abelianos Finitos, sabemos que

$$G \cong \mathbb{Z}_{e_1} \times \mathbb{Z}_{e_2} \times \cdots \times \mathbb{Z}_{e_s}$$

con $e_s \mid e_{s-1} \mid \cdots \mid e_2 \mid e_1$. Como $e_1 e_2 \dots e_s = p^\alpha$ y $e_i \geq 2$ para todo $i = 1, 2, \dots, s$, obtenemos que para cada $i = 1, 2, \dots, s$, $e_i = p^{\beta_i}$ con β_i enteros positivos. Dado que $p^{\beta_1}p^{\beta_2}\dots p^{\beta_s} = p^\alpha$ y $p^{\beta_s} \mid p^{\beta_{s-1}} \mid \cdots \mid p^{\beta_2} \mid p^{\beta_1}$, tenemos que $\beta_1 + \beta_2 + \cdots + \beta_s = \alpha$ y $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_s \geq 1$. ■

Por lo tanto, la determinación de todas las listas posibles de factores invariantes de un grupo de orden p^α queda reducida a la obtención de todas las particiones posibles del entero α (ordenada en forma decreciente). Las condiciones (FI1)-(FI3) para los factores invariantes descrito antes se transforman ahora en las siguientes. Para cada potencia α debemos hallar todas las sucesiones $(\beta_1, \dots, \beta_s)$ tales que:

(DE1) $\beta_j \geq 1$ para todo $j \in \{1, 2, \dots, s\}$,

(DE2) $\beta_i \geq \beta_{i+1}$,

Divisores Elementales Particiones de 5	Grupos Abelianos
5	$\mathbb{Z}_{p^5}$
4 + 1	$\mathbb{Z}_{p^4} \times \mathbb{Z}_p$
3 + 2	$\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$
3 + 1 + 1	$\mathbb{Z}_{p^3} \times \mathbb{Z}_p \times \mathbb{Z}_p$
2 + 2 + 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$
2 + 1 + 1 + 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
1 + 1 + 1 + 1 +1	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Cuadro 3.2: Todos los grupos abelianos de orden p^5.

(DE3) $\beta_1 + \cdots + \beta_s = \alpha$.

En consecuencia, el número de grupos abelianos no isomórficos de orden p^α es igual al número de particiones de α.

Ahora por las dos proposiciones anteriores observamos que cada grupo abeliano G de orden $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ se puede representar como

$$G \cong \mathbb{Z}_{p_1^{\beta_1^1}} \times \cdots \times \mathbb{Z}_{p_1^{\beta_{s_1}^1}} \times \cdots \times \mathbb{Z}_{p_k^{\beta_1^k}} \times \cdots \times \mathbb{Z}_{p_k^{\beta_{s_k}^k}} \tag{3.1}$$

donde para cada $i = 1, 2, \dots, k$ tenemos que $\beta_1^i + \cdots + \beta_{s_i}^i = \alpha_i$ y $\beta_{s_i}^i \geq \cdots \geq \beta_2^i \geq \beta_1^i$. Los enteros p^β descritos en el párrafo anterior, dados por las Proposiciones 3.2.15 y 3.2.16, son llamados los **divisores elementales** de G. La descripción de G en (3.1) es llamada la **descomposición en divisores elementales** de G.

Por las Proposiciones 3.2.15 y 3.2.16, para encontrar todos los grupos abelianos de orden $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ uno debe encontrar para cada $i = 1, 2, \dots, k$ todas las particiones posibles $(\beta_1^i, \dots, \beta_{s_i}^i)$ de α_i tal que $\alpha_i = \beta_1^i + \cdots + \beta_{s_i}^i$ y $\beta_{s_i}^i \geq \cdots \geq \beta_1^i$. Así, para describir, salvo isomorfismos, a todos los grupos abelianos de orden $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, elegimos para cada $i = 1, \dots, k$, una tal partición $(\beta_1^i, \dots, \beta_{s_i}^i)$ de α_i y formamos el grupo

$$G \cong \mathbb{Z}_{p_1^{\beta_1^1}} \times \cdots \times \mathbb{Z}_{p_1^{\beta_{s_1}^1}} \times \cdots \times \mathbb{Z}_{p_k^{\beta_1^k}} \times \cdots \times \mathbb{Z}_{p_k^{\beta_{s_k}^k}}$$

La ventaja de este proceso en comparación con el descrito anteriormente radica en el hecho que es más fácil sistematizar cómo obtener todas las particiones $(\beta_1, \dots, \beta_s)$ de un α.

Ejemplo 3.2.17. Determinemos todos lo grupos abelianos, salvo isomorfismo, de orden p^5 con p un primo arbitrario. Para ello encontramos todas las particiones posibles del entero 5 que cumplan las condiciones (DE1)-(DE3), ver el Cuadro 3.2. Podemos observar que la determinación, y así el número, de grupos abelianos de orden p^5 no depende del primo p. ■

Observemos que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ y q_i es el número de particiones posibles de α_i entonces el número de grupos abelianos de orden n es igual a $q_1 q_2 \dots q_k$.

Ejemplo 3.2.18. Sea $n = 1800 = 2^3 3^2 5^2$ y listemos todos los grupos abelianos de orden n. Para ello determinamos primero todas las particiones posibles de cada una de las potencias de los primos 2, 3 y 5, lo cual se muestra en el Cuadro 3.3.

Orden p^β	Particiones de β	Grupos Abelianos
2^3	$3;\quad 2+1;\quad 1+1+1$	$\mathbb{Z}_8,\quad \mathbb{Z}_4 \times \mathbb{Z}_2,\quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
3^2	$2;\quad 1+1$	$\mathbb{Z}_9,\quad \mathbb{Z}_3 \times \mathbb{Z}_3$
5^2	$2;\quad 1+1$	$\mathbb{Z}_{25},\quad \mathbb{Z}_5 \times \mathbb{Z}_5$

Cuadro 3.3: Determinación de los grupos abelianos de orden 1800.

Ahora, obtenemos los grupos abelianos de orden 1800 tomando un grupo abeliano de cada una de las tres listas en el Cuadro 3.3 y haciendo su producto directo. Por ejemplo,

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}, \quad \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5.$$

El lector puede continuar listando todos los restantes. Por el Cuadro 3.3 comprobamos que hay $3.2.2 = 12$ grupos abelianos de orden 1800. ■

Ejemplo 3.2.19. Veamos con un ejemplo cómo pasar de una descomposición en factores invariantes a su descomposición en divisores elementales. Sea G un grupo abeliano de orden 3456 y sea $(24, 12, 6, 2)$ sus factores invariantes. Entonces $G \cong \mathbb{Z}_{24} \times \mathbb{Z}_{12} \times \mathbb{Z}_6 \times \mathbb{Z}_2$. Factorizamos:

$$24 = 2^3 \cdot 3 \qquad 12 = 2^2 \cdot 3 \qquad 6 = 2 \cdot 3 \qquad 2 = 2.$$

Entonces, los divisores elementales de G son

$$2^3,\ 3,\ 2^2,\ 3,\ 2,\ 3,\ 2.$$

Por lo tanto,

$$G \cong \underbrace{\mathbb{Z}_8 \times \mathbb{Z}_3}_{\mathbb{Z}_{24}} \times \underbrace{\mathbb{Z}_4 \times \mathbb{Z}_3}_{\mathbb{Z}_{12}} \times \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_3}_{\mathbb{Z}_6} \times \mathbb{Z}_2. \quad ■$$

Ejemplo 3.2.20. Veamos con un ejemplo cómo pasar de una descomposición en divisores elementales a su descomposición en factores invariantes. Sea G un grupo abeliano de orden 1800 tal que su divisores elementales son 2, 3, 2, 25, 3, 2. Entonces $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_2$. Entonces, primero reordenamos agrupando los $\mathbb{Z}_{p^\alpha}$ con el mismo primo p de base:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_2 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_{25}.$$

Luego, volvemos a reordenar agrupando un $\mathbb{Z}_{p^\alpha}$ de cada grupo $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_3 \times \mathbb{Z}_3$ y $\mathbb{Z}_{25}$:

$$G \cong \underbrace{(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25})}_{\mathbb{Z}_{150}} \times \underbrace{(\mathbb{Z}_2 \times \mathbb{Z}_3)}_{\mathbb{Z}_6} \times \mathbb{Z}_2 \cong \mathbb{Z}_{150} \times \mathbb{Z}_6 \times \mathbb{Z}_2.$$

Por lo tanto, los factores invariantes de G son $(2 \cdot 3 \cdot 5^2,\ 2 \cdot 3,\ 2) = (150, 6, 2)$. ■

Concluimos este capítulo mostrando que en el caso de grupos abelianos finitos se cumple la afirmación recíproca del Teorema de Lagrange.

Proposición 3.2.21. *Si G es un grupo abeliano finito y d es un divisor del orden de G, entonces existe un subgrupo H de G de orden d.*

Demostración. Supongamos primero que $o(G) = p^n$ con p un entero positivo primo y se d tal que $d \mid p^n$. Consideremos la descomposición en divisores elementales de G:

$$G \cong \mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_k}}$$

con $\beta_1 \geq \cdots \geq \beta_k$ y $\beta_1 + \cdots + \beta_k = n$. Como $d \mid p^n$, $d = p^t$ con $t \leq n$. Entonces, podemos considerar una partición de t como

$$t = t_1 + \cdots + t_k$$

tal que $0 \leq t_1 \leq \beta_1, \ldots, 0 \leq t_k \leq \beta_k$. Luego, para cada $i = 1, \ldots, k$, $p^{t_i} \mid p^{\beta_i}$ y así para cada $i = 1, \ldots, k$ existe un subgrupo H_i de $\mathbb{Z}_{p^{\beta_i}}$ de orden p^{t_i}. Entonces,

$$H_1 \times \cdots \times H_k \leq \mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_k}}$$

con $o\left(H_1 \times \cdots \times H_k\right) = p^{t_1} . \ldots . p^{t_k} = p^t$.

Ahora probemos el caso general. Sea G un grupo abeliano de orden $n = p_1^{\alpha_1} . \ldots . p_k^{\alpha_k}$. Luego, por la Proposición 3.2.15, tenemos que

$$G = G_{p_1^{\alpha_1}} \oplus \cdots \oplus G_{p_k^{\alpha_k}}$$

donde $o(G_{p_i^{\alpha_i}}) = p_i^{\alpha_i}$. Sea $d \mid n$. Entonce $d = p_1^{\beta_1} . \ldots . p_k^{\beta_k}$ con $0 \leq \beta_i \leq \alpha_i$ para todo $i = 1, \ldots, k$. Así, por lo anteriormente probado, para cada $i = 1, \ldots, k$, existe un subgrupo H_i de $G_{p_i^{\alpha_i}}$ de orden $p_i^{\beta_i}$. Con lo cual

$$H := H_1 \oplus \cdots \oplus H_k$$

es un subgrupo de $G_{p_1^{\alpha_1}} \oplus \cdots \oplus G_{p_k^{\alpha_k}} = G$ de orden $p_1^{\beta_1} . \ldots . p_k^{\beta_k} = d$. ∎

Ejercicios propuestos

Ejercicio 3.1. Probar que $G_1 \times G_2 \cong G_2 \times G_1$.

Ejercicio 3.2. Sea G_1, G_2, G_3 grupos. Sea $G = G_1 \times G_2 \times G_3$ y $\widehat{G_1} = \{(a, e_2, e_3) : a \in G_1\}$. Probar que $G/\widehat{G_1} \cong G_2 \times G_3$.

Ejercicio 3.3. Sean $m_1, \ldots, m_k$ enteros positivos. Probar que $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ es un grupo cíclico si y sólo si $m_1, \ldots, m_k$ son relativamente primos dos a dos.

Ejercicio 3.4. Sean $n, m \in \mathbb{N}$. Probar que para todo $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, se tiene que $o(a, b) \leq mcm(m, n)$.
(*Sug.: Ver el Ejemplo 3.1.9.*)

Ejercicio 3.5. Sean $s, t \in \mathbb{N}$ relativamente primos. Probar que $\mathrm{U}(\mathbb{Z}_{s.t}) \cong \mathrm{U}(\mathbb{Z}_s) \times \mathrm{U}(\mathbb{Z}_t)$.

Ejercicio 3.6. Sea $n = n_1.n_2.\cdots n_k$ tal que los $n_1, n_2, \ldots, n_k$ son relativamente primos dos a dos. Probar que $\mathrm{U}(\mathbb{Z}_n) \cong \mathrm{U}(Z_{n_1}) \times \mathrm{U}(\mathbb{Z}_{n_2}) \times \cdots \times \mathrm{U}(\mathbb{Z}_{n_k})$.

Ejercicio 3.7. Hallar un elemento de $\mathbb{Z}_{15} \times \mathbb{Z}_{27} \times \mathbb{Z}_{405}$ de orden $mcm(15, 27, 405)$.

Ejercicio 3.8. Sea G un grupo abeliano y sean H_1 y H_2 dos subgrupos de G. Probar que $H_1 \times H_2/\Delta \cong H_1 + H_2$, donde $\Delta = \{(a, -a) : a \in H_1 \cap H_2\}$.

Ejercicio 3.9. Probar las afirmaciones hechas en el Ejemplo 3.2.2 (2).

Ejercicio 3.10. Probar que $\mathbb{Z}_{12} = \langle\overline{4}\rangle \oplus \langle\overline{3}\rangle$.

Ejercicio 3.11. Sea G un grupo de orden n. Probar que G es cíclico si y sólo si $\exp(G) = n$.

Ejercicio 3.12. Considere el grupo abeliano elemental de orden p^3 (p primo) $E_{p^3} = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. Probar que E_{P^3} tiene exactamente $p^2 + p + 1$ subgrupos de orden p. Si consideramos un $n \in \mathbb{Z}^+$ arbitrario, ¿cuántos subgrupos de orden p tiene el grupo abeliano elemental E_{p^n}?

Ejercicio 3.13. Sea $G := \mathbb{Z}_{12} \times \mathbb{Z}_9$.

(a) Hallar el exponente de G.

(b) Hallar un elemento $a \in G$ tal que $o(a) = \exp(G)$.

(c) Escribir a G como $\langle a\rangle \oplus T$ y describir quien es T.

Ejercicio 3.14. Hallar mediante la descomposición en factores invariantes todos los grupos abelianos (salvo isomorfismos) de orden

(a) $n = 1800$. (b) $n = 3600$. (c) $n = 10800$. (d) $n = 68607$.

Ejercicio 3.15. Hallar mediante la descomposición en divisores elementales todos los grupos abelianos (salvo isomorfismos) de orden

(a) $n = 37800$. (b) $n = 762048$. (c) $n = 36000$. (d) $n = 982762$.

Ejercicio 3.16. Determinar la descomposición en factores invariantes y la descomposición en divisores elementales de los siguientes grupos

(a) $G_1 := \mathbb{Z}_{15} \times \mathbb{Z}_{24} \times \mathbb{Z}_{30} \times \mathbb{Z}_{700}$. (b) $G_2 := \mathbb{Z}_{20} \times \mathbb{Z}_{175} \times \mathbb{Z}_{539}$.

Ejercicio 3.17. Probar que $\mathbb{Z}_{24} \times \mathbb{Z}_{36} \times \mathbb{Z}_{60} \cong \mathbb{Z}_{360} \times \mathbb{Z}_{12} \times \mathbb{Z}_{12}$.

Ejercicio 3.18. Sea G un grupo abeliano y $n \in \mathbb{Z}$. Probar que $G_n = \{a \in G : n.a = 0\}$ es un subgrupo de G. Dar un ejemplo de un grupo G y un $n \in \mathbb{N}$ tal que $o(G) \neq n$.

Ejercicio 3.19. Considere el grupo $\mathbb{Z}_{30}$. Hallar los subgrupos G_1, G_2 y G_3 de $\mathbb{Z}_{30}$ tales que $\mathbb{Z}_{30} = G_1 \oplus G_2 \oplus G_3$, y $o(G_1) = 2$, $o(G_2) = 3$ y $o(G_3) = 5$.

Ejercicio 3.20. Sea G un grupo abeliano de orden n. Probar que si $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, con los p_i distintos dos a dos, entonces $G \cong \mathbb{Z}_n$ (*Pista: Usar la Proposición 3.2.14.*).

Ejercicio 3.21. Sea G un grupo abeliano finito tal que (24,12,6,2) son sus factores invariantes. Hallar la descomposición en divisores elementales de G.

Ejercicio 3.22. Sea G un grupo abeliano finito tal que 2, 3, 2, 25, 3, 2 son sus divisores elementales. Hallar la descomposición en factores invariantes de G.

Ejercicio 3.23. Probar que si G es un grupo abeliano de orden $n = 10.k$, entonces G tiene un subgrupo cíclico de orden 10.

Ejercicio 3.24. Obtener las descomposiciones en factores invariante y en divisores elementales de los grupos multiplicativos $\mathrm{U}(\mathbb{Z}_{15})$ y $\mathrm{U}(\mathbb{Z}_9)$.

Ejercicios con GAP

Ejercicio 3.25. Generar el grupo $G = \langle a \rangle$ cíclico de orden 12.

(a) Hallar un elemento b de G de orden 4 y uno c de orden 3.

(b) Generar los subgrupos $H_1 = \langle b \rangle$, $H_2 = \langle c \rangle$ y el grupo producto $H = H_1 \times H_2$.

(c) Determinar si H y G son isomorfos.

Ejercicio 3.26. Se necesitará usar la función `orderFrequency`.

(a) Generar los siguientes grupos $D_{10} \times \mathbb{Z}_2$, $D_5 \times \mathbb{Z}_4$, $\mathbb{Z}_{20} \times \mathbb{Z}_2$ y D_{20}.

(b) Para cada uno de los grupos productos del inciso anterior encontrar el número de elementos de cada orden posible.

(c) Determinar si los grupos del inciso (a) son isomorfos entre sí.

Ejercicio 3.27. Se necesitará usar la función `orderFrequency`.

(a) Generar, salvo isomorfismos, los únicos 4 grupos abelianos finitos de orden $n = 180$.

(b) Para cada uno de los grupos anteriores, hallar el número de elementos de cada orden posible.

(c) Argumentar que estos cuatros grupos no son isomorfos dos a dos.

Ejercicio 3.28. (a) Generar el grupo $G = \mathbb{Z}_{24} \times \mathbb{Z}_{36} \times \mathbb{Z}_{60}$.

(b) Generar el subgrupo $H := \langle (8, 9, 15) \rangle$ de G.

(c) Generar el grupo cociente $F := G/H$ y calcular su orden.

(d) Dado F es un grupo abeliano finito, por el Teorema Fundamental de Grupos Abelianos Finitos, tenemos que F debe ser isomorfo a algún de los siguientes:

$$\mathbb{Z}_8 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 \quad \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \quad \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

Calcular los órdenes de los elementos de cada uno de los nueve grupos anteriores, y los órdenes de los elementos de F y determinar a cual de ellos es isomorfo F[15].

Ejercicio 3.29. (a) Generar el grupo multiplicativo $\mathrm{U}(\mathbb{Z}_{65})$. Calcular el orden de $\mathrm{U}(\mathbb{Z}_{65})$. Calcular el número de elementos de cada orden (use la función `orderFrequency`).

(b) Usando el Teorema Fundamental de los Grupos Abelianos Finitos, generar todos los grupos abelianos finitos $\mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_s}$ de orden 16 (véase la página 67).

(c) Determinar a que grupo $\mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_s}$.

[15]Usar la afirmación: Dos grupos abelianos finitos son isomorfos si y sólo si ellos tienen el mismo número de elementos de cada orden.

Capítulo 4

Anillos

Como vimos en los capítulos anteriores, la teoría de grupo estudia aquellas estructuras algebraicas teniendo una sola operación binaria cumpliendo ciertas propiedades. Además, hemos probado que los grupos se comportan como los grupos de permutaciones (ver Teorema 2.1.22). También podemos decir que los grupos abelianos son un análogo abstracto del grupo de los enteros con la suma. En este capítulo estudiaremos ciertas estructuras algebraicas, llamadas *anillos*, que cuentan con dos operaciones binarias satisfaciendo algunas condiciones. Veremos que los anillos pueden ser considerados como una generalización abstracta de la estructura de los enteros con las operaciones de suma y multiplicación.

4.1. Definiciones y propiedades

Definición 4.1.1. Diremos que una estructura $\langle A, +, \cdot \rangle$ es un **anillo** si A es un conjunto no vacío, $+$ y $\cdot$ son operaciones binarias sobre A que cumplen lo siguiente:

(A1) $\langle A, + \rangle$ es un grupo abeliano;

(A2) la operación $\cdot$ es asociativa;

(A3) la operación $\cdot$ distribuye con respecto a $+$, esto es, para cualesquiera $a, b, c \in A$

$$a.(b + c) = a.b + a.c \quad \text{y} \quad (b + c).a = b.a + c.a.$$

Al igual que en el caso de grupos, frecuentemente denotaremos a un anillo $\langle A, +, \cdot \rangle$ simplemente por su conjunto universo A. Sea A un anillo. Diremos que A es un **anillo conmutativo** si la operación $\cdot$ es conmutativa. Un anillo A se dice con **identidad** si existe un elemento $1 \in A$ tal que $1 \neq 0$ y $1.a = a.1 = a$ para todo $a \in A$.

Recordemos lo siguiente. Como en un anillo $\langle A, +, \cdot \rangle$ tenemos que $\langle A, + \rangle$ es un grupo abeliano, denotamos su elemento neutro por 0; es decir $0 \in A$ y $a + 0 = 0$. También, el opuesto de un elemento $a \in A$ se denota por $-a$. Luego $a + (-a) = 0$. Además, denotamos $a + (-b) = a - b$ (como es usual en el anillo de enteros).

Comenzamos probando algunas propiedades básicas de anillos.

Proposición 4.1.2. *Sea A un anillo. Entonces, para cualesquiera $a, b, c \in A$:*

(1) $a.0 = 0.a = 0$;

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

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

(4) *Si A tiene una identidad 1, entonces la identidad es única y se cumple que $-a = (-1).a$.*

Demostración. (1)

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

(2)

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

Dejamos el resto de las igualdades de (2) y (3) como ejercicio.

(4) Es similar al caso de grupo, véase la Proposición 1.1.7. ■

Definición 4.1.3. Sea A un anillo.

(1) Un elemento no nulo $a \in A$ ($a \neq 0$) se dice **divisor de cero** si existe $b \in A$ tal que $b \neq 0$ y, $a.b = 0$ o $b.a = 0$.

(2) El anillo A es llamado un **dominio de integridad** si es un anillo conmutativo con identidad que no posee divisores de cero.

Proposición 4.1.4. *Sea A un anillo y sean $a, b, c \in A$ tal que a no es divisor de cero. Si $a.b = a.c$, entonces $b = c$.*

Demostración. A cargo del lector. ■

Definición 4.1.5. (1) Sea A un anillo con identidad. Un elemento $a \in A$ es llamado **invertible** o **unidad** si existe $b \in A$ tal que $a.b = b.a = 1$.

(2) Un anillo A con identidad donde todos sus elementos no nulos son invertibles, será llamado un **anillo con división**.

(3) Un anillo conmutativo con división es llamado **cuerpo**.

Sea A un anillo con identidad. Si $a \in A$ es invertible, entonces el elemento b tal que $a.b = 1$, es único y lo denotaremos por a^{-1}. Como es usual, llamaremos a a^{-1} el **inverso de** a. También denotaremos por $\mathrm{U}(A)$ al conjunto de todos los elementos invertibles de A. Esto es,

$$\mathrm{U}(A) = \{a \in A : a \text{ es invertible en } A\}$$

Dado un anillo A, denotaremos al conjunto de los elementos no nulos de A por $A^* := \{a \in A : a \neq 0\}$. Notemos que A es un anillo con división si $A^* = \mathrm{U}(A)$. También, es importante notar que un cuerpo es un anillo $\langle A, +, \cdot \rangle$ tal que $\langle A, + \rangle$ y $\langle A^*, \cdot \rangle$ son grupos abelianos y la operación $\cdot$ distribuye con respecto a la operación $+$.

Proposición 4.1.6. *Si A es un dominio de integridad finito, entonces A es un cuerpo.*

Demostración. Sólo resta probar que todo elemento no nulo de A es invertible. Como A es finito, sea $A^* = \{a_1, \ldots, a_n\}$. Notemos que dentro de A^* también se encuentra la identidad de A. Consideremos los productos a_1a_1, a_1a_2, a_1a_3, $\ldots$, a_1a_n. Como A es un dominio de integridad, todos esos productos son distintos dos a dos, esto es, si $i, j \in \{1, \ldots, n\}$ e $i \neq j$, entonces $a_1a_i \neq a_1a_j$. Entonces $A^* = \{a_1a_1, a_1a_2, \ldots, a_1a_n\}$. Con lo cual existe un i tal que $a_1a_i = 1$. Es decir, probamos que a_1 es invertible. De igual forma podemos probar que cada a_k es invertible. ■

Proposición 4.1.7. *Sea A un anillo con identidad. Entonces, $\langle \mathrm{U}(A), \cdot \rangle$ es un grupo. Además, si A es conmutativo, $\langle \mathrm{U}(A), \cdot \rangle$ es abeliano.*

Demostración. Similar a la demostración de la Proposición 1.4.8 (véase el párrafo anterior a dicha proposición). ■

Ejemplo 4.1.8.

(1) $\langle \mathbb{Z}, +, . \rangle$ es un dominio de integridad.

(2) $\langle \mathbb{Z}_n, +, . \rangle$ es un anillo conmutativo con identidad (véanse las Proposiciones 1.4.3 y 1.4.4). El anillo $\mathbb{Z}_n$ no es necesariamente un dominio de integridad. Por ejemplo, en $\mathbb{Z}_6$, los elementos $\overline{2}$ y $\overline{3}$ son divisores de cero, pues $\overline{2}.\overline{3} = \overline{6} = \overline{0}$. También, $\overline{4}$ es un divisor de cero en $\mathbb{Z}_6$. En cambio, puede comprobar que $\mathbb{Z}_3$ y $\mathbb{Z}_5$ no tienen divisores de cero, es decir, $\mathbb{Z}_3$ y $\mathbb{Z}_5$ son dominios de integridad.

(3) El conjunto $\mathrm{M}_2(\mathbb{R})$ de las matrices cuadradas de orden 2 con la suma y multiplicación usuales entre matrices es un anillo con identidad, el cual no es conmutativo y tiene divisores de cero.

(4) Sea A un anillo conmutativo con identidad. Se define el anillo de polinomios con coeficientes en A de una manera similar al caso de polinomios con coeficientes reales. Sea X una indeterminada. La expresión formal

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

con $n \geq 0$ y cada $a_i \in A$ es llamado **un polinomio en X con coeficientes en A**. Si $p(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ con $a_n \neq 0$ se dice que $p(X)$ tiene **grado** n y a_n es llamado el **coeficiente principal de** $p(X)$. Vamos a denotar al conjunto de todos los polinomios en X con coeficientes en A por $A[X]$. Las operaciones $+$ y $.$ en $A[X]$ se definen como en el caso real. Sean $p(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ y $q(X) = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$ polinomios en $A[X]$. Entonces,

$$p(X) + q(X) = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \cdots + (a_1 + b_1)X + (a_0 + b_0)$$

$$p(X)q(X) = (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \ldots$$

(en general, el coeficiente correspondiente a la potencia X^k en el producto $p(X)q(X)$ será $\sum_{i=0}^{k} a_ib_{k-i}$). Por lo tanto, no es difícil comprobar que $A[X]$ con estas operaciones es un anillo conmutativo con identidad y al cual llamamos el **anillo de polinomios con coeficientes en** A. Además observe que el anillo A aparece en $A[X]$ como los polinomios constantes. Estudiaremos más en detalle el anillo de polinomios con coeficientes en un anillo A en la Sección 5.6 del Capítulo 5. Entre otras cosas daremos una definición formal de polinomio.

(5) Una clase importante de anillos es obtenida considerando anillos de funciones. Sea X un conjunto arbitrario no vacío y sea A un anillo. Sea A^X el conjunto de todas las funciones $f\colon X \to A$. En A^X se definen las operaciones suma y multiplicación como sigue: sean $f, g \in A^X$ entonces

$$(f+g)(x) = f(x) + g(x) \quad \text{y} \quad (fg)(x) = f(x)g(x)$$

para cada $x \in X$. Usando las propiedades del anillo A, se puede probar sin dificultad que A^X, con las operciones recién definidas, es un anillo. Además, A está representado en A^X como las funciones constantes. ■

Proposición 4.1.9. *$\mathbb{Z}_n$ es un cuerpo si y sólo si n es primo.*

Demostración. ($\Rightarrow$) Supongamos que $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ es un cuerpo. Entonces todo elemento no nulo $\overline{k}$, $k = 1, \ldots, n-1$, es invertible en $\mathbb{Z}_n$. Por lo tanto, por la Proposición 1.4.5, todo $k = 1, \ldots, n-1$ es relativamente primo con n. Con lo cual, n es primo.

($\Leftarrow$) A cargo del lector. ■

Definición 4.1.10. Sea A un anillo. Un subconjunto no vacío B de A es llamado un **subanillo** de A si se cumplen las siguientes condiciones:

(1) si $x, y \in B$, entonces $x - y \in B$;

(2) si $x, y \in B$, entonces $x.y \in B$.

Si además A tiene identidad 1, entonces se debe cumplir que $1 \in B$.

Se puede observar que B es un subanillo de A si B es un subgrupo de $\langle A, + \rangle$ y es cerrado bajo la operación producto.

Ejemplo 4.1.11.

(1) $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, $\mathbb{Q}$ es un subanillo de $\mathbb{R}$ y $\mathbb{R}$ es un subanillo de $\mathbb{C}$.

(2) $\mathrm{M}_2(\mathbb{Z})$ es un subanillo de $\mathrm{M}_2(\mathbb{Q})$.

(3) Sea $\mathbb{Z}$ el anillo de los enteros. Todo subgrupo de $\mathbb{Z}$ es un subanillo de $\mathbb{Z}$.

(4) Sea $C([0,1],\mathbb{R})$ la colección de todas las funciones $f\colon [0,1] \to \mathbb{R}$ continuas. Entonces $C([0,1],\mathbb{R})$ es un subanillo del anillo de funciones $\mathbb{R}^{[0,1]}$.

(5) Una función $f\colon \mathbb{R} \to \mathbb{R}$ es llamada de *soporte compacto* si existen $a, b \in \mathbb{R}$ tal que $f(x) = 0$ para todo $x \notin [a, b]$. Entonces, el conjunto de todas las funciones $f\colon \mathbb{R} \to \mathbb{R}$ de soporte compacto es un subanillo del anillo de funciones $\mathbb{R}^{\mathbb{R}}$. ■

En el caso de teoría de grupos, vimos que una herramienta importante para el estudio de un grupo era el conocimiento de sus subgrupos y más específicamente el conocimiento de sus subgrupos normales. En el caso de anillos ocurre algo similar, además de subanillos, otra subestructura importante para entender la estructura algebraica de un anillo es la de ideal.

Definición 4.1.12. Sea A un anillo y sea I un subconjunto no vacío de A. Diremos que

(1) I es un **ideal izquierdo** de A si cumple con:

(a) si $x, y \in I$, entonces $x - y \in I$;

(b) si $a \in A$ y $x \in I$, entonces $a.x \in I$.

(2) I es un **ideal derecho** de A si cumple con:

(a) si $x, y \in I$, entonces $x - y \in I$;

(b) si $a \in A$ y $x \in I$, entonces $x.a \in I$.

(3) I es llamado un **ideal** de A si lo es a izquierda y derecha.

Observe que todo ideal a izquierda o derecha de una anillo A es en particular un subanillo de A. Además, es claro que si A es un anillo conmutativo entonces ideales a izquierda y derecha coinciden y, simplemente los llamamos ideales.

Ejemplo 4.1.13.

(1) Dado un anillo A, A y $\{0\}$ son ideales de A y son llamados los **ideales triviales** de A.

(2) Sea A un anillo y $x \in A$. Entonces, $Ax := \{a.x : \ a \in A\}$ es un ideal izquierdo de A.

(3) En un anillo con división A, los únicos ideales son los triviales: A y $\{0\}$ ¿por qué? ■

El siguiente resultado, el cual es una recíproca del Ejemplo 4.1.13 (3), muestra que efectivamente cierta información sobre los ideales de un anillo nos da cierta información sobre la estructura del anillo.

Proposición 4.1.14. *Sea A un anillo con identidad. Si los únicos ideales (a izquierda o derecha) de A son los triviales, entonces A es un anillo con división.*

Demostración. Sea $a \in A$ no nulo. Consideremos el ideal izquierdo $Aa = \{b.a : b \in A\}$. Como los únicos ideales de A son $\{0\}$ y A, tenemos que $Aa = A$, porque $Aa \neq \{0\}$. Entonces $1 \in A = Aa$. Con lo cual existe $b \in A$ tal que $1 = ba$. De igual forma, se tiene que $aA = A$. Con lo cual existe $c \in A$ tal que $1 = ac$. Se puede probar que (véase el Ejercicio 4.4) $b = c$, y así a es invertible. Por lo tanto, A es un anillo con división. ■

Sea A un anillo conmutativo con identidad y sea X un subconjunto de A. Observemos primero que siempre hay un ideal de A que contiene a X, es el mismo A. Además no es difícil probar, y es un buen ejercicio para el estudiante (ver Ejercicio 4.11), que la intersección arbitraria de una colección de ideales de A es un ideal de A. Entonces, podemos considerar el siguiente ideal

$$\langle X\rangle = \bigcap\{I : \ I \text{ es un ideal de } A \text{ y } X \subseteq I\}.$$

Por lo tanto, $\langle X\rangle$ es un ideal de A que contiene a X y además si J es un ideal de A tal que $X \subseteq J$, entonces $\langle X\rangle \subseteq J$. En otras palabras, $\langle X\rangle$ es el menor ideal de A que contiene a X. El ideal $\langle X\rangle$ es llamado el **ideal generado por** X. La siguiente proposición nos da una caracterización útil del ideal generado por un subconjunto.

Proposición 4.1.15. *Sea A un anillo conmutativo con identidad y sea $X \subseteq A$ no vacío. Entonces,*

$$\langle X\rangle = \{a_1.x_1 + \cdots + a_n.x_n : \ n \geq 1, \ a_i \in A, \ x_i \in X\}.$$

Para conjuntos unitarios $\{x\}$, denotamos al ideal generado por $\{x\}$ por $\langle x\rangle$ en lugar de $\langle\{x\}\rangle$. Los ideales de la forma $\langle x\rangle$ son llamados **ideales principales**.

Ejemplo 4.1.16.

(1) Consideremos el anillo de enteros $\mathbb{Z}$. Para cada $n \in \mathbb{Z}$, los ideales principales son $\langle n\rangle = \{kn : \ k \in \mathbb{Z}\}$. Sea I un ideal no nulo de $\mathbb{Z}$. Sea n el menor entero positivo tal que $n \in I$. Como $n \in I$, se sigue que $\langle n\rangle \subseteq I$. Sea $m \in I$. Por el algoritmo de la división, existen enteros q y r tales que $m = nq + r$ con $0 \leq r < n$. Dado que $r = m - nq$ y $m, nq \in I$, obtenemos que $r \in I$. Entonces, $r = 0$. Así, $m = nq \in \langle n\rangle$ con lo que hemos probado que $I \subseteq \langle n\rangle$. En consecuencia, $I = \langle n\rangle$. Por lo tanto, hemos demostrado que *todo ideal del anillo $\mathbb{Z}$ es principal.*

(2) Consideremos el anillo de polinomios con coeficientes enteros $\mathbb{Z}[X]$ y tomemos el ideal generado por los polinomios 2 y X, esto es, $\langle 2, X\rangle = \{2.a(X) + X.b(X) : \ a(X), b(X) \in \mathbb{Z}[X]\}$. Probaremos que $\langle 2, X\rangle$ no es un ideal principal. Para ello supongamos hacia una contradicción que $\langle 2, X\rangle = \langle p(X)\rangle$. Como $2 \in \langle p(X)\rangle$, debe existir un $a(X) \in \mathbb{Z}[X]$ tal que $2 = p(X).a(X)$. Entonces, $p(X)$ y $a(X)$ deben ser constantes y dado que 2 es primo tenemos que $p(X), a(X) \in \{\pm 1, \pm 2\}$. Si $p(X) = \pm 1$, obtenemos que $\langle p(X)\rangle = \langle 2, X\rangle$ es todo $\mathbb{Z}[X]$, lo cual es imposible. Entonces, $p(X) = \pm 2$. Así, obtenemos que $X \in \langle p(X)\rangle = \langle 2\rangle$ y entonces existe $a(X)$ con coeficientes enteros tal que $X = 2.a(X)$. Lo cual es claramente imposible. Por lo tanto, $\langle 2, X\rangle$ *es un ideal no-principal.* ■

4.2. Homomorfismos y cocientes de anillos

En este sección introduciremos las otras dos nociones importantes en el estudio de anillos y las cuales son: la de homomorfismo y la de anillo cociente.

Definición 4.2.1. Sean A y B dos anillos. Una aplicación $f\colon A \to B$ es llamada un **homomorfismo de anillo** si cumple con:

(1) $f(x+y) = f(x) + f(y)$, para todo $x, y \in A$;

(2) $f(x.y) = f(x).f(y)$, para todo $x, y \in A$.

Además, diremos que f es un **monomorfismo de anillos** si f es una función inyectiva y f es llamada un **epimorfismo de anillos** si es sobreyectiva. Por último, f is dicha a ser un **isomorfismo de anillos** si es mono y epimorfismo. Si el contexto es claro y no hay peligro de confusión eliminaremos el adjetivo anillo de las definiciones anteriores.

Proposición 4.2.2. *Sea $f\colon A \to B$ un homomorfismo de anillos. Entonces,*

(1) $f(0_A) = 0_B$;

(2) $f(-a) = -f(a)$.

Si A y B tienen identidad y $f(1_A) = 1_B$, entonces se cumple que:

(3) *si $a \in \mathrm{U}(A)$, entonces $f(a) \in \mathrm{U}(B)$ y $f(a)^{-1} = f(a^{-1})$.*

Demostración. A cargo del lector. ■

Sean A y B dos anillos y sea $f\colon A \to B$ un homomorfismo. El conjunto

$$\mathrm{Nu}(f) := \{a \in A : \ f(a) = 0_B\}$$

es llamado el **núcleo** de f.

Proposición 4.2.3. *Sea $f\colon A \to B$ un homomorfismo de anillos. Entonces,*

(1) $\mathrm{Nu}(f)$ *es un ideal de A;*

(2) $\mathrm{Im}(f)$ *es una subanillo de B.*

(3) Si J es un ideal de B, entonces $f^{-1}(B)$ es un ideal de A.

(4) Si f es sobreyectiva e I es un ideal de A, entonces $f(I)$ es un ideal de B

Demostración. A cargo del lector. ■

Sea A un anillo e I un ideal (izquierdo y derecho). Como I es un subgrupo del grupo abeliano $\langle A, +\rangle$, podemos tomar el grupo cociente $\langle A/I, +\rangle$. Como A es más que un grupo abeliano, es un anillo e I es más que un subgrupo, es un ideal de A, podemos dotar al grupo cociente A/I de una operación que lo haga un anillo: definimos para $[a], [b] \in A/I$,

$$[a].[b] = [a.b].$$

El lector debe chequear que la nueva opercación . en A/I está bien definida.

Teorema 4.2.4. *Sea A un anillo y sea I un ideal de A. Entonces, $\langle A/I, +, .\rangle$ es un anillo y es llamado el* **anillo cociente de** *A por I. Además, si A es conmutativo así lo es A/I. La función $\pi_A\colon A \to A/I$ definida por $\pi_A(a) = [a]$ es un epimorfismo y $\mathrm{Nu}(\pi_A) = I$. La función π_A es llamada el* **epimorfismo canónico** *de A sobre A/I.*

El teorema anterior, que caracteriza la existencia y construcción de un anillo cociente, será de gran importancia para construir ejemplos de dominios de integridad y cuerpos.

Ejemplo 4.2.5. Sea $\mathbb{Z}[X]$ el anillo de polinomios con coeficientes enteros. Sea I el conjunto de todos los polinomios $p(X) = a_nX^n + \cdots + a_1X + a_0$ tal que $a_0 = a_1 = 0$ junto con el polinomio nulo. El conjunto I es un ideal del anillo $\mathbb{Z}[X]$. Observemos que para cada par $p(X) = a_nX^n + \cdots + a_1X + a_0, q(X) = b_nX^n + \cdots + b_1X + b_0 \in \mathbb{Z}[X]$

$$\begin{aligned} [p(X)] = [q(X)] &\iff p(X) - q(X) \in I \\ &\iff a_0 - b_0 = 0 \text{ y } a_1 - b_1 = 0 \\ &\iff a_0 = b_0 \text{ y } a_1 = b_1. \end{aligned}$$

En consecuencia se sigue que un conjunto completo de representativos del anillo cociente $\mathbb{Z}[X]/I$ es dado por los polinomios de la forma $aX + b$, esto es, $\mathbb{Z}[X]/I = \{[aX + b] : a, b \in \mathbb{Z}\}$. Observe que en este anillo cociente $\mathbb{Z}[X]/I$ tenemos que $[X][X] = [X^2] = [0]$, con lo cual $\mathbb{Z}[X]/I$ tiene divisores de cero, aunque el anillo $\mathbb{Z}[X]$ no tiene divisores de cero. Esto muestra que la propiedad de no tener divisores de cero no se preserva bajo cocientes. ■

Ahora estamos en condiciones de establecer tres teoremas sobre homomorfismos y cocientes de anillos. El lector debe percatarse de la similitud de estos teoremas con los Teoremas 2.3.2, 2.3.6 y 2.3.7 para grupos. Omitimos las demostraciones de los tres teoremas abajo y las dejamos como un buen ejercicio para lector.

Teorema 4.2.6 (Primer Teorema de Isomorfismo para anillos)**.** *Sea $f\colon A \to B$ un epimorfismo de anillos. Entonces,*

$$A/\mathrm{Nu}(f) \cong B.$$

Demostración. A cargo del lector. ■

Ejemplo 4.2.7. Sea A un anillo, X un conjunto no vacío y consideremos el anillo de funciones A^X. Para cada $c \in X$ definimos la función

$$E_c\colon A^X \to A \quad \text{por} \quad E_c(f) = f(c)$$

(llamada *evaluación en c*). La función E_c es un epimorfismo de anillos y $\mathrm{Nu}(E_c) = \{f \in A^X : E_c(f) = 0\} = \{f \in A^X : \ f(c) = 0\}$. Por lo tanto, $A^X/\mathrm{Nu}(E_c) \cong A$. ■

Teorema 4.2.8 (Teorema de Correspondencia)**.** *Sea A un anillo y sea I un ideal de A. Entonces, la aplicación que envía cada ideal J de A que contiene a I al ideal J/I del anillo cociente A/I es una correspondencia biunívoca.*

Demostración. A cargo del lector. ■

Ejemplo 4.2.9. Hallemos todos los ideales de $\mathbb{Z}_6$. Notemos que $\mathbb{Z}_6 = \mathbb{Z}/\langle 6\rangle$. Luego, por el Teorema de Correspondencia, tenemos que los ideales de $\mathbb{Z}_6$ son exactamente los ideales de la forma $J/\langle 6\rangle$ con J un ideal de $\mathbb{Z}$ tal que $\langle 6\rangle \subseteq J$. Recordemos que todos los ideales de $\mathbb{Z}$ son principales; además $\langle 6\rangle \subseteq \langle n\rangle \iff n \mid 6$. Entonces, los ideales de $\mathbb{Z}_6$ son

$$\begin{aligned}
\langle 6\rangle/\langle 6\rangle &= \{\overline{a} : a \in \langle 6\rangle\} = \{\overline{0}\}\\
\langle 3\rangle/\langle 6\rangle &= \{\overline{a} : a \in \langle 3\rangle\} = \{\overline{0}, \overline{3}\}\\
\langle 2\rangle/\langle 6\rangle &= \{\overline{a} : a \in \langle 2\rangle\} = \{\overline{0}, \overline{2}, \overline{4}\}\\
\langle 1\rangle/\langle 6\rangle &= \{\overline{a} : a \in \langle 1\rangle = \mathbb{Z}\} = \mathbb{Z}_6 \quad ■
\end{aligned}$$

Teorema 4.2.10. *Sea $f\colon A \to B$ un epimorfismo de anillo. Sea J un ideal de B y sea $I := f^{-1}[J]$. Entonces, I es un ideal de A y*

$$A/I \cong B/J$$

Demostración. A cargo del lector. ■

Corolario 4.2.11. *Sea A un anillo y sean I y J ideales de A tales que $J \subseteq I \subseteq A$. Entonces,*

$$A/I \cong (A/J)/(I/J).$$

Demostración. A cargo del lector. ■

4.3. Cuerpo cociente

En esta sección veremos cuáles anillos se pueden sumergir en un cuerpo. En otras palabras, veremos que para ciertos anillos podemos construir un cuerpo, a partir del anillo original, tal que el anillo este representado dentro de dicho cuerpo.

Sea A un dominio de integridad, esto es, un anillo conmutativo con identidad y sin divisores de cero. Además recuerde que A no es trivial, es decir, $1 \neq 0$. Ahora consideremos el siguiente conjunto:

$$M = \{(a, b) : a, b \in A \text{ y } b \neq 0\}.$$

Se define la relación binaria $\sim$ sobre M como sigue:

$$(a, b) \sim (c, d) \iff ad = bc. \tag{4.1}$$

Se observa sin dificultad que la relación $\sim$ se reflexiva y simétrica. Veamos que es también transitiva: supongamos que $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$. Luego, por la definición (4.1), tenemos que $ad = bc$ y $cf = de$. Entonces $adf = bcf = bde$. Dado que A es un dominio de integridad y $d \neq 0$, tenemos que $af = be$ y así $(a, b) \sim (e, f)$. Por lo tanto, $\sim$ es una relación de equivalencia sobre M y así determina una partición de M. Vamos a denotar a la clase de equivalencia del par (a, b) por a/b, esto es, $a/b = \{(c, d) \in M : (c, d) \sim (a, b)\}$. Según esta definición y (4.1) tenemos que

$$\frac{a}{b} = \frac{c}{d} \iff (a, b) \sim (c, d) \iff ad = bc.$$

A continuación vamos a dotar al conjunto cociente $M/\!\sim$ con dos operaciones: suma + y producto .. Ellas se definen como la suma y producto usuales en los números racionales:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{y} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Lo primero que debemos chequear es que las operaciones de suma y producto están bien definidas en $M/\!\sim$. Observemos que $bd \neq 0$ ya que A es un dominio de integridad y $b \neq 0$ y $d \neq 0$. Supongamos que $a/b = a'/b'$ y $c/d = c'/d'$. Entonces

$$ab' = a'b \quad \text{y} \quad cd' = c'd. \tag{4.2}$$

Multiplicando en (4.2) la primera identidad por dd' y la segunda por bb' obtenemos

$$\begin{array}{ccc} ab'.dd' = a'b.dd' & \text{y} & cd'.bb' = c'd.bb' \\ ad.b'd' = a'd'.bd & \text{y} & bc.b'd' = b'c'.bd. \end{array}$$

Sumando correspondientemente obtenemos

$$\begin{aligned} adb'd' + bcb'd' &= a'd'bd + b'c'bd \\ (ad + bc)b'd' &= (a'd' + b'c')bd. \end{aligned}$$

Entonces

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

lo cual implica que

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}.$$

Por lo tanto, la suma está bien definida. Para el producto, multiplicamos en (4.2) la primera igualdad por cd' y la segunda por $a'b$:

$$\begin{array}{ccc} ab'cd' = a'bcd' & \text{y} & cd'a'b = c'da'b \\ ac.b'd' = a'cbd' & \text{y} & a'cbd' = a'c'.bd. \end{array}$$

Entonces,

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

Teorema 4.3.1. *Para cada dominio de integridad A, la estructura $\langle M/\!\sim, +, .\rangle$ es un cuerpo y la función $\varphi\colon A \to M/\!\sim$ definida por $\varphi(a) = a/1$ es un monomorfismo de anillos.*

Demostración. Las pruebas de que las operaciones suma y producto en $M/\!\sim$ son asociativas y conmutativas son sencillas y se dejan a cargo del lector. Además, es directo comprobar que $0/1$ es elemento neutro con respecto a $+$, $(-a)/b$ es el opuesto de a/b y que $1/1$ es la identidad con

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\varphi"'] & K \\ M/\sim \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

Figura 4.1: $M/\sim$ es el menor cuerpo en el cual A está sumergido.

respecto al producto. El inverso multiplicativo de a/b con $a \neq 0$ es b/a. En efecto, como $a \neq 0$, $b/a \in M/\sim$ y

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}.$$

Por lo tanto, $M/\sim$ es un cuerpo. Ahora probemos que φ es un monomorfismo. Sean $a, a' \in A$. Observe que es sencillo comprobar que

$$\frac{a}{1} + \frac{a'}{1} = \frac{a+a'}{1} \quad \text{y} \quad \frac{a}{1} \cdot \frac{a'}{1} = \frac{aa'}{1}.$$

Entonces esto implica que $\varphi(a)+\varphi(a') = \varphi(a+a')$ y $\varphi(a).\varphi(a') = \varphi(aa')$ y además por definición $\varphi(1) = 1/1$. Así tenemos que φ es un homomorfismo de anillo. Las siguientes implicaciones muestran que φ es inyectiva:

$$\varphi(a) = \varphi(a') \implies \frac{a}{1} = \frac{a'}{1} \implies a.1 = 1.a' \implies a = a'.$$

Por lo tanto, φ es un monomorfismo. Esto completa la demostración. ■

El cuerpo $M/\sim$ es llamado el **cuerpo cociente** o **cuerpo de fracciones** del dominio de integridad A. El teorema anterior nos dice que A está sumergido en su cuerpo de cocientes $M/\sim$ y como es natural a los elementos de la forma $a/1$, los que representan a los elementos de A en $M/\sim$, los denotamos simplemente por a.

La siguiente proposición nos muestra que el cuerpo cociente de un dominio de integridad A es el *menor* cuerpo en el cual A está sumergido.

Proposición 4.3.2. *Sea A un dominio de integridad. Si K es un cuerpo y $f\colon A \to K$ es un monomorfismo de anillos, entonces existe un monomorfismo $h\colon M/\sim \to K$ tal que $f = h \circ \varphi$ (véase la Figura 4.1).*

Además, el cuerpo cociente $M/\sim$ de A es, salvo isomorfismo, el único con esta propiedad. Esto es, si L es un cuerpo tal que existe un monomorfismo $\alpha\colon A \to L$ con la propiedad: para todo cuerpo K y todo monomorfismo $f\colon A \to K$ existe un monomorfismo $h\colon L \to K$ tal que $\alpha = f \circ h$, entonces $L \cong M/\sim$.

Demostración de la Proposición 4.3.2. Definimos la función $h\colon M/\sim \to K$ como sigue: $h(a/b) = f(a).f(b)^{-1}$. Observemos que esta definición es admisible ya que $f(b) \neq 0$. Como es usual, lo primero que debemos mostrar es que h está bien definida:

$$\begin{aligned} \frac{a}{b} = \frac{a'}{b'} &\implies ab' = ba' \implies f(a)f(b') = f(b)f(a') \\ &\implies f(a)f(b)^{-1} = f(a')f(b')^{-1} \implies h(a/b) = h(a'/b'). \end{aligned}$$

Ahora probemos que h es un homomorfismo de anillos. Sean $a/b, c/d \in M/\sim$. Entonces,

$$\begin{aligned} h\left(\frac{a}{b}+\frac{c}{d}\right) &= h\left(\frac{ad+bc}{bd}\right) = f(ad+bc).f(bd)^{-1} \\ &= f(ad).f(bd)^{-1} + f(bc).f(bd)^{-1} = f(a).f(b)^{-1} + f(c).f(d)^{-1} \\ &= h\left(\frac{a}{b}\right) + h\left(\frac{c}{d}\right). \end{aligned}$$

y

$$\begin{aligned} h\left(\frac{a}{b}\cdot\frac{c}{d}\right) &= h\left(\frac{ac}{bd}\right) = f(ac).f(bd)^{-1} \\ &= f(a)f(b)^{-1}.f(c)f(d)^{-1} = h\left(\frac{a}{b}\right).h\left(\frac{c}{d}\right). \end{aligned}$$

Además, $h(1/1) = f(1).f(1)^{-1} = 1$. Luego, h es un homomorfismo. Ahora vemos que h es inyectiva:

$$\begin{aligned} h\left(\frac{a}{b}\right) = h\left(\frac{c}{d}\right) &\implies f(a)f(b)^{-1} = f(c)f(d)^{-1} \\ &\implies f(a)f(d) = f(c)f(b) \implies f(ad) = f(cb) \\ &\implies ad = cb \implies \frac{a}{b} = \frac{c}{d}. \end{aligned}$$

Por lo tanto, h es un monomorfismo y además $f(a) = f(a)f(1)^{-1} = h(a/1) = h(\varphi(a))$, esto es, $f = h \circ \varphi$. ■

Ejemplo 4.3.3. Sabemos que el cuerpo de los números racionales $\mathbb{Q}$ contiene al dominio de integridad de los enteros $\mathbb{Z}$. Se cumple que si K es un cuerpo y $f\colon \mathbb{Z} \to K$ es un monomorfismo, entonces $h\colon \mathbb{Q} \to K$ definida por $h(n/m) = f(n).f(m)^{-1}$ es un monomorfismo tal que para todo $n \in \mathbb{Z}$, $h(n) = f(n)$. Entonces, $\mathbb{Q}$ es el menor cuerpo que contiene a $\mathbb{Z}$ y por lo tanto, por la proposición anterior, $\mathbb{Q}$ es el cuerpo cociente (o cuerpo de fracciones) de $\mathbb{Z}$. ■

Ejemplo 4.3.4. Si A es un subanillo con identidad de un cuerpo K, entonces el cuerpo cociente de A es $F := \{a.b^{-1} : a \in A, b \in A^*\}$ el cual es un subcuerpo de K. ■

Ejemplo 4.3.5. Como $\mathbb{Z}$ es un dominio de integridad, el anillo de polinomios $\mathbb{Z}[X]$ es también un dominio de integridad. El cuerpo de fracciones de $\mathbb{Z}[X]$ es el cuerpo de *funciones racionales* en la indeterminada X sobre $\mathbb{Z}$. Denotamos a este cuerpo cociente como

$$\mathrm{R}(\mathbb{Z}[X]) = \left\{\frac{p(X)}{q(X)} : p(X), q(X) \in \mathbb{Z}[X] \text{ y } q(X) \neq 0\right\}.$$

Observemos que el cuerpo $\mathrm{R}(\mathbb{Z}[X])$ contiene al cuerpo de fracciones de $\mathbb{Z}$, es decir, $\mathrm{R}(\mathbb{Z}[X])$ contiene a $\mathbb{Q}$.

Por otro lado, $\mathbb{Q}[X]$ es un dominio de integridad (no es cuerpo) y su cuerpo cociente es el de las funciones racionales sobre $\mathbb{Q}$:

$$\mathrm{R}(\mathbb{Q}[X]) = \left\{\frac{p(X)}{q(X)} : p(X), q(X) \in \mathbb{Q}[X],\ q(X) \neq 0\right\}.$$

$$
\begin{tikzcd}
\mathbb{Z} \arrow[r, hook] \arrow[d, hook] & \mathbb{Q} \arrow[d, hook] \\
\mathbb{Z}[X] \arrow[r, hook] \arrow[d, hook] & \mathbb{Q}[X] \arrow[d, hook] \\
\mathrm{R}(\mathbb{Z}[X]) \arrow[r, leftrightarrow] & \mathrm{R}(\mathbb{Q}[X])
\end{tikzcd}
$$

Figura 4.2: El cuerpo de funciones racionales sobre $\mathbb{Z}$ y $\mathbb{Q}$.

Es claro que $\mathrm{R}(\mathbb{Z}[X]) \subseteq \mathrm{R}(\mathbb{Q}[X])$. Ahora, sea $\frac{p(X)}{q(X)} \in \mathrm{R}(\mathbb{Q}[X])$ y sea m el común denominador de todos los coeficientes en $p(X)$ y $q(X)$. Entonces $\frac{p(X)}{q(X)} = \frac{m.p(X)}{m.q(X)} \in \mathrm{R}(\mathbb{Z}[X])$. Luego $\mathrm{R}(\mathbb{Q}[X]) \subseteq \mathrm{R}(\mathbb{Z}[X])$ y por lo tanto ambos cuerpos de funciones racionales coinciden. Por lo tanto hemos obtenido lo siguiente: como $\mathbb{Q}$ es el cuerpo cociente de $\mathbb{Z}$, los cuerpos cocientes de los dominios integrales $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$ coinciden. Esto es resumido en la Figura 4.2, donde las flechas representan la inclusión entre conjuntos. ■

4.4. Teorema chino de los restos

El Teorema chino de los restos es uno de los resultados más importante y útiles en la Teoría de Números. Aquí presentamos una de sus formas más abstracta en la teoría de anillos y la aplicamos para determinar su forma más clásica en la teoría de los números enteros, la cual nos permite resolver sistemas lineales de congruencias.

Primeros necesitamos algunas definiciones y resultados generales en la teoría de anillos. Para aquellos resultados en los que no se presente una demostración, ellas quedan a cargo del lector.

Definición 4.4.1. Sean $A_1, \ldots, A_n$ anillos. Se definen en el producto cartesiano $A_1 \times \cdots \times A_n$ las siguientes operaciones:
para $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in A_1 \times \cdots \times A_n$,

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n) \quad \text{y}$$

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Proposición 4.4.2. *Para cualesquiera $A_1, \ldots, A_n$ anillos, el producto cartesiano $A_1 \times \cdots \times A_n$ con las operaciones antes definidas es un anillo. Además:*

(1) *si todos los anillos $A_1, \ldots, A_n$ tienen identidad, entonces el anillo $A_1 \times \cdots \times A_n$ tiene una identidad;*

(2) *si todos los anillos $A_1, \dots, A_n$ son conmutativos, entonces el anillo $A_1 \times \cdots \times A_n$ es conmutativo.*

Observación 4.4.3. Si A y B son dos dominios de integridad, entonces el anillo producto $A \times B$ no es necesariamente un dominio de integridad. Por ejemplo, el elemento $(1, 0)$ es un divisor de cero en $\mathbb{Z} \times \mathbb{Z}$.

Definición 4.4.4. Sea A un anillo con identidad. Dos ideales I y J de A son llamados **comaximales** si $I + J = A$. Un número finito de ideales $I_1, \dots, I_n$ son llamados **comaximales** si son comaximales de a pares, esto es, si $I_k + I_r = A$ para todos $k \neq r$.

Proposición 4.4.5. *Sea A un anillo con identidad. Si I_1, I_2 y J son ideales de A tales que J es comaximal con I_1 y J es comaximal con I_2, entonces J es comaximal con $I_1 \cap I_2$.*

Demostración. Sea $a \in A$. Como $A = J + I_1$ y $A = J + I_2$, existen $j_1, j_2 \in J$, $i_1 \in I_1$ e $i_2 \in I_2$ tales que $1 = j_1 + i_1$ y $a = j_2 + i_2$. Entonces, $a = 1.a = (j_1 + i_1)(j_2 + i_2) \in J + (I_1 \cap I_2)$. Por lo tanto, $A = J + (I_1 \cap I_2)$, es decir, J es comaximal con $I_1 \cap I_2$. ■

Ahora estamos listo para presentar el resultado principal de esta sección. Para un ideal I de un anillo A, la notación $a \equiv b(\text{mód}\, I)$ significa, como es habitual en $\mathbb{Z}$, que $a/I = b/I$, esto es, a y b son dos representantes de la misma clase de equivalencia en el cociente A/I.

Teorema 4.4.6 (Teorema chino de los restos)**.** *Sea A un anillo con identidad. Sean $I_1, \dots, I_n$ ideales comaximales de A y sean $a_1, \dots, a_n \in A$. Entonces, existe un elemento $a \in A$ tal que*

$$a \equiv a_1(\text{mód}\, I_1), \ \dots, \ a \equiv a_n(\text{mód}\, I_n).$$

Además, a está unívocamente determinado módulo $I_1 \cap \cdots \cap I_n$.

Demostración. Vamos a probar el teorema para $n = 2$ y luego probamos el caso general por inducción. Como $I_1 + I_2 = A$, tenemos que $1 = u_1 + u_2$ para algunos $u_1 \in I_1$ y $u_2 \in I_2$. Tomemos $a := a_2u_1 + a_1u_2$. Usando el hecho que I_1 es un ideal y $u_2 - 1 = -u_1$ obtenemos que

$$\begin{aligned} a - a_1 = a_2.u_1 + a_1.u_2 - a_1 = a_2.u_1 + a_1.(u_2 - 1) = \\ a_2.u_1 - a_1.u_1 = (a_2 - a_1).u_1 \in I_1. \end{aligned}$$

Luego, $a \equiv a_1(\text{mód}\, I_1)$. Análogamente, se obtiene que $a \equiv a_2(\text{mód}\, I_2)$. Además, si b es otro elemento en A que cumple con $b \equiv a_1(\text{mód}\, I_1)$ y $b \equiv a_2(\text{mód}\, I_2)$, entonces $a - b \in I_1 \cap I_2$. Luego $a/I_1 \cap I_2 = b/I_1 \cap I_2$.

Ahora pasamos al caso general. Supongamos que el teorema es válido para n y sean $I_1, \dots, I_n, I_{n+1}$ ideales comaximales de A y sean $a_1, \dots, a_n, a_{n+1} \in A$. Como $I_1, \dots, I_n$ son comaximales, por la hipótesis inductiva tenemos que existe un elemento $b \in A$ tal que

$$b \equiv a_1(\text{mód}\, I_1), \ \dots, \ b \equiv a_n(\text{mód}\ I_n).$$

Ahora, por la Proposición 4.4.5, sabemos que los ideales $I_1 \cap \cdots \cap I_n$ y I_{n+1} son comaximales. Entonces, como ya hemos probado, existe un elemento $a \in A$ tal que

$$a \equiv b(\text{mód}\, I_1 \cap \cdots \cap I_n) \quad \text{y} \quad a \equiv a_{n+1}(\text{mód}\, I_{n+1}).$$

La primera equivalencia implica que $a \equiv b(\text{mód } I_1)$, ..., $a \equiv b(\text{mód } I_n)$. Luego, usando transitividad obtenemos

$$a \equiv a_1(\text{mód } I_1),\ \ldots,\ a \equiv a_n(\text{mód } I_n) \text{ y } a \equiv a_{n+1}(\text{mód } I_{n+1}). \qquad \blacksquare$$

Ahora veamos como aplicar el Teorema chino de los restos para resolver un sistema lineal de congruencias de la forma:

$$\begin{cases} x \equiv a_1(\text{mód } n_1) \\ x \equiv a_2(\text{mód} n_2) \\ \quad\vdots \\ x \equiv a_k(\text{mód } n_k). \end{cases} \tag{4.3}$$

Sean m y n enteros relativamente primos. Entonces, existen enteros s y t tales que $1 = m.s+n.t$. Luego, para todo entero k, $k = m.s.k + n.t.k$. Por lo tanto, $\mathbb{Z} = \langle m\rangle + \langle n\rangle$, esto es, los ideales $\langle m\rangle$ y $\langle n\rangle$ son comaximales. Además, es claro que

$$a \equiv b(\text{mód}\langle n\rangle) \iff a/\langle n\rangle = b/\langle n\rangle \iff n \mid a-b \iff a \equiv b(\text{mód } n).$$

Teorema 4.4.7. *Sean $n_1, \ldots, n_k$ enteros positivos y relativamente primos dos a dos. Si $a_1, \ldots, a_k$ son enteros cualesquiera, entonces el sistema de congruencias* (4.3) *tiene una solución a que es única módulo $n_1.n_2.\ldots.n_k$.*

Demostración. Consideremos los ideales $\langle n_1\rangle, \ldots, \langle n_k\rangle$ que son comaximales ya que los enteros $n_1, \ldots, n_k$ son relativamente primos dos a dos y además sabemos que $x \equiv a_i(\text{ mód } n_i) \iff x \equiv a_i(\text{mód}\,\langle n_i\rangle)$ para cada $i = 1, \ldots, k$. Entonces, por el Teorema chino de los restos, existe un elemento a que es solución del sistema (4.3) y es único módulo $\langle n_1\rangle \cap \cdots \cap \langle n_k\rangle = \langle n_1.n_2.\ldots.n_k\rangle$. $\blacksquare$

Para cerrar esta sección, veamos un algoritmo para hallar las soluciones de los sistemas de congruencias (4.3) y obtener la única solución módulo $n_1.n_2.\ldots.n_k$. Supongamos que tenemos el sistema (4.3), entonces:

(1) para cada $i = 1, \ldots, k$, calcular $M_i = \dfrac{\prod_{j=1}^{k} n_j}{n_i}$;

(2) para cada $i = 1, \ldots, k$, hallar el inverso d_i de M_i módulo n_i;

(3) una solución particular del sistema es:

$$x_0 := a_1.M_1.d_1 + \cdots + a_k.M_k.d_k;$$

(4) la única solución módulo $n_1.n_2.\ldots.n_k$ es el resto de dividir la solución x_0 por $n_1.n_2.\ldots.n_k$;

(5) todas las soluciones del sistema son de la forma:

$$x = x_0 + (n_1.n_2.\ldots.n_k).t \qquad \text{para } t \in \mathbb{Z}.$$

Ejemplo 4.4.8. Determinemos las soluciones del siguiente sistema de congruencias:

$$\begin{cases} x \equiv 2(\text{mód } 3) \\ x \equiv 3(\text{mód } 5) \\ x \equiv 5(\text{mód } 7). \end{cases}$$

Vamos a seguir los pasos del algoritmo descrito recién:

(1) $M_1 = 5.7 = 35$, $M_2 = 3.7 = 21$ y $M_3 = 3.5 = 15$.

(2) Como $35 \equiv 2(\text{mód } 3)$, entonces $d_1 = 2$ (esto es, $2/\langle 3\rangle$ es el inverso de $35/\langle 3\rangle$ en Z_3); como $21 \equiv 1(\text{mód } 5)$, entonces $d_2 = 1$ y; como $15 \equiv 1(\text{mód } 7)$, entonces $d_3 = 1$.

(3) Una solución del sistema es:

$$x_0 = a_1.M_1.d_1 + a_2.M_2.d_2 + a_3.M_3.d_3 = 2.35.2 + 3.21.1 + 5.15.1 = 278.$$

(4) La solución única módulo $3.5.7 = 105$ es 68, ya que es el resto de dividir 278 por 105 o equivalentemente $278 \equiv 68(\text{mód } 105)$.

(5) Todas las soluciones del sistemas son:

$$x = 278 + 105.t \quad \text{con } t \in \mathbb{Z}. \quad \blacksquare$$

4.5. Ideales maximales y primos

En esta sección todos los anillos considerados, a menos que se indique otra cosa, serán anillos conmutativos con identidad. Aquí estudiaremos dos clases importantes de ideales: ideales máximales e ideales primos.

Diremos que un ideal I de un anillo A es **propio** si $I \neq A$.

Definición 4.5.1. Sea A un anillo. Un ideal I de A es llamado **maximal** si es propio y no está contenido estrictamente en ningún otro ideal propio de A. Esto es, I es maximal cuando se cumple que para cada ideal propio J de A, si $I \subseteq J$, entonces $I = J$.

Lo primero que debemos probar es la existencia de ideales máximales. Esto es consecuencia del Lema de Zorn (véase el Capítulo **??**).

Proposición 4.5.2. *Sea A un anillo. Cada ideal propio de A está contenido en un ideal maximal de A.*

Demostración. Sea I un ideal propio de A. Consideremos el conjunto

$$\mathcal{H} = \{J : J \text{ es un ideal propio de } A \text{ y } I \subseteq J\}$$

ordenado por la relación de inclusión: $\subseteq$. Veamos que el conjunto ordenado $\mathcal{H}$ cumple las hipótesis del Lema de Zorn. Primero, $\mathcal{H} \neq \emptyset$. En efecto, se tiene que $I \in \mathcal{H}$ por ser I un ideal propio de A e $I \subseteq I$. Sea $\mathcal{C} = \{J_\alpha : \alpha \in \Gamma\}$ una cadena de $\mathcal{H}$. Probemos que $J := \bigcup_{\alpha\in\Gamma} J_\alpha$ pertenece a $\mathcal{H}$, es decir, probemos que J es un ideal propio de A y $I \subseteq J$.

- J es ideal de A:
  - Para cualquier $\alpha \in \Gamma$, $0 \in J_\alpha \subseteq J$. Entonces $J \neq \emptyset$.
  - Sean $a, b \in J$. Entonces existen $\alpha, \beta \in \Gamma$ tales que $a \in J_\alpha$ y $b \in J_\beta$. Como $\mathcal{C}$ es una cadena tenemos que $J_\alpha \subseteq J_\beta$ o $J_\beta \subseteq J_\alpha$. Supongamos que $J_\alpha \subseteq J_\beta$ (igual si $J_\beta \subseteq J_\alpha$). Entonces, $a, b \in J_\beta$. Como J_β es ideal, tenemos que $a - b \in J_\beta \subseteq J$.
  - Sea $a \in J$ y $b \in A$. Entonces, existe $\alpha \in \Gamma$ tal que $a \in J_\alpha$. Como J_α es ideal tenemos que $ab \in J_\alpha \subseteq J$.
- J es propio. Como cada $J_\alpha \in \mathcal{H}$, J_α es propio. Con lo cual $1 \notin J_\alpha$ para todo $\alpha \in \Gamma$. Entonces $1 \notin J$.
- $I \subseteq J$. En efecto, sea $\alpha \in \Gamma$. Como $J_\alpha \in \mathcal{H}$, se tiene que $I \subseteq J_\alpha \subseteq J$.

Por lo tanto, $J = \bigcup_{\alpha\Gamma} J_\alpha \in \mathcal{H}$ y es claramente una cota superior de la cadena $\mathcal{C} = \{J_\alpha : \alpha \in \Gamma\}$. Por lo tanto, por el Lema de Zorn, existe un elemento maximal de $\mathcal{H}$. Esto es, existe un ideal maximal M de A tal que $I \subseteq M$. ■

Observemos que en todo anillo A existe al menos un ideal máximal. El ideal trivial $\{0\}$ es propio ($1 \notin \{0\}$), entonces existe un ideal máximal M (el cual obviamente contiene a 0).

Proposición 4.5.3. *Sea A un anillo conmutativo y sea M un ideal propio de A. Entonces, M es un ideal máximal si y sólo si A/M es un cuerpo.*

Demostración. Supongamos que M es maximal. Ya sabemos que A/M es un anillo conmutativo. Veamos que todo elemento no nulo $[a]$ de A/M es invertible. Como $[a]$ es no nulo, $a \notin M$. Consideremos el ideal $Aa + M = \{x.a + m : \ x \in A, \ m \in M\}$. Es claro que $a \in Aa + M$ y $M \subsetneq Aa + M$. Por la maximalidad de M, $A = Aa + M$. Con lo cual, $1 \in Aa + M$. Así, $1 = x.a + m$ para algunos $x \in A$ y $m \in M$. Entonces,

$$[a][x] = [a.x] = [1 - m] = [1] - [m] = [1]^1.$$

Entonces, $[x]$ es el inverso multiplicativo de $[a]$.

Recíprocamente, supongamos ahora que A/M es un cuerpo y probemos que M es maximal. Como A/M es un cuerpo, los únicos ideales de A/M son $\{0\}$ y A/M (véase el Ejercicio 4.10). Por el Teorema de Correspondencia en anillos, tenemos que los únicos ideales de A que contienen a M son M y A. Por lo tanto, M es máximal. ■

La proposición anterior es una herramienta útil para comprobar que un ideal es maximal. Veamos el siguiente ejemplo.

Ejemplo 4.5.4.

[1] Pues, $m \in M$, entonces $[m]$ es el cero de A/M.

(1) Sea n un entero positivo. Es claro que $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ es el anillo cociente de $\mathbb{Z}$ por el ideal $\langle n\rangle$. Entonces,

$$\begin{aligned}\text{el ideal } \langle n\rangle \text{ es maximal } &\iff \mathbb{Z}_n \text{ es un cuerpo}\\ &\iff n \text{ es primo.}\end{aligned}$$

(2) El ideal $\langle 2, X\rangle$ de $\mathbb{Z}[X]$ es maximal porque el anillo cociente $\mathbb{Z}[X]/\langle 2, X\rangle$ es isomorfo a $\mathbb{Z}_2$ que es un cuerpo. En efecto, considere la función $\varphi\colon \mathbb{Z}[X] \to \mathbb{Z}_2$ definida por $\varphi(p(X)) = \overline{p(0)}$ para cada $p(X) \in \mathbb{Z}[X]$. Entonces, φ es un epimorfismo de anillos y $\mathrm{Nu}(\varphi) = \langle 2, X\rangle$. Luego, por el Primer Teorema de Isomorfismo, nos queda que $\mathbb{Z}[X]/\langle 2, X\rangle \cong \mathbb{Z}_2$ (véase el Ejercicio 4.21). ■

Si en la Proposición anterior ponemos una condición más débil que la de ser A/M un cuerpo, como por ejemplo que sea un dominio de integridad, ¿que tipo de ideal debería ser M?

Definición 4.5.5. Un **ideal primo** en un anillo conmutativo A es un ideal propio P que verifica la siguiente condición: para cualesquiera $a, b \in A$,

$$a.b \in P \implies a \in P \text{ o } b \in P.$$

Podemos motivar la definición anterior mirando en los ideales $\langle n\rangle$ del anillo de los enteros $\mathbb{Z}$. Sea $p \in \mathbb{Z}$. El ideal $\langle p\rangle$ es primo si y sólo si

$$p \mid a.b \Longrightarrow p \mid a \text{ o } p \mid b$$

lo cual es equivalente al requerimiento de que p sea primo.

Ejemplo 4.5.6. Probemos que el ideal $\langle X\rangle$ es primo en $\mathbb{Z}[X]$. Primero observemos que

$$\langle X\rangle = \{X.a(X) : a(X) \in \mathbb{Z}[X]\} = \{p(X) \in \mathbb{Z}[X] : p(0) = 0\}.$$

Ahora es claro que $\langle X\rangle$ es propio, porque $1 \notin \langle X\rangle$. Ahora probemos que $\langle X\rangle$ cumple la condición para ser primo. Sean $p(X), q(X) \in \mathbb{Z}[X]$ y supongamos que $p(X).q(X) \in \langle X\rangle$. Entonces $p(0)q(0) = 0$. Como $p(0), q(0) \in \mathbb{Z}$ y $\mathbb{Z}$ es un dominio de integridad, tenemos que $p(0) = 0$ o $q(0) = 0$. Con lo cual $p(X) \in \langle X\rangle$ o $q(X) \in \langle X\rangle$. Por lo tanto, $\langle X\rangle$ es primo. ■

Proposición 4.5.7. *Sea A un anillo conmutativo y P un ideal de A. Entonces, P es primo si y sólo si A/P es un dominio de integridad.*

Demostración. Supongamos primero que P es un ideal primo de A. Sabemos que A/P es un anillo conmutativo. El elemento cero (o neutro) del anillo cociente A/P es P. Sean $a, b \in A$ y supongamos que $[a][b] = P$. Entonces, $[a.b] = P$ y así $a.b \in P$. Por ser P primo, $a \in P$ o $b \in P$. Esto es, $[a] = P$ o $[b] = P$.

Recíprocamente, supongamos que A/P es un dominio de integridad. Así, P es propio[2]. Supongamos que $a.b \in P$. Entonces, $[a].[b] = [a.b] = P$ y como sabemos P es el elemento nulo de A/P. Luego, como A/P es un dominio de integridad, $[a] = P$ o $[b] = P$. Entonces, $a \in P$ o $b \in P$. Por lo tanto, P es un ideal primo de A. ■

[2]Pues, si $P = A$ entonces A/P tendría solo un elemento con lo cual $1 = 0$ lo que no puede ser.

Corolario 4.5.8. *Sea A un anillo conmutativo. Entonces, todo ideal maximal de A es primo.*

Demostración. Sea A un anillo conmutativo. Si I es un ideal maximal de A, entonces por la Proposición 4.5.3 tenemos que A/I es un cuerpo. Con lo cual, A/I es en particular un dominio de integridad. Entonces, por la Proposición 4.5.7, I es primo. ■

Ejemplo 4.5.9. Sea $\mathbb{Z}[X]$ el anillo de polinomios con coeficientes enteros. Probemos que el ideal $\langle 2\rangle$ es primo y no maximal en $\mathbb{Z}[X]$. El ideal generado por 2 es

$$\begin{aligned}\langle 2\rangle &= \{2.a(X) : a(X) \in \mathbb{Z}[X]\}\\ &= \{f(X) \in \mathbb{Z}[X] : \text{ todos los coeficientes de } f(X) \text{ son enteros pares}\}.\end{aligned}$$

Tenemos que $\langle 2\rangle$ es un ideal propio ya que $X \notin \langle 2\rangle$. Veamos que el ideal $\langle 2\rangle$ es primo. Consideremos el epimorfismo $\psi : \mathbb{Z}[X] \to \mathbb{Z}_2[X]$ dado por $\psi(f(X)) = \overline{f}(X)$, donde $\overline{f}$ indica que los coeficientes de $f(X)$ son reducidos módulo 2. Esto es, si $f(X) = a_nX^n + \cdots + a_1X + a_0$, entonces $\psi(f(X)) = \overline{f}(X) = \overline{a_n}X^n + \cdots + \overline{a_1}X + \overline{a_0}$. Notemos que $\mathrm{Nu}(\psi) = \langle 2\rangle$ (véase el Ejercicio 4.20). Del hecho que $\mathbb{Z}_2[X]$ es un dominio de integridad (véase la Proposición 5.6.3) y por el corolario anterior, obtenemos que $\langle 2\rangle$ es un ideal primo. Además, $\langle 2\rangle$ no es máximal pues está incluido estrictamente en $\langle 2, X\rangle$. ■

El siguiente corolario es consecuencia de las Proposiciones 4.5.3 y 4.5.7, y del Primer Teorema de Isomorfismo para anillos.

Corolario 4.5.10. *Sea $f\colon A \to B$ un epimorfismo de anillos conmutativos. Entonces,*

(1) *B es un cuerpo si y sólo si $\mathrm{Nu}(f)$ es un ideal maximal de A;*

(2) *B es un dominio integral si y sólo si $\mathrm{Nu}(f)$ es un ideal primo de A.*

Demostración. Ejercicio para el lector. ■

Ejercicios propuestos

Definiciones y propiedades

Ejercicio 4.1. Sea X un conjunto arbitrario no vacío y sea A un anillo. Sea

$$A^X = \{f : f\colon X \to A \text{ es función}\}$$

el conjunto de todas las funciones $f\colon X \to A$. En A^X se definen las operaciones suma y multiplicación como sigue: sean $f, g \in A^X$ entonces

$$(f+g)(x) = f(x) + g(x) \quad \text{y} \quad (fg)(x) = f(x)g(x), \qquad \text{para cada } x \in X.$$

Probar que $\langle A^X, +, \cdot\rangle$ es un anillo.

Ejercicio 4.2. Sea A un conjunto no vacío y $+$ y $\cdot$ dos operaciones binarias sobre A tal que $\langle A, +\rangle$ es un grupo (no se asume que sea abeliano), la operación $\cdot$ es asociativa con una identidad 1 y la operación $\cdot$ distribuye con respecto a $+$ (ver (A3)). Entonces, probar que $\langle A, +, \cdot\rangle$ es un anillo con identidad. (Observe que solo tiene que verificar que la operación $+$ sea conmutativa).

Ejercicio 4.3. Sea A un anillo conmutativo con identidad. Probar que A es un dominio de integridad si y sólo si cumple que: para todos $a, b, c \in A$, si $a \neq 0$ y $ab = ac$, entonces $b = c$.

Ejercicio 4.4. Sea A un anillo con identidad. Sean $a, b, c \in A$. Probar que si $a.b = 1$ y $c.a = 1$, entonces $b = c$. Y por lo tanto, a es invertible.

Ejercicio 4.5. Sea A un anillo con identidad 1. Probar que el inverso de un elemento $a \in A$ es único.

Ejercicio 4.6. Sea A un anillo. Probar que para todo número entero n se cumple que $(n.a)b = n.(ab)$ para todos $a, b \in A$. Indique en cada paso de la demostración que propiedad de anillos se utilizo.

Ejercicio 4.7. Sea A un anillo y sea B un subanillo de A. Probar que:

(a) Si A es conmutativo, entonces B es conmutativo.

(b) Si A es un dominio de integridad, entonces B es un dominio de integridad.

(c) $\mathrm{U}(B) \subseteq \mathrm{U}(A)$.

Ejercicio 4.8. Sea $\mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Probar que $\mathbb{Z}[\sqrt{-3}]$ es un dominio de integridad.

Ejercicio 4.9. Sea A un anillo con identidad. Probar que si I es un ideal de A tal que $1 \in I$, entonces $I = A$.

Ejercicio 4.10. Sea A un anillo conmutativo con identidad. Probar que A es un cuerpo si y sólo si A los únicos ideales de A son los triviales (es decir, los únicos ideales de A son $\{0\}$ y A).

Ejercicio 4.11. Sea A un anillo conmutativo con identidad y sea $\{I_\alpha : \alpha \in \Gamma\}$ una familia de ideales de A. Probar que la intersección $\bigcap_{\alpha\in\Gamma} I_\alpha$ es un ideal de A.

Ejercicio 4.12. Sea A un anillo. Sean I y J ideales de A. Probar que:

(a) $I + J := \{a + b : a \in I \text{ y } b \in J\}$ es un ideal de A.

(b) $I \cdot J := \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : n \in \mathbb{N},\ a_i \in I,\ b_i \in J\}$ es un ideal de A.

(c) $I \cdot J \subseteq I \cap J$.

(d) Si $I + J = A$, entonces $I \cdot J = I \cap J$.

Ejercicio 4.13. Considerar el anillo $\mathbb{Z}$. En cada uno de los siguientes incisos hallar un entero positivo a tal que

(a) $\langle a\rangle = \langle 2\rangle + \langle 3\rangle$. (b) $\langle a\rangle = \langle 6\rangle + \langle 8\rangle$. (c) $\langle a\rangle = \langle 15\rangle + \langle 21\rangle$. (d) $\langle a\rangle = \langle n\rangle + \langle m\rangle$.

Ejercicio 4.14. Considerar el anillo $\mathbb{Z}$. En cada uno de los siguientes incisos hallar un entero positivo a tal que

(a) $\langle a\rangle = \langle 2\rangle \cdot \langle 3\rangle$. (b) $\langle a\rangle = \langle 6\rangle \cdot \langle 8\rangle$. (c) $\langle a\rangle = \langle n\rangle \cdot \langle m\rangle$.

Ejercicio 4.15. Considerar el anillo de polinomios $\mathbb{Z}[X]$ con coeficientes enteros. Sea $I = \{p(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X] : a_1 = a_0 = 0\}$. Probar que $I = \langle X^2\rangle$.

Ejercicio 4.16. Sean $n \in \mathbb{N}$. Probar que todo ideal de $\mathbb{Z}_n$ es principal.

Ejercicio 4.17. Sean $A_1, \ldots, A_n$ anillos. Considerar las siguientes operaciones sobre el producto cartesiano $A_1 \times \cdots \times A_n$: para todos $\overline{a} = (a_1, \ldots, a_n), \overline{b} = (b_1, \ldots, b_n) \in A_1 \times \cdots \times A_n$,

$$\overline{a} + \overline{b} = (a_1 + b_1, \ldots, a_n + b_n) \quad \text{y} \quad \overline{a}.\overline{b} = (a_1b_1, \ldots, a_nb_n).$$

(a) Probar que $A_1 \times \cdots \times A_n$ con las operaciones recién definidas es un anillo.

(b) Probar que si cada anillo A_i es conmutativo, entonces $A_1 \times \cdots \times A_n$ es conmutativo.

(c) Probar que si cada anillo A_i tiene identidad, entonces $A_1 \times \cdots \times A_n$ tiene identidad.

(d) Probar que si cada anillo A_i es un dominio de integridad, entonces $A_1 \times \cdots \times A_n$ es un dominio de integridad.

(e) Probar que si cada anillo A_i es un cuerpo, entonces $A_1 \times \cdots \times A_n$ es un cuerpo.

Homomorfismos y cocientes de anillos

Ejercicio 4.18. Sea $f\colon A \to B$ un homomorfismo de anillos. Entonces, f es inyectivo si y sólo si $\mathrm{Nu}(f) = \{0_B\}$.

Ejercicio 4.19. Considerar el anillo de polinomios $\mathbb{Z}[X]$. Probar que:

(a) $\langle X\rangle = \{p(X) \in \mathbb{Z}[X] : p(0) = 0\}$.

(b) La función $\varphi\colon \mathbb{Z}[X] \to \mathbb{Z}$ definida por $\varphi(p(X)) = p(0)$ es un epimorfismo de anillos.

(c) $\mathrm{Nu}(\varphi) = \langle X\rangle$.

(d) $\mathbb{Z}[X]/\langle X\rangle \cong \mathbb{Z}$.

Ejercicio 4.20. Considerar el anillo de polinomios $\mathbb{Z}[X]$. Probar que:

(a) $\langle 2\rangle = \{p(X) \in \mathbb{Z}[X] :$ todos los coeficientes de $p(X)$ son múltiplos de $2\}$.

(b) Sea $\mathbb{Z}_2[X]$ el anillo de polinomios con coeficientes en $\mathbb{Z}_2$. La función $\psi\colon \mathbb{Z}[X] \to \mathbb{Z}_2[X]$ definida por: si $p(X) = a_nX^n + \cdots + a_1X + a_0$, entonces $\psi(p(X)) = \overline{a_n}X^n + \cdots + \overline{a_1}X + \overline{a_0}$ es un epimorfismo de anillos.

(c) $\mathrm{Nu}(\psi) = \langle 2 \rangle$.

(d) $\mathbb{Z}[X]/\langle 2 \rangle \cong \mathbb{Z}_2[X]$.

Ejercicio 4.21. Considerar el anillo de polinomios $\mathbb{Z}[X]$. Probar que:

(a) $\langle 2, X \rangle = \{p(X) \in \mathbb{Z}[X] : p(0) \text{ es par}\}$.

(b) La función $\varphi\colon \mathbb{Z}[X] \to \mathbb{Z}_2$ definida por $\varphi(p(X)) = \overline{p(0)}$ es un epimorfismo de anillos.

(c) $\mathrm{Nu}(\varphi) = \langle 2, X \rangle$.

(d) $\mathbb{Z}[X]/\langle 2, X \rangle \cong \mathbb{Z}_2$.

Ejercicio 4.22. Sea $A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$.

(a) Probar que A es un subanillo de $M_2(\mathbb{R})$.

(b) Sea $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R} \right\}$. Probar que I es un ideal de A.

(c) Probar que $A/I \cong \mathbb{R}$.

Ejercicio 4.23. Sean $I_1, \ldots, I_n$ ideales de un anillo A. Pruebe que la aplicación $\psi\colon A/\bigcap_{k=1}^{n} I_k \to A/I_1 \times \cdots \times A/I_n$ definida por $\psi([a]) = (\pi_1(a), \ldots, \pi_n(a))$ es un monomorfismo, donde cada π_k es el epimorfismo canónico determinado por el anillo cociente A/I_k.

Ejercicio 4.24. Considerar el anillo de polinomios $\mathbb{R}[X]$ y el cuerpo de números complejos $\mathbb{C}$.

(a) Probar que la función $\varphi\colon \mathbb{R}[X] \to \mathbb{C}$ definida por $\varphi(f(X)) = f(i)$ es un epimorfismo de anillo.

(b) Probar que $\mathrm{Nu}(\varphi) = \langle X^2 + 1 \rangle$.

(c) Probar que $\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}$.

Ejercicio 4.25. Suponga que hay un número real r con la propiedad que $r + 1/r$ es un entero impar. Probar que r es irracional.

Cuerpo cociente

Ejercicio 4.26. (a) Demostrar que $\mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{R}$, conmutativo con identidad y sin divisores de cero, es decir $\mathbb{Z}[\sqrt{3}]$ es un dominio de integridad.

(b) Demostrar que $\mathbb{Q}[\sqrt{3}] := \{q_1 + q_2\sqrt{3} : q_1, q_2 \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$ y es el cuerpo cociente del dominio de integridad $\mathbb{Z}[\sqrt{3}]$. (*Sug.*: Usar el resultado del Ejemplo 4.3.4.)

Teorema chino de los restos

Ejercicio 4.27. Considere la situación del Ejercicio 4.23. Pruebe la siguiente afirmación: el monomorfismo ψ es un isomorfismo si y sólo si los ideales $I_1, \ldots, I_n$ son comaximales.

Ejercicio 4.28. Para cada uno de los siguientes sistemas de congruencias hallar el conjunto de soluciones y la solución única módulo $n_1.n_2.\ldots.n_k$.

(a) $\begin{cases} x \equiv 1 (\text{mód } 8) \\ x \equiv 2 (\text{mód } 25) \\ x \equiv 3 (\text{mód } 81). \end{cases}$

(b) $\begin{cases} x \equiv 5 (\text{mód } 8) \\ x \equiv 12 (\text{mód } 25) \\ x \equiv 47 (\text{mód } 81). \end{cases}$

Ejercicio 4.29. Utilice algún programa computacional para escribir un programa que realice computacionalmente el algoritmo, descrito en la página 87, para la determinación de las soluciones y de la única solución (bajo cierto módulo) de un sistema de congruencias.

Ideales maximales y primos

Ejercicio 4.30. Considere el anillo $A := 2.\mathbb{Z}$ con las operaciones usuales. Probar que $M := 4.\mathbb{Z}$ es un ideal maximal de A y mostrar que $A/M = \{\overline{0}, \overline{2}\}$ donde $\overline{2}.\overline{2} = \overline{0}$. Esto es, A/M no es un cuerpo. Explique por qué esto no contradice la Proposición 4.5.3.

Ejercicio 4.31. Hallar todos los ideales de $\mathbb{Z}_{24}$ e indicar cuáles de ellos son maximales.

Ejercicio 4.32. Probar que el ideal $\langle X \rangle$ es maximal en $\mathbb{Q}[X]$.

Ejercicio 4.33. Determinar si el ideal $\langle X \rangle$ es primo o no en los anillos $\mathbb{Z}_5[X]$ y $\mathbb{Z}_6[X]$.

Ejercicio 4.34. Sea A un anillo conmutativo con identidad finito. Probar que todo ideal primo de A es maximal.

Ejercicio 4.35. Sean A y B anillos conmutativos con identidad. Sea $f\colon A \to B$ un homomorfismo. Probar que:

(a) Si Q es un ideal primo de B, entonces $f^{-1}(Q) = A$ o $f^{-1}(Q)$ es un ideal primo de A.

(b) Si f es sobreyectiva y M es un ideal maximal de B, entonces $f^{-1}(M)$ es un ideal maximal de A.

Capítulo 5

Dominios

5.1. Dominios de factorización única (DFU)

El dominio de integridad de los números enteros $\mathbb{Z}$ tiene una propiedad muy importante, a saber, el *teorema de factorización única* (o *teorema fundamental de la aritmética*). El cual expresa que todo entero no nulo distinto de ± 1 puede escribirse de manera única, salvo el orden de los factores, como producto de enteros positivos primos. Entonces, una pregunta que surge de manera natural es: ¿existen otros dominios integrales aparte de los enteros en los cuales valga un teorema de factorización única? O de forma más general y abstracta: ¿sobre qué anillos o dominios de integridad podemos enunciar un teorema de factorización única, convenientemente generalizado? Comenzamos con las nociones abstractas de divisibilidad, elemento primo e irreducible en dominios de integridad, las cuales generalizan las nociones usuales de divisibilidad y de número primo en $\mathbb{Z}$.

En esta sección, a menos que se indique otra cosa, **todos los anillos considerados son dominios de integridad.**

Definición 5.1.1. Sea A un dominio de integridad. Sean $a, b \in A$.

- Diremos que a **divide** a b, o que b es un **múltiplo** de a (o también que a es un **divisor** de b) si $b = a.c$ para algún $c \in A$ y lo denotamos por $a \mid b$.
- Diremos que a y b son **asociados** si $a = b.u$ para alguna unidad u de A.

En la siguiente proposición establecemos algunas de las propiedades usuales de la relación divide, análogas a aquellas válidas en $\mathbb{Z}$.

Proposición 5.1.2. *Sea A un dominio de integridad. Para todos $a, b, c \in A$ se tiene:*

(1) *$a \mid a$;*

(2) *si $a \mid b$ y $b \mid c$, entonces $a \mid c$;*

(3) *$a \mid b$ y $b \mid a$ si y sólo si a y b son asociados;*

(4) *si $a \mid b$ y $a \mid c$, entonces $a \mid b.x + c.y$ para todos $x, y \in A$;*

(5) *$a \mid b$ si y sólo si $\langle b\rangle \subseteq \langle a\rangle$;*

(6) *para todo $u \in \mathrm{U}(A)$, $\langle a\rangle = \langle u.a\rangle$.*

Definición 5.1.3. Sea $a \in A$ un elemento no nulo y no invertible. Consideramos las siguientes definiciones:

- a es llamado **irreducible** cuando se cumple que si $a = b.c$, entonces b o c debe ser una unidad;
- a es llamado **primo** cuando se cumple que si $a \mid b.c$, entonces $a \mid b$ o $a \mid c$.

Proposición 5.1.4. *Sea $p \in A$ no nulo. Entonces, p es primo si y sólo si $\langle p\rangle$ es un ideal primo de A.*

Demostración. Supongamos primero que p es un elemento primo. Si $a.b \in \langle p\rangle$, entonces $p \mid a.b$. Como p es primo, tenemos que $p \mid a$ o $p \mid b$, esto es, $a \in \langle p\rangle$ o $b \in \langle p\rangle$. Entonces, $\langle p\rangle$ es un ideal primo. Recíprocamente, supongamos ahora que $\langle p\rangle$ es un ideal primo y probemos que p es un elemento primo. Si $p \mid a.b$, entonces $a.b \in \langle p\rangle$. Luego, $a \in \langle p\rangle$ o $b \in \langle p,\rangle$, esto es, $p \mid a$ o $p \mid b$. Por lo tanto p es primo. ■

Ejemplo 5.1.5. Observemos que en $\mathbb{Z}$, un entero a es primo (la noción usual que conocemos) si cumple la condición de irreducibilidad de la Definición 5.1.3. ¿Entonces por qué lo llamamos "primos" y no "irreducible"? El hecho es que se puede probar que un entero a es irreducible si y sólo si a es primo (según la Definición 5.1.3). Probaremos esto en breve en un contexto más general. ■

Proposición 5.1.6. *Si p es primo, entonces p es irreducible.*

Demostración. Sea p un elemento primo. Supongamos que $p = a.b$. Luego $p \mid ab$ y como p es primo, tenemos que $p \mid a$ o $p \mid b$. Si $p \mid a$, entonces $a = p.c$ para algún $c \in A$. Así $p = pc.b$ y esto implica que $1 = cb$. Con lo cual b es una unidad. Análogamente, si $p \mid b$, entonces a es una unidad. Por lo tanto, p es un elemento irreducible. ■

Vamos a dar un ejemplo de un elemento que es irreducible pero no primo. Consideremos el dominio de integridad $\mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} : \ a, b \in \mathbb{Z}\}$. En $\mathbb{Z}[\sqrt{-3}]$, el 2 es irreducible y no es primo. Para probar que 2 es irreducible deberíamos conocer cuáles son las unidades del dominio $\mathbb{Z}[\sqrt{-3}]$. Esto será completamente resuelto en la Sección 5.4. Aquí es suficiente observar que $1, -1 \in \mathbb{Z}[\sqrt{-3}]$ y son unidades de $\mathbb{Z}[\sqrt{-3}]$. Ahora si probemos que 2 es irreducible. Supongamos que

$$2 = (a + ib\sqrt{3})(c + id\sqrt{3}).$$

Tomando el conjugado complejo nos queda que

$$2 = (a - ib\sqrt{3})(c - id\sqrt{3}).$$

Si multiplicamos las ultimas dos ecuaciones obtenemos que

$$4 = (a^2 + 3b^2)(c^2 + 3d^2).$$

Como los factores del miembro derecho de la ultima igualdad son divisores positivos de 4 y claramente distintos de 2, tenemos que uno de ellos debe ser igual a 4 y el otro igual a 1. Supongamos que $a^2 + 3b^2 = 1$. Entonces, $a = \pm 1$ y $b = 0$. Así, en la factorización de 2 uno de los factores es una unidad. Por lo tanto, 2 es irreducible. Ahora, note que 2 divide a $(1+i\sqrt{3})(1-i\sqrt{3}) = 4$ y 2 no divide a ninguno de los factores[1] y por lo tanto 2 no es primo.

Ahora daremos una definición abstracta del Teorema Fundamental de la Aritmética en $\mathbb{Z}$.

Definición 5.1.7. Un **dominio de factorización única** (DFU) es un dominio de integridad A satisfaciendo las siguientes propiedades:

(DF1) cada elemento no nulo a en A el cual no es una unidad puede ser expresado como $a = u.p_1 \dots p_n$ donde u es una unidad y los p_i son elementos irreducibles de A;

(DF2) si a tiene otra factorización, digamos $a = v.q_1 \dots q_m$, donde v es una unidad y los q_i son irreducibles, entonces $n = m$ y, después de reordenar si fuera necesario, p_i y q_i son asociados.

Lo primero que probamos es que en un dominio de factorización única las nociones de elemento primo e irreducible coinciden.

Proposición 5.1.8. *En un dominio de factorización única, a es irreducible syss a es primo.*

Demostración. Ya sabemos que si a es primo, entonces a es irreducible. Supongamos que a es irreducible y que a divide a bc. Esto es, $bc = ar$ para algún $r \in A$. Factorizamos b, c y r en irreducibles para obtener

$$v.b_1 \dots b_s u.c_1 \dots c_t = aw.r_1 \dots r_m.$$

con u, v, w unidades y b_i, c_j, r_k elementos irreducibles de A. Como a es irreducible y por la unicidad de la factorización (DF2), a debe ser asociado de algún b_i o c_j. Entonces, a divide a b o c. ■

Ejemplo 5.1.9. El primer ejemplo de un dominio de factorización única es el dominio de integridad $\mathbb{Z}$. Ya se ha probado en un curso de álgebra básica que todo entero a que no es unidad ($a \neq 0, \pm 1$) es producto de una unidad (± 1) por enteros primos positivos. ■

En analogía con el dominio de factorización única de los enteros $\mathbb{Z}$ tenemos las siguientes definiciones. Sea A un (DFU) y sean $a, b \in A$. Un elemento $d \in A$ es llamado **máximo común divisor** (mcd) de a y b si verifica las siguientes condiciones:

(I) $d \mid a$ y $d \mid b$;

(II) si $e \mid a$ y $e \mid b$, entonces $e \mid d$.

Observación 5.1.10. Si d y d' son dos mcd de a y b (es decir, d y d' satisfacen las condiciones (I) y (II)), entonces tenemos que $d' \mid d$ y $d \mid d'$, con lo cual d y d' son asociados.

[1]Si 2 divide a $1+i\sqrt{3}$ entonces existe un $a+ib\sqrt{3} \in A$ tal que $1+i\sqrt{3} = 2(a+ib\sqrt{3})$. Por la unicidad de la igualdad, nos queda que $1 = 2a$ donde $a \in \mathbb{Z}$, lo cual es absurdo.

Proposición 5.1.11. *Sea A un* (DFU) *y sean a y b elementos no nulos de A. Si d es un elemento de A tal que $\langle a, b\rangle = \langle d\rangle$, entonces:*

(1) *d se puede escribir como una combinación lineal de a y b, esto es, existen $x, y \in A$ tales que $d = a.x + b.y$;*

(2) *d es un mcd de a y b;*

(3) *d es único salvo multiplicación por una unidad de A.*

Así podemos hablar de *el* máximo común divisor de a y b, cuando este existe, salvo asociados.

Un elemento no nulo m es un **mínimo común múltiplo** (*mcm*) de a y b si cumple con:

(I) $a \mid m$ y $b \mid m$

(II) si $a \mid e$ y $b \mid e$, entonces $m \mid e$.

Máximos común divisores y mínimos común múltiplos siempre existen en un (DFU) y ellos pueden ser determinados de manera similar al caso de los enteros.

Sea A un (DFU). Es común en una factorización asociar los primos (irreducibles) repetidos, en el sentido de asociados. Esto es, los elementos de A tienen representaciones del tipo $u.p_1^{e_1}p_2^{e_2}\dots p_n^{e_n}$ donde los p_i son primos no asociados. También es usual, como en el caso de los números enteros, agregar primos con exponentes cero para obtener representaciones usando los mismos primos. Esto es, si a y b son elementos no nulos de un (DFU) A, entonces por (DF1) tenemos que $a = u.p_1^{e_1}.\dots.p_n^{e_n}$ y $b = v.p_1^{f_1}.\dots.p_n^{f_n}$ para ciertos primos $p_1, \dots, p_n$ con $e_i \geq 0$ y $f_i \geq 0$ para $i = 1, \dots, n$. Luego, la condición de unicidad (DF2) expresa que

$$u.p_1^{e_1}p_2^{e_2}\dots p_n^{e_n} = v.p_1^{f_1}p_2^{f_2}\dots p_n^{f_n} \implies e_i = f_i \ \forall i = 1, \dots, n.$$

Proposición 5.1.12. *Sea A un* (DFU), *$a = u.p_1^{e_1}p_2^{e_2}\dots p_n^{e_n}$ y $b = v.p_1^{f_1}p_2^{f_2}\dots p_n^{f_n}$ con los p_i primos, $e_i, f_i \geq 0$ y $u, v \in \mathrm{U}(A)$. Entonces,*

$$a \mid b \Longleftrightarrow e_i \leq f_i \ \forall i = 1, \dots, n.$$

Demostración. Supongamos primero que $e_i \leq f_i$ para todo $i = 1, \dots, n$. Sea $c = u^{-1}vp_1^{g_1}\dots p_n^{g_n}$ donde $g_i = f_i - e_i \geq 0$. Entonces, $b = ac$ y así $a \mid b$. Recíprocamente, supongamos que $a \mid b$. Entonces, $b = ac$. Por (DF1), $c = wp_1^{g_1}\dots p_n^{g_n}$. Luego,

$$vp_1^{f_1}\dots p_n^{f_n} = uwp_1^{g_1+e_1}\dots p_n^{g_n+e_n}.$$

La unicidad de las descomposiciones muestra que $f_i = g_i + e_i$ para todo $i = 1, \dots, n$. Con lo cual, $e_i \leq f_i$ para todo i. ■

Proposición 5.1.13. *Sea A un* (DFU) *y sean a y b elementos no nulos de A. Sean*

$$a = u.p_1^{e_1}.\dots.p_n^{e_n} \quad y \quad b = v.p_1^{f_1}.\dots.p_n^{f_n}$$

las dos factorizaciones en producto de primos. Entonces el mcd d y el mcm m (salvo asociados) de a y b son dados por:

$$d := p_1^{\alpha_1}.\dots.p_n^{\alpha_n} \quad y \quad m := p_1^{\beta_1}.\dots.p_n^{\beta_n}$$

donde para cada $i = 1, \dots, n$, $\alpha_i := \min\{e_i, f_i\}$ y $\beta_i := \max\{e_i, f_i\}$.

5.2. Dominios de ideales principales (DIP)

Anteriormente, motivamos la definición de DFU por el Teorema Fundamental de la Aritmética en $\mathbb{Z}$. Ahora, recordemos que en el dominio $\mathbb{Z}$, y también en cada $\mathbb{Z}_n$, todos sus ideales son principales. Entonces podemos extraer esta propiedad y realizar la siguiente definición. Luego veremos que que $\mathbb{Z}$ y $\mathbb{Z}_n$ no son los únicos dominios en los cuales todos sus ideales son principales.

Definición 5.2.1. Un **dominio de ideales principales** (DIP) es un dominio de integridad en el cual cada ideal es principal.

Probaremos primero que todo DIP es un DFU. Para ello necesitamos el siguiente teorema, el cual es una caracterización para que un dominio de integridad sea un DFU.

Teorema 5.2.2. *Sea A un dominio de integridad. Entonces:*

(1) *Si A es un* DFU*, entonces A satisface la condición de cadena ascendente* (cca) *sobre ideales principales, esto es, si $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \dots$, entonces existe un n tal que $\langle a_n\rangle = \langle a_{n+1}\rangle = \dots$.*

(2) *Si A satisface la condición de cadena ascendente sobre ideales principales, entonces A satisface* (DF1)*.*

(3) *Si A satisface* (DF1) *y además cada elemento irreducible en A es primo, entonces A es un* (DFU)*.*

Por lo tanto, A es un (DFU) *si y sólo si A satisface la* (cca) *sobre ideales principales y cada elemento irreducible de A es primo.*

Demostración. (1) Si $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \dots$ entonces $a_{i+1} \mid a_i$. Así, por la proposición anterior, los factores primos de a_{i+1} consisten de algunos (o todos) de los factores primos de a_i (teniendo en cuenta la multiplicidad). Ya que a_1 tiene un número finito de factores primos y todos $a_i \mid a_1$, en algún momento los factores primos van a ser siempre los mismos, con los cual $\langle a_n\rangle = \langle a_{n+1}\rangle = \dots$.

(2) Sea a_1 un elemento no nulo de A. Supongamos que a_1 no puede ser factorizado como producto de irreducibles, esto es, (DF1) no se cumple para a_1. En particular a_1 no es irreducible y así $a_1 = a_2.a_2'$ donde a_2 y a_2' no son unidades y no pueden ambos ser factorizados en producto de irreducibles. Supongamos que a_2 no puede ser factorizado en producto de irreducibles. Como $a_2 \mid a_1$, tenemos que $\langle a_1\rangle \subseteq \langle a_2\rangle$ y esta inclusión es propia ya que $a_2 \notin \langle a_1\rangle$ (si $a_2 \in \langle a_1\rangle$, entonces $a_2 = a_1c$; con lo cual, $a_1 = a_2a_2' = a_1ca_2'$ y así $1 = ca_2'$, esto es, a_2' es una unidad, absurdo). Luego, en particular a_2 no es irreducible y así $a_2 = a_3.a_3'$ donde a_3 y a_3' no son unidades y ambos no pueden ser factorizados en producto de irreducibles. Supongamos que a_3 no puede ser factorizado en producto de irreducibles. También tenemos que $\langle a_2\rangle \subseteq \langle a_3\rangle$ y esta inclusión es propia porque $a_3 \notin \langle a_2\rangle$. Como a_3 no puede ser factorizado en producto de irreducibles, tenemos, bajo los mismos argumentos recién usados, que existe un elemento a_4 tal que $\langle a_3\rangle \subset \langle a_4\rangle$. Luego, por un argumento inductivo, obtenemos una cadena estrictamente

creciente $\langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \langle a_4\rangle \ldots$ de ideales principales, lo que contradice la hipótesis. Por lo tanto, a_1 puede ser factorizado como producto de irreducbles, esto es, la condición (DF1) se cumple.

(3) Supongamos que $a = u.p_1 \ldots p_n = v.q_1 \ldots q_m$ donde los p_i y q_j son elementos irreducibles y u, v son unidades. Entonces, p_1 es un divisor primo de $vq_1 \ldots q_m$, y así p_1 divide algún q_j, digamos (reordenando si fuera necesario) que p_1 divide a q_1. Como q_1 es irreducible, p_1 y q_1 son asociados. Luego tenemos, salvo multiplicación por unidades, que

$$p_2 \ldots p_n = q_2 \ldots q_m.$$

Si suponemos que $n < m$ y continuamos con el razonamiento anterior obtendríamos que (salvo multiplicación por unidades)

$$1 = q_{n+1} \ldots q_m.$$

Con lo cual, q_{n+1} es una unidad, lo que es absurdo pues todos los q_j son irreducibles. Entonces, $n \geq m$ y, similarmente $n \leq m$. Entonces, $n = m$ y, después de reordenar, p_i y q_i son asociados para cada i. ■

Teorema 5.2.3. *Cada dominio de ideales principales es un dominio de factorización única.*

Demostración. Sea A un (DIP). Sea $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \ldots$ una cadena ascendente de ideales principales de A. Tomemos $I = \bigcup_{i\geq 1}\langle a_i\rangle$. Luego, I es un ideal de A y entonces, por ser A un (DIP), se sigue que $I = \langle b\rangle$. Como $b \in I$, existe un $n \geq 1$ tal que $b \in \langle a_n\rangle$. Con lo cual,

$$\langle a_i\rangle \subseteq I = \langle b\rangle \subseteq \langle a_n\rangle \subseteq \langle a_i\rangle$$

para todo $i \geq n$. Esto es, $\langle a_n\rangle = \langle a_{n+1}\rangle = \ldots$ y por lo tanto A satisface (cca). Ahora probemos que todo elemento irreducible de A es primo. Sea $a \in A$ un elemento irreducible. Así, el ideal $\langle a\rangle$ es propio (pues, si $\langle a\rangle = A$ entonces $1 \in \langle a\rangle$ y lo que implicaría que a es una unidad, lo que no puede ser porque a es irreducible). Por la Proposición 4.5.2, sabemos que existe un ideal máximal I tal que $\langle a\rangle \subseteq I$. Como A es (DIP), $I = \langle b\rangle$ para algún $b \in A$. Luego, $a \in \langle b\rangle$. Como a es irreducible y b no es una unidad (pues el ideal $\langle b\rangle$ es propio), a y b son asociados. Lo que implica $\langle a\rangle = \langle b\rangle = I$. Como I es maximal, tenemos que I es un ideal primo y entonces $\langle a\rangle$ es un ideal primo. Luego, a es un elemento primo de A. Por lo tanto, del Teorema 5.2.2, podemos concluir que A es (DFU). ■

Ejemplo 5.2.4. En el Ejemplo 4.1.16 hemos probado que en el dominio de integridad $\mathbb{Z}$, todo ideal es principal. Por lo tanto, $\mathbb{Z}$ es un dominio de ideales principales, y así es un dominio de factorización única. Además, como en un DFU los elementos primos coinciden con los irreducible, entonces hemos probado que en $\mathbb{Z}$ todo entero distinto de 0, 1 y -1 (las únicas unidades de $\mathbb{Z}$) se puede expresar de forma única como producto enteros primos. Por lo tanto, hemos probado el Teorema Fundamental de la Aritmética. ■

Proposición 5.2.5. *Sea A un dominio de ideales principales y sea $a \in A$. Entonces, a es irreducible si y sólo si el ideal $\langle a\rangle$ es maximal.*

Demostración. Supongamos que a es un elemento irreducible. Sea I un ideal de A tal que $\langle a\rangle \subseteq I$. Si $I = A$ no hay nada que probar. Supongamos que I es propio, esto es, $I \neq A$. Como A es un (DIP), $I = \langle b\rangle$ para algún $b \in A$ y, ya que I es propio, b no es una unidad. Luego, $b \mid a$. Así, $a = bc$. Como a es irreducible y b no es unidad, tenemos que c es una unidad. Con lo cual, a y b son asociados. Por lo tanto $\langle a\rangle = \langle b\rangle = I$. Hemos probado que $\langle a\rangle$ es maximal.

Reíprocamente, asumamos que $\langle a\rangle$ es maximal. Entonces, por el Corolario 4.5.8, el ideal $\langle a\rangle$ es primo. Luego, a es un elemento primo de A y por lo tanto a es irreducible. ■

Teorema 5.2.6. *Si A es un* (DIP)*, cada ideal primo no nulo de A es maximal.*

Demostración. Sea $I = \langle a\rangle$ un ideal primo no nulo de A. Entonces a es un elemento primo de A, así es irreducible. Entonces $I = \langle a\rangle$ es máximal. ■

Ejemplo 5.2.7.

(1) En el Ejemplo 4.1.16 (2) vimos que el ideal $\langle 2, X\rangle$ de $\mathbb{Z}[X]$ no es principal. Entonces el dominio de integridad $\mathbb{Z}[X]$ no es un (DIP). En la Sección 5.6 veremos que si A es un (DFU), entonces $A[X]$ es un (DFU). Así, tenemos que $\mathbb{Z}[X]$ es un (DFU). Luego, vemos que no todo (DFU) es un (DIP). Además, ya que $\mathbb{Z}$ es un (DIP), vemos también que si A es un (DIP), entonces no necesariamente $A[X]$ es un (DIP).

(2) El subanillo $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} :\ a, b \in \mathbb{Z}\} = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$ de $\mathbb{C}$ es un dominio de integridad, ya que $\mathbb{C}$ es un cuerpo. Afirmamos que los elementos 2, 3, $1 + \sqrt{5}i$ y $1 - \sqrt{5}i$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$ (ver la Sección 5.4 para probarlo). Ahora observe que

$$6 = 2.3 = (1 + \sqrt{5}i).(1 - \sqrt{5}i).$$

Esto es, el elemento $6 \in \mathbb{Z}[\sqrt{-5}]$ tiene dos factorizaciones diferentes en productos de elementos irreducibles, lo que muestra que la condición (DF2) no se cumple. Entonces $\mathbb{Z}[\sqrt{-5}]$ no es un (DFU). ■

5.3. Los enteros de Gauss

En esta sección estudiaremos un anillo particular que es importante en Teoría de números y el cual nos servirá como motivación para introducir algunas nociones en las secciones siguientes.

Consideremos el conjunto $\mathbb{Z}[i] = \{a + bi :\ a, b \in \mathbb{Z}\}$ con las operaciones de suma y multiplicación usuales de números complejos. Es claro que ellas son cerradas en $\mathbb{Z}[i]$ y una simple verificación muestra que $\mathbb{Z}[i]$ es un subanillo de $\mathbb{C}$ y por lo tanto es un dominio de integridad. Pero $\mathbb{Z}[i]$ no llega a ser un cuerpo porque no todo elemento de $\mathbb{Z}[i]$ tiene un inverso. En efecto, sea $a \in \mathbb{Z}$ tal que $a \neq \pm 1$. Así $a \in \mathbb{Z}[i]$ pero $1/a \notin \mathbb{Z}[i]$, pues si $1/a = x + yi$ con $x, y \in \mathbb{Z}$ tendríamos que $1/a = x \in \mathbb{Z}$, lo cual es una contradicción. Los elemento de $\mathbb{Z}[i]$ son llamados los **enteros de Gauss** y el anillo $\mathbb{Z}[i]$ es denominado como el **anillo de los enteros de Gauss**. Observe que $\mathbb{Z}$ es un subanillo de $\mathbb{Z}[i]$.

Observemos que para todo $\alpha = a + bi \in \mathbb{Z}[i]$, podemos considerar su conjugado complejo $\overline{\alpha} = a - bi \in \mathbb{Z}[i]$. Al igual que en $\mathbb{C}$, también podemos considerar la **norma** $\mathrm{N}\colon \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ definida por $\mathrm{N}(\alpha) = a^2 + b^2$ para cada $\alpha = a + bi \in \mathbb{Z}[i]$. No es difícil comprobar que para todo $\alpha, \beta \in \mathbb{Z}[i]$, $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ and $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

Proposición 5.3.1. *Sea $\alpha \in \mathbb{Z}[i]$. Entonces, α es invertible si y sólo si $\mathrm{N}(\alpha) = 1$. Por lo tanto, $\mathrm{U}(\mathbb{Z}[i]) = \{1, i, -1, -i\}$.*

Demostración. Primero supongamos que α es invertible en $\mathbb{Z}[i]$. Entonces, existe $\beta \in \mathbb{Z}[i]$ tal que $\alpha\beta = 1$. Luego, $1 = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ y dado que $\mathrm{N}(\alpha), \mathrm{N}(\beta) \in \mathbb{N}$ obtenemos que $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 1$. Recíprocamente, supongamos que $\mathrm{N}(\alpha) = 1$. Entonces, $1 = \mathrm{N}(\alpha) = \alpha\overline{\alpha}$. Luego, como $\overline{\alpha} \in \mathbb{Z}[i]$, se sigue que $\overline{\alpha}$ es el inverso de α. Para probar la ultima afirmación observemos que $\alpha = a+bi \in \mathbb{Z}[i]$ es una unidad si y sólo si $a^2+b^2 = 1$. Entonces, α es invertible si y sólo si ($a^2 = 1$ y $b = 0$) o ($a = 0$ y $b^2 = 1$). Por lo tanto, $\mathrm{U}(\mathbb{Z}[i]) = \{1, i, -1, -i\}$. ■

Proposición 5.3.2. *Sean $\alpha, \beta \in \mathbb{Z}[i]$ con $\alpha \neq 0$. Entonces, existen $\mu, \rho \in \mathbb{Z}[i]$ tal que $\beta = \mu\alpha+\rho$ con $\mathrm{N}(\rho) < \mathrm{N}(\alpha)$.*

Demostración. Dado que $\alpha \neq 0$ podemos considerar el cociente β/α en $\mathbb{C}$. Una simple computación muestra que $\beta/\alpha = r + si$ con $r, s \in \mathbb{Q}$. Luego, existen números enteros x e y tales que $|x - r| \leq 1/2$ y $|y - s| \leq 1/2$. Tomemos $\mu = x + yi$ y $\rho = (\beta/\alpha - \mu)\alpha$. Es claro que μ y ρ son enteros de Gauss y $\beta = \mu\alpha+\rho$. Notemos que $\mathrm{N}(\beta/\alpha-\mu) = (r-x)^2+(s-y)^2 \leq 1/4+1/4 = 1/2$. Entonces, $\mathrm{N}(\rho) = \mathrm{N}((\beta/\alpha - \mu)\alpha) = \mathrm{N}(\beta/\alpha - \mu)\mathrm{N}(\alpha) \leq 1/2\mathrm{N}(\alpha) < \mathrm{N}(\alpha)$. ■

Observación 5.3.3.

(1) Podemos observar que la Proposición anterior nos afirma de la existencia de una "**división Euclidiana**" en $\mathbb{Z}[i]$ similar a la división Euclidiana en $\mathbb{Z}$ donde μ es un **cociente** y ρ es un **resto** de dividir β por α. Pero tiene un desventaja notable: los enteros de Gauss μ y ρ en la Proposición anterior no son necesariamente únicos (esto se puede notar en la demostración de la proposición cuando elegimos los enteros x e y).

(2) También observemos que en la prueba de la proposición anterior no sólo hemos demostrado la existencia de un cociente y un resto, μ y ρ, respectivamente, sino que también obtuvimos un algoritmo para encontrarlos.

Ejemplo 5.3.4. Determinemos en $\mathbb{Z}[i]$ el cociente y resto de dividir $\beta = 5 - 2i$ por $\alpha = 1 + 3i$. Como

$$\frac{5-2i}{1+3i} = -\frac{1}{10} - \frac{17}{10}i,$$

los enteros x e y que están a una distancia menor o igual que $1/2$ de $-1/10$ y $-17/10$, respectivamente, son $x = 0$ e $y = -2$. Así, tomamos $\mu = -2i$ y

$$\rho = \beta - \mu\alpha = (5 - 2i) - (-2i)(1 + 3i) = -1.$$

Por lo tanto, un cociente es $\mu = 2i$ y un resto es $\rho = -1$. ■

La siguiente proposición nos da un criterio para determinar algunos elementos irreducibles en $\mathbb{Z}[i]$. Cabe mencionar que en teoría de números, a los elementos irreducibles en $\mathbb{Z}[i]$ se llaman **primos gaussianos**. En la Sección 5.5 veremos que de hecho $\mathbb{Z}[i]$ es un DIP, por lo tanto, los elementos irreducibles y primos coinciden.

Proposición 5.3.5. *Sea $\alpha \in \mathbb{Z}[i]$. Si la norma de α es un entero primo, entonces α es irreducible.*

Demostración. Sea $\alpha \in \mathbb{Z}[i]$ tal que $\mathrm{N}(\alpha) = p$ entero positivo primo. Supongamos que $\alpha = \beta\mu$. Entonces, $p = \mathrm{N}(\alpha) = \mathrm{N}(\beta)\mathrm{N}(\mu)$. Entonces, como p es primo, $\mathrm{N}(\beta) = 1$ o $\mathrm{N}(\mu) = 1$. Con lo cual, β o μ es una unidad. Por lo tanto, α es irreducible. ■

Ejemplo 5.3.6. El entero gaussiano $1 + i$ es irreducible, pues su norma $\mathrm{N}(1 + i) = 2$ es un entero primo. ■

La recíproca de la proposición anterior no vale. Esto es, existen elementos irreducibles cuyas normas no son un entero primo. En el siguiente ejemplo mostramos que 3 es un elemento irreducible de $\mathbb{Z}[i]$ cuya norma es $\mathrm{N}(3) = 9$ que no es un entero primo.

Ejemplo 5.3.7. El entero primo 3 es irreducible en $\mathbb{Z}[i]$. En efecto, supongamos que $3 = \alpha\beta$. Luego, $9 = \mathrm{N}(3) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. Con lo cual, tenemos que $\mathrm{N}(\alpha) = 1$, 3 o 9 (podríamos concluir lo mismo para $\mathrm{N}(\beta)$). Si $\mathrm{N}(\alpha) = 1$ entonces α es una unidad. Si $\mathrm{N}(\alpha) = 9$, entonces β es una unidad. Y si $\mathrm{N}(\alpha) = 3$ y $\alpha = a + bi$, obtenemos que $a^2 + b^2 = 3$, lo cual es imposible en $\mathbb{Z}$. Entonces, 3 no tiene otros divisores que las unidades y sus asociados. Que el entero primo 3 sea irreducible en $\mathbb{Z}[i]$ podría llevarnos a pensar que todo entero primo (en $\mathbb{Z}$) es irreducible en $\mathbb{Z}[i]$, lo cual rápidamente vemos que no es verdad. El 2 es un entero primo pero no irreducible en $\mathbb{Z}[i]$, pues $2 = (1 + i)(1 - i)$, y $1 + i$ y $1 - i$ no son unidades en $\mathbb{Z}[i]$. ■

Proposición 5.3.8. *Todo entero primo p tal que $p \equiv -1 (\text{mód } 4)$ es irreducible en $\mathbb{Z}[i]$.*

Demostración. Supongamos que $p = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[i]$. Luego, $p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. Entonces, $\mathrm{N}(\alpha) = 1$, p o p^2 (también $\mathrm{N}(\beta) = 1$, p o p^2). Supongamos que $\mathrm{N}(\alpha) = p$ y $\alpha = a + bi$. Entonces $a^2 + b^2 = p$. Reduciendo la igualdad anterior módulo 4 (es decir, utilizando el homomorfismo $\mathbb{Z} \to \mathbb{Z}_4$) tendríamos $\overline{3} = \overline{a}^2 + \overline{b}^2$. Lo cual es imposible, ya que los únicos cuadrados de $\mathbb{Z}_4$ son $\overline{0} = \overline{0}^2 = \overline{2}^2$ y $\overline{1} = \overline{1}^2 = \overline{3}^2$. Tenemos entonces que $\mathrm{N}(\alpha) = 1$ (y $\mathrm{N}(\beta) = p^2$) o $\mathrm{N}(\beta) = 1$ (y $\mathrm{N}(\alpha) = p^2$). Con lo cual, α o β es una unidad. Por lo tanto, los únicos divisores posibles de p en $\mathbb{Z}[i]$ son las unidades y sus asociados. En consecuencia, p es irreducible en $\mathbb{Z}[i]$. ■

Los siguientes resultados, consecuencia de la división euclidiana, sobre el dominio de integridad $\mathbb{Z}[i]$ son análogos a los correspondientes en $\mathbb{Z}$.

Proposición 5.3.9. *Sean α y β enteros de Gauss no ambos nulos. Entonces, existe un entero δ de $\mathbb{Z}[i]$ con las siguientes propiedades:*

(1) *$\delta \mid \alpha$ y $\delta \mid \beta$;*

(2) *si* δ' *es un entero de Gauss tal que* $\delta' \mid \alpha$ *y* $\delta' \mid \beta$*, entonces* $\delta' \mid \delta$*;*

(3) *existen* $\kappa, \nu \in \mathbb{Z}[i]$ *tal que* $\delta = \kappa\alpha + \nu\beta$*.*

Cualesquiera dos enteros de Gauss teniendo las propiedades (1) *y* (2) *son asociados.*

Cualquier entero de Guass δ con las propiedades (1) y (2) anteriores es llamado un **máximo común divisor** ((mcd) para abreviar) de α y β, en cuyo caso escribimos $(\alpha, \beta) = \delta$

Demostración. La prueba de la existencia de un entero de Gauss que cumpla las condiciones (1)-(3) es análoga al caso de $\mathbb{Z}$ usando el algoritmo Euclidiano[2]. La ultima afirmación es consecuencia del hecho que si δ_1 y δ_2 son (mcd) de α y β, entonces $\delta_1 \mid \delta_2$ and $\delta_2 \mid \delta_1$. Con lo cual, δ_1 y δ_2 son asociados. ■

Proposición 5.3.10. *Si* $\alpha \mid \beta\gamma$ *y* $(\alpha, \beta) = 1$*, entonces* $\alpha \mid \gamma$*.*

Demostración. Ya que $(\alpha, \beta) = 1$, tenemos por la proposición anterior que existen $\kappa, \nu \in \mathbb{Z}[i]$ tales que $1 = \kappa\alpha + \nu\beta$. Luego, $\gamma = \gamma\kappa\alpha + \gamma\nu\beta$. Como α divide a $\kappa\alpha$ y a $\gamma\beta$, obtenemos que α divide al miembro derecho de la ultima igualdad y por lo tanto, $\alpha \mid \gamma$. ■

Proposición 5.3.11. *Sean* $\rho, \rho_1, \ldots, \rho_n \in \mathbb{Z}[i]$ *irreducibles tales que* $\rho \mid \rho_1 \ldots \rho_n$*. Entonces,* ρ *es asociado de* ρ_i *para algún* $i \in \{1, 2, \ldots, n\}$*.*

Demostración. Supongamos que $\rho \mid \rho_1 \ldots \rho_n$ y ρ es distinto de $\rho_1, \ldots, \rho_{n-1}$ y de todos sus asociados. Luego, como $\rho, \rho_1, \ldots, \rho_{n-1}$ son irreducibles distintos, tenemos que $(\rho, \rho_i) = 1$ para todo $i \in \{1, 2, \ldots, n-1\}$ y entonces $(\rho, \rho_1 \ldots \rho_{n-1}) = 1$. En consecuencia, de la proposición anterior obtenemos que $\rho \mid \rho_n$. Por lo tanto, ya que ρ_n es irreducible, ρ y ρ_n son asociados. ■

Teorema 5.3.12 (Teorema de Factorización Única en $\mathbb{Z}[i]$)**.** *Cada entero de Gauss* α *tal que* $\mathrm{N}(\alpha) > 1$ *puede ser representado como un producto de elementos irreducibles. Esta representación es única salvo el orden de los factores y la presencia de unidades.*

Demostración. Tenemos que probar dos cosas: la existencia y la unicidad de una tal representación. Probamos primero la existencia. Usaremos inducción sobre $\mathrm{N}(\alpha)$. Si $\mathrm{N}(\alpha) = 2$, entonces α es $1 + i$, $1 - i$, $-1 + i$ o $-1 - i$, los cuatro posibles enteros de Gauss de norma 2. El entero de Gauss $1 + i$ es irreducible (como vimos en el Ejemplo 5.3.7) y los restantes tres enteros de Gauss son asociados de $1 + i$, entonces todos ellos son irreducibles. Ahora supongamos que α es un entero de Gauss tal que todo otro entero de Gauss β tal que $\mathrm{N}(\beta) < \mathrm{N}(\alpha)$ tiene una representación en producto de elementos irreducibles. Si α es un elemento irreducible, ya tenemos la representación. Supongamos que α no es irreducible. Entonces, $\alpha = \beta\gamma$ con β y γ no unidades y no asociados a α. Con lo cual, se tiene que $1 < \mathrm{N}(\beta) < \mathrm{N}(\alpha)$ y $1 < \mathrm{N}(\gamma) < N(\alpha)$. Por la hipótesis inductiva tenemos que

$$\beta = \rho_1 \ldots \rho_n \quad \text{y} \quad \gamma = \rho'_1 \ldots \rho'_m$$

[2]También puede el lector ver el Teorema 5.5.7 en un contexto más general.

con los ρ_i y ρ'_j irreducibles. Por lo tanto,

$$\alpha = \beta\gamma = \rho_1 \dots \rho_n \rho'_1 \dots \rho'_m.$$

Solo nos resta probar la unicidad. Supongamos que α tiene dos tales representaciones, esto es,

$$\alpha = \rho_1 \dots \rho_n = \rho'_1 \dots \rho'_m.$$

Entonces, $\rho_1 \mid \rho'_1 \dots \rho'_m$ y con lo cual, por la proposición anterior, obtenemos que ρ_1 es asociado de algún irreducible $\rho'_1, \dots, \rho'_m$. Sin perdida de generalidad (reordenando si fuera necesario) podemos suponer que ρ_1 y ρ'_1 son asociados. Así,

$$\rho_1 \dots \rho_n = \sigma\rho_1 \dots \rho'_m$$

con σ una unidad. Entonces, $\rho_2 \dots \rho_n = \sigma\rho'_2 \dots \rho'_m$. Este argumento puede ser repetido de la misma manera. Si $n < m$, obtendríamos que $1 = \sigma'\rho'_{m-n} \cdots \rho'_m$, lo cual es imposible (análogamente si suponemos que $m < n$). Entonces, $n = m$ y, ρ_i y ρ'_i son asociados. Por lo tanto, la representación es única salvo el orden de los factores y la presencia de unidades. ∎

Corolario 5.3.13. *$\mathbb{Z}[i]$ es un DFU.*

Ejemplo 5.3.14. Determinemos la factorización de $\alpha = 4 - 6i$. Primero $\mathrm{N}(\alpha) = 52 = 2 \cdot 2 \cdot 13$. Ahora tratamos de encontrar dos enteros de Gauss β y γ tales que $\mathrm{N}(\beta) = 2$ y $\mathrm{N}(\gamma) = 13$. En estas condiciones, por la Proposición 5.3.5, nos aseguramos que β y γ sean irreducibles. Para β podemos elegir por ejemplo $\beta = 1 + i$ (y sus asociados). Y para γ podemos elegir por ejemplo $\gamma = 3 + 2i$. Utilizando un asociado de β, por ejemplo $-1 + i$, hacemos:

$$(1 + i)(-1 + i)(3 + 2i) = -6 - 4i.$$

Multiplicamos ambos lados por i

$$(1 + i)(-1 - i)(3 + 2i) = 4 - 6i.$$

Por la unicidad, esta es la representación de $\alpha = 4 - 6i$ en producto de irreducibles. ∎

Todo entero primo distinto de 2 es de la forma $4k+1$ o $4k-1$ (¿por qué?). Hemos visto en la Proposición 5.3.8 que todo entero primo de la forma $4k - 1$ es también un elemento irreducible de $\mathbb{Z}[i]$. Nos resta ver que pasa con el resto de enteros primos, es decir, los enteros primos de la forma $4k + 1$.

Proposición 5.3.15. *Cada entero primo p tal que $p \equiv 1(\text{mód } 4)$ es producto en $\mathbb{Z}[i]$ de dos enteros de Gauss irreducibles no-asociados.*

Demostración. Sea p un entero primo tal que $p \equiv 1(\text{mód } 4)$. Esto es, $p - 1 = 4k$, para algún entero k. Entonces, podemos afirmar que -1 es un residuo cuadrático[3] de p (Ver [11, pag. 59]),

[3] Un entero a es llamado un *residuo cuadrático* de p si existe un entero x tal que $x^2 \equiv a(\text{mod } p)$.
Criterio de Euler: Un entero a es un residuo cuadrático de un primo impar p si y sólo si se cumple que $a^{(p-1)/2} \equiv 1(\text{mod } p)$. (Ver [**?**, pag. 59])

esto es, tenemos que existe un entero x tal que $x^2 \equiv -1(\text{mód } p)$. Así $p \mid (x^2+1)$. Ahora, en $\mathbb{Z}[i]$ tenemos que $x^2+1=(x+i)(x-i)$. Si p fuera un primo en $\mathbb{Z}[i]$ tendríamos que p divide a uno de los factores $x+i$ o $x-i$, lo cual implicaría que $p \mid 1$ o $p \mid -1$ lo que es imposible. Por lo tanto, p no es un elemento irreducible en $\mathbb{Z}[i]$ y entonces, por el Teorema 5.3.12, se puede poner como el producto de dos factores que no son unidades.

Supongamos que $p=\alpha\beta$ con α y β que no son unidades. Luego tenemos que $p^2=\mathrm{N}(\alpha)\mathrm{N}(\beta)$ y, como α y β no son unidades, obtenemos que $\mathrm{N}(\alpha)=\mathrm{N}(\beta)=p$. Entonces, $\alpha\overline{\alpha}=p=\beta\overline{\beta}$. Así,

$$p=\alpha\beta=\alpha\overline{\alpha}$$

lo que implica que $\beta=\overline{\alpha}$. Si α no fuera primo tendríamos que $\alpha=\rho_1\ldots\rho_n$ con $n>1$ y entonces $p=\mathrm{N}(\alpha)=\mathrm{N}(\rho_1)\ldots\mathrm{N}(\rho_n)$, lo cual es claramente imposible ya que p es primo. Concluimos que α es primo. Similarmente, β es primo. Resumiendo, tenemos que $p=\alpha\overline{\alpha}$ con α y $\overline{\alpha}$ primos de $\mathbb{Z}[i]$. Solo nos resta verificar que ellos no son asociados. Supongamos que $\alpha=a+bi$ y que $\alpha=u\overline{\alpha}$ con $u\in\{1,i,-1,-i\}$. Si analizamos el caso $u=i$, tenemos que $a+bi=i(a-bi)=b+ai$, con lo cual $a=b$. Entonces, $p=a^2+a^2=2a^2$ y esto es una contradicción. De la misma manera analizando los otros casos llegamos igualmente a una contradicción. Por lo tanto, α y $\overline{\alpha}$ no son asociados. ■

Por la Proposición 5.3.8 podemos concluir que todo entero primo $p\equiv -1(\text{ mód } 4)$ no puede escribirse como la suma de dos cuadrados. En efecto, si $p=a^2+b^2=(a+bi)(a-bi)$ entonces, ya que p es un elemento irreducible en $\mathbb{Z}[i]$, $\mathrm{N}(a+bi)=1$ o $\mathrm{N}(a-bi)=1$. Esto implica que $p=1$. Ahora si p es un entero primo tal que $p\equiv 1(\text{ mód } 4)$, tenemos por la proposición anterior que $p=\alpha\overline{\alpha}=a^2+b^2$. Este es un resultado importante de Teoría de Número:

Teorema 5.3.16. *Cada primo p de la forma $4k+1$ puede ser expresado como la suma de dos cuadrados, $p=a^2+b^2$, y esta representación es única salvo el orden y signo de a y b.*

5.4. Extensiones cuadráticas

En esta sección presentamos una generalización de los enteros de Gauss introducidos en la sección anterior. Los dominios de integridad estudiados en esta sección son también de fundamental importancia en la teoría de números.

Sea d un número entero no nulo. Consideremos $\sqrt{d}\in\mathbb{C}$ que es una raíz cuadrada de d. Definimos el conjunto

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

Un simple calculo permite demostrar que $\mathbb{Z}[\sqrt{d}]$ es un subanillo de $\mathbb{C}$ (con unidad). Entonces, en particular, $\mathbb{Z}[\sqrt{d}]$ es un dominio de integridad y es llamado **dominio cuadrático**. Observe que si $d>0$, entonces $\mathbb{Z}[\sqrt{d}]\subseteq\mathbb{R}$ y si $d<0$, entonces $\mathbb{Z}[\sqrt{d}]\subseteq\mathbb{C}$ y $\mathbb{Z}[\sqrt{d}]\nsubseteq\mathbb{R}$.

Sea $d\in\mathbb{Z}$ un cuadrado, esto es, $d=a^2$ para algún $a\in\mathbb{Z}$. Luego, no necesariamente se cumple que si $a+b\sqrt{d}=x+y\sqrt{d}$, entonces $a=x$ y $b=y$. Por ejemplo, $2+2\sqrt{4}=4+1.\sqrt{4}$. Necesitamos evitar estos casos, para obtener unicidad en la representación de los números en $\mathbb{Z}[\sqrt{d}]$.

Proposición 5.4.1. *Sea $d \in \mathbb{Z}$ que no es un cuadrado. Si $a + b\sqrt{d} = x + y\sqrt{d}$, entonces $a = x$ y $b = y$.*

Demostración. Es suficiente con probar que $a + b\sqrt{d} = 0$ implica que $a = b = 0$. Observe que se cumple que: $a = 0$ si y sólo si $b = 0$. Luego, suponemos por absurdo que $a \neq 0$ y $b \neq 0$. Podemos suponer sin perdida de generalidad que a y b son relativamente primos (si no lo son, podemos dividir $a + b\sqrt{d}$ por el $mcd(a, b)$). Ahora, tenemos que $a^2 = b^2 d$. Como $mcd(a, b) = 1$, esto implica que a^2 divide a d[4]. Entonces $d = a^2.q$ para un $q \in \mathbb{Z}$. Así $a^2 = b^2.d = b^2 a^2.q$ y simplificando obtenemos que $1 = b^2.q$. Esto implica que $q = b^2 = 1$. Luego $a^2 = d$. Pero esto es absurdo, pues d no es un cuadrado. Por lo tanto obtenemos que $a = b = 0$. ■

En consecuencia, en lo que queda de sección se asumirá siempre que <u>d no es un cuadrado</u>. Ahora podemos definir la siguiente función $\sigma\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ como

$$\sigma(a + b\sqrt{b}) = a - b\sqrt{d}.$$

Es inmediato verificar que la función σ es un isomorfismo de anillos. Además, si $d < 0$ entonces σ es el conjugado usual de números complejos.

Ahora vamos a definir lo que sería la **norma** en $\mathbb{Z}[\sqrt{d}]$. Definimos la función $\mathrm{N}\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ por

$$\mathrm{N}(z) = z.\sigma(z) = a^2 - db^2$$

para todo $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Veamos ahora algunas propiedades básicas de la norma N.

Proposición 5.4.2. *Las siguientes propiedades se cumplen para todo $z \in \mathbb{Z}[\sqrt{d}]$ y $a \in \mathbb{Z}$:*

1. $\mathrm{N}(z) = 0$ *si y sólo si* $z = 0$;
2. $\mathrm{N}(1) = 1$;
3. $\mathrm{N}(z.w) = \mathrm{N}(z).\mathrm{N}(w)$;
4. $\mathrm{N}(a.z) = a^2.\mathrm{N}(z)$.

Demostración. Las propiedades se deducen del hecho que σ es un autoisomorfismo. ■

Observemos que si $d < 0$, entonces $\mathrm{N}(z) \geq 0$ para todo $z \in \mathbb{Z}[\sqrt{d}]$ y así N tiene una propiedad importante que debería tener una norma.

Veamos ahora, igual que en la Proposición 5.3.1, como podemos caracterizar las unidades de $\mathbb{Z}[\sqrt{d}]$.

Proposición 5.4.3. *Sea $z \in \mathbb{Z}[\sqrt{d}]$. Entonces, z es una unidad si y sólo si* $\mathrm{N}(z) = \pm 1$.

Demostración. Supongamos que $\mathrm{N}(z) = \pm 1$. Luego, $z.\sigma(z) = \pm 1$, y así z es una unidad. Recíprocamente, supongamos que z es una unidad, esto es, $z.w = 1$ para un $w \in \mathbb{Z}[\sqrt{d}]$. Luego, $1 = \mathrm{N}(1) = \mathrm{N}(z.w) = \mathrm{N}(z).\mathrm{N}(w)$. Entonces $\mathrm{N}(z) = \pm 1$. ■

[4] Escribamos $a = p_1^{\alpha_1}.\ldots.p_n^{\alpha_n}$, $b = q_1^{\beta_1}.\ldots.\beta_m^{\beta_m}$ y $d = p_1^{\gamma_1}.\ldots.p_n^{\gamma_n}.q_1^{\delta_1}.\ldots.q_m^{\delta_m}$. Entonces, como $a^2 = b^2.d$ y la factorización en primos es única obtenemos que $\delta_i = \beta_i$ para todo $i = 1, \ldots, m$

Ejemplo 5.4.4. Ya hemos visto que las unidades en $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ son ± 1 y $\pm i$. Supongamos ahora que $d < -1$. Sea $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ invertible. Entonces $1 = a^2 - d.b^2 = a^2 + |d|.b^2$. Así, necesariamente tenemos que $b = 0$ y entonces $a = \pm 1$. Por lo tanto, si $d < -1$, entonces las unidades de $\mathbb{Z}[\sqrt{d}]$ son 1 y -1. Un problema diferente es la obtención de los elementos invertibles de $\mathbb{Z}[\sqrt{d}]$ cuando $d > 0$. Este caso esta fuera de los alcances de estos apuntes. El lector interesado puede consultar [11, pag. 106]. ■

Ejemplo 5.4.5. Probemos que $1 + \sqrt{5}i$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$. Por el ejemplo anterior sabemos que las únicas unidades de $\mathbb{Z}[\sqrt{-5}]$ son 1 y -1. Supongamos que $1 + \sqrt{5}i = \alpha\beta$. Entonces $6 = \mathrm{N}(1 + \sqrt{5}i) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. Entonces $\mathrm{N}(\alpha) = 1$, 2, 3 o 6. Si $\mathrm{N}(\alpha) = 1$, entonces α es una unidad. Supongamos que $\mathrm{N}(\alpha) = 2$ o 3. Si $\alpha = a + b\sqrt{5}i$, entonces $2 = a^2 + 5b^2$ o $3 = a^2 + 5b^2$. Lo cual es, en ambos casos, absurdo. Finalmente, si $\mathrm{N}(\alpha) = 6$, entonces $\mathrm{N}(\beta) = 1$. Así β es una unidad. Entonces tenemos que α es unidad o β es unidad. Por lo tanto, $1 + \sqrt{5}i$ es irreducible en $\mathbb{Z}[\sqrt{-5}]$. ■

En el Ejemplo 5.4.4 mencionamos que no es tarea sencilla determinar las unidades de los dominios $\mathbb{Z}[\sqrt{d}]$ cuando $d > 0$. Con lo cual, tampoco es sencillo determinar si un elemento dado es o no irreducible en $\mathbb{Z}[\sqrt{d}]$ con $d > 0$. El siguiente ejemplo muestra una estrategia útil.

Ejemplo 5.4.6. Probemos que 5 es irreducible en $\mathbb{Z}[\sqrt{3}]$. Supongamos que no lo es. Entonces, existen $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ que no son unidades y tal que $5 = \alpha\beta$. Entonces $25 = \mathrm{N}(5) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. Con lo cual tenemos que $\mathrm{N}(\alpha) = \pm 1, \pm 5, \pm 25$ e igual para $\mathrm{N}(\beta)$. Ahora, como α ni β son unidades, tenemos por la Proposición 5.4.3 que $\mathrm{N}(\alpha) = \pm 5$. Luego, si $\alpha = a + b\sqrt{3}$, entonces $\pm 5 = a^2 - 3b^2$. Ahora reduciendo esta ecuación módulo 3, llegamos $\overline{2} = \overline{a}^2$. La cual no es resoluble en $\mathbb{Z}_3$, es decir, no existe $x \in \mathbb{Z}_3$ tal que $\overline{2} = x^2$. Con lo cual, llegamos a un absurdo. Por lo tanto, 5 es irreducible en $\mathbb{Z}[\sqrt{3}]$. ■

Como ya hemos visto, en los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ existe una división euclideana. Veremos otro ejemplo de un dominio cuadrático en el cual existe una división ecuclideana[5] (Proposición 5.4.7). Pero no es verdad que en todo dominio cuadrático $\mathbb{Z}[\sqrt{d}]$ existe una división euclideana, véase el Ejemplo 5.5.5.

Proposición 5.4.7. *Sean $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ tal que $\alpha \neq 0$. Entonces, existen $\mu, \rho \in \mathbb{Z}[\sqrt{-2}]$ tales que $\beta = \mu.\alpha + \rho$ y $\mathrm{N}(\rho) < \mathrm{N}(\alpha)$.*

Demostración. La demostración sigue el mismo argumento que en la demostración de la Proposición 5.3.2. Dado que $\alpha \neq 0$, podemos considerar el cociente β/α en $\mathbb{C}$. Un simple calculo muestra que $\beta/\alpha = r + s\sqrt{2}i$ con $r, s \in \mathbb{Q}$. Podemos elegir números enteros x e y tales que $|x - r| \leq 1/2$ y $|y - s| \leq 1/2$. Tomemos ahora $\mu = x + yi$ y $\rho = (\beta/\alpha - \mu)\alpha$. Notemos que $\mathrm{N}(\beta/\alpha - \mu) = (r - x)^2 + 2(s - y)^2 \leq 1/4 + 2.1/4 = 3/4 < 1$. Entonces, $\mathrm{N}(\rho) = \mathrm{N}((\beta/\alpha - \mu).\alpha) = \mathrm{N}(\beta/\alpha - \mu).\mathrm{N}(\alpha) \leq 3/4.\mathrm{N}(\alpha) < \mathrm{N}(\alpha)$. ■

[5]Para ver un ejemplo de un dominio euclideano $\mathbb{Z}[\sqrt{d}]$ con $d > 0$ en el cual existe una división euclideana véase el Ejemplo **??**.

5.5. Dominios Euclidianos

En la Sección 5.3 estudiamos el dominio de integridad $\mathbb{Z}[i]$ a través de la norma $\mathrm{N}\colon \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$, la cual nos permitió obtener un algoritmo de división y en consecuencia deducimos varios resultados análogos que se cumplen en $\mathbb{Z}$. Podemos abstraer esta noción de "norma" a un dominio de integridad y estudiar aquellos dominios en los cuales es posible definir una dicha norma.

Definición 5.5.1. Sea D un dominio de integridad. Llamaremos a D un **dominio Euclidiano** (DU) si existe una función $\mathrm{N}\colon D \to \mathbb{Z}_{\geq 0}$ que verifica las siguientes propiedades:

(E1) $\mathrm{N}(a) \leq \mathrm{N}(a.b)$ para todos $a, b \in D$ no nulos;

(E2) si $a, b \in D$ con $b \neq 0$, entonces existen $q, r \in D$ tal que $a = bq+r$ con $r = 0$ o $\mathrm{N}(r) < \mathrm{N}(b)$.

Ejemplo 5.5.2.

(1) $\mathbb{Z}$ con el valor absoluto $|.|\colon \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ es un dominio Euclidiano.

(2) $\mathbb{Z}[i]$ con la norma $\mathrm{N}\colon \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ como definida en la sección anterior es un (DU).

(3) Sea $\mathbb{R}$ el cuerpo de los números reales. Consideremos el dominio de integridad de los polinomios con coeficientes reales, $\mathbb{R}[X]$. Definimos $\mathrm{N}\colon \mathbb{R}[X] \to \mathbb{Z}_{\geq 0}$ como $\mathrm{N}(0) = 0$ y para cada $f \in \mathbb{R}[X]$, $f \neq 0$, $\mathrm{N}(f) = \mathrm{gr}(f)$. Entonces, $\mathbb{R}[X]$ con N es un dominio Euclidiano, donde el algoritmo de la división es el usual estudiado en un curso de Álgebra básica. Más adelante veremos que $\mathbb{R}$ se puede reemplazar por cualquier cuerpo K.

(4) Un cuerpo K es trivialmente un dominio euclideano definiendo $\mathrm{N}(0) = 0$ y $\mathrm{N}(a) = 1$ para todo $a \in K$ no nulo. ■

Teorema 5.5.3. *Todo dominio Euclidiano D es un dominio de ideales principales.*

Demostración. Sea I un ideal de D. Si $I = \{0\}$, entonces I es trivialmente un ideal principal. Supongamos que $I \neq \{0\}$. Luego, existe $a \in I$ tal que

$$\mathrm{N}(a) = \text{mín}\{\mathrm{N}(x) : \ x \in I \setminus \{0\}\}.$$

Ahora queremos probar que $I = \langle a \rangle$. Es claro que $\langle a \rangle \subseteq I$. Sea $x \in I$. Por la condición (E2), existen $q, r \in D$ tal que $x = aq + r$ con $r = 0$ o $\mathrm{N}(r) < \mathrm{N}(a)$. Observemos que $r = x - aq$ y así $r \in I$. Pero como $\mathrm{N}(a)$ es el mínimo, tenemos que $r = 0$. Con lo cual, $x = aq$ y entonces $x \in \langle a \rangle$. Por lo tanto, $I = \langle a \rangle$. ■

Ejemplo 5.5.4. En Teoría Algebraica de Números es probado que el anillo $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ es un dominio de ideales principales. En 1949, T. S. Motzkin probó que $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ no es un dominio euclideano mostrando que no tiene una propiedad que los dominios euclideanos tienen. Para más detalles dirigimos al lector a [14, p. 153-154]. ■

Ejemplo 5.5.5. En el Ejemplo 5.2.7 vimos que $\mathbb{Z}[\sqrt{-5}]$ no es un DFU. Entonces, $\mathbb{Z}[\sqrt{-5}]$ no es un DIP, y por lo tanto, no es un dominio euclideano. ■

Proposición 5.5.6. *Sea D un dominio euclideano con norma* N. *Entonces:*

(1) $\mathrm{N}(1) \leq \mathrm{N}(a)$ *para todo* $a \in D$ *no nulo.*

(2) $a \in D$ *es una unidad si y sólo si* $\mathrm{N}(a) = \mathrm{N}(1)$.

Demostración. (1) Sea $a \in D$ no nulo. Por la condición (E1), tenemos que $\mathrm{N}(1) \leq \mathrm{N}(1.a) = \mathrm{N}(a)$.

(2) ($\Rightarrow$) Supongamos que $a \in D$ es una unidad. Entonces, $\mathrm{N}(a) \leq \mathrm{N}(a.a^{-1}) = \mathrm{N}(1)$. Por lo tanto, de (1), tenemos que $\mathrm{N}(a) = \mathrm{N}(1)$.
($\Leftarrow$) Sea $a \in D$ y supongamos que $\mathrm{N}(a) = \mathrm{N}(1)$. Por la condición (E2), existen $q, r \in D$ tales que $1 = aq + r$ con $r = 0$ o $\mathrm{N}(r) < \mathrm{N}(a)$. Si $r \neq 0$, entonces $\mathrm{N}(r) < \mathrm{N}(a)$. Luego se tiene que $\mathrm{N}(r) < \mathrm{N}(1)$. Lo cual es imposible por (1). Entonces $r = 0$. Con lo cual, $1 = aq$. Por lo tanto, a es una unidad. ■

Como todo dominio Euclidiano es un dominio de ideales principales (y así también un dominio de factorización única), para todo par de elementos a y b sabemos que existe el máximo común divisor de a y b. Pero, si no conocemos la factorización de a y b como producto de primos no tenemos una manera de determinar el mcd. Ahora, si estamos en un dominio Euclidiano tenemos un algoritmo que nos permite calcular el mcd de todo par de elementos. Dicho algoritmo es llamado el **algoritmo de Euclides** (el cual es análogo al algoritmo de Euclides conocido en los enteros).

Teorema 5.5.7 (Algoritmo de Euclides). *Sea D un dominio Euclidiano y sean $a, b \in D$ con $a \neq 0$. Consideremos las divisiones sucesivas*

$$\begin{array}{rcl} b & = & aq_0 + r_1, \quad \mathrm{N}(r_1) < \mathrm{N}(a) \\ a & = & r_1q_1 + r_2, \quad \mathrm{N}(r_2) < \mathrm{N}(r_1) \\ r_1 & = & r_2q_2 + r_3, \quad \mathrm{N}(r_3) < \mathrm{N}(r_2) \\ \vdots & = & \vdots \\ r_i & = & r_{i+1}q_{i+1} + r_{i+2}, \quad \mathrm{N}(r_{i+2}) < \mathrm{N}(r_{i+1}) \\ \vdots & = & \vdots \end{array}$$

Entonces, existe un $n \geq 1$ tal que

$$r_n = r_{n+1}q_{n+1}$$

y r_{n+1} es el máximo común divisor de a y b. Además, el máximo común divisor se puede escribir como combinación lineal de a y b.

5.6. Anillos de polinomios

En esta sección introduciremos una noción formal de "polinomio" sobre un anillo. En lo que sigue los anillos considerados serán siempre **anillos conmutativos con identidad**. También, por conveniencia, consideraremos el conjunto de números naturas (enteros positivos) junto con el cero. Es decir, en esta sección tenemos que $\mathbb{N} = \{0, 1, 2, \dots\}$ (el conjunto de enteros no negativos).

Sea A un anillo. Denotamos por $A^{\mathbb{N}}$ al conjunto de todas las funciones $f \colon \mathbb{N} \to A$. También nos será de utilidad representar a los elementos f de $A^{\mathbb{N}}$ como sucesiones:

$$f = (a_i : i \geq 0) = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Esto quiere decir que $f(i) = a_i$ para todo $i \in \mathbb{N}$. Usaremos indistintamente las dos notaciones para los elementos de $A^{\mathbb{N}}$ (como funciones o sucesiones).

Definimos dos operaciones binarias sobre $A^{\mathbb{N}}$, una suma y un producto, de la siguiente manera:

$$(f + g)(n) = f(n) + g(n) \ \forall n \geq 0 \tag{5.1}$$

$$\begin{aligned}(f.g)(n) &= f(0)g(n) + f(1)g(n-1) + \cdots + f(n-1)g(1) + f(n)g(0) \\ &= \sum_{i+j=n} f(i)g(j) \quad \forall n \geq 0.\end{aligned} \tag{5.2}$$

No es difícil pero si tedioso verificar que $A^{\mathbb{N}}$ con las operaciones recién definidas es un anillo conmutativo con identidad. El anillo A puede ser identificado (es decir, inmerso) en el anillo $A^{\mathbb{N}}$, dado que la aplicación $a \in A \mapsto (a, 0, 0, \dots, 0 \dots) \in A^{\mathbb{N}}$ es un monomorfismo. Con esta identificación tenemos que

$$a.(a_0, a_1, \dots, a_n, \dots) = (aa_0, aa_1, \dots, aa_n, \dots) \text{ si } a \in A.$$

Sea $X := (0, 1, 0, \dots, 0, \dots) \in A^{\mathbb{N}}$. Entonces se verifica que $X^n = (0, \dots, 0, 1, 0, \dots)$ (un único 1 en la n-esima posición). Utilizando la identificación anterior tenemos que

$$a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + a_nX^n = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots).$$

Definición 5.6.1. Diremos que un elemento $f \in A^{\mathbb{N}}$ es un **polinomio** si existe un $u \in \mathbb{N}$ tal que $f(i) = 0$ para todo $i \geq u$. Si $f \neq 0$ es un polinomio, al mayor n tal que $f(n) \neq 0$ se lo llama el **grado** de f y, en tal caso $f(n)$ es llamado el **coeficiente principal** de f. Denotaremos el grado de un polinomio no nulo f por $\mathrm{gr}(f)$; el coeficiente principal de f será denotado por $\mathrm{cp}(f)$. Si $f = a_nX^n + \cdots + a_1X + a_0$, entonces el coeficiente $f(0) = a_0$ es llamado el **término independiente** de f. Los polinomios cuyos coeficientes principales son 1 serán llamados **mónicos**.

La definición anterior nos dice que los polinomios son sucesiones $f \in A^{\mathbb{N}}$ de la forma $f = (a_0, a_1, \dots, a_n, 0, 0, \dots)$. Y por la observación anterior, vamos a escribir a los polinomios de la forma tradicional

$$f = a_0 + a_1X + \cdots + a_nX^n.$$

Denotaremos por $A[X]$ al conjunto de todos los polinomios de $A^{\mathbb{N}}$. Como vimos $A^{\mathbb{N}}$ con la suma y el producto antes definidos es un anillo, ahora veremos que $A[X]$ con esas operaciones es también un anillo, esto es, un subanillo de $A^{\mathbb{N}}$. Sean $f = (a_i)$ y $g = (b_i)$ dos polinomios y supongamos que $a_i = 0$ para todo $i \geq u$ y que $b_i = 0$ para todo $i \geq v$. Entonces, es claro que $a_i + b_i = 0$ para todo $i \geq \text{máx}(u, v)$. Entonces, $f + g$ es un polinomio. Si $n \geq u + v$ en la fórmula (5.2), tenemos que $a_i = 0$ o $b_j = 0$[6], con lo cual $(f.g)(n) = 0$. Entonces, $f.g$ es un polinomio. Por lo tanto, $A[X]$ es un anillo conmutativo con identidad con las operaciones suma y producto como definidas en (5.1) y (5.2). Llamaremos a $A[X]$ **el anillo de polinomios con coeficientes en** A.

Observemos que si $f(X) = a_nX^n + \cdots + a_1X + a_0$ y $g(X) = b_mX^m + \cdots + b_1X + b_0$, entonces la suma y el producto de f y g son:

$$f(X) + g(X) = a_nX^n + \cdots + a_{m+1}X^{m+1} + (a_m + b_m)X^m + \cdots + (a_1 + b_1)X + (a_0 + b_0) \quad (5.3)$$

si $n > m$ (similiarmente para $n < m$ y $n = m$)

$$f(X).g(X) = (a_nb_m)X^{n+m} + \cdots + c_kX^k + \cdots + (a_1b_0 + a_0b_1)X + (a_0b_0) \quad (5.4)$$

donde el coeficiente general c_k es:

$$c_k = \sum_{i+j=k} a_ib_j = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0 \quad \text{para } k = 0, 1, \ldots, n + m.$$

Cada polinomio $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ define una aplicación de A en A dada por

$$\alpha \in A \mapsto a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \in A.$$

Denotaremos por $f(\alpha) := a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ para cada polinomio $f \in A[X]$ y cada $\alpha \in A$.

Proposición 5.6.2. *Sean $f, g \in A[X]$ no nulos. Entonces,*

(1) $\text{gr}(f + g) \leq \text{máx}(\text{gr}(f), \text{gr}(g))$;

(2) $\text{gr}(f.g) \leq \text{gr}(f) + \text{gr}(g)$; *si el coeficiente principal de f no es un divisor de cero en A, entonces* $\text{gr}(f.g) = \text{gr}(f) + \text{gr}(g)$.

(3) $(f.g)(0) = f(0).g(0)$.

Demostración. Utilizar las ecuaciones (5.3) y (5.4). Se dejan los detalles a cargo del lector. ■

Proposición 5.6.3. *Sea A un dominio de integridad. Entonces*

(1) $\text{cp}(f.g) = \text{cp}(f).\text{cp}(g)$.

(2) $\text{gr}(f.g) = \text{gr}(f) + \text{gr}(g)$ *si f y g son polinomios no nulos;*

[6] Tenemos $n \geq u + v$ y $i + j = n$. Entonces, $i \geq u$ o $j \geq v$. Pues, si $i < u$ y $j < v$ entonces $n = i + j < u + v$ lo cual es absurdo.

(3) *los elementos invertibles de* $A[X]$ *son exactamente los elementos invertibles de* A*;*

(4) $A[X]$ *es un dominio de integridad.*

Demostración. Utilizar las ecuaciones (5.3) y (5.4). Se dejan los detalles a cargo del lector. ■

Sea I un ideal de un anillo A. Ahora, considere el ideal $\langle I\rangle$ de $A[X]$ generado por I. Una comprobación directa prueba que $\langle I\rangle$ es el conjunto de todos los polinomios de $A[X]$ con coeficientes en I. Esto es, $\langle I\rangle = I[X]$ (véase el Ejercicio 5.30). Ahora, veremos cuál es la conexión entre los ideales de A y los de $A[X]$.

Proposición 5.6.4. *Sea* I *un ideal de un anillo* A *y sea* $\langle I\rangle$ *el ideal de* $A[X]$ *generado por* I*. Entonces,*

$$A[X]/\langle I\rangle \cong (A/I)[X].$$

Además, si I *es un ideal primo de* A*, entonces* $\langle I\rangle$ *es un ideal primo de* $A[X]$*.*

Demostración. Consideremos la siguiente función $\varphi\colon A[X] \to (A/I)[X]$ definida por

$$\varphi(a_nX^n + \cdots + a_1X + a_0) = [a_n]X^n + \cdots + [a_1]X + [a_0].$$

De aquí obtenemos directamente que φ es un epimorfismo de anillos tal que $\mathrm{Nu}(\varphi) = I[X] = \langle I\rangle$ (la comprobación de estos dos hechos se deja a cargo del lector). Por lo tanto, por el Primer Teorema de Isomorfismo de anillos tenemos que

$$A[X]/\langle I\rangle \cong (A/I)[X].$$

Supongamos que I es un ideal primo de A. Luego, por la Proposición **??**, A/I es un dominio de integridad. Entonces $(A/I)[X]$ es un dominio de integridad. En consecuencia, por el isomorfismo anterior, $A[X]/\langle I\rangle$ es un dominio de integridad y usando de nuevo la Proposición **??** obtenemos que $\langle I\rangle$ es un ideal primo de $A[X]$. ■

Observación 5.6.5. Note que en la última afirmación de la proposición anterior no podemos reemplazar el adjetivo primo por el de maximal. Es decir, no es verdad que si I es un ideal maximal de un anillo A, entonces el ideal $\langle I\rangle$ del anillo de polinomios $A[X]$ generado por I es maximal. En efecto, es claro que el ideal $I = \langle 2\rangle$ de $\mathbb{Z}$ es maximal. Pero ya hemos probado (ver Ejemplo 4.5.9) que el ideal $\langle I\rangle = \{p(X) \in \mathbb{Z}[X] : \text{todos los coeficientes de } p(X) \text{ son pares}\}$ de $\mathbb{Z}[X]$ no es un ideal maximal de $\mathbb{Z}[X]$.

A pesar de la observación anterior, tenemos el siguiente resultado.

Proposición 5.6.6. *Sea* A *un anillo. Si* I *es un ideal maximal de* A*, entonces el ideal* $\langle I, X\rangle$ *de* $A[X]$ *generado por* I *y* X *es maximal en* $A[X]$*.*

Demostración. La demostración de este resultado es una reproducción, convenientemente generalizada, del argumento usado en el Ejemplo 4.5.4 (2) donde se probó que el ideal $\langle 2, X\rangle$ de $\mathbb{Z}[X]$ es maximal. Veamos primero que $\langle I, X\rangle = \{p(X) \in A[X] : p(0) \in I\}$. Sea $p(X) \in \langle I, X\rangle$. Entonces existen polinomios $f(X)$, $g(X)$ y $h(X)$ tales que $f(X) \in I[X]$ y $p(X) = f(X).g(X)+$

$h(X).X$. Luego, $p(0) = f(0).g(0) \in I$ porque $f(0) \in I$ e I es un ideal de A. Recíprocamente, supongamos que $p(X)$ es un polinomio tal que $p(0) \in I$. Supongamos que $p(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Entonces, $p(X) = (a_nX^{n-1} + a_{n-1}X^{n-2} + \cdots + a_1)X + 1.a_0 \in \langle I, X\rangle$. Por lo tanto, obtenemos la igualdad buscada. Ahora vamos a definir la función $\varphi\colon A[X] \to A/I$ como $\varphi(p(X)) = [p(0)]$. Es directo chequear que φ es un epimorfismo y $\mathrm{Nu}(\varphi) = \langle I, X\rangle$. Luego, por el Teorema 4.2.6, tenemos que $A[X]/\langle I, X\rangle \cong A/I$. Como I es un ideal maximal de A, A/I es un cuerpo y así $A[X]/\langle I, X\rangle$ es un cuerpo. Por lo tanto, $\langle I, X\rangle$ es un ideal maximal de $A[X]$. ■

Teorema 5.6.7. *Sea $f \in A[X]$, $f \neq 0$ y supongamos que el coeficiente principal de f es invertible. Si $g \in A[X]$, entonces existen $q, r \in A[X]$ tales que $g = f.q + r$ con $r = 0$ o $\mathrm{gr}(r) < \mathrm{gr}(f)$. Además, q y r están univocamente determinados.*

Demostración. Si $\mathrm{gr}(g) < \mathrm{gr}(f)$ tenemos que $g = f.0 + g$. Supongamos entonces que $\mathrm{gr}(f) \leq gr(g)$. Sea $f = a_nX^n + \cdots + a_1X + a_0$ con a_n invertible en A y sea $g = b_mX^m + \cdots + b_1X + b_0$ con $b_m \neq 0$. El polinomio $g - b_ma_n^{-1}X^{m-n}f$ es de grado menor que $\mathrm{gr}(g)$. Por inducción sobre el grado de g podemos suponer que existen q_1 y r tales que

$$g - b_ma_n^{-1}X^{m-n}f = f.q_1 + r \text{ con } r = 0 \text{ o } \mathrm{gr}(r) < \mathrm{gr}(f).$$

Tomando $q = q_1 + b_ma_n^{-1}X^{m-n}$, nos queda que

$$g = q.f + r$$

con $r = 0$ o $\mathrm{gr}(r) < \mathrm{gr}(f)$.

Supongamos que $g = f.q_1 + r_1$ con $r_1 = 0$ o $\mathrm{gr}(r_1) < \mathrm{gr}(f)$. Además supongamos que $q \neq q_1$. Tenemos que $(q - q_1).f = r_1 - r$ y como el coeficiente principal de f es invertible (en particular no es divisor de cero), $\mathrm{gr}(f) \leq \mathrm{gr}(q - q_1) + \mathrm{gr}(f) = \mathrm{gr}((q - q_1).f) = \mathrm{gr}(r_1 - r) < \mathrm{gr}(f)$, lo que es absurdo. Entonces, $q_1 = q$, de donde resulta también que $r = r_1$. ■

Los polinomios $q(X)$ y $r(X)$ en el teorema anterior son llamados el **cociente** y **resto**, respectivamente, de dividir $g(X)$ por $f(X)$. El siguiente teorema es un corolario directo del teorema anterior.

Teorema 5.6.8 (Algoritmo de la División)**.** *Sea K un cuerpo. Entonces para cualesquiera polinomios $f, g \in K[X]$ con $f \neq 0$, existen dos únicos polinomios q y r en $\in K[X]$ tales que $g = f.q + r$ con $r = 0$ o $\mathrm{gr}(r) < \mathrm{gr}(f)$.*

Igual que en los casos de polinomios con coeficientes en conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ tenemos los dos algoritmos para hallar el cociente y resto en una división.

Ejemplo 5.6.9 (División larga)**.** Consideremos hallar el cociente y resto de dividir el polinomio $f(X) = 2X^4 + X^3 + 1$ por $g(X) = 2X^2 + X + 1$ en $\mathbb{Z}_3[X]$. Entonces:

$$\begin{array}{rrrrrrrrrrrr|l}
- & 2X^4 & + & X^3 & + & 0X^2 & + & 0X & + & 1 & & & 2X^2+X+1 \\
 & 2X^4 & + & X^3 & + & X^2 & & & & & & & X^2+1 \\
\hline
- & & & & & 2X^2 & & & + & 1 & & & \\
 & & & & & 2X^2 & + & X & + & 1 & & & \\
\hline
 & & & & & & & 2X & & & & &
\end{array}$$

Por lo tanto, $c(X) = X^2 + 1$ y $r(X) = 2X$ son, respectivamente, el cociente y resto de dividir $f(X)$ por $g(X)$ en $\mathbb{Z}_3[X]$. ■

Ejemplo 5.6.10 (Ragla de Ruffini)**.** Consideremos determinar el cociente y resto de dividir el polinomio $f(X) = 3X^4 + 2X^3 + X^2 + 4$ por el polinomio $X + 3$ en $\mathbb{Z}_5[X]$. Entonces:

$$\begin{array}{r|rrrr|r}
 & 3 & 2 & 1 & 0 & 4 \\
-3 & & -9 & 21 & -66 & 198 \\
\hline
 & 3 & -7 & 22 & -66 & 202
\end{array}$$

Teniendo en cuenta que los coeficientes están en $\mathbb{Z}_5$ tenemos que el cociente es: $c(X) = 3X^3 - 7X^2 + 22X - 66 = 3X^3 + 3X^2 + 2X + 4$; y el resto es $r(X) = 202 = 2$. Comprobar que

$$f(X) = (X + 3)(3X^3 + 3X^2 + 2X + 4) + 2. \quad ■$$

Ahora veremos algunas consecuencias importantes del teorema anterior. Sea K un cuerpo. Consideremos la función $\mathrm{N}\colon K[X] \to \mathbb{N}$ definida por $\mathrm{N}(0) = 0$ y si $p(X) \neq 0$, entonces $\mathrm{N}(p(X)) = \mathrm{gr}(p(X)) =$ grado de $p(X)$. Entonces, por el teorema anterior y por la Proposición 5.6.3, tenemos lo siguiente:

Proposición 5.6.11. *Si K un cuerpo, entonces el anillo de polinomio $K[X]$ es un dominio Euclideano.*

Una consecuencia directa de la proposición anterior es que para cada cuerpo K, el anillo de polinomios $K[X]$ es un dominio de ideales principales y así también un dominio de factorización única. Por lo tanto, es interesante e importante conocer los elementos irreducibles de $K[X]$. La siguiente definición considera un caso un poco más general.

Definición 5.6.12. Sea A un dominio de integridad. Diremos que un polinomio no constante $f(X)$ es **irreducible** en $A[X]$ si no puede escribirse como producto de dos polinomios no constantes. Esto es, $f(X)$ es irreducible si y sólo si $f(X) = p(X).q(X)$ para algunos $p(X), q(X) \in A[X]$ implica que $p(X) \in A$ o $q(X) \in A$ (esto es, $p(X)$ o $q(X)$ son constantes). En caso contrario, diremos que f es **reducible**

Como A es un dominio de integridad, no todos los elementos no nulos son invertibles y así esta definición no coincide exactamente con la Definición 5.1.3 de elemento irreducible en un anillo. Pero si nos restringimos a un cuerpo K y tenemos en cuenta que los elementos invertibles (las unidades) del dominio $K[X]$ son exactamente los elementos invertibles de K (esto es, todo los elementos no nulos de K) obtenemos que ambas definiciones coinciden. Luego, tenemos el siguiente resultado análogo en el contexto de $\mathbb{Z}$.

Teorema 5.6.13 (Teorema Fundamental de la Aritmética en $K[X]$). *Sea K un cuerpo. Entonces todo polinomio no constante $f(X) \in K[X]$ puede expresarse como*

$$f(X) = ap_1(X)^{\alpha_1}.p_2(X)^{\alpha_2}.\ldots.p_n(X)^{\alpha_n}$$

donde $n \in \mathbb{N}$, cada $\alpha_i \in \mathbb{N}$, $a \in K$, y cada $p_i(X)$ es un polinomio irreducible mónico de $K[X]$. Esta factorización es única, salvo el orden de los factores.

Determinar si un polinomio es irreducible o no, es a menudo una tarea difícil de llevar a cabo. El objetivo ahora será presentar algunas herramientas y criterios para determinar la irreducibilidad de polinomios.

Proposición 5.6.14. *Sea A un dominio de integridad. Todo polinomio de $A[X]$ de grado 1 es irreducible en $A[X]$.*

Demostración. Es consecuencia de la Proposición 5.6.3. Se dejan los detalles al lector. ■

En la proposición anterior, la hipótesis que A es un dominio de integridad no puede debilitarse. Es decir, si A es un anillo conmutativo con identidad, pero no dominio de integridad, entonces no es necesariamente verdad que todo polinomio de grado 1 en $A[X]$ es irreducible en $A[X]$. Por ejemplo, en $\mathbb{Z}_6[X]$ se tiene que $X = (3X + 4)(4X + 3)$. Con lo cual X no es irreducible en $\mathbb{Z}_6[X]$.

Proposición 5.6.15 (Teorema del resto). *Sea A un anillo y $f(X) \in A[X]$. Sea $a \in A$. Entonces el resto de dividir $f(X)$ por $X - a$ es $f(a)$.*

Demostración. Ejercicio para el lector. ■

Definición 5.6.16. Sea A un anillo y $f(X) \in A[X]$. Un elemento $a \in A$ es llamado una **raíz** de $f(X)$ si $f(a) = 0$.

Proposición 5.6.17 (Corolario del Teorema del resto). *Sea $f(X) \in A[X]$, $f(X) \neq 0$. Para que $a \in A$ sea raíz de $f(X)$ es necesario y suficiente que el polinomio $X - a$ sea un divisor de $f(X)$.*

Demostración. Es consecuencia de la Proposición 5.6.15. Se dejan los detalles al lector. ■

Ejemplo 5.6.18. Sabiendo que 1 es una raíz del polinomio $p(X) = X^4 + 3X^3 + 2X + 4$ en $\mathbb{Z}_5[X]$, escribir a $p(X)$ como producto de polinomios irreducibles de $\mathbb{Z}_5[X]$. Aplicamos la Regla de Ruffini (operando en $\mathbb{Z}_5$) varias veces consecutivas, para dividir al polinomio $p(X)$ por $X - 1$. Así obtenemos que $p(X) = (X - 1)^3(X + 1)$. Como los polinomios $X - 1$ y $X + 1$ son de grado 1, sabemos que son irreducibles en $\mathbb{Z}_5[X]$. ■

Definición 5.6.19. Diremos que una raíz a de un polinomio $p(X)$ tiene **orden de multiplicidad** k, si k es el mayor entero positivo tal que $p(X) = (X - a)^k.q(X)$ con $q(X) \in A[X]$. En otras palabras, la raíz a tiene orden de multiplicidad k si $p(X) = (X - a)^k.q(X)$ para un polinomio $q(X)$ tal que $q(a) \neq 0$.

Se dice que un elemento a es una **raíz múltiple** de un polinomio $p(X)$ si su orden de multiplicidad es mayor o igual a 2. Si el orden de multiplicidad de a es 1, entonces se dice que a es una **raíz simple** de $p(X)$.

Proposición 5.6.20. *Sea A un dominio de integridad y $p(X) \in A[X]$. Si $a_1, \ldots, a_s$ son raíces distintas de $p(X)$, entonces*

$$p(X) = (X - a_1)^{k_1}. \ldots .(X - a_s)^{k_s}.q(X)$$

donde $k_1, \ldots, k_s$ son las multiplicidades de las raíces $a_1, \ldots, a_s$, respectivamente y $q(X)$ es un polinomio tal que $q(a_i) \neq 0$ para todo $i = 1, \ldots, s$. Además $k_1 + \cdots + k_s \leq \mathrm{gr}(p(X))$.

Demostración. Procedemos por inducción sobre el número de raíces distintas de un polinomio. Para $s = 1$, es trivial por definición del orden de multiplicidad. Supongamos que para todo polinomio con s raíces distintas, tenemos el resultado de la proposición. Sean $a_1, \ldots, a_s, a_{s+1}$ $s + 1$ raíces distintas de $p(X)$. Si k_1 es el orden de multiplicidad de a_1, entonces $p(X) = (X - a_1)^{k_1}.q(X)$ con $q(X)$ tal que $q(a_1) \neq 0$. Como A es un dominio de integridad, tenemos que $a_2, \ldots, a_{s+1}$ son raíces distintas del polinomio $q(X)$. Luego, por la hipótesis inductiva, tenemos que $q(X) = (X - a_2)^{k_2}. \ldots .(X - a_{s+1})^{k_{s+1}}.q'(X)$ donde $k_2, \ldots, k_{s+1}$ son los órdenes de multiplicidad de las raíces $a_2, \ldots, a_{s+1}$, respectivamente, y $q'(X)$ es un polinomio tal que $q'(a_j) \neq 0$ para todo $j = 2, \ldots, s + 1$. Observemos que $q'(a_1) \neq 0$. Entonces $p(X) = (X - a_1)^{k_1}. \ldots .(X - a_{s+1})^{k_{s+1}}.q'(X)$. Además es claro que $k_1 + \cdots + k_{s+1} \leq \mathrm{gr}(p(X))$. ■

Corolario 5.6.21. *Sea A un dominio de integridad. Si $f(X) \in A[X]$ es un polinomio de grado n, entonces $f(X)$ tiene a lo sumo n raíces, contando multiplicidades.*

El corolario anterior no es verdad si A no es dominio de integridad. Por ejemplo, el polinomio $X^2 + 7$ en $\mathbb{Z}_8[X]$ tiene a 1, 3, 5 y 7 como raíces.

Proposición 5.6.22. *Sea K un cuerpo y sea $f(X) \in K[X]$. Si $f(X)$ es de grado mayor que 1 y tiene una raíz en K, entonces $f(X)$ no es irreducible (es reducible) en $K[X]$.*

Demostración. Ejercicio para el lector. ■

La contrarecíproca de la proposición anterior es:

si $f(X)$ es irreducible en $K[X]$ y de grado mayor que 1, entonces no tiene raíces en K.

Pero la recíproca no es verdad. Es decir, existen polinomios en $K[X]$ que no tienen raíces y no son irreducibles.

Ejemplo 5.6.23. Considerar el polinomio $f(X) = X^4 + 2X^2 + 1 \in \mathbb{R}[X]$. Un cálculo sencillo nos permite determinar que $f(X) = (X^2 + 1)^2$. Esto nos muestra que $f(X)$ no tiene raíces en $\mathbb{R}$ y no es irreducible. ■

En el caso de polinomios de grado 2 o 3 tenemos que sí vale la recíproca de la Proposición 5.6.22.

Proposición 5.6.24. *Sea K un cuerpo. Un polinomio $f(X) \in K[X]$ de grado dos o tres es irreducible en $K[X]$ si y sólo si no tiene raíces en K.*

Demostración. La implicación ($\Rightarrow$) es consecuencia de la Proposición 5.6.22. La implicación ($\Leftarrow$) es consecuencia de la Proposición 5.6.3. Se dejan los detalles a cargo del lector. ■

Ejemplo 5.6.25. El polinomio $p(X) = X^2 + X + 1$ es irreducible en $\mathbb{Z}_2[X]$ porque es de grado 2 y no tiene raíces en $\mathbb{Z}_2$. En cambio, $p(X)$ no es irreducible en $\mathbb{Z}_3[X]$, porque $1 \in \mathbb{Z}_3$ es raíz de $p(X)$. ■

El siguiente criterio para chequear irreducibilidad de polinomios usa la Proposición 5.6.4 y consiste en reducir los coeficientes del polinomio en cuestión módulo algún ideal. En particular, este criterio no es útil en caso de polinomios con coeficientes en cuerpos, ya que en un cuerpo los únicos ideales son los triviales.

Proposición 5.6.26. *Sea A un dominio de integridad e I un ideal propio de A. Sea $p(X)$ un polinomio mónico no constante de $A[X]$. Si la imagen de $p(X)$ en $(A/I)[X]$ (ver Proposición 5.6.4) no puede ser factorizado en $(A/I)[X]$ en el producto de dos polinomios de menor grado, entonces $p(X)$ es irreducible en $A[X]$.*

Demostración. Supongamos que la imagen de $p(X)$ en $(A/I)[X]$ no puede ser factorizado en $(A/I)[X]$ y que $p(X)$ es reducible en $A[X]$. Luego, existen polinomios no constantes $f(X)$ y $g(X)$ tales que $p(X) = f(X).g(X)$. Sin perdida de generalidad podemos suponer que $f(X)$ y $g(X)$ son mónicos[7]. Entonces, por la Proposición 5.6.4, reduciendo los coeficientes en $p(X) = f(X).g(X)$ módulo I obtenemos una factorización en $(A/I)[X]$ de la imagen de $p(X)$ en dos polinomios no constantes de menor grado, lo cual es una contradicción. ■

Esta proposición nos dice que si podemos encontrar un ideal propio para el cual el polinomio reducido no puede ser factorizado en el cociente, entonces el polinomio mismo es irreducible. Esto no implica que no puedan existir polinomios irreducibles cuyas reducciones módulo bajo cualquier ideal propio sean reducibles. Por ejemplo, en $\mathbb{Z}[X]$ el polinomio $X^4 + 1$ es irreducible en $\mathbb{Z}[X]$ (véase el Ejemplo 5.6.35) pero es reducible módulo cada ideal primo de $\mathbb{Z}$ (una prueba de esto puede verse en [1]) y el polinomio $X^4 - 72X^2 + 4$ es irreducible en $\mathbb{Z}[X]$ (véase el Ejercicio 5.39) pero es reducible módulo cada ideal de $\mathbb{Z}$.

Ejemplo 5.6.27. Consideremos el polinomio $p(X) = X^2+X+1$ en $\mathbb{Z}[X]$. Tomemos la reducción de $p(X)$ en $\mathbb{Z}_2[X]$, así este es el mismo $p(X) = X^2 + X + 1$. Este polinomio es irreducible en $\mathbb{Z}_2[X]$ porque no tiene raíces en $\mathbb{Z}_2$. Entonces, por la proposición anterior, $p(X)$ es irreducible también en $\mathbb{Z}[X]$. El polinomio $q(X) = X^2 + 1$ es irreducible en $\mathbb{Z}[X]$ porque su reducción es irreducible en $\mathbb{Z}_3[X]$ (ya que no tiene raíces en $\mathbb{Z}_3$) pero la reducción de $q(X)$ a $\mathbb{Z}_2[X]$ es reducible (porque $1 \in \mathbb{Z}_2$ es raíz de la reducción de $q(X)$). Esto muestra que la recíproca de la proposición anterior no se cumple. ■

[7] Si $f(X)$ y $g(X)$ no fueran mónicos hacemos lo siguiente. Si a_n y b_m son los coeficientes principales de $f(X)$ y $g(X)$, respectivamente, entonces se tiene que $a_n.b_m = 1$, porque $p(X)$ es mónico y $p(X) = f(X)g(X)$. Luego consideramos los polinomios $f'(X) = b_m.f(X)$ y $g'(X) = a_n.g(X)$. f' y g' son mónicos y del mismo grado que f y g, respectivamente. Y se cumple que $p(X) = f'(X)g'(X)$.

Proposición 5.6.28 (Lema de Gauss)**.** *Sea A un (DFU) y sea K su cuerpo cociente. Sea $p(X)$ un polinomio de $A[X]$. Si $p(X) = f(X).g(X)$ para algunos polinomios no constantes $f(X)$ y $g(X)$ de $K[X]$, entonces existen elementos no nulos r y s de K tales que $f'(X) := r.f(X)$ y $g'(X) := s.g(X)$ son polinomios de $A[X]$ y $p(X) = f'(X).g'(X)$. Esto implica que si $p(X)$ es un polinomio de $A[X]$ reducible en $K[X]$, entonces $p(X)$ es reducible en $A[X]$.*

Demostración. Una prueba de este resultado puede verse en [1, Capítulo 9.3] (véase también [8, Teorema 4.6.3]). ■

La proposición anterior nos dice que: si K es el cuerpo cociente del DFU A y $p(X) \in A[X]$, entonces

$$p(X) \text{ es irreducible en } A[X] \text{ si y sólo si } p(X) \text{ es irreducible en } K[X].$$

Ejemplo 5.6.29. Probemos que el polinomio $p(X) = X^3 + 3X^2 - 8$ es irreducible en $\mathbb{Q}[X]$. Por el Lema de Gauss, ya que $\mathbb{Q}$ es el cuerpo cociente de $\mathbb{Z}$, tenemos que $p(X)$ es irreducible en $\mathbb{Q}[X]$ si y sólo si $p(X)$ es irreducible en $\mathbb{Z}[X]$. Ahora veamos que efectivamente $p(X)$ es irreducible en $\mathbb{Z}[X]$. Como $p(X)$ es de grado 3, vamos a probar que no tiene raíces en $\mathbb{Z}$. Supongamos que

$$X^3 + 3X^2 - 8 = 0 \implies X^3 + 3X^2 = 8 \implies X^2(X + 3) = 8.$$

Entonces tenemos que ($X^2 = 1$ y $X + 3 = 8$) o ($X^2 = 4$ y $X + 3 = 2$). En ambos casos es absurdo. Entonces $p(X)$ no tiene raíces en $\mathbb{Z}$. Por lo tanto, $p(X)$ es irreducible en $\mathbb{Z}[X]$, y así también en $\mathbb{Q}[X]$. ■

Ejemplo 5.6.30. Probemos que el polinomio $q(X) = 3X^4 - 12X^3 + X^2 + 1$ es irreducible en $\mathbb{Q}[X]$. Es suficiente probar que $q(X)$ es irreducible en $\mathbb{Z}[X]$. No podemos tomar la reducción del polinomio $q(X)$ en ningún $\mathbb{Z}_n[X]$ porque $q(X)$ no es mónico. En su lugar consideramos el polinomio $f(X) = 3^3q(X) = 3^4X^4 - 12.3^3X^3 + 3^3X^2 + 3^3$. Observemos que si el polinomio $f(X)$ es irreducible, entonces $q(X)$ es irreducible. Así que nos enfocamos en probar que $f(X)$ es irreducible. Ahora hacemos un cambio de variable para transformar a $f(X)$ en un polinomio mónico. Sea $Y := 3X$. Entonces, $g(Y) = f(X) = Y^4 - 12Y^3 + 3Y^2 + 3^3$. Notemos también que la irreducibilidad de $g(Y)$ implica la irreducibilidad de $f(X)$. Ahora tomemos la reducción de $g(Y)$ módulo 2: $\overline{g}(Y) = Y^4 + Y^2 + 1$. Probemos que este polinomio es irreducible en $\mathbb{Z}_2[X]$. Supongamos que no lo es. Entonces, existen dos polinomios no constantes mónicos $a(X)$ y $b(X)$ en $\mathbb{Z}_2[X]$ tal que $Y^4 + Y^2 + 1 = a(X)b(X)$. Por la Proposición 5.6.3, tenemos que $\text{gr}(a)$ es 1, 2 o 3, y correspondientemente el $\text{gr}(b)$ es 1, 2 o 3. Observemos que el polinomio $\overline{g}(Y) = Y^4 + Y^2 + 1$ no tiene raíces en $\mathbb{Z}_2$, entonces $a(X)$ y $b(X)$ no tienen raíces en $\mathbb{Z}_2$. Entonces $a(X)$ y $b(X)$ no pueden ser de grado 1. Entonces $\text{gr}(a) = \text{gr}(b) = 2$. Hay exactamente cuatro polinomios mónicos de grado 2 en $\mathbb{Z}_2[X]$. Dividiendo el polinomio $\overline{g}(Y) = Y^4 + Y^2 + 1$ por cada uno de los cuatros polinomios mónicos de grado dos, vemos que ningún es un factor de $\overline{g}(Y)$. Por lo tanto, $\overline{g}(Y)$ es irreducible en $\mathbb{Z}_2[X]$. Por lo tanto, $g(Y)$ es irreducible en $\mathbb{Z}[X]$. Entonces, por lo antes dicho, el polinomio original $q(X)$ es irreducible en $\mathbb{Z}[X]$. ■

Ejemplo 5.6.31. Sea $f(X) = X^5 + 2X + 4$. Probemos que $f(X)$ es irreducible en $\mathbb{Z}[X]$ (y así también lo será en $\mathbb{Q}[X]$). Vamos a considerar una reducción adecuada módulo p. Tomemos la reducción en $\mathbb{Z}_3$: $\overline{f}(X) = X^5 + 2X + 1$. Primero observemos que $\overline{f}$ no tiene raíces en $\mathbb{Z}_3$. Supongamos que $\overline{f}(X)$ no es irreducible, es decir, que es reducible. Entonces existen dos polinomios no constantes $a(X)$ y $b(X)$ en $\mathbb{Z}_3[X]$ tal que $\overline{f}(X) = a(X)b(X)$. Podemos asumir sin perdida de generalidad que $a(X)$ y $b(X)$ son mónicos (porque $\overline{f}(X)$ lo es). Entonces los posibles grados de $a(X)$ y $b(X)$ son: 2 y 3 (¿por que ni $a(X)$ ni $b(X)$ pueden tener grado 1?). Supongamos que $\mathrm{gr}(a(X)) = 2$. Sabemos que hay exactamente 9 polinomios mónicos de grado 2 en $\mathbb{Z}_3[X]$. Con lo cual $a(X)$ tiene que ser igual a uno de ellos. De estos nueve polinomios, descartamos aquellos que tienen una raíz en $\mathbb{Z}_3$. Así que nos quedan sólo los siguientes: $X^2 + 1$, $X^2 + X + 2$ y $X^2 + 2X + 2$. Realizando la división de $\overline{f}(X)$ por cada uno de esos tres polinomios (en $\mathbb{Z}_3[X]$) vemos que ninguno de lo divide (las divisiones dan resto no nulo). Esto es absurdo porque $a(X) \mid \overline{f}(X)$. Por lo tanto, $\overline{f}(X)$ es irreducible en $\mathbb{Z}_3[X]$, con lo cual $f(X) = X^5 + 2X + 4$ es irreducible en $\mathbb{Z}[X]$. ■

Proposición 5.6.32 (Gauss)**.** *Sea $f(X) = a_nX^n + \cdots + a_1X + a_0$ en $\mathbb{Z}[X]$ de grado n (esto es, $a_n \neq 0$). Si $t/s \in \mathbb{Q}$ (con t y s relativamente primos) y $p(t/s) = 0$, entonces $t \mid a_0$ y $s \mid a_n$.*

Demostración. A cargo del lector. ■

Ejemplo 5.6.33. Consideremos el polinomio $p(X) = 2X^3 - 3X^2 + 2X - 3$. Probemos que $p(X)$ no es irreducible en $\mathbb{Q}[X]$. Es suficiente con probar que $p(X)$ tiene al menos una raíz en $\mathbb{Q}$. Por la Proposición 5.6.32, las posibles raíces racionales son $\frac{t}{s} = \pm 1, \pm\frac{1}{2}, \pm 3, \pm\frac{3}{2}$. Aplicando la regla de Ruffini, podemos comprobar que $\frac{3}{2}$ es raíz de $p(X)$, además se tiene que $p(X) = (X - \frac{3}{2})(2X^2 + 2)$. Por el Lema de Gauss, podemos concluir también que $p(X)$ no es irreducible en $\mathbb{Z}[X]$. De hecho, $p(X) = (2X - 3)(X^2 + 1)$. ■

El siguiente es otro criterio importante para testear la irreducibilidad de polinomios.

Proposición 5.6.34 (Criterio de Eisenstein)**.** *Sea $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un polinomio de $\mathbb{Z}[X]$. Si existe un entero primo p tal que $p \mid a_0$, $p \mid a_1$, $\ldots$, $p \mid a_{n-1}$, $p \nmid a_n$ y $p^2 \nmid a_0$, entonces $f(X)$ es irreducible en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$.*

Demostración. Véase en [5, Theorem 17.4]. ■

Ejemplo 5.6.35.

(1) Sea $p(X) = X^5 - 6X^3 + 4X^2 - 10$. Como 2 divide a los coeficientes -6, 4 y al -10 y además $4 = 2^2$ no divide al -10, entonces el criterio Eisenstein asegura que el polinomio $p(X)$ es irreducible en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$.

(2) Sea $p(X) = X^4 + 1$. Tal como está el polinomio $p(X)$, no se puede aplicar directamente el criterio de Eisenstein. Consideremos el polinomio $q(X) := p(X + 1) = (X + 1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$. Ahora si aplicamos el criterio de Eisenstein al polinomio $q(X)$ con el primo 2, entonce $q(X)$ es irreducible en $\mathbb{Z}[X]$. Luego, la irreducibilidad de $q(X)$ implica la irreducibilidad de $p(X)$.

(3) Sea $p(X) = 5X^4 - 7X + 7$. Podemos aplicar el criterio de Eisenstein con $p = 7$. Por lo tanto, $p(X)$ es irreducible en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$. ■

Sea K un cuerpo. Sabemos entonces que el anillo de polinomios $K[X]$ es un dominio Euclideano y así, en particular, es un (DIP). Entonces, por la Proposición 5.2.5, tenemos que un polinomio $p(X)$ de $K[X]$ es irreducible si y sólo si el ideal principal $\langle p(X)\rangle$ de $K[X]$ es maximal. Esto nos permite concluir directamente el siguiente resultado:

Proposición 5.6.36. *Sea K un cuerpo y sea $p(X)$ un polinomio de $K[X]$. Entonces, $K[X]/\langle p(X)\rangle$ es un cuerpo si y sólo si $p(X)$ es irreducible.*

La proposición anterior nos muestra como los polinomios irreducibles juegan en $K[X]$ el papel que los números primos juegan en $\mathbb{Z}$. Recordemos como obteníamos cuerpos finitos a partir de $\mathbb{Z}$ y números primos: tomando un primo p de $\mathbb{Z}$, los enteros módulo p formaban un cuerpo y además vimos que $\mathbb{Z}_p = \mathbb{Z}/\langle p\rangle$ y donde $\langle p\rangle$ es un ideal maximal.

Sea A un dominio de integridad. Sea $f \in A[X]$ un polinomio mónico de grado n, digamos $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Sea $\langle f\rangle$ el ideal generado por f y tomemos el anillo cociente $A[X]/\langle f\rangle$. A continuación veremos que las clases de equivalencia de $A[X]/\langle f\rangle$ están en correspondencia uno a uno con los polinomios de grado menor que n. Es decir, probaremos que en cada clase de equivalencia de $A[X]/\langle f\rangle$ hay uno y sólo un polinomio de grado menor que n.

Para el elemento neutro de $A[X]/\langle f\rangle$, $\langle f\rangle = [0]$, es claro. Sea $g \in A[X]$ y $g \notin \langle f\rangle$. Podemos escribir $g = fq + r$ con $q, r \in A[X]$ y $\operatorname{gr}(r) < \operatorname{gr}(f) = n$. Luego, $g - r = fq \in \langle f\rangle$ y esto implica que $[g] = [r]$. Así, tenemos que toda clase de equivalencia contiene un polinomio de grado menor que n. Sean $h_1, h_2 \in A[X]$ tales que $\operatorname{gr}(h_1), \operatorname{gr}(h_2) < n$ y $[h_1] = [h_2]$. Entonces, $h_1 - h_2 = fg$ para algún $g \in A[X]$. Como $\operatorname{gr}(h_1 - h_2) < n$ y $\operatorname{gr}(fg) = \operatorname{gr}(f) + \operatorname{gr}(g) \geq n$, necesariamente se tiene que $g = 0$. Lo cual implica que $h_1 = h_2$. Por lo tanto, en cada clase de equivalencia no nula hay uno y sólo un polinomio de grado menor que n. Dada una clase de equivalencia, para determinar su polinomio representante de grado menor que n, basta tomar cualquier elemento de la clase, dividirlo por f y tomar el resto. Además, si el anillo A es finito, podemos concluir que el cardinal de $A[X]/\langle f\rangle$ es $|A|^n$. Esto es,

$$|A[X]/\langle f\rangle| = |A|^n.$$

Sea A un dominio de integridad y sea $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$. Consideremos la aplicación $\varphi : A \to A[X]/\langle f\rangle$ dada por $\varphi(r) = [r]$. Es claro que φ es un homomorfismo inyectivo, con lo cual nos permite identificar cada clase $[r]$ con su representante $r \in A$. Si $\alpha \in A[X]/\langle f\rangle$, entonces existe un único polinomio $g \in A[X]$ de grado menor a n, digamos $g = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, tal que $\alpha = [g]$. Así,

$$\alpha = [g] = [c_0] + [c_1][X] + \cdots + [c_{n-1}][X^{n-1}] = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}$$

donde hemos utilizado la identificación $c_i \longleftrightarrow [c_i]$ y hemos reemplazado $[X]$ por θ. Por otra parte, tenemos que

$$0 = [0] = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} + \theta^n.$$

Por lo tanto, podemos ver que los elementos de $A[X]/\langle f\rangle$ tienen una única expresión de la forma $c_0+c_1\theta+\cdots+c_{n-1}\theta^{n-1}$ con $c_i\in A$ y tal que $a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}+\theta^n=0$. Entonces, utilizando las expresiones de $A[X]/\langle f\rangle$, la relación de $f(\theta)=0$ y las propiedades de anillos podemos determinar las operaciones de $A[X]/\langle f\rangle$.

Ejemplo 5.6.37. Sea $f(X)=X^2+1\in\mathbb{Z}_3[X]$. Notemos que $f(X)$ es irreducible, pues es de grado 2 y no tiene raíces en $\mathbb{Z}_3$. Así tenemos que el ideal $\langle f(X)\rangle$ es maximal y por lo tanto $\mathbb{Z}_3[X]/\langle f(X)\rangle$ es un cuerpo de orden $3^2=9$. Los elementos de $\mathbb{Z}_3[X]/\langle f(X)\rangle$ son de la forma $a+b\theta$ con $a,b\in\mathbb{Z}_3$, esto es,

$$\mathbb{Z}_3[X]/\langle f(X)\rangle=\{a+b\theta : a,b\in\mathbb{Z}_3\}.$$

Para operar en $\mathbb{Z}_3[X]/\langle f\rangle$ utilizamos las operaciones de anillo en $\mathbb{Z}_3$ y la relación $\theta^2+1=0$, es decir, $\theta^2=-1=2$:

$$\begin{aligned}(a+b\theta)+(c+d\theta)&=(a+c)+(b+d)\theta\\ (a+b\theta)(c+d\theta)&=ac+ad\theta+bc\theta+bd\theta^2=(ac+2bd)+(ad+bc)\theta.\end{aligned}$$

Por ejemplo, $(1+\theta)(1+\theta)=1+2\theta+\theta^2=1+2\theta+2=2\theta$; $(1+\theta)\theta=\theta+\theta^2=\theta+2$. ■

Ejercicios propuestos

Dominios de factorización única y dominios de ideales principales

Ejercicio 5.1. Sea A un dominio de integridad y sean $a,b\in A$. Probar que a y b son asociados si y sólo si $\langle a\rangle=\langle b\rangle$.

Ejercicio 5.2. Sea A un dominio de integridad. Probar que:

(a) Si $a\in A$ es irreducible, entonces todo elemento asociado a a es también irreducible.

(b) si $a,b\in A$ y $b\neq 0$, entonces $\langle ab\rangle\subsetneq\langle b\rangle$ si y sólo si a no es una unidad de A.

Ejercicio 5.3. Sea A un dominio de factorización única y sea u una unidad de A. Entonces, para cualquier elemento $a\in A$, el máximo común divisor de u y a es (salvo asociados) u.

Ejercicio 5.4. Sea A un dominio de integridad y sea $p\in A$ primo. Probar que para todo $n\in\mathbb{N}$ y todos $a_1,\ldots,a_n\in A$, si $p\mid a_1\cdot\cdots\cdot a_n$, entonces $p\mid a_i$ para algún $i\in\{1,\ldots,n\}$.

Ejercicio 5.5.

(a) Sea A un dominio de integridad. Sea p un elemento primo de A. Probar que $A/\langle p\rangle$ es un dominio de integridad.

(b) Sea A un DIP y sea I un ideal de A. Probar que el anillo cociente A/I es un DIP.

(c) Sea A un DIP y $p\in A$ primo. Probar que $A/\langle p\rangle$ es un cuerpo.

Los enteros de Gauss

Ejercicio 5.6. Hallar el cociente y resto de dividir $a = 3 - 4i$ por $b = 2 + 5i$ en $\mathbb{Z}[i]$.

Ejercicio 5.7. Determinar si los siguientes elementos son o no irreducibles (primos gaussianos) en $\mathbb{Z}[i]$.

(a) 2. (b) 3. (c) 5. (d) $2 - 3i$.

Ejercicio 5.8. Expresar a 13 y $5 + i$ como producto de elementos irreducibles de $\mathbb{Z}[i]$.

Extensiones cuadráticas

Ejercicio 5.9. Sea $d \in \mathbb{Z}$ que no es un cuadrado. Probar que la función $\sigma\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ es un isomorfismo de anillos.

Ejercicio 5.10. ¿es $\alpha = 1 + \sqrt{2}$ una unidad de $\mathbb{Z}[\sqrt{2}]$?

Ejercicio 5.11. Probar que los siguientes elementos son irreducibles en $\mathbb{Z}[\sqrt{-5}]$.

(a) 3. (b) 7. (c) $4 + \sqrt{5}i$. (d) $4 - \sqrt{5}i$. (e) $1 + 3\sqrt{5}i$.

Ejercicio 5.12. Probar que 21 se puede escribir de dos formas distintas como producto de elementos irreducibles de $\mathbb{Z}[\sqrt{-5}]$.

Ejercicio 5.13. Consideremos el dominio de integridad $\mathbb{Z}[\sqrt{-6}]$.

(a) Probar que 10 se factoriza en producto de irreducibles de dos formas distintas.

(b) ¿Es $\mathbb{Z}[\sqrt{-6}]$ un DFU?

(c) ¿Es $\mathbb{Z}[\sqrt{-6}]$ un DIP?

Ejercicio 5.14. Probar que en $\mathbb{Z}[\sqrt{-5}]$ el elemento $1 + 3\sqrt{5}i$ es irreducible pero no primo.

Ejercicio 5.15. Probar que $\mathbb{Z}[\sqrt{-3}]$ no es un DIP.

Ejercicio 5.16. Probar que 2 y $1 + \sqrt{5}$ son elementos irreducibles de $\mathbb{Z}[\sqrt{5}]$ pero no primos. ¿Es $\mathbb{Z}[\sqrt{5}]$ un DFU?

Ejercicio 5.17. Probar que 7 es irreducible en $\mathbb{Z}[\sqrt{5}]$ y en $\mathbb{Z}[\sqrt{6}]$.

Ejercicio 5.18. Probar que para cada $n \in \mathbb{N}$, los elementos $(3+2\sqrt{2})^n$ son unidades de $\mathbb{Z}[\sqrt{2}]$.

Ejercicio 5.19. Sea $d \in \mathbb{Z}$ que no es un cuadrado. Sean $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$. Probar que si $\alpha.\beta$ es una unidad, entonces α y β son unidades.

Dominios euclideanos

Ejercicio 5.20. Sea D un dominio euclideano con norma N. Probar que si $a, b \in D$ son asociados, entonces $\mathrm{N}(a) = \mathrm{N}(b)$.

Ejercicio 5.21. Sea d un entero que no es un cuadrado. Probar que la función $\sigma\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ definida por $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$ es un autoisomorfismo.

Ejercicio 5.22. Probar las propiedades de la Proposición 5.4.2.

Ejercicio 5.23. Sea $d \in \mathbb{Z}$ tal que d no es un cuadrado. Probar que si $\alpha \in \mathbb{Z}[\sqrt{d}]$ es tal que $N(\alpha) = p$ es un entero primo, entonces α es un elemento irreducible de $\alpha \in \mathbb{Z}[\sqrt{d}]$.

Ejercicio 5.24. Probar que todo entero primo p tal que $p \equiv -1 (\text{mód } 4)$ es un elemento irreducible de $\mathbb{Z}[\sqrt{-5}]$.

Ejercicio 5.25. (a) Probar que $\mathbb{Z}[i]$ es un DIP.

(b) Sea $I = \langle a + bi \rangle$ un ideal de $\mathbb{Z}[i]$. Probar que $a^2 + b^2 \in I$.

(c) Sea $c + di \in \mathbb{Z}[i]$. Sean r_c y r_d los restos de dividir c y d por $a^2 + b^2$, respectivamente. Probar que $(c + di) + I = (r_c + r_d i) + I$.

(d) Probar que $\mathbb{Z}[i]/I$ es finito.

(e) Sea $\alpha = 2 + i$. Describir el anillo cociente $\mathbb{Z}[i]/\langle 2 + i \rangle$. ¿Es $\mathbb{Z}[i]/\langle 2 + i \rangle$ un cuerpo?

Ejercicio 5.26. Probar que el dominio de integridad $\mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2} : \ x, y \in \mathbb{Z}\}$ con la función $\mathrm{N}\colon \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_{\geq 0}$ definida por

$$\mathrm{N}(x + y\sqrt{2}) = |x^2 - 2y^2|$$

para cada $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, es un dominio Euclidiano.
(*Sug. Véase la prueba de la Proposición 5.4.7. También será útil probar que* $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.)

Anillos de polinomios

Ejercicio 5.27. Sean A y B anillos conmutativos con identidad. Probar que si A y B son isomorfos, entonces $A[X]$ y $B[X]$ son isomorfos.

Ejercicio 5.28. Sea A un dominio de integridad y sea $f(X) \in A[X]$. Probar que para todo $n \in \mathbb{N}$ se tiene que

$$\mathrm{cp}(f^n) = \mathrm{cp}(f)^n \qquad \text{y} \qquad \mathrm{gr}(f^n) = n\mathrm{gr}(f).$$

Ejercicio 5.29. Probar que el polinomio $f(X) = 2X + 1$ in $\mathbb{Z}_4[X]$ es invertible, es decir, tiene un inverso en $\mathbb{Z}_4[X]$. ¿Esto contradice la afirmación (3) de la Proposición 5.6.3? Explicar.

Ejercicio 5.30. Sea A un anillo conmutativo con identidad. Sea I un ideal de A. Probar que el conjunto

$$I[X] = \{a_nX^n + \cdots + a_1X + a_0 \in A[X] : a_0, a_1, \ldots, a_n \in I\}$$

es el ideal de $A[X]$ generado por I.

Ejercicio 5.31. Para cada uno de los siguientes incisos, hallar el cociente y resto de dividir $f(X)$ por $g(X)$ en los dominios indicados.

(a) $f(X) = 3X^4 + X^3 + 2X^2 + 1$ y $g(X) = X^2 + 4X + 2$; en $\mathbb{R}[X]$.

(b) $f(X) = 3X^4 + X^3 + 2X^2 + 1$ y $g(X) = X^2 + 4X + 2$; en $\mathbb{Z}_5[X]$.

(c) $f(X) = 2X^5 + X^3 + 2X^2 + 2$ y $g(X) = X - 1$; en $\mathbb{Z}_3[X]$.

(d) $f(X) = 5X^4 + 3X^3 + 1$ y $g(X) = 3X^2 + 2X + 1$ en $\mathbb{Z}_7[X]$.

Ejercicio 5.32. Sea K un cuerpo.

(a) Sea $f(X) = a_nX^n + \cdots + a_1X + a_0 \in K[X]$. Probar que $X - 1$ divide a $f(X)$ si y sólo si $a_0 + a_1 + \cdots + a_n = 0$.

(b) Sea $I = \{f(X) = a_nX^n + \cdots + a_1X + a_0 \in K[X] : a_0 + a_1 + \cdots + a_n = 0\}$. Probar que I es un ideal de $K[X]$. Hallar un generador de I.

Ejercicio 5.33. Sea $\varphi\colon \mathbb{Z}[X] \to \mathbb{Z}$ la función definida por $\varphi(f(X)) = f(1)$. Probar que φ es un epimorfismo. Probar que $\mathbb{Z}[X]/\mathrm{Nu}(\varphi) \cong \mathbb{Z}$.

Ejercicio 5.34. Listar todos los polinomios de grado 3 sobre $\mathbb{Z}_2$ e indicar cuáles de ellos son irreducibles. ¿Cúantos polinomios distintos de grado 3 hay sobre $\mathbb{Z}_3$?

Ejercicio 5.35. Probar que el polinomio $f(X) = (X - 1)(X - 2) \ldots (X - n) - 1$ es irreducible en $\mathbb{Z}[X]$ para todo $n \in \mathbb{N}$.
(*Sug.: Suponer por absurdo que $f(X) = p(X)q(X)$ con $p(X)$ y $q(X)$ no constantes. Analizar los grados de p, q y del polinomio $p(X)+q(X)$. Evaluar f en 1,2,...,n. A partir de esto determinar el número posible de raíces del polinomio $p(X) + q(X)$, y en consecuencia el grado nuevamente de $p(X) + q(X)$.*)

Ejercicio 5.36. Hallar todas las raíces y sus multiplicidades del polinomio $f(X) = X^5 + 4X^4 + 4X^3 + 4X^2 + X + 1$ sobre $\mathbb{Z}_5$ y factorizarlo en producto de irreducibles en $\mathbb{Z}_5[X]$.

Ejercicio 5.37. Sea p un entero primo positivo.

(a) Probar $a = 1, 2, \ldots, p - 1$ son raíces del polinomio $X^{p-1} - 1$.
(*Sug. Utilizar el Pequeño Teorema de Fermat, Teorema 1.4.13*).

(b) Probar que $X^{p-1} - 1 = (X - 1)(X - 2) \ldots (X - (p - 1))$.
(*Sug. Usar la Proposición 5.6.20*).

Ejercicio 5.38. Sea A un dominio de integridad y sea $f(X) \in A[X]$. Probar que $a \in A$ es raíz de $f(X)$ de orden k si y sólo si $f(X)$ es divisible por $(X-a)^k$ pero no lo es por $(X-a)^{k+1}$.

Ejercicio 5.39. Probar que el polinomio $f(X) = X^4 - 72X^2 + 4$ es irreducible en $\mathbb{Z}[X]$.
(*Sug.: Usar la Proposición 5.6.32 para determinar que $f(X)$ no tiene raíces enteras. Luego suponer por absurdo que $f(X)$ es reducible en $\mathbb{Z}[X]$.*)

Ejercicio 5.40. Probar que el polinomio $p(X) = X^3 + nX + 2$ es irreducible en $\mathbb{Z}[X]$ para todo entero $n \neq 1, -3, -5$.
(*Sug.: Utilizar las Proposiciones 5.6.24 y 5.6.32.*)

Ejercicio 5.41. Determinar cuales de los siguientes polinomios son irreducibles en los anillos indicados.

(a) $a(X) = 18X^5 - 30X^2 + 120X + 360$ en $\mathbb{Z}[X]$.

(b) $g(X) = X^3 + 6$ en $\mathbb{Z}_7[X]$.

(c) $a(X) = 3X^4 - 12X^3 + X^2 + 1$ en $\mathbb{Q}[X]$.

(d) $b(X) = 8X^3 - 6X + 1$ en $\mathbb{Q}[X]$.

(e) $c(X) = X^5 + 5X^2 + 1$ en $\mathbb{Q}[X]$.

(f) $d(X) = (5/2)X^5 + (9/2)X^4 + 15X^3 + (3/7)X^2 + 6X + 3/14$ en $\mathbb{Q}[X]$.

(g) $e(X) = X^4 + 1$ en $\mathbb{R}[X]$.

(h) $f(X) = X^4 + 15X^3 + 7$ en $\mathbb{Q}[X]$.

(i) $e(X) = X^4 + 1$ en $\mathbb{Z}_p[X]$ con p entero primo.

(j) $f(X) = X^2 + X + 4$ en $\mathbb{Z}_{11}[X]$.

(k) $g(X) = X^4 + 10X^2 + 1$ en $\mathbb{Z}[X]$.

(l) $h(X) = X^4 + 4X^3 + 6X^2 + 2X + 1$ en $\mathbb{Z}[X]$.

Ejercicio 5.42. Expresar cada uno de los siguientes polinomios en producto de irreducibles en los dominios indicados.

(a) $a(X) = X^3 + X^2 + X + 1 \in \mathbb{Z}_2[X]$.

(b) $b(X) = X^3 + 6 \in \mathbb{Z}_7[X]$.

(c) $c(X) = X^5 + 4X^4 + 4X^3 - X^2 - 4X + 1 \in \mathbb{Z}_5[X]$.

(d) $d(X) = X^8 - 1$ en $\mathbb{Z}[X]$.

(e) $d(X) = X^8 - 1$ en $\mathbb{Z}_2[X]$.

(f) $d(X) = X^8 - 1$ en $\mathbb{Z}_3[X]$.

(g) $e(X) = X^6 - 1$ en $\mathbb{Z}[X]$.

(h) $e(X) = X^6 - 1$ en $\mathbb{Z}_2[X]$.

(i) $e(X) = X^6 - 1$ en $\mathbb{Z}_3[X]$.

Ejercicio 5.43. Sea K un cuerpo. Sea $p(X)$ un polinomio irreducible en $K[X]$. Probar que para todos $a(X), b(X) \in K[X]$, si $p(X) \mid a(X)b(X)$, entonces $p(X) \mid a(X)$ o $p(X) \mid a(X)$.
(*Sug. Utilizar la Proposición 5.6.36*).

Ejercicio 5.44. Sea K un cuerpo y sea $f(X)$ un polinomio reducible de $K[X]$. Probar que el ideal $\langle f(X) \rangle$ no es primo en $K[X]$.

Ejercicio 5.45. Hallar todos los polinomios mónicos irreducibles de grado 2 en $\mathbb{Z}_3[X]$.

Ejercicio 5.46. Describir el anillo cociente $\mathbb{Z}_2[X]/\langle X^2 \rangle$. Construir las tablas de sus operaciones.

Ejercicio 5.47. Encontrar y describir todos los ideales en $\mathbb{Z}_3[X]/\langle X^2+2 \rangle$. ¿Es $\mathbb{Z}_3[X]/\langle X^2+2 \rangle$ un dominio de integridad?

Ejercicio 5.48. Para cada uno de los siguientes n, hallar un cuerpo con n elementos y describir las operaciones de suma y producto dando tres ejemplos de suma y tres ejemplos de productos.

(a) $n = 8$.

(b) $n = 9$.

(c) $n = 25$.

(d) $n = 49$.

(e) $n = 125$.

Capítulo 6

Extensiones de Cuerpos

En este capítulo presentamos una breve introducción al estudio de la teoría de cuerpos, con especial atención al concepto de extensiones de cuerpos. Podemos decir, a grandes rasgo, que el material presentado en este capítulo constituye la base o tal vez mejor dicho, los pre requisitos necesarios para comenzar el estudio de la Teoría de Galois.

El estudio de extensiones de cuerpos permite, entre otras muchas e importantes cosas, realizar una clasificación completa de todos los cuerpos finitos. También se verá en este capítulo que todo polinomio $P(X)$ sobre un cuerpo F tiene al menos una raíz en alguna *extensión* de F $(F \subset K)$ convenientemente elegida.

6.1. Cuerpos

En esta sección vamos a introducir algunos conceptos básicos de la teoría de cuerpos. Comenzamos con la siguiente definición.

Definición 6.1.1. Sea K un cuerpo. Un subconjunto no vacío F de K es llamado **subcuerpo** de K si F es un subanillo de K el cual es de hecho un cuerpo.

La siguiente proposición da una caracterización útil y sencilla de la noción de subcuerpo. Dejamos los detalles de la demostración a cargo del lector.

Proposición 6.1.2. *Sea K un cuerpo y F un subconjunto no vacío de K. Entonces, F es un subcuerpo de K si y sólo si se cumplen las siguientes condiciones:*

(1) $1 \in F$,

(2) *si* $a, b \in F$, *entonces* $a - b \in F$ *y*

(3) *si* $a, b \in F$ *y* $b \neq 0$, *entonces* $ab^{-1} \in F$

Definición 6.1.3. Sea K un cuerpo. Diremos que K tiene (o es de) **característica** $p \neq 0$ si p es el menor entero positivo n tal que $n.a = 0$ para todo $a \in K$. Si no existe un tal p que verifique la condición se dirá que K es de característica 0.

Ejemplo 6.1.4.

(1) Sea p un entero positivo primo. Entonces el cuerpo $\mathbb{Z}_p$ es de característica p.

(2) Todo cuerpo finito es de característica no nula. Si K es un cuerpo con n elementos, entonces sabemos (considerando a K como grupo abeliano con respecto a $+$) que $n.a = 0$ para todo $a \in K$. Así, por el Principio de Buena Ordenación de los números naturales, sabemos que existe un entero positivo p tal que es el menor que verifica que $p.a = 0$ para todo $a \in K$.

(3) En el Ejemplo 5.6.37 vimos que $\mathbb{Z}_3[X]/\langle X^2+1\rangle$ es un cuerpo con 9 elementos. Es claro que $3.(a\theta+b) = 0$ para todo elemento $a\theta+b$ de $\mathbb{Z}_3[X]/\langle X^2+1\rangle$ y así la característica de dicho cuerpo es 3. ■

Proposición 6.1.5. *La característica de cualquier cuerpo K es cero o un número primo p.*

Demostración. Sea K un cuerpo. Si la característica de K es cero, entonces no hay nada que probar. Supongamos que la característica de K es p. Si p no es primo, entonces $p = s.t$ con $1 < s < p$ y $1 < t < p$. Como $(s.1_K)(t.1_K) = (st)1_K = p.1_K = 0$ y K es en particular un dominio de integridad, tenemos que $s.1_K = 0$ o $t.1_K = 0$. Si $s.1_K = 0$, entonces para todo elemento $a \in K$, $s.a = (s.1_K).a = 0.a = 0$. Lo cual es imposible pues p es la característica de K y $1 < s < p$. Análogamente si $t.1_K = 0$. Por lo tanto, p es un número primo. ■

La siguiente proposición muestra una propiedad interesante y útil de aquellos cuerpos que tiene característica no nula.

Proposición 6.1.6. *Sea K un cuerpo de característica $p \neq 0$. Entonces, para todos $a, b \in K$ y todo entero positivo n, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.*

Demostración. Afirmamos primero que el teorema del binomio de Newton $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}.b^k$ es válido en todo dominio de integridad (se deja la prueba a cargo del lector). Ya que p es primo, tenemos que para cada $0 < k < p$, p divide al coeficiente binomial $\binom{p}{k}$[1]. Entonces, como la característica de K es p y cada coeficiente binomial $\binom{p}{k}$ con $0 < k < p$ es un múltiplo de p, tenemos que

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}.b^k = a^p + b^p.$$

Ahora probaremos $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ por inducción sobre n. Para $n = 1$, lo acabamos de probar. Supongamos que es válido para $n-1$. Entonces,

$$(a+b)^{p^n} = \left((a+b)^{p^{n-1}}\right)^p = \left(a^{p^{n-1}} + b^{p^{n-1}}\right)^p = a^{p^n} + b^{p^n}.$$ ■

Los cuerpos $\mathbb{Q}$ y $\mathbb{Z}_p$ con p primo, juegan un rol importante en el estudio de la teoría de cuerpos. Una de las propiedades que comparten estos cuerpos es que ellos no poseen subcuerpos propios y, como veremos enseguida, todo cuerpo contiene como subcuerpo una copia isomorfica de uno u otro de ellos.

[1]Dado que $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$, se sigue que $p \mid k.\binom{p}{k}$ y como p es primo y $k < p$, obtenemos que $p \mid \binom{p}{k}$.

Sea K un cuerpo de característica 0. Entonces los elementos de la forma $n.1_K$ (donde $n \in \mathbb{Z}$ y 1_K es la identidad de K) son todos distintos (véase Ejercicio 6.8) y ellos forman un subanillo isomorfo a $\mathbb{Z}$. Tenemos ahora que el conjunto

$$\begin{aligned} P(K) &:= \left\{ m1_K(n1_K)^{-1} : m, n \in \mathbb{Z} \text{ con } n \neq 0 \right\} \\ &= \left\{ \frac{m.1_K}{n.1_K} : m, n \in \mathbb{Z} \text{ con } n \neq 0 \right\} \\ &= \left\{ \frac{m}{n} : m, n \in \mathbb{Z} \text{ con } n \neq 0 \right\} \end{aligned}$$

es de hecho un subcuerpo de K isomorfo a $\mathbb{Q}$. En otras palabras, el subcuerpo $P(K)$ es el cuerpo de fracciones del dominio de integridad $A = \{n.1_K : n \in \mathbb{Z}\}$.

Supongamos ahora que K es un cuerpo de característica p. Entonces se puede probar que el conjunto

$$P(K) := \{0_K, 1_K, 2.1_K, \ldots, (p-1).1_K\} = \{0, 1, 2, \ldots, (p-1)\}$$

(dejamos los detalles al lector) es de hecho un subcuerpo de K y es isomorfo al cuerpo $\mathbb{Z}_p$.

Para cualquier cuerpo K, una propiedad importante del subcuerpo $P(K)$ es que el está contenido en todo subcuerpo de K (pues, todo subcuerpo contiene los elementos 0_K y 1_K). El subcuerpo $P(K)$ es llamado el **subcuerpo primo de** K.

6.2. Espacios vectoriales

En esta sección presentamos los conceptos básicos de la teoría de espacios vectoriales que serán necesarios para la exposición en las secciones siguientes.

Definición 6.2.1. Un **espacio vectorial** V sobre un cuerpo K es un grupo abeliano $\langle V, + \rangle$ con una operación externa $.: K \times V \to V$ (estos es, para cada $k \in K$ y cada $v \in V$, $k.v \in V$) que verifica los siguientes axiomas:

(V1) $k.(v_1 + v_2) = k.v_1 + k.v_2$, para todos $v_1, v_2 \in V$ y $k \in K$;

(V2) $(k_1 + k_2).v = k_1.v + k_2.v$, para todos $k_1, k_2 \in K$ y $v \in V$;

(V3) $k_1(k_2.v) = (k_1k_2).v$, para todos $k_1, k_2 \in K$ y $v \in V$;

(V4) $1.v = v$, para todo $v \in V$.

Es usual llamar **vectores** a los elementos de un espacio vectorial V sobre un cuerpo K y **escalares** a los elementos de K.

Ejemplo 6.2.2.

(1) Sea K un cuerpo. Sea $V = K^n = \{(k_1, \ldots, k_n) : k_1, \ldots, k_n \in K\}$. Sabemos que V es un grupo abeliano con respecto a la suma. Se define el producto externo como $k.(k_1, \ldots, k_n) = (kk_1, \ldots, kk_n)$. Luego, no es difícil de comprobar que V es un espacio vectorial sobre el cuerpo K.

(2) Sea K un cuerpo y consideremos el anillo de polinomios $K[X]$. El grupo abeliano $\langle K[X], +\rangle$ con el producto externo definido, para cada $p(X) = a_nX^n + \cdots + a_1X + a_0$ y $k \in K$, como

$$k.p(X) = ka_nX^n + \cdots + ka_1X + ka_0$$

es un espacio vectorial sobre K.

(3) Sean K y F cuerpos tales que F es un subanillo de K, $F \subseteq K$. Entonces K es un espacio vectorial sobre el cuerpo F. La operación externa de un elemento de F por uno de K es simplemente el producto en el cuerpo K.

(4) Por el punto anterior tenemos que $\mathbb{C}$ es un espacio vectorial sobre el cuerpo $\mathbb{R}$. ■

Veamos algunas propiedades básicas de los espacios vectoriales. Las pruebas de ellas se dejan a cargo del lector.

Proposición 6.2.3. *Sea V un espacio vectorial sobre un cuerpo K. Entonces, para todo $v \in V$ y $k \in K$,*

(1) $k.0 = 0$;

(2) $0.v = 0$;

(3) *si* $kv = 0$, *entonces* $k = 0$ *o* $v = 0$;

(4) $(-k)v = -(kv)$.

Sea V un espacio vectorial sobre un cuerpo K. Sean $v_1, \ldots, v_n \in V$. Se dice que un vector $v \in V$ es **combinación lineal** de los vectores $v_1, \ldots, v_n$ si existen escalares $k_1, \ldots, k_n \in K$ tales que $v = k_1.v_1 + \cdots + k_n.v_k$. Denotaremos por $\langle v_1, \ldots, v_n\rangle$ al conjunto de todas las combinaciones lineales de los vectores $v_1, \ldots, v_n$. Esto es,

$$\langle v_1, \ldots, v_n\rangle := \{k_1.v_1 + \cdots + k_n.v_n : k_1, \ldots, k_n \in K\}.$$

El siguiente resultado será de mucha utilidad para probar algunos resultados en la teoría de espacios vectoriales. Sea K un cuerpo. Consideremos el sistema homogéneo de ecuaciones lineales presentado en (6.1) donde los $k_{ij} \in K$ y las soluciones son n-uplas de elementos de K.

$$\begin{cases} k_{11}x_1 + k_{12}x_2 & + \ldots + k_{1n}x_n & = 0 \\ k_{21}x_1 + k_{22}x_2 & + \ldots + k_{2n}x_n & = 0 \\ \quad\vdots \quad + \quad \vdots & + \ldots + \quad \vdots & = 0 \\ k_{i1}x_1 + k_{i2}x_2 & + \ldots + k_{in}x_n & = 0 \\ \quad\vdots \quad + \quad \vdots & + \ldots + \quad \vdots & = 0 \\ k_{m1}x_1 + k_{m2}x_2 & + \ldots + k_{mn}x_n & = 0 \end{cases} \tag{6.1}$$

Lema 6.2.4. *Si en el sistema* (6.1) *el número de incógnitas es mayor que el número de ecuaciones ($n > m$), entonces* (6.1) *tiene una solución no trivial en K.*

Demostración. Procedemos por inducción sobre el número m de ecuaciones. Si $m = 1$, el sistema (6.1) es $k_{11}x_1+k_{12}+\cdots+k_{1n}x_n = 0$ con $n > 1$. Para no tener una trivialidad estamos asumiendo que no todos los coeficientes k_{ij} son ceros. Podemos suponer sin perdida de generalidad que k_{11} es no nulo. Entonces, la ecuación anterior tiene como solución no trivial a: $x_2 = \cdots = x_n = 1$ y $x_1 = -(1/k_{11})(k_{12} + \cdots + k_{1n})$.

Ahora suponemos que el lema es verdad para para todo sistema con r ecuaciones (y el número de incógnitas excede al de ecuaciones). Supongamos que en el sistema (6.1) $m = r + 1$ y $n > r+1$. Como antes, no todos los k_{ij} son nulos. Asumamos que $k_{11} \neq 0$. Vamos a eliminar x_1 de las ecuaciones. Para esto se resta a cada ecuación $i \geq 2$ la primera ecuación multiplicada por k_{i1}/k_{11}. Luego, sin tener en cuenta la primera ecuación, obtenemos un nuevo sistema homogéneo con r ecuaciones en $n-1$ incógnitas como se muestra en (6.2) y en donde $s_{ij} = k_{ij} - k_{i1}/k_{11}$.

$$\begin{cases} s_{22}x_2+ & \ldots & + & s_{2n}x_n = & 0 \\ \vdots\ + & \ldots & + & \vdots\ = & 0 \\ s_{i2}x_2+ & \ldots & + & s_{in}x_n = & 0 \\ \vdots\ + & \ldots & + & \vdots\ = & 0 \\ s_{r+1,2}x_2+ & \ldots & + & s_{r+1,n}x_n = & 0 \end{cases} \tag{6.2}$$

Además note que $n-1 > r$. Entonces, por la hipótesis inductiva, el sistema (6.2) tiene una solución no trivial $(y_2, \ldots, y_n)$ en K. Sea $y_1 = -(k_{12}y_2 + \cdots + k_{1n}y_n)/k_{11}$. Ahora se puede verificar directamente que la n-upla $(y_1, y_2, \ldots, y_n)$ así obtenida es una solución no trivial del sistema (6.1). Esto completa la demostración. ■

Definición 6.2.5. Sea V un espacio vectorial sobre K. Un subconjunto W de V es llamado un **subespacio** de V si W es un subgrupo de V y para todo $w \in W$ y todo $k \in K$, el producto externo $k.w \in W$.

Proposición 6.2.6. *Sea V un espacio vectorial sobre K y sean $v_1, \ldots, v_n \in V$. Entonces $\langle v_1, \ldots, v_n\rangle$ es un subespacio de V y es llamado el **subespacio de V generado por los vectores** $v_1, \ldots, v_n$.*

Diremos que un espacio vectorial V sobre K es **finitamente generado** si existen vectores $v_1, \ldots, v_n \in V$ tal que $V = \langle v_1, \ldots, v_n\rangle$. En otras palabras, un espacio vectorial V es finitamente generado si existen n vectores $v_1, \ldots, v_n$ tal que todo elemento de V es una combinación lineal de los vectores $v_1, \ldots, v_n$.

Definición 6.2.7. Sea V un espacio vectorial sobre un cuerpo K. Diremos que n vectores $v_1, \ldots, v_n$ de V son **linealmente independientes** sobre K si $k_1v_1 + \cdots + k_nv_n = 0$ para $k_1, \ldots, k_n \in K$, implica que $k_1 = k_2 = \cdots = k_n = 0$. En caso contrario diremos que son **linealmente dependientes**.

Proposición 6.2.8. *Sea V un espacio vectorial sobre K y sean $v_1, \ldots, v_n \in V$. Entonces las siguientes afirmaciones son equivalentes:*

(1) *los vectores* $v_1, \ldots, v_n$ *son linealmente independientes sobre* K*;*

(2) *todo elemento* $v \in \langle v_1, \ldots, v_n \rangle$ *tiene una representación única como combinación lineal de* $v_1, \ldots, v_n$.

Demostración. (1) $\Rightarrow$ (2) Sea $v \in \langle v_1, \ldots, v_n \rangle$ y supongamos que v tiene dos representaciones, esto es, $v = k_1 v_1 + \cdots + k_n v_n = s_1 v_1 + \cdots + s_n v_n$ con $k_i, s_i \in K$. Luego, tenemos que $(k_1 - s_1).v_1 + \cdots + (k_n + s_n).v_n = 0$ y como los vectores $v_1, \ldots, v_n$ son linealmente independientes sobre K, obtenemos que $k_1 = s_1, \ldots, k_n = s_n$.

(2) $\Rightarrow$ (1) Es claro ya que $k_1 v_1 + \cdots + k_n v_n = 0 = 0v_1 + \cdots + 0v_n$ implica que $k_1 = 0, \ldots, k_n = 0$. ■

Definición 6.2.9. Sea V un espacio vectorial sobre K. Un conjunto $\{v_1, \ldots, v_n\}$ de vectores de V es llamado una **base** de V sobre K si los vectores $v_1, \ldots, v_n$ son linealmente independientes y generan a V.

Proposición 6.2.10 (Teorema de la dimensión)**.** *Sea* V *un espacio vectorial sobre* K*. Si* $\{v_1, \ldots, v_n\}$ *y* $\{w_1, \ldots, w_m\}$ *son dos bases finitas de* V *sobre* K*, entonces* $n = m$*. Es decir, dos bases finitas de* V *deben tener el mismo número de elementos.*

Demostración. Se puede ver una prueba en [7, p. 62]. ■

La proposición anterior nos permite considerar la siguiente definición.

Definición 6.2.11. Sea V un espacio vectorial sobre un cuerpo K y sea $\{v_1, \ldots, v_n\}$ una base de V. Se define la **dimensión** de V como el número de elementos de la base $\{v_1, \ldots, v_n\}$ y la denotaremos por $\dim_K(V)$, esto es, $\dim_K(V) = n$.

Ejemplo 6.2.12.

(1) $\dim_{\mathbb{R}}(\mathbb{C}) = 2$. Se puede comprobar que $\{1, i\}$ es una base del espacio $\mathbb{C}$ sobre el cuerpo $\mathbb{R}$. Entonces, $\dim_{\mathbb{R}}(\mathbb{C}) = 2$.

(2) Sea K un cuerpo. Consideremos el espacio vectorial $V = K^n$ (con $n \in \mathbb{N}$) sobre K. Un argumento directo prueba que los vectores $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 0, 1)$ forman una base para V. Entonces $\dim_K(K^n) = n$. ■

Proposición 6.2.13. *Sea* V *un espacio vectorial sobre* K *tal que* $\dim_K(V) = n$*. Entonces cualquier conjunto de* $m > n$ *vectores de* V *son linealmente dependientes.*

Demostración. Sean $w_1, \ldots, w_m$ vectores de V y sea $\{v_1, \ldots, v_n\}$ una base de V sobre K. Entonces, existen escalares k_{ij} en K tales que

$$\begin{aligned} w_1 &= k_{11} v_1 + \cdots + k_{1n} v_n \\ w_2 &= k_{21} v_1 + \cdots + k_{2n} v_n \\ &\vdots \\ w_m &= k_{m1} v_1 + \cdots + k_{mn} v_n. \end{aligned}$$

Para probar que los vectores $w_1, \dots, w_m$ son linealmente dependientes consideremos la ecuación $s_1w_1 + s_2w_2 + \cdots + s_mw_m = 0$ con los s_i escalares de K. Luego tenemos que

$$s_1(k_{11}v_1 + \cdots + k_{1n}v_n) + s_2(k_{21}v_1 + \cdots + k_{2n}v_n) + \dots$$
$$\cdots + s_m(k_{m1}v_1 + \cdots + k_{mn}v_n) = 0.$$

Con lo cual

$$(k_{11}s_1 + \cdots + k_{m1}s_m).v_1 + (k_{12}s_1 + \cdots + k_{m2}s_m).v_2 + \dots$$
$$\cdots + (k_{1n}s_1 + \cdots + k_{mn}s_m).v_n = 0.$$

Como los vectores $\{v_1, \dots, v_n\}$ son linealmente independientes obtenemos el siguiente sistema

$$\begin{cases} k_{11}s_1 + k_{21}s_1 & + \dots + k_{m1}s_m & = 0 \\ k_{12}s_1 + k_{22}s_1 & + \dots + k_{m2}s_m & = 0 \\ \quad\vdots \quad + \quad \vdots & + \dots + \quad \vdots & = 0 \\ k_{1n}s_1 + k_{2n}s_1 & + \dots + k_{mn}s_m & = 0 \end{cases}$$

que tiene n ecuaciones, m incógnitas $(s_1, \dots, s_n)$ y $m > n$. Entonces, por el Lema 6.2.4, existe una solución $s_1, \dots, s_n$ no trivial de escalares. Esto muestra que los vectores $w_1, \dots, w_m$ no son linealmente independientes, es decir, son linealmente dependientes. ∎

Proposición 6.2.14. *Sea V un espacio vectorial sobre un cuerpo K tal que $\dim_K(V) = n$. Entonces, cualquier conjunto de n vectores linealmente independientes forman una base de V sobre K.*

Demostración. Sea $B = \{v_1, \dots, v_n\}$ un conjunto cualesquiera de vectores linealmente independientes de V. Para probar que B es una base de V solo resta chequear que B genera todo V. Sea $v \in V$. Por la Proposición 6.2.13, tenemos que los vectores $v_1, \dots, v_n, v$ son linealmente dependientes. Es decir, existen escalares $k_1, \dots, k_n, k$ de K no todo nulos tales que $0 = k_1v_1 + \dots k_nv_n + kv$. Afirmamos que $k \neq 0$. Pues si $k = 0$, entonces tendríamos que $0 = k_1v_1 + \cdots + k_nv_n$ con los escalares $k_1, \dots, k_n$ no todos nulos, lo que contradice el hecho que los vectores $v_1, \dots, v_n$ son linealmente independientes. Luego podemos hacer

$$v = (-1/k)(k_1v_1 + \cdots + k_nv_n) = s_1v_1 + \cdots + s_nv_n$$

con $s_i = -k_i/k$. Así, los vectores $v_1, \dots, v_n$ generan a todo V y por lo tanto $B = \{v_1, \dots, v_n\}$ forma una base de V. ∎

6.3. Extensiones de Cuerpos

Sean K y F dos cuerpos. Diremos que K es una **extensión** de F si $F \subset K$, esto es, si F es un subcuerpo de K. También diremos que K es un **cuerpo extensión del cuerpo** F. Recordemos que si K es una extensión de F, $F \subset K$, entonces K es un espacio vectorial sobre el cuerpo F. Diremos que K es un **extensión finita** de F si $\dim_F(K)$ es finita. Es usual denotar $\dim_F(K)$ como $[K : F]$ y se lo llama el **grado de K sobre F**.

Ejemplo 6.3.1.

(1) El cuerpo de números reales $\mathbb{R}$ es una extensión infinita del cuerpo de números racionales $\mathbb{Q}$, pues cualquier extensión finita de $\mathbb{Q}$ debe ser de cardinal infinito numerable y sabemos que $\mathbb{R}$ es infinito no numerable.

(2) El cuerpo de números complejos $\mathbb{C}$ es una extensión finita de $\mathbb{R}$. En efecto, los números 1 e i forman una base de $\mathbb{C}$ sobre $\mathbb{R}$ ya que todo número complejo z se escribe como $z = a + ib$ con $a, b \in \mathbb{R}$. ■

Veamos ahora algunas propiedades básicas acerca del grado de extensiones.

Proposición 6.3.2. *Sean $F \subset K \subset L$ cuerpos tales que los grados $[L : K]$ y $[K : F]$ son finitos. Entonces L es una extensión finita de F y $[L : F] = [L : K].[K : F]$.*

Demostración. Lo que haremos para probar la proposición es exhibir explicitamente una base de L sobre el cuerpo F. Supongamos que $[L : K] = m$ y $[K : F] = n$. Entonces L tiene una base $\{v_1, \ldots, v_m\}$ sobre K y K tiene una base $\{w_1, \ldots, w_n\}$ sobre F. Se puede probar directamente que los vectores $\{v_i w_j : 1 \leq i \leq m \text{ y } 1 \leq j \leq n\} = \{v_1 w_1, \ldots, v_1 w_n, \ldots, v_m w_1, \ldots, v_m w_n\}$ forman una base de L sobre el cuerpo F, mostrando que ellos generan a todo L y son linealmente independientes sobre F. Dejamos los detalles a cargo del lector. Por lo tanto, L es una extensión finita de F y además podemos concluir que $[L : F] = mn = [L : K].[K : F]$. ■

Proposición 6.3.3. *Sea K un cuerpo extensión de F. Entonces, $K = F$ si y sólo si $[K : F] = 1$.*

Demostración. Si $K = F$, entonces es claro que $\{1\}$ es una base de K sobre F y por lo tanto $[K : F] = 1$. Recíprocamente, supongamos que $[K : F] = 1$. Entonces existe $\alpha \neq 0$ de K tal que $\{\alpha\}$ es una base de K sobre F. Luego, debe existir un escalar $a \in F$ tal que $1 = a.\alpha$. Entonces $\alpha = 1/a \in F$. Para cada $\beta \in K$, existe $b \in F$ tal que $\beta = b.\alpha = b/a \in F$. Esto es, $K \subseteq F$. Por lo tanto, $K = F$. ■

Proposición 6.3.4. *Sea K una extensión finita de F de grado n. Entonces, para todo elemento u de K existen $n + 1$ elementos $a_0, a_1, \ldots, a_n$ de F no todos nulos, tales que*

$$a_0 + a_1 u + \cdots + a_n u^n = 0.$$

Demostración. Sea $u \in K$. Como $[K : F] = \dim_F(K) = n$ y $1, u, u^2, \ldots, u^n$ son en total $n + 1$ elementos de K, tenemos por la Proposición 6.2.13 que ellos son linealmente dependientes sobre F. Entonces, existen $n + 1$ escalares $a_0, a_1, \ldots, a_n$ no todos nulos de F tales que

$$a_0.1 + a_1 u + \cdots + a_n u^n = 0.$$ ■

Una conclusión directa de la proposición anterior es que si K es una extensión finita de un cuerpo F, entonces para todo elemento u de K existe un polinomio no trivial $p(X) = a_n X^n + \cdots + a_1 X + a_0$ de $F[X]$ tal que u es una raíz de $p(X)$. Esto nos sugiere la siguiente definición general.

Definición 6.3.5. Sea K un cuerpo extensión de un cuerpo F. Se dice que un elemento $\alpha \in K$ es **algebraico sobre** F si existe un polinomio $p(X)$ no nulo de $F[X]$ tal que $p(\alpha) = 0$. Un elemento de K que no es algebraico sobre F es llamado **trascendente sobre** F. Diremos que K es una **extensión algebraica** de F si todo elemento de K es algebraico sobre F.

Notemos que por la Proposición 6.3.4, tenemos que si K es una extensión finita de F, entonces todo elemento de K es algebraico sobre F. Luego, podemos concluir el siguiente corolario:

Corolario 6.3.6. *Si K es una extensión finita de F, entonces K es una extensión algebraica de F.*

La afirmación recíproca no es verdad; una extensión algebraica K de F no es necesariamente una extensión finita de F.

Ejemplo 6.3.7.

(1) El número complejo i es algebraico sobre $\mathbb{Q}$, pues $p(X) = X^2 + 1$ es un polinomio de $\mathbb{Q}[X]$ y $p(i) = 0$. En general, diremos que un número complejo es un **número algebraico** si es algebraico sobre $\mathbb{Q}$.

(2) Consideremos la extensión $\mathbb{Q} \subset \mathbb{R}$. Para todo número real a, si a es racional, entonces a es algebraico. En efecto, se considera $p(X) = X - a$.

(3) Consideremos de nuevo la extensión $\mathbb{Q} \subset \mathbb{R}$. El número $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, pues es raíz del polinomio $p(X) = X^2 - 2$. Veamos que el número $\sqrt{1+\sqrt{3}}$ es algebraico sobre $\mathbb{Q}$. Llamemos $a = \sqrt{1+\sqrt{3}}$. Entonces $a^2 = 1 + \sqrt{3}$ y así $a^2 - 1 = \sqrt{3}$. Luego $(a^2-1)^2 = 3$ y con lo cual $a^4 - 2a^2 - 2 = 0$. Por lo tanto, es claro que a es una raíz del polinomio $p(X) = X^4 - 2X^2 - 2$. Entonces, efectivamente $\sqrt{1+\sqrt{3}}$ es algebraico sobre $\mathbb{Q}$.

(4) Los números reales e y π son conocidos a ser trascendentes sobre $\mathbb{Q}$. La prueba de esto no es sencilla. Que el número e es trascendente sobre $\mathbb{Q}$ fue probado por Hermite en 1873 y la demostración de que π es trascendente fue realizada por Lindemann en 1882. $\blacksquare$

Hay una forma bastante sencilla de obtener números reales trascendentes a través de lo que se conoce como el *Criterio de Liouville* (J. Liouville 1809-1882). El matemático Liouville probó que todo número algebraico (de grado n) debe satisfacer una cierta propiedad. El criterio es de tal naturaleza que se pueden construir, sin demasiada dificultad, números reales que no cumplen la propiedad establecida por Liouville y así, dichos números deben ser trascendentes. Para más detalles acerca del Criterio de Liouvulle y la forma de obtener números reales trascendentes, dirigimos al lector a [8, Sección 6.6].

Ahora veremos como producir extensiones finitas de cuerpos a partir de elementos algebraicos, usando como herramienta los polinomios mínimos. El siguiente lema es un resultado que necesitaremos para alcanzar nuestro objetivo.

Lema 6.3.8. *Sea A un dominio de integridad. Si A es un espacio vectorial de dimensión finita sobre un cuerpo F, entonces A es de hecho un cuerpo.*

Demostración. Solo debemos probar que todo elemento no nulo de A es invertible. Sea $a \in A$ no nulo. Digamos que $\dim_F(A) = n$. Así, los elementos $1, a, a^2, \ldots, a_n$ son linealmente dependientes en A sobre F, esto es, existen escalares $b_0, b_1, \ldots, b_n$ de F no todos nulos tal que

$$b_0.1 + b_1.a + \cdots + b_n.a^n = 0.$$

Entonces, podemos tomar un polinomio $p(X) = c_m X^m + \cdots + c_1 X + c_0$ no nulo de F de grado mínimo tal que $p(a) = 0$. Afirmamos que $c_0 \neq 0$. Supongamos lo contrario, $c_0 = 0$. Entonces

$$0 = c_1.a + \cdots + c_m.a^m = (c_1 + \cdots + c_m.a^{m-1}).a.$$

Como A es un dominio de integridad, obtenemos que $c_1 + \cdots + c_m.a^{m-1} = 0$ y entonces $q(X) = c_1 + \cdots + c_m X^{m-1}$ es un polinomio de grado menor que $p(X)$ tal que $q(a) = 0$; esto contradice la minimalidad del grado de $p(X)$. Ahora, usando que $c_0 \neq 0$, tenemos que

$$1 = -\frac{c_m.a^m + \cdots + c_1.a}{c_0} = \left(\frac{c_m.a^{m-1} + \cdots + c_1}{c_0}\right).a.$$

Entonces, a es invertible y por lo tanto A es un cuerpo. ■

Definición 6.3.9. Sea K un cuerpo extensión de F. Diremos que un elemento algebraico $\alpha \in K$ sobre F es de **grado** n si existe un polinomio mónico $p(X)$ en $F[X]$ de grado n tal que $p(\alpha) = 0$ y ningún otro polinomio no nulo de grado menor en $F[X]$ tiene esta propiedad. Llamaremos al polinomio $p(X)$ el **polinomio mínimo de** α **sobre** F.

Observación 6.3.10. Notemos que el polinomio mínimo de todo elemento algebraico α siempre existe y es único. Como α es algebraico, el conjunto

$$\{m \in \mathbb{Z}_{\geq 0} : \exists p(X) \in F[X] \text{ mónico de } \mathrm{gr}(p(X)) = m \text{ y } p(\alpha) = 0\}$$

es no vacío, así que podemos tomar el mínimo de esos enteros no negativos, digamos n y el polinomio correspondiente $p(X)$. Ahora, si α es algebraico de grado n y $p(X)$ y $q(X)$ son dos polinomios mónicos de grado n tales que $p(\alpha) = q(\alpha) = 0$, entonces $h(X) = p(X) - q(X)$ es un polinomio tal que $\mathrm{gr}(h(X)) \leq n - 1 < n$ y $h(\alpha) = 0$. Lo cual implica que existe un polinomio mónico $h'(X)$ de grado menor que n tal que $h'(\alpha) = 0$; esto contradice que α es algebraico de grado n.

Proposición 6.3.11. *Sea α un elemento algebraico de grado n de K sobre F con polinomio mínimo $p(X)$ en $F[X]$. Entonces, $p(X)$ es irreducible en $F[X]$.*

Demostración. A cargo del lector. ■

Proposición 6.3.12. *Sea K un cuerpo extensión de un cuerpo F y sea $\alpha \in K$. Si $p(X)$ es un polinomio mónico e irreducible en $F[X]$ tal que $p(\alpha) = 0$, entonces $p(X)$ es el polinomio mínimo de α sobre F.*

Demostración. Sea $f(X)$ el polinomio mínimo de α. Por el algoritmo de la división para polinomios, tenemos que existen polinomios $q(X)$ y $r(X)$ de $F[X]$ tales que $p(X) = f(X).q(X)+r(X)$ con $r(X) = 0$ o $\mathrm{gr}(r) < \mathrm{gr}(f)$. Como $r(\alpha) = 0$ y $f(X)$ es el polinomio mínimo de α, tenemos que $r(X) = 0$. Entonces $p(X) = f(X)q(X)$. Ya que $p(X)$ es irreducible y $f(X)$ es no-constante, tenemos que $q(X) = cte = a \in F$. Pero, dado que $p(X)$ y $f(X)$ son mónicos, $q(X) = 1$ y así $p(X) = f(X)$; lo que muestra que $p(X)$ es el polinomio mínimo de α. ■

Ejemplo 6.3.13. Como hemos visto en el Ejemplo 6.3.7 (4), el número real $\alpha = \sqrt{1+\sqrt{3}}$ es una raíz del polinomio $p(X) = X^4 - 2X^2 - 2$, el cual pertenece a $\mathbb{Q}[X]$. Por el criterio Eisenstein con el número primo 2, podemos observar que $p(X) = X^4 - 2X^2 - 2$ es irreducible en $\mathbb{Q}[X]$. Entonces, por la Proposición 6.3.12, $p(X) = X^4 - 2X^2 - 2$ es el polinomio mínimo de $\alpha = \sqrt{1+\sqrt{3}}$ y así $\alpha = \sqrt{1+\sqrt{3}}$ es algebraico de grado 4 sobre $\mathbb{Q}$. ■

Sea F un cuerpo y sea K una extensión de F. Sea S un subconjunto de K. Denotemos por $F(S)$ a la intersección de todos los subcuerpos de K conteniendo a $F \cup S$. Es claro que $F(S)$ es un subcuerpo de K y es el menor subcuerpo de K tal que contiene a $F \cup S$. Se llama a $F(S)$ el **subcuerpo de K generado sobre F por** S. Si $S = \{\alpha_1, \ldots, \alpha_n\}$ es finito, escribimos $F(\alpha_1, \ldots, \alpha_n)$ en lugar de $F(S)$. Observemos que $F(S)$ es de hecho una extensión de F. También se puede comprobar sin mucha dificultad que $F(S \cup \{\alpha\}) = F(S)(\alpha)$, esto es, el subcuerpo de K generado sobre F por $S \cup \{\alpha\}$, $F(S \cup \{\alpha\})$, coincide con el subcuerpo de K generado sobre $F(S)$ por $\{\alpha\}$, $F(S)(\alpha)$.

Aquí estamos particularmente interesados en el caso que el conjunto S es unitario, digamos $S = \{\alpha\}$ con α algebraico de orden n. Como ya hemos hecho, en otros contextos, trataremos ahora de caracterizar al subcuerpo $F(\alpha)$ generado sobre F por α (algebraico de orden n).

Proposición 6.3.14. *Sea K un cuerpo extensión de F y sea $\alpha \in K$ algebraico de grado n sobre F. Entonces $F(\alpha) = \{f(\alpha) : f(X) \in F[X]\}$.*

Demostración. Probaremos que $F[\alpha] := \{f(\alpha) : f(X) \in F[X]\}$ es el menor subcuerpo de K que contiene a F y α. Considerando $f(X) = a$ (polinomio constante) con $a \in F$ y $g(X) = X$, tenemos que $F \cup \{\alpha\} \subseteq F[\alpha]$ y dado que todo elemento de $F[\alpha]$ es una combinación lineal de potencias de α, obtenemos que $F[\alpha] \subseteq K$. Es directo chequear que $F[\alpha]$ es de hecho un subanillo de K y así es un dominio de integridad. También podemos observar que $F[\alpha]$ es un espacio vectorial sobre el cuerpo F.

Sea $p(X)$ el polinomio mínimo de α sobre F. Sea $f(X) \in F[X]$. Por el algoritmo de la división, existen polinomios $q(X), r(X) \in F[X]$ tales que $f(X) = p(X).q(X) + r(X)$ con $r(X) = 0$ o $\mathrm{gr}(r(X)) < \mathrm{gr}(p(X))$. Así, $f(\alpha) = p(\alpha).q(\alpha) + r(\alpha)$ y con lo cual $f(\alpha) = r(\alpha)$. Como $r(X) = 0$ o $\mathrm{gr}(r(X)) < \mathrm{gr}(p(X))$, tenemos que $f(\alpha)$ es una expresión polinómica en α de grado $n-1$ a lo sumo. Entonces

$$\begin{aligned} F[\alpha] &= \{f(\alpha) : f(X) = a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in F[X]\} \\ &= \{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 : a_{n-1}, \ldots, a_1, a_0 \in F\}. \end{aligned} \tag{6.3}$$

Esto muestra que $F[\alpha]$ esta generado, como espacio vectorial, por los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Entonces, $F[\alpha]$ es de dimensión finita sobre F (con $\dim_F F[\alpha] \le n$). Luego, por el Lema 6.3.8, tenemos que de hecho $F[\alpha]$ es un cuerpo y así un subcuerpo de K. Solo nos resta probar que $F[\alpha]$ es el menor subcuerpo de K que contiene a $F \cup \{\alpha\}$. Sea F' un subcuerpo de K tal que $F \cup \{\alpha\} \subseteq F'$. Como todo elemento de $F[\alpha]$ es una combinación lineal de los elementos $1, \alpha, \ldots, \alpha^{n-1}$ sobre F, tenemos claramente que $F[\alpha] \subseteq F'$. Por lo tanto, tenemos demostrado que $F[\alpha]$ es el menor subcuerpo de K que contiene a $F \cup \{\alpha\}$ y esto muestra que $F[\alpha] = F(\alpha)$. ■

Ahora podemos concluir el siguiente resultado.

Teorema 6.3.15. *Sea K un cuerpo extensión de F y sea $\alpha \in K$ algebraico de grado n. Entonces, $F(\alpha)$ es una extensión finita de F y $[F(\alpha) : F] = n$.*

Demostración. Por lo probado en la proposición anterior podemos afirmar que $F(\alpha)$ es una extensión finita de F. Para ver que $[F(\alpha) : F] = n$, veamos que el conjunto generador $\{1, \alpha, \ldots, \alpha^{n-1}\}$ (ver (6.3)) es linealmente independiente sobre F. Denotemos por $p(X)$ al polinomio mínimo de α sobre F. Supongamos que $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ con $a_i \in F$. Luego, el polinomio $q(X) = a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ es tal que $q(\alpha) = 0$ y $\mathrm{gr}(q) < \mathrm{gr}(p)$, lo que contradice que $p(X)$ es el polinomio mínimo de α sobre F. Entonces $q(X) = 0$ y así $a_{n-1} = \cdots = a_1 = a_0 = 0$. Por lo tanto, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forma una base de $F(\alpha)$ sobre F; con lo cual $[F(\alpha) : F] = n$. Esto completa la demostración. ■

Para un cuerpo extensión K de F y un elemento algebraico α de K sobre F de grado n, llamaremos a $F(\alpha)$ una **extensión algebraica simple de** F. Además, por lo probado en la Proposición 6.3.14 y en el Teorema 6.3.15 tenemos que:

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F\}$$

y cada elemento de $F(\alpha)$ se escribe de forma única como $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ con $a_i \in F$.

Ejemplo 6.3.16.

(1) El número complejo $\sqrt{3}i$ es algebraico de grado 2 sobre $\mathbb{Q}$ con polinomio mínimo $p(X) = X^2 + 3$. Entonces, tenemos que

$$\mathbb{Q}(\sqrt{3}i) = \mathbb{Q}[\sqrt{3}i] = \{a + b\sqrt{3}i : a, b \in \mathbb{Q}\}$$

y $\mathbb{Q}(\sqrt{3}i)$ es una extensión finita de $\mathbb{Q}$ de grado 2.

(2) Probemos que $\sqrt{2} + \sqrt{3}$ es algebraico sobre $\mathbb{Q}$ y hallemos su polinomio mínimo. Consideremos la extensión $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Veamos primero que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Es claro que $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Entonces $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recíprocamente, como $(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 1$, se sigue que $\sqrt{3} - \sqrt{2} = (\sqrt{3} + \sqrt{2})^{-1} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Entonces podemos obtener que $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Luego, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Observemos que tenemos las siguientes extensiones:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Tenemos que $p(X) = X^2 - 2$ es el polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$. Entonces $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ y $\{1, \sqrt{2}\}$ es una base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. De forma similar podemos notar que $q(X) = X^2 - 3$ es el polinomio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$; entonces $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ y $\{1, \sqrt{3}\}$ es una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. Por lo tanto, por la Proposición 6.3.2, tenemos que

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})].[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.2 = 4$$

y $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$.

Por el Teorema 6.3.15 sabemos que el polinomio mínimo de $\sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$ debe ser de grado 4. Por otro lado, sea $\alpha = \sqrt{2} + \sqrt{3}$. Luego, $\alpha^2 = 5 + 2\sqrt{6}$ y así $(\alpha^2 - 5)^2 = 24$. Entonces, $\alpha^4 - 10\alpha^2 + 1 = 0$. Por lo tanto, podemos concluir que $X^4 - 10X^2 + 1$ es el polinomio mínimo de $\sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$. Además, observemos que por la Proposición 6.3.11 tenemos que el polinomio $X^4 - 10X^2 + 1$ es irreducible sobre $\mathbb{Q}$. ■

En el Ejemplo 6.3.7 (4) hemos indicado que los números e y π son trascendente. Ahora daremos una demostración, no constructiva, del hecho que números trascendentes existen. El argumento no constructivo que daremos para probar la existencia de números trascendentes es debido a Cantor. Comenzamos con el siguiente resultado.

Proposición 6.3.17. *Sean $F \subset K \subset L$ cuerpos extensiones y sea $\alpha \in L$. Si α es algebraico sobre F, entonces α es algebraico sobre K.*

Demostración. Es consecuencia de que todo polinomio sobre F es un polinomio sobre K, en otras palabras, $F[X] \subseteq K[X]$. ■

Proposición 6.3.18. *Sea K una extensión de un cuerpo F. Sea $\mathcal{A}(K)$ el conjunto de todos elementos algebraicos de K sobre F. Entonces, $\mathcal{A}(K)$ es un subcuerpo de K.*

Notemos que de hecho $\mathcal{A}(K)$ es además una extensión del cuerpo F; esto es, $F \subseteq \mathcal{A}(K) \subseteq K$.

Demostración. Sean $\alpha, \beta \in \mathcal{A}(K)$. Debemos probar que $\alpha - \beta \in \mathcal{A}(K)$ y $\alpha\beta^{-1} \in \mathcal{A}(K)$ si $\beta \neq 0$. Vamos a utilizar que $F(\alpha, \beta) = F(\alpha)(\beta)$ (ver p. 141). Es claro que $\alpha - \beta, \alpha\beta^{-1} \in F(\alpha, \beta) = F(\alpha)(\beta)$. Como $\beta \in K$ es algebraico sobre F y $F \subset F(\alpha) \subset K$, tenemos por la Proposición 6.3.17 que β es algebraico sobre $F(\alpha)$. Entonces, por el Teorema 6.3.15 sabemos que $[F(\alpha)(\beta) : F(\alpha)]$ es finito. Ahora, como $[F(\alpha, \beta) : F(\alpha)]$ y $[F(\alpha) : F]$ son finitos, se sigue de la Proposición 6.3.2 que $[F(\alpha, \beta) : F]$ es finito. Por el Corolario 6.3.6 sabemos que todo extensión finita es algebraica, entonces $\alpha - \beta, \alpha\beta^{-1} \in F(\alpha, \beta) \subset K$ son algebraicos sobre F, esto es, $\alpha - \beta, \alpha\beta^{-1} \in \mathcal{A}(K)$. ■

Teorema 6.3.19. *El cuerpo $\mathcal{A}(\mathbb{C})$ de números algebraicos es infinito numerable.*

Demostración. Sabemos que el cardinal de $\mathbb{Q}$ es $\aleph_0$ (infinito numerable). Ya que $\mathbb{Q} \subseteq \mathcal{A}(\mathbb{C})$, tenemos que $\#(\mathcal{A}(\mathbb{C})) \geq \aleph_0$.

Ahora, el número total de polinomios mónicos de grado n con coeficientes en $\mathbb{Q}$ es $\aleph_0^n = \aleph_0$. Cada polinomio mónico de grado n tiene a lo sumo n raíces complejas distintas; y así el número total de raíces de polinomios mónicos de grado n es a lo sumo de $n.\aleph_0 = \aleph_0$. Entonces, el número total de raíces de polinomios mónicos de todos los grados posibles es a lo sumo $\aleph_0.\aleph_0 = \aleph_0$. Por lo tanto, $\#(\mathcal{A}(\mathbb{C})) \leq \aleph_0$. Así obtenemos que $\#(\mathcal{A}(\mathbb{C})) = \aleph_0$. ■

Ahora, ya que sabemos que $\mathbb{C}$ es infinito no numerable, obtenemos directamente el resultado que buscábamos:

Corolario 6.3.20. *Existen números complejos trascendentes.*

Además, como $\#(\mathbb{C}) = 2^{\aleph_0} > \aleph_0$ y $\#(\mathcal{A}(\mathbb{C})) = \aleph_0$, tenemos que $\#(\mathbb{C} \setminus \mathcal{A}(\mathbb{C})) = 2^{\aleph_0} > \aleph_0 = \#(\mathcal{A}(\mathbb{C}))$ y así podemos decir "que hay más" números trascendentes que algebraicos.

6.4. Extensiones y polinomios

El objetivo de esta sección será mostrar un tipo de recíproca de los resultados en la sección anterior. En la sección anterior probamos que si α es un elemento algebraico de un cuerpo extensión K sobre un cuerpo F, entonces existe el polinomio mínimo de α sobre F y $F(\alpha)$ es una extensión finita de F. Ahora nos planteamos la siguiente situación: dado un cuerpo F y un polinomio irreducible $p(X)$ de $F[X]$, ¿existe un cuerpo K y un elemento $\alpha \in K$ tal que K sea una extensión finita de F y α sea algebraico sobre F con polinomio mínimo $p(X)$?

Teorema 6.4.1 (Kronecker)**.** *Sea F un cuerpo y sea $p(X)$ un polinomio mónico e irreducible de $F[X]$. Entonces, existe un cuerpo extensión K de F y un elemento α de K tal que $p(\alpha) = 0$.*

Demostración. Como el polinomio $p(X)$ es irreducible en $F[X]$, sabemos por la Proposición 5.2.5 que el ideal $\langle p(X)\rangle$ es maximal y así el anillo cociente $F[X]/\langle p(X)\rangle$ es un cuerpo. Podemos considerar sin perdida de generalidad que F es de hecho un subcuerpo de $K := F[X]/\langle p(X)\rangle$, ya que la función $\varphi\colon F \to F[X]/\langle p(X)\rangle$ definida por $\varphi(b) = b/\langle p(X)\rangle = b + \langle p(X)\rangle$, para cada $b \in F$, es un monomorfismo de anillos. Identificaremos a los elementos $b/\langle p(X)\rangle$ del cuerpo $K = F[X]/\langle p(X)\rangle$ simplemente con b, y a K como un cuerpo extensión de F. Ahora sólo nos resta mostrar que K contiene una raíz de $p(X)$. Sea $\alpha := X/\langle p(X)\rangle \in K$. Ahora evaluemos el polinomio $p(X)$ en α: si $p(X) = a_nX^n + \cdots + a_1X + a_0$, entonces

$$\begin{aligned} p(\alpha) &= a_n\alpha^n + \cdots + a_1\alpha + a_0 = a_n(X/\langle p(X)\rangle)^n + \cdots + a_1(X/\langle p(X)\rangle) + a_0 \\ &= (a_nX^n + \cdots + a_1X + a_0)/\langle p(X)\rangle = p(X)/\langle p(X)\rangle = 0 \end{aligned}$$

en $K = F[X]/\langle p(X)\rangle$. Por lo tanto, hemos encontrado que $\alpha \in K$ es tal que $p(\alpha) = 0$. Esto completa la demostración. ■

Observación 6.4.2. Una de las consecuencias que podemos extraer del teorema anterior es que todo polinomio no constante (el cual sabemos que puede ser factorizado en producto de polinomios irreducibles) con coeficientes en un cuerpo F tiene una raíz en algún cuerpo extensión K de F (véase específicamente el Corolario 6.4.4).

Ahora vamos a ver que el teorema anterior nos dice un poco más.

Corolario 6.4.3. *Para todo cuerpo F y todo polinomio mónico e irreducible $p(X)$ de $F[X]$ de grado n, existe una extensión finita K de F de grado n y un elemento $\alpha \in K$ tal que $p(X)$ es su polinomio mínimo.*

Demostración. Por el Teorema anterior tenemos que $K = F[X]/\langle p(X)\rangle$ es una extensión de F y $\alpha = X/\langle p(X)\rangle = X + \langle p(X)\rangle \in K$ es tal que $p(\alpha) = 0$. Ahora, como α es algebraico sobre F, tenemos por la Proposición 6.3.14 que $F(\alpha) = \{f(\alpha) : f(X) \in F(X)\}$. Sea $f(X) = a_0 + a_1X + \cdots + a_mX^m \in F(X)$. Entonces,

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \cdots + a_m\alpha^m \\ &= a_0 + a_1(X/\langle p(X)\rangle) + \cdots + a_m(X/\langle p(X)\rangle)^m \\ &= a_0 + a_1(X/\langle p(X)\rangle) + \cdots + a_m(X^m/\langle p(X)\rangle) \\ &= (a_0 + a_1X + \cdots + a_mX^m)/\langle p(X)\rangle \\ &= f(X)/\langle p(X)\rangle. \end{aligned}$$

Luego, hemos probado que $K = F[X]/\langle p(X)\rangle = F(\alpha)$. Ahora, como $p(X)$ es mónico e irreducible sobre F, tenemos por la Proposición 6.3.12 que $p(X)$ es el polinomio mínimo de α. Entonces $K = F(\alpha)$ es una extensión finita de F de grado $\mathrm{gr}(p) = n$. ■

Corolario 6.4.4. *Sea F un cuerpo y $f(X)$ un polinomio no constante de $F[X]$ de grado n. Entonces, existe una extensión finita K de F y $\alpha \in K$ tal que $f(\alpha) = 0$ y $[K : F] \leq n$.*

Demostración. Como $F[X]$ es un dominio euclideano (y así en particular un DIP), sabemos que $f(X)$ se puede factorizar en producto de polinomios irreducibles. Si $f(X)$ es de hecho irreducible, entonces estamos en las condiciones del corolario anterior. Supongamos que $f(X) = p(X).q(X)$ donde $p(X)$ es un polinomio irreducible de $F[X]$ y $q(X) \in F[X]$ (no necesariamente irreducible). Luego $\mathrm{gr}(p) < \mathrm{gr}(f)$. Aplicando el corolario anterior al polinomio $p(X)$, tenemos que existe una extensión finita K de F de grado $\mathrm{gr}(p)$ y un $\alpha \in K$ tal que $p(\alpha) = 0$. Por lo tanto, el cuerpo K y el elemento α son los deseados. ■

Ejemplo 6.4.5.

(1) Sea $F = \mathbb{R}$ y $p(X) = X^2 + 1$. Como $p(X)$ no tiene raíces en $\mathbb{R}$, tenemos que es irreducible en $\mathbb{R}[X]$. Denotemos por K al cuerpo $\mathbb{R}[X]/\langle p(X)\rangle$. Por el Corolario 6.4.3 sabemos que K es una extensión finita de $\mathbb{R}$ de grado 2 y además $K = \mathbb{R}(\alpha) = \{a + b\alpha : a, b \in \mathbb{R}\}$. También observemos que $p(\alpha) = 0$, esto es, $\alpha^2 = -1$. Por lo tanto, podemos observa que $K = \mathbb{R}(\alpha)$ no es otra cosa que el cuerpo $\mathbb{C}$ de números complejos.

(2) Sabemos que el polinomio $p(X) = X^2 + X + 1$ es irreducible en $\mathbb{Z}_2[X]$ (pues, no tiene raíces en $\mathbb{Z}_2$). Por el Teorema 6.4.1, existe un cuerpo extensión K de $\mathbb{Z}_2$ conteniendo una raíz α de $p(X) = X^2 + X + 1$. Como $p(X)$ es irreducible y mónico, es el polinomio mínimo de α sobre $\mathbb{Z}_2$. Entonces la extensión algebraica simple $\mathbb{Z}_2(\alpha)$ de $\mathbb{Z}_2$ es de grado 2; y tenemos que cada elemento β de $\mathbb{Z}_2(\alpha)$ se escribe de manera única como $\beta = a_0 + a_1\alpha$ con $a_0, a_1 \in \mathbb{Z}_2$. Esto es, los elementos de $\mathbb{Z}_2(\alpha)$ son 0, 1, α y $1 + \alpha$. Así, obtenemos un nuevo cuerpo con cuatro

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$.$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Cuadro 6.1: Operaciones en la extensión algebraica simple $\mathbb{Z}_2(\alpha)$ de $\mathbb{Z}_2$.

elementos. Las operaciones suma y producto en $\mathbb{Z}_2(\alpha)$ se pueden realizar fácilmente usando que $\alpha^2+\alpha+1=0$ (por ser α una raíz del polinomio $p(X)$), es decir, $\alpha^2=-\alpha-1=\alpha+1$. Ver el Cuadro 6.1 para las operaciones de suma y producto en el cuerpo $\mathbb{Z}_2(\alpha)$. Por ejemplo, $\alpha.(1+\alpha)=\alpha+\alpha^2=\alpha+\alpha+1=2\alpha+1=1$. ■

Proposición 6.4.6. *Sea F un cuerpo y sea $f(X)\in F[X]$ de grado n. Entonces existe una extensión finita K de F de grado a lo sumo $n!$ sobre F tal que $f(X)$ tiene n raíces, contando multiplicidades, en K.*

Demostración. Vamos a proceder por inducción sobre n. Si $n=1$, entonces f es de la forma $f(X)=aX+b$. Luego, F mismo es una extensión finita de F tal que $[F:F]=1!$ y $\alpha:=-b/a$ es una raíz de $f(X)$. Ahora supongamos que el resultado es válido para todo polinomio de grado n sobre un cuerpo y sea $f(X)$ un polinomio de $F[X]$ de grado $n+1$. Por el Corolario 6.4.4, tenemos que existe una extensión finita L de F y un elemento $\alpha_1\in L$ tal que $[L:F]\le n+1$ y $f(\alpha_1)=0$. Entonces, $f(X)$ se factoriza en $L[X]$ como $f(X)=(X-\alpha_1).g(X)$ para un polinomio $g(X)\in L[X]$. Como $\mathrm{gr}(g(X))=n$, podemos aplicar la hipótesis inductiva para afirmar que existe una extensión finita K de L de grado a lo sumo $n!$ tal que $g(X)$ tiene n raíces en K. Es claro que las n raíces de $g(X)$ son también raíces de $f(X)$. Por lo tanto, tenemos que $f(X)$ tiene $n+1$ raíces (no necesariamente distintas) en la extensión K y $[K:F]=[K:L].[L:F]\le n!.(n+1)=(n+1)!$. Esto completa la demostración. ■

Observación 6.4.7. Sea $f(X)$ un polinomio de grado n sobre un cuerpo F. Entonces, por la proposición anterior, existe una extensión finita K de F tal que $[K:F]\le n!$ y $f(X)$ se factoriza en $K[X]$ en un producto de polinomios lineales, esto es, existen $\alpha_1,\ldots,\alpha_n\in K$ (no necesariamente distintos) tales que

$$f(X)=\beta.(X-\alpha_1).\ldots.(X-\alpha_n).$$

6.5. Cuerpos finitos

El objetivo de esta sección es obtener una descripción de la estructura de "todos" los cuerpos finitos. Veremos que todo cuerpo finito es de orden p^n para un número primo p y n un entero positivo, y además que para cada número primo p y cada entero positivo n existe uno y sólo un cuerpo finito de p^n elementos, salvo isomorfismo. A dicho cuerpo se lo suele llamar el **cuerpo de Galois de orden p^n**.

Con los conceptos y resultados que ya tenemos a mano, por los capítulos anteriores, podemos probar ahora que el grupo multiplicativo de los elementos no nulos $\langle K^*, .\rangle$ de todo cuerpo finito K es cíclico. Probaremos un resultado un poco más fuerte y como corolario se obtendrá directamente esta afirmación.

Proposición 6.5.1. *Sea K un cuerpo. Si G es un subgrupo finito del grupo multiplicativo $\langle K^*, .\rangle$, entonces G es cíclico.*

Demostración. Como G es un grupo abeliano finito, sabemos por los Lemas 3.2.15 y 3.2.16 (ver también (3.1) en p. 67) que $G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$, donde cada d_i es la potencia de un número primo p_i (no necesariamente distintos). Vamos a considerar a cada grupo cíclico $\mathbb{Z}_{d_i}$ con la notación multiplicativa. Sea m el mínimo común múltiplo de los $d_1, d_2, \ldots, d_r$. Notemos que $m \leq d_1.d_2.\ldots.d_r$. Si $a \in \mathbb{Z}_{d_i}$, entonces $a^{d_i} = 1$ y así $a^m = 1$ ya que d_i divide a m. Entonces, para cada $\alpha \in G$, $\alpha^m = 1$ y así cada elemento de G es una raíz del polinomio $X^m - 1$. Como G tiene $d_1.d_2.\ldots.d_r$ elementos y el polinomio $x^m - 1$ tiene a lo sumo m raíces (ver Corolario 5.6.21), tenemos que $d_1.d_2.\ldots.d_r \leq m$. Luego $m = d_1.d_2.\ldots.d_r$. Esto prueba que los números primos $p_1, p_2, \ldots, p_r$ son todos distintos. Por lo tanto, si $n := d_1.d_2.\ldots.d_r$, tenemos que

$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} = \mathbb{Z}_n$$

lo prueba que G es cíclico. ■

Corolario 6.5.2. *Si K es un cuerpo finito, entonces el grupo multiplicativo $\langle K^*, .\rangle$ de elementos no nulos de K es cíclico.*

Ahora mostraremos que todo cuerpo finito es de orden la potencia de un número primo.

Sea K un cuerpo finito. Entonces sabemos que K es de característica un número primo p y que $P(K) = \{0, 1, 2, \ldots, (p-1)\} \cong \mathbb{Z}_p$ es el subcuerpo primo de K. Vamos a considerar que de hecho $\mathbb{Z}_p$ es el cuerpo primo de K, así $\mathbb{Z}_p \subseteq K$.

Proposición 6.5.3. *Sea F un cuerpo finito de orden r. Si K es una extensión finita de F de grado n, entonces K tiene r^n elementos.*

Demostración. Como K es una extensión de F de grado n, K tiene una base de n elementos sobre F, digamos $\{v_1, \ldots, v_n\}$. Entonces, todo elemento w de K se escribe de manera única en la forma

$$w = a_1v_1 + a_2v_2 + \cdots + a_nv_n$$

con $a_1, \ldots, a_n \in F$. Luego, ya que cada escalar a_i puede tomar cualquiera de los r elementos de F, tenemos que todas las posibilidades de elegir los a_i en F es r^n. ■

Proposición 6.5.4. *Sea K un cuerpo finito de característica p. Entonces K tiene p^n elementos para algún entero positivo n.*

Demostración. Ya que K es de característica $p \neq 0$, tenemos que $\mathbb{Z}_p \cong P(K)$ es un subcuerpo de K, en otras palabras, K es una extensión del cuerpo primo $\mathbb{Z}_p$. Como K es finito, es directo que K es un extensión finita de $\mathbb{Z}_p$, digamos $[K : \mathbb{Z}_p] = n$ para algún entero positivo n. Luego, por la proposición anterior, tenemos que K tiene p^n elementos. ■

Ahora la idea es probar que para todo número primo p y todo entero positivo n existe un único cuerpo K de orden p^n.

Lema 6.5.5. *Sea p un número primo y n un entero positivo. Entonces, el polinomio $f(X) = X^{p^n} - X$ de $\mathbb{Z}_p[X]$ no tiene raíces múltiples en ningún cuerpo de característica p.*

Demostración. Sea K cualquier cuerpo de característica p. Con lo cual K es una extensión de $\mathbb{Z}_p$. Es claro que 0 es una raíz del polinomio $f(X) = X^{p^n} - X = X(X^{p^n-1} - 1)$ y no es raíz del polinomio $X^{p^n-1} - 1$. Entonces 0 es una raíz simple de $f(X)$. Supongamos ahora que $\alpha \in K$ es una raíz de $f(X)$. Entonces $\alpha^{p^n} = \alpha$. Luego por la Proposición 6.1.6 tenemos lo siguiente:

$$f(X - \alpha) = (X - \alpha)^{p^n} - (X - \alpha) = X^{p^n} - \alpha^{p^n} - X + \alpha = X^{p^n} - X = f(X).$$

Con lo cual,

$$f(X) = f(X - \alpha) = (X - \alpha)^{p^n} - (X - \alpha) = (X - \alpha)\left[(X - \alpha)^{p^n-1} - 1\right].$$

Así podemos notar que $f(X)$ es divisible por $X - \alpha$ y como $(X - \alpha)^{p^n-1} - 1$ no es divisible por $X - \alpha$ (ya que es claro que α no es una raíz de $(X - \alpha)^{p^n-1} - 1$), entonces $(X - \alpha)^2$ no divide $f(X)$. Esto implica que α es una raíz simple (no múltiple) de $f(X) = X^{p^n} - X$. ■

Teorema 6.5.6. *Para todo entero primo p y cualquier entero positivo n, existe un cuerpo K de p^n elementos.*

Demostración. Consideremos el polinomio $f(X) = X^{p^n} - X$ de $\mathbb{Z}_p[X]$. Por la Observación 6.4.7, sabemos que existe un extensión finita K de $\mathbb{Z}_p$ tal que el polinomio $f(X)$ se factoriza en $K[X]$ como

$$f(X) = (X - \alpha_1). \dots .(X - \alpha_{p^n}).$$

Por el Lema 6.5.5, tenemos que las raíces $\alpha_1, \dots, \alpha_{p^n}$ son simples. Entonces $\alpha_1, \dots, \alpha_{p^n}$ son p^n elementos distintos de K. Además, por el Corolario 5.6.21, sabemos que $\alpha_1, \dots, \alpha_{p^n}$ son todas las raíces del polinomio $f(X) = X^{p^n} - X$, ya que $f(X)$ es de grado p^n.

Ahora tomemos el conjunto de todas las raíces de $f(X)$

$$A = \{\alpha \in K : f(\alpha) = 0\} = \{\alpha \in K : \alpha^{p^n} = \alpha\}.$$

Como vimos en el párrafo anterior, A tiene exactamente p^n elementos. Veamos ahora que A es un cuerpo, de hecho un subcuerpo de K. Es claro que $1 \in A$. Sean $\alpha, \beta \in A$. Luego, $(\alpha.\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha.\beta$ y entonces $\alpha.\beta \in A$. Para ver que $\alpha + \beta \in A$, notemos que K es de característica p (por ser una extensión finita de $\mathbb{Z}_p$), entonces por la Proposición 6.1.6 tenemos que $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta$. Luego, por ser A un subconjunto finito del cuerpo K cerrado bajo las operaciones de K (ver Ejercicio 6.1), obtenemos que A es un subcuerpo de K. Por lo tanto, A es un cuerpo con p^n elementos. ■

Ejercicios propuestos

Ejercicio 6.1. Sea K un cuerpo y sea $A \subseteq K$ finito tal que $1 \in A$ y A es cerrado bajo las operaciones de suma y producto de K. Entonces, A es un subcuerpo de K.

Ejercicio 6.2. Probar que todo subcuerpo de $\mathbb{R}$ contiene a $\mathbb{Q}$.
(*Sug.:Probar que todo subcuerpo de* $\mathbb{R}$ *contiene a* $\mathbb{Z}$*, y notar que* $\mathbb{Q}$ *es el cuerpo cociente de* $\mathbb{Z}$*.*)

Ejercicio 6.3. (a) Sea K un cuerpo de característica 0. Sea $Z = \{n.1_K : n \in \mathbb{Z}\}$. Probar que Z es un subanillo de K y es isomorfo a $\mathbb{Z}$.

(b) Sea $P(K) = \{m.1_K(n.1_K)^{-1} : m, n \in \mathbb{Z} \text{ con } n \neq 0\}$. Probar que $P(K)$ es un subcuerpo de K y es isomorfo a $\mathbb{Q}$.

Ejercicio 6.4. Sea K un cuerpo de característica p primo. Sea $P(K) = \{0_K, 1_K, 2.1_K, \ldots, (p-1).1_K\}$. Probar que $P(K)$ es un subcuerpo de K, y que es isomorfo a $\mathbb{Z}_p$.

Ejercicio 6.5. Probar que los cuerpos $\mathbb{Q}$ y $\mathbb{Z}_p$ no contienen subcuerpos propios no triviales.

Ejercicio 6.6. Probar que si K es una extensión finita del cuerpo $\mathbb{Z}_p$, entonces K es de característica p.

Ejercicio 6.7. Sea p primo. Sea $f(X)$ un polinomio de grado n irreducible de $\mathbb{Z}_p[X]$. Determinar la característica del cuerpo $\mathbb{Z}_p[X]/\langle f(X)\rangle$.

Ejercicio 6.8. Sea K un cuerpo y sea p un entero positivo. Probar que p es la característica de K si y sólo si p es el menor entero positivo n tal que $n.1_K = 0$.

Ejercicio 6.9. Sea L un cuerpo extensión de K tal que $[L : K]$ es un número primo. Probar que no existe un subcuerpo E de L tal que $K \subset E \subset L$.

Ejercicio 6.10. Probar la Proposición 6.3.11.

Ejercicio 6.11. Sea K un cuerpo extensión de F y sea $\alpha \in K$ algebraico sobre F con polinomio mínimo $p(X) \in F[X]$. Probar que si $f(X) \in F[X]$ es tal que $f(\alpha) = 0$, entonces $p(X)$ divide a $f(X)$.

Ejercicio 6.12. Sea K un cuerpo extensión de F. Sean $S \subseteq K$ y $\alpha \in K$. Probar que $F(S \cup \{\alpha\}) = F(S)(\alpha)$.

Ejercicio 6.13. Probar que los siguientes números son algebraicos sobre $\mathbb{Q}$.

(a) $\alpha = \sqrt{3} + \sqrt{7} \in \mathbb{R}$. (b) $\alpha = \sqrt{5}i \in \mathbb{C}$. (c) $\alpha = \sqrt{3} + \sqrt[3]{2} \in \mathbb{R}$.

Ejercicio 6.14.

(a) Encontrar $\left[\mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right) : \mathbb{Q}\left(\sqrt{15}\right)\right]$ (primero compruebe que $\mathbb{Q}\left(\sqrt{15}\right) \subset \mathbb{Q}\left(\sqrt{3}+\sqrt{5}\right)$).

(b) Probar que $\mathbb{Q}(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{15})(\sqrt{3}+\sqrt{5})$.

(c) Hallar una base de $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ sobre $\mathbb{Q}(\sqrt{15})$.

Ejercicio 6.15. (a) Probar que $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$.

(b) Hallar el polinomio mínimo de $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{3})$.

(c) Hallar el polinomio mínimo de $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ sobre $\mathbb{Q}$.

Ejercicio 6.16. Hallar el polinomio mínimo de $\sqrt{1+\sqrt{2}}$ sobre $\mathbb{Q}$. Probar que $\sqrt{1+\sqrt{2}} \notin \mathbb{Q}[\sqrt{2}]$ y hallar su polinomio sobre $\mathbb{Q}(\sqrt{2})$.

Ejercicio 6.17. Probar que $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-2+\sqrt{2})$.

Ejercicio 6.18. Describir los elementos de $\mathbb{Q}(\sqrt[3]{5})$ e ejemplificar el producto de alguno de sus elementos.

Ejercicio 6.19. Sea F un cuerpo y sea $p(X)$ un polinomio irreducible en $F[X]$. Si α es una raíz de $p(X)$ en alguna extensión K de F, entonces $F(\alpha)$ es isomorfo a $F[X]/\langle p(X)\rangle$. Además, si $\mathrm{gr}(p) = n$, entonces

$$F(\alpha) = \{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 : a_0, a_1, \ldots, a_{n-1} \in F\}.$$

Ejercicio 6.20. Encontrar un polinomio $p(X)$ en $\mathbb{Q}[X]$ tal que $\mathbb{Q}\left(\sqrt{1+\sqrt{5}}\right)$ sea isomorfo a $\mathbb{Q}[X]/\langle p(X)\rangle$.

Ejercicio 6.21. Sea $f(X) = X^3 + X + 1$ en $\mathbb{Z}_2[X]$. Suponga que α es una raíz de $f(X)$ en alguna extensión K de $\mathbb{Z}_2$. Determinar cuántos elementos tiene $F(\alpha)$. Describir los elementos de $F(\alpha)$ en termino de α. Hacer una tabla completa de la operación producto para $F(\alpha)$.

Ejercicio 6.22. Sea $F(\alpha)$ el cuerpo descrito en el Ejercicio 6.21.

(a) Expresar los elementos α^5, α^{-2} y α^{100} en la forma $c_0 + c_1\alpha + c_2\alpha^2$ (con $c_i \in \mathbb{Z}_2$).

(b) Probar que α^2 y $\alpha^2+\alpha$ son raíces del polinomio $f(X) = X^3 + X + 1$.

Ejercicio 6.23. Probar que si K y L son dos cuerpos finitos del mismo orden (misma cantidad de elementos), entonces son isomorfos.

Capítulo 7

Módulos

En este capítulo veremos los conceptos más básicos de la teoría de módulos. Podemos decir que un módulo es como un espacio vectorial, pero en lugar de usar un cuerpo como escalares se utiliza un anillo conmutativo.

A lo largo de este capítulo, A denotará siempre, a menos que se indique otra, un anillo conmutativo con unidad 1 o 1_A (si queremos enfatizar que es la unidad correspondiente al anillo A). También, trabajaremos con grupos abelianos, así que denotaremos a la operación del grupo por $+$, al elemento neutro del grupo por 0 y al opuesto de un elemento a por $-a$.

7.1. Definición y ejemplos. Submódulos.

Definición 7.1.1. Sea A un anillo conmutativo. Un **módulo sobre** A es un grupo abeliano M junto con un **producto escalar** $\cdot : A \times M \to M$, denota por $(a, m) \mapsto am$, tal que se cumplen las siguientes condiciones para todos $m, n \in M$, $a, b, 1 \in A$:

(M1) $a(m + n) = am + an$;

(M2) $(a + b)m = am + bm$;

(M3) $a(bm) = (ab)m$;

(M4) $1m = m$.

Llamaremos a M un A-**módulo**.

Ejemplo 7.1.2. (1) Todo espacio vectorial V sobre un cuerpo K es un K-módulo.

(2) Todo anillo conmutativo A, es en si mismo un A-módulo. Tenemos que $\langle A, +\rangle$ es un grupo abeliano, y el producto escalar es el producto mismo del anillo A.

(3) Todo ideal I de un anillo conmutativo A es un A-módulo.

(4) Por las propiedades de múltiplo, todo grupo abeliano G es un $\mathbb{Z}$-módulo. ■

Proposición 7.1.3. *Sea M un A-módulo. Entonces:*

1. $a0 = 0$, *para todo* $a \in A$.

2. $0m = 0$, *para todo* $m \in M$.

3. $(-1)m = -m$, *para todo* $m \in M$.

Definición 7.1.4. Sea M un A-módulo. Un subconjunto $N \subseteq M$ es llamado un A-**submódulo** de M si N es un subgrupo de M y cerrado bajo el producto escalar, esto es, para todo $n \in N$ y todo $a \in A$, $an \in N$.

Proposición 7.1.5. *Sea* M *un* A*-módulo y* $N \subseteq M$ *no vacío. Entonces las siguientes condiciones son equivalentes:*

1. N *es un* A*-submódulo de* M.

2. *Para todos* $n, n' \in N$ *y todo* $a \in A$, $n + n', an \in N$.

Ejemplo 7.1.6. Sea M un A-módulo.

1. Sea $a \in A$. Entonces el conjunto $aM = \{am : m \in M\}$ es un A-submódulo de M.

2. Sea I un ideal de A. Entonces el conjunto

$$IM := \{a_1m_1 + \cdots + a_km_k : a_i \in I \text{ y } m_i \in M\}$$

es un A-submódulo de M.

3. Sean S y T A-submódulos de M. Entonces el conjunto

$$S + T = \{s + t : s \in S \text{ y } t \in T\}$$

es un A-submódulo de M que contiene a S y T.

4. Si $\{S_\alpha : \alpha \in \Gamma\}$ es una familia de A-submódulos de M, entonces $\bigcap_{\alpha\in\Gamma} S_\alpha$ es también un A-submódulo. ■

Definición 7.1.7. Sea M un A-módulo. Sea $X \subseteq M$. El A-**submódulo generado por** X es el menor A-submódulo de M que contiene a X, y lo denotamos por $\langle X\rangle$.

Proposición 7.1.8. *Sea* M *un* A*-módulo. Sea* $X \subseteq M$*. Entonces:*

1. $\langle X\rangle = \bigcap\{S : S$ *es un* A*-submódulo de* M *y* $X \subseteq S\}$.

2. $\langle X\rangle = \{a_1x_1 + \cdots + a_kx_k : a_i \in A$ *y* $x_i \in X\}$.

Definición 7.1.9. Un A-módulo es **finitamente generado** si es generado por un conjunto finito.

7.2. Homomorfismos, módulo cociente, y teoremas de isomorfismos

Definición 7.2.1. Sean M y N dos A-módulos. Una función $f\colon M \to N$ es un **A-homomorfismo** si, para todos $m_1, m_2 \in M$ y todo $a \in A$ se cumplen:

(1) $f(m_1 + m_2) = f(m_1) + f(m_2)$;

(2) $f(am_1) = af(m_1)$.

Diremos que un A-homomorfismo $f\colon M \to N$ es un A-**monomorfismo** si f es inyectivo; diremos que f es un A-**epimorfismo** si f es sobreyectiva; y finalmente diremos que f es un A-**isomorfismo** si f es biyectiva.

Ejemplo 7.2.2. 1. Sean G y H dos grupos abelianos. Luego, ellos son $\mathbb{Z}$-módulos. Entonces, todo homomorfismo (de grupo) $f\colon G \to H$ es un $\mathbb{Z}$-homomorfismo.

2. Sea M un A-módulo. Para cada $a \in A$, la función $f_a\colon M \to M$ definida por $f_a(m) = am$, es un A-homomorfismo. ■

Definición 7.2.3. Sean M y N A-módulos, y sea $f\colon M \to N$ un A-homomorfismo. Se define el **Núcleo!A-homomorfismo** de f por $\mathrm{Nu}(f) = \{m \in M : f(m) = 0\}$.

Proposición 7.2.4. *Sea $f\colon M \to N$ un A-homomorfismo. Entonces:*

1. $\mathrm{Nu}(f)$ *es un A-submódulo de M.*

2. *f es un A-monomorfismo si y sólo si* $\mathrm{Nu}(f) = \{0\}$.

Sean M y N A-módulos. Se define el conjunto

$$\mathrm{Hom}_A(M, N) : \{f : f\colon M \to N \text{ es un } A\text{-homomorfismo}\}.$$

Sobre el conjunto $\mathrm{Hom}_A(M, N)$ se puede definir la siguiente operación: para todos $f, g \in \mathrm{Hom}_A(M, N)$, sea $f + g\colon M \to N$ definida por

$$(f + g)(m) = f(m) + g(m)$$

Para todo $m \in M$. También podemos definir un producto escalar $\cdot\colon A \times \mathrm{Hom}_A(M, N) \to \mathrm{Hom}(M, N)$ por: para cada $a \in A$ y $f \in \mathrm{Hom}_A(M, n)$, se define $af\colon M \to N$ por

$$(af)(m) = af(m)$$

para todo $m \in M$.

Proposición 7.2.5. *El conjunto* $\mathrm{Hom}_A(M, N)$ *con las operaciones antes definidas es un A-módulo.*

Definición 7.2.6. Sea M un A-módulo y sea N un A-submódulo de M. El A-**módulo cociente** de M por N es el grupo cociente M/N equipado con el producto escalar: $a(m+N) = am+N$. La función natural $\pi\colon M \to M/N$ dada por $\pi(m) = m+N$ es un A-homomorfismo.

Teorema 7.2.7 (Primer teorema de isomorfismo)**.** *Si $f\colon M \to N$ es un A-epimorfismo, entonces existe un A-isomorfismo $\varphi\colon M/\mathrm{Nu}(f) \to N$ tal que $f = \varphi \circ \pi$.*

Teorema 7.2.8 (Segundo teorema de isomorfismo)**.** *Sea M un A-módulo y sean S y T A-submódulos de M. Entonces,*

$$\frac{S}{S \cap T} \cong \frac{S+T}{T}.$$

Teorema 7.2.9 (Tercer teorema de isomorfismo)**.** *Sea M un A-módulo y sean S y T A-submódulos de M tales que $T \subseteq S \subseteq M$. Entonces,*

$$\frac{\frac{M}{T}}{\frac{S}{T}} \cong \frac{M}{S}.$$

Teorema 7.2.10 (Teorema de correspondencia)**.** *Sea T un A-submódulo de un A-módulo M. Entonces, hay una correspondencia biunívoca*

$$\varphi\colon \{S : S \text{ } A\text{-submódulo de } M \text{ tal que } T \subseteq S\} \to \{N : N \text{ } A\text{-submódulo de } M/T\}$$

dada por

$$\varphi(S) = S/T.$$

Proposición 7.2.11. *Un A-módulo M is cíclico si y sólo si $M \cong A/I$ para algún ideal I de A.*

Definición 7.2.12. Un A-módulo M es llamada **simple** si $M \neq \{0\}$ y no tiene A-submódulos propios no nulos. Es decir, M es simple si sus únicos A-submódulos son $\{0\}$ y M.

Proposición 7.2.13. *Un A-módulo M es simple si y sólo si $M \cong A/I$ para algún ideal maximal I de A.*

7.3. Productos y sumas directas

Sean M y N dos A-módulos. Recordemos que $M \times N$ con la operación

$$(m_1, n_1).(m_2, n_2) = (m_1.m_2, n_1.n_2)$$

es un grupo abeliano, llamado el grupo producto. Definiendo el siguiente producto escalar: para cada par ordenado $(m, n) \in M \times N$ y todo $a \in A$,

$$a(m, n) = (am, an)$$

tenemos que $M \times N$ es un A-módulo, llamado el **producto directo** de M por N.

Proposición 7.3.1. *Sea M un A-módulo y sean S y T A-submódulos de M. Las siguientes afirmaciones son equivalentes.*

1. *La función $f\colon S \times T \to (S+T)$ definida por $f(s,t) = s+t$ es un A-isomorfismo.*

2. *$S \cap T = \{0\}$.*

3. *Cada elemento m de $S+T$ se escribe de forma única como $m = s+t$ con $s \in S$ y $t \in T$.*

Si alguna de las condiciones de la proposición anterior se cumplen, diremos que la suma $S+T$ es **directa**, y lo denotaremos por $S \oplus T$.

Si M es un A-módulo tal que $M = S \oplus T$, diremos que S y T son **sumando directos de1** M.

Definición 7.3.2. Sea S un A-submódulo de un A-módulo M. Diremos que S es un **retracto** de M si existe un A-homomorfismo $f\colon M \to S$, llamado una **retracción**, tal que $f(s) = s$ para todo $s \in S$.

Proposición 7.3.3. *Un A-submódulo S es un sumando directo de un A-módulo M si y sólo si existe una retracción $\sigma\colon M \to S$.*

Definición 7.3.4. Un A-módulo M es dicho a ser **libre sobre un subconjunto** X de M si cada elemento m de M puede escribirse de forma única como combinación lineal de elementos de X. Esto es, para cada $n \in M$, existen únicos elementos no nulos $a_1, \ldots, a_n \in A$ y únicos elementos $x_1, \ldots, x_n \in X$ tal que $m = a_1x_1 + \cdots + a_nx_n$.

Si M es un A-módulo libre sobre el conjunto X, diremos que X es una **base** o un **conjunto de generadores libres** para M. También diremos que M es **libremente generado por** X.

Observación 7.3.5. Queremos enfatizar la unicidad en la representación de los módulos libres. Supongamos que M es un A-módulo libre sobre el conjunto X. Sea $m \in M$. Si m se puede escribir de dos formas como

$$m = a_1x_1 + \cdots + a_sx_s \quad \text{y} \quad m = b_1y_1 + \cdots + b_ty_t$$

con los a_i y los b_j no nulos, entonces $s = t$, $a_i = b_i$ y $x_i = y_i$ para todo $i = 1, 2, \ldots, s = t$.

Teorema 7.3.6. *Sea M un A-módulo libre sobre un subconjunto X. Entonces, para cada A-módulo N y cada función $f\colon X \to N$, existe un único A-homomorfismo $\varphi\colon M \to N$ tal que $\varphi(x) = f(x)$, para todo $x \in X$.*

Demostración. Sea N un A-módulo y $f\colon X \to N$ una función. Recordemos que cada elemento $m \in M$ se escribe de forma única como $m = a_1x_1 + \cdots + a_kx_r$ con $a_i \in A$ no nulos y $x_i \in X$. Definimos $\varphi\colon M \to N$ por: para cada $m = a_1x_1 + \cdots + a_kx_r$ de M,

$$\varphi(m) = a_1 f(x_1) + \cdots + a_k f(x_k).$$

De la unicidad en la forma de escribir m, se deduce que φ está bien definida. Es sencillo probar de forma directa que φ es un A-homomorfismo. Además, observemos que cada $x \in X$ se escribe de forma única como $x = 1_A x$. Entonces, $\varphi(x) = 1_A f(x) = f(x)$. ■

Proposición 7.3.7. *Sea M un A-módulo libremente generado por X y sea N un A-módulo libremente generado por Y. Si $X \cong Y$, entonces $M \cong N$.*

Teorema 7.3.8. *Para cualquier conjunto X existe un A-módulo libre $M(X)$ sobre el conjunto X.*

Demostración. Sea $M(X)$ el conjunto de todas las funciones $f\colon X \to A$ tal que $f(x) = 0$ para todo $x \in X$ salvo un número finito[1]. Definimos sobre $M(X)$ una operación y un producto escalar sobre el anillo A como sigue: para cada $f, g \in M(X)$ y $a \in A$:

$$(f+g)(x) = f(x) + g(x) \qquad \text{y} \qquad (af)(x) = af(x).$$

Es sencillo probar que efectivamente $M(X)$ con las operaciones recién definidas es un A-módulo. Ahora identificamos cada elemento x del conjunto X con la función f_x, donde $f_x(y) = 0$ para todo $y \neq x$ y $f_x(x) = 1_A$. Denotemos el conjunto de todas las funciones f_x, $x \in X$, por $\overline{X}$. Es claro que $X \cong \overline{X}$. Por la Proposición 7.3.7, es suficiente probar que $M(X)$ es libremente generado por $\overline{X}$. Sea $f \in M(X)$.

• Sea $\{x_1, \ldots, x_k\} \subseteq X$ tal que $f(x_i) \neq 0$, y $f(x) = 0$ para todo $x \neq x_i$, con $i = 1, \ldots, k$. Digamos que $f(x_i) = a_i$, para $i = 1, \ldots, k$. Para cada $i = 1, \ldots, k$, sea $f_{x_i}\colon X \to A$ dada por

$$f_{x_i}(x) = \begin{cases} 1 & \text{si } x = x_i \\ 0 & \text{si } x \neq x_i \end{cases}$$

Obviamente cada $f_{x_i} \in M(X)$. Entonces, se puede comprobar que $f = a_1 f_{x_1} + \cdots + a_k f_{x_k}$.

• Supongamos que $f = a_1 f_{x_1} + \cdots + a_s f_{x_s}$ y $f = b_1 f_{y_1} + \cdots + b_t f_{x_t}$ con los a_i y los b_j no nulos. Primero podemos comprobar que $\{x_1, \ldots, x_s\} = \{y_1, \ldots, y_t\}$. Supongamos que un $x_i \notin \{y_1, \ldots, y_t\}$. Entonces tenemos que:

$$f(x_i) = a_i \qquad \text{y} \qquad f(x_i) = 0$$

Con lo cual, $a_i = 0$. Absurdo!. Entonces, $\{x_1, \ldots, x_s\} \subseteq \{y_1, \ldots, y_y\}$. Análogamente, se puede obtener la otra inclusión. Así $s = t$ y $\{x_1, \ldots, x_s\} = \{y_1, \ldots, y_t\}$. Ahora para cada $i = 1, \ldots, s$, tenemos que $f(x_i) = a_i$ y $f(x_i) = b_i$. Entonces, $a_i = b_i$. ■

Corolario 7.3.9. *Si $X = \{x_1, \ldots, x_n\}$ es finito, entonces A^n es, salvo isomorfismo, el A-módulo libremente generado por X.*

Definición 7.3.10. Un elemento m de un A-módulo M es llamado un **elemento de torsión** si $am = 0$ para algún $a \in A$ no nulo. El conjunto de elementos de torsión de M es denotado por

$$T(M) = \{m \in M : am = 0 \text{ para algún } a \in A \text{ no nulo}\}.$$

Proposición 7.3.11. *Si A es un dominio de integridad y M es un A-módulo, entonces $T(M)$ es un A-submódulo de M.*

[1] En otras palabras, $M(X)$ es el conjunto de todas las funciones $f\colon Z \to A$ para las cuales el conjunto $\{x \in X : f(x) \neq 0_A\}$ es finito (posiblemente vacío).

Ejemplo 7.3.12. Consideramos el anillo $\mathbb{Z}_6$. Entonces $\mathbb{Z}_6$ es un $\mathbb{Z}_6$-módulo. Se tiene que $T(\mathbb{Z}_6) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Por ejemplo, $\overline{3}.\overline{4} = \overline{0}$, entonces ambos $\overline{3}$ y $\overline{4}$ están en $T(\mathbb{Z}_6)$. Pero $T(M)$ no es un $\mathbb{Z}_6$-submódulo de $\mathbb{Z}_6$, pues $\overline{1} + \overline{4} = \overline{5} \notin T(\mathbb{Z}_6)$. ■

Si A es un dominio de integridad y M es un A-módulo, el A-submódulo $T(M)$ es llamado **el A-submódulo torsión de** M.

Definición 7.3.13. Un A-módulo M es llamado un **A-módulo de torsión** si $T(M) = M$. Si $T(M) = \{0\}$, M es llamado A-**módulo libre de torsión**.

En otras palabras, un A-módulo M es un A-módulo torsión si para cada $m \in M$, existe un $a \in A$ no nulo tal que $am = 0$. En general, la existencia del a depende del m.

Ejemplo 7.3.14. Todo grupo abeliano finito es un $\mathbb{Z}$-módulo torsión. ■

Proposición 7.3.15. *Sea A un dominio de integridad, y sean M y N A-módulos. Sea $f\colon M \to N$ un A-homomorfismo. Entonces:*

1. *$T(M/T(M)) = \{0\}$.*
2. *Si N es libre de torsión, entonces $T(M) \subseteq \mathrm{Nu}(f)$.*
3. *Si M es de torsión, entonces $Im(f) \subseteq T(N)$.*

Ejercicios propuestos

Ejercicio 7.1. Sean A y B anillos conmutativos, y sea $f\colon A \to B$ un homomorfismo de anillos. Probar que si M es un B-módulo, entonces es posible definir un producto escalar tal que M sea también un A-módulo.

Ejercicio 7.2. Sean M y N dos A-módulos, y sea $f\colon M \to N$ una función. Probar que f es un A-homomorfismo si y sólo si para todos $a, b \in A$ y $m_1, m_2 \in M$ se cumple que

$$f(am_1 + bm_2) = af(m_1) + bf(m_2).$$

Ejercicio 7.3. Sea $M = \langle X \rangle$ un A-módulo generado por X. Probar que si $f, g\colon M \to N$ son dos A-homomorfismos tales que $f(x) = g(x)$ para todo $x \in X$, entonces $f = g$.

Ejercicio 7.4. Probar que efectivamente M/N de la Definición 7.2.6 es un A-módulo. Probar también que $\pi\colon M \to M/N$ es un A-homomorfismo.

Ejercicio 7.5. Sea $f\colon M \to N$ un A-homomorfismo y sea S un A-submódulo de N. Probar que $f^{-1}(S)$ es un A-submódulo de M tal que $\mathrm{Nu}(f) \subseteq f^{-1}(S)$.

Ejercicio 7.6. Sea A un anillo conmutativo. Probar que los A-submódulos de A (visto A como A-módulo) son exactamente los ideales de A.

Ejercicio 7.7. Sea M un A-módulo finitamente generado por el conjunto $X = \{x_1, \dots, x_k\}$. Sea F un A-módulo libremente generado por el conjunto $\{v_1, \dots, v_k\}$. Probar que existe un único A-epimorfismo $f\colon F \to M$ tal que $f(x_i) = v_i$.

Ejercicio 7.8. Sea A un anillo conmutativo con divisores de cero. Sea M A-módulo. Probar que $T(M) \neq \{0\}$. Es decir, probar que existe al menos un elemento de torsión no nulo.

Ejercicio 7.9. Sea M un A-módulo. Se define el conjunto

$$\overline{T}(M) := \{m \in M : am = 0 \text{ para algún } a \in A \text{ que no es un divisor de cero de } A\}.$$

Probar que $\overline{T}(M)$ es un A-submódulo de M.

Ejercicio 7.10. Sea P el conjunto de todos los enteros positivos primos. Supongamos que $P = \{p_1, p_2, \dots, p_k, \dots\}$. Sea M el conjunto de todas las sucesiones $\overline{a} = (a_1, a_2, \dots) \in \prod_{p \in P} \mathbb{Z}_p$ que tiene en todas sus coordenadas, salvo en un número finito, el valor cero. Entonces, M es un subgrupo del grupo abeliano producto $\prod_{p \in P} \mathbb{Z}_p$. Probar que el $\mathbb{Z}$-módulo M es un $\mathbb{Z}$-módulo torsión. Esto es, probar que $T(M) = M$.

Índice de símbolos

$Z(a)$	centralizador de a	48
A^*	los elementos no nulos del anillo A	75
$\mathrm{U}(A)$	el conjunto de los elementos invertibles del anillo A	75
$\langle X \rangle$	subanillo generado por X	78
$a \mid b$	a divide a b	97
$\mathbb{Z}[\sqrt{d}]$	dominio cuadrático	108
$\dim_K(V)$	dimensión del espacio vectorial V sobre el cuerpo K	136
$[K : F]$	grado de K sobre F	137
$F(S)$	subcuerpo generado sobre F por S	141
$F(a)$	extensión algebraica simple de F	142

Lista de comandos de GAP

Vamos a listar algunos de los comandos predefinidos de GAP, dando una breve explicación de cómo utilizarlo.

Comandos básicos

1. `quit;` Para cerrar el programa, o cuando se produce un error y queda `brk>`.

2. Utilizar la flecha $\uparrow$ para ir a los comandos anteriormente ingresados.

3. Ingresando `?divisors;` Le pedimos a GAP ayuda, en este caso, para hallar los divisores de un entero.

4. `:=` es para asignar un valor a una variable en GAP.

5. `k mod n;` Determina el resto de dividir `k` por `n`.

6. `Gcd(a,b);` Máximo común divisor entre `a` y `b`.

7. `Lcm(a,b);` Mínimo común múltiplo entre `a` y `b`.

8. `Gcdex(a,b);` Provee el máximo común divisor de `a` y `b`, junto con los valores s y t con los cuales se puede escribir al máximo común divisor como combinación lineal de `a` y `b`.
```
gap> Gcdex(4,15);
rec( coeff1:=4, coeff2:=-1, coeff3:=-15, coeff4:=4, gcd:=1)
gap>
```

Grupos

1. `sn:=SymmetricGroup(n);` Genera el grupo simétrico S_n de orden n.

2. `Dn:=DihedralGroup(IsPermGroup, 2n);` Genera el grupo Dihedral de orden n como un grupo permutación.

3. `CyclicGroup(IsPermGroup, n);` Genera una grupo cíclico de orden `n` como un grupo de permutaciones.

4. `GL(n,p);` Genera el grupo multiplicativo de las matrices cuadradas de orden `n` con entradas en $\mathbb{Z}_p$.

5. `SL(n,p);` Genera el grupo multiplicativo de las matrices cuadradas de orden `n` con entradas en $\mathbb{Z}_p$ cuyo determinante es igual a 1.

6. `An:=AlternatingGroup(n);` Genera el grupo alternante de orden `n`.

Propiedades sobre grupos

7. `Size(G);` Determina el orden del grupo `G`.

8. `Elements(G);` Lista (si es posible) los elementos del grupo `G`.

9. `Elements(G)[i];` Da el elemento del grupo `G` que ocupa el lugar `i`-ésimo en la lista que genera el comando `Elements(G)`.

10. `a:=Dn.i;` Asigna a la variable `a` el i-ésimo generador del grupo Dihedral `Dn`.

11. `Inverse(a);` Da como resultado el inverso de `a`.

12. `Order(a);` Da el orden del elemento `a`.

13. `IsAbelian(G);` Le pregunta a GAP si el grupo `G` es abeliano.

14. `IsCyclic(G);` Le pregunta a GAP si el grupo `G` es cíclico.

15. `Subgroup(G, [a,b]);` Genera el subgrupo de `G` generado por `a` y `b`.

16. `G=H;` Le pregunta a GAP si los grupos `G` y `H` son iguales.

17. `GeneratorsOfGroup(G);` Da como resultado un conjunto de generadores del grupo G.

18. `Intersection(G,h);` Genera el grupo que es intersección de los grupos `G` y `H`.

19. `GroupHomomorphismByImages(G,H,[lista de generadores de G], [lista de las imagenes de estos generadores]);`

20. `Center(G)` Genera el centro del grupo `G`.

21. `RightCosets(G,H);` Genera las clases laterales derechas del subgrupo `H`.

22. `Elements(RightCoset(H,a));` Da como resultado la clase del elemento `a` con respecto al subgrupo `H`.

23. `FactorGroup(G,H);` Genera el grupo cociente del grupo `G` con respecto al subgrupo normal `H`.

Algunos comandos extras de GAP

1. `Read("C:/Users/Dropbox/Algebra/GAP/nombre.txt");` GAP lee este archivo que contiene la función `nombre`. Ahora esta disponible para usarla en GAP.

2. `Read("C:/Users/Dropbox/Algebra/GAP/ulist.txt");` GAP lee este archivo que contiene la función `ulist`. Ahora esta disponible para usarla en GAP. Ejemplo:

   - `ulist(n);` Genera el grupo multiplicativo $U(n)$ de los enteros módulo n que son invertibles.

3. `cyclic(n,a);` Genera la lista de elementos del subgrupo cíclico de $U(n)$ generado por elemento `a` de $U(n)$.

4. `orderFrequency(G);` Determina la cantidad de elementos de cada orden del grupo `G`.

Índice alfabético

Bibliografía

[1] D. S. Dummit and R. M. Foote. *Abstract Algebra.* John Wiley & Sons, Inc., third edition, 2004.

[2] N. A. Fava. *El número.* Docencia S.A., Buenos Aires, 1978.

[3] J. B. Fraleigh. *A first course in abstract algebra.* Addison-Wesley, seven edition, 2003.

[4] J. Gallian. On the converse of Lagrange's Theorem. *Mathematics Magazine*, 66(1):23, 1993.

[5] J. Gallian. *Contemporary abstract algebra.* Cengage Learning, ninth edition, 2017.

[6] E. R Gentile. *Estructuras algebraicas.* Number 3 in Serie de Matemática. Unión Panamericana, 1967.

[7] E. R. Gentile. *Estructuras algebraicas II.* Secretaría General de la Organización de los Estados Americanos, 1971.

[8] I. N. Herstein. *Abstract Algebra.* Prentice-Hall, Inc., third edition, 1996.

[9] J. M. Howie. *Fields and Galois Theory.* Springer-Verlag, 2006.

[10] N. Jacobson. *Lectures in Abstract Algebra*, volume 30 of *Graduate Texts in Mathematics.* Springer-Verlag, 1951.

[11] W. J. LeVeque. *Elementary theory of numbers.* Dover Publications, 1990.

[12] J. Rivaud. *Ejercicios de Álgebra. Tomos 1-2..* Editorial Reverté S. A., 1981

[13] J. J. Rotman. *An Introduction to the Theory of Groups.* Springer-Verlag, fourth edition, 1995.

[14] J. J. Rotman. *Advanced Modern Algebra.* Prentice Hall, second edition, 2003.