

# Matemáticas

Roberto Cadena Vega

28 de diciembre de 2014



# Índice general

<b>1. Álgebra abstracta</b>	<b>7</b>
1.1. Grupos . . . . .	7
Definiciones . . . . .	7
Reglas de cancelación . . . . .	9
Subgrupos . . . . .	10
Subgrupo Normal . . . . .	16
Homomorfismos de grupo . . . . .	17
Teoremas de isomorfismos . . . . .	23
1.2. Anillos . . . . .	25
Definiciones . . . . .	25
Homomorfismos de anillo . . . . .	27
Ideales . . . . .	28
Teoremas de isomorfismos . . . . .	31
1.3. Dominios Enteros . . . . .	33
Definiciones . . . . .	33
Máximo Común Divisor . . . . .	33
mínimo común múltiplo . . . . .	34
Algoritmo de la división de Euclides . . . . .	34
<b>2. Álgebra lineal</b>	<b>39</b>
<b>3. Ecuaciones diferenciales</b>	<b>41</b>



# Todo list

Falta escribir ejemplo . . . . .	8
Falta escribir ejemplo . . . . .	34
Falta escribir ejemplo . . . . .	34



# Capítulo 1

# Álgebra abstracta

## 1.1. Grupos

### Definiciones

**Definición 1.1.1.** Un grupo es un conjunto no vacío  $G$  en el que está definida la operación  $\star$ , tal que:

$$\begin{aligned} \star: G, G &\rightarrow G \\ (a, b) &\rightarrow (a \star b) \end{aligned} \tag{1.1.1}$$

Existen definiciones parciales de grupo dependiendo de las propiedades que cumple su operación:

**Cerradura**  $a \star b \in G \quad \forall a, b \in G$

**Asociatividad**  $a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c, \in G$

**Identidad**  $\exists e \in G \ni a \star e = e \star a = a \quad \forall a \in G$

**Inverso**  $\exists b \in G \ni a \star b = b \star a = e \quad \forall a \in G$

Cuando se cumplen las propiedades de *cerradura* y *asociatividad* se le llama *semigrupo*; si adicionalmente se cumple la propiedad de *existencia de identidad* se le llama *monoide*; si adicionalmente se cumple la propiedad de *existencia de inverso* se le llama *grupo*.

**Ejercicio 1.1.1.** Demostrar que el grupo cimpuesto por las matrices de la forma:

$$\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}, \quad \forall \theta \in \mathbb{R}$$

es un grupo.

**Definición 1.1.2.** Se dice que un grupo  $G$  es abeliano si:

$$a \star b = b \star a$$

(1.1.2)

**Ejemplo 1.1.1.** El conjunto  $\mathbb{Z}/n\mathbb{Z}$

**Ejercicio 1.1.2.** Consideremos a  $\mathbb{Z}$  con el producto usual ¿Es este un grupo?

**Ejercicio 1.1.3.** Consideremos a  $\mathbb{Z}^+$  con el producto usual ¿Es este un grupo?

**Ejercicio 1.1.4.** Sea  $G = \mathbb{R} \setminus \{0\}$ . Si definimos  $a \star b = a^2b$  ¿ $G$  es un grupo?

**Definición 1.1.3.** Orden de un grupo es el numero de elementos que tiene dicho grupo y se denota por  $|G|$ .  
Un grupo  $G$  será finito si tiene orden finito, de lo contrario será infinito.

**Ejemplo 1.1.2.** Si  $G = \{e\}$ , su orden será  $|G| = 1$

**Ejemplo 1.1.3.** El orden del conjunto de numeros reales es infinito  $|\mathbb{R}| = \infty$ .

**Proposición 1.1.1.** Si  $G$  es un grupo, entonces:

1. El elemento identidad es único.
2. El elemento inverso  $a^{-1} \quad \forall a \in G$  es único.
3. El elemento inverso del inverso del un elemento del grupo es el mismo elemento  $(a^{-1})^{-1} = a \quad \forall a \in G$ .
4. El elemento inverso de la operación de dos elementos del grupo es la operacion de los inversos de los elementos en orden inverso  $(a \star b)^{-1} = b^{-1} \star a^{-1}$
5. En general lo anterior se cumple para cualquier numero de elementos  $(a_1 \star a_2 \star \dots \star a_n)^{-1} = a_n^{-1} \star \dots \star a_2^{-1} \star a_1^{-1}$ .

*Demostración.*

1. Dados  $e_1$  y  $e_2$  identidades del grupo, son identicos. Si aplicamos la identidad  $e_2$  a  $e_1$ , tenemos como resultado  $e_1$ , y si aplicamos la identidad  $e_1$  a  $e_2$  obtenemos como resultado  $e_2$ :

$$e_1 = e_2 \star e_1 = e_1 \star e_2 = e_2$$

por lo que podemos ver que ambas identidades son la misma.



2. Sean  $b, c$  inversos de  $a$ , entonces:

$$\begin{aligned}b \star a &= e \\ a \star c &= e\end{aligned}$$

por lo que podemos ver que:

$$b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c$$

3. Sabemos que existe un inverso  $a^{-1}$  tal que:

$$a \star a^{-1} = a^{-1} \star a = e \quad \forall a \in G$$

asi pues, se sigue que:

$$(a^{-1})^{-1} \star a^{-1} = e$$

y como sabemos que el elemento que operado con el inverso sea la identidad es el elemento mismo tenemos que:

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

4. Si operamos por la izquierda el termino  $b^{-1} \star a^{-1}$  con  $a \star b$ :

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

de la misma manera si operamos por la derecha:

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

por lo tanto:

$$b^{-1} \star a^{-1} = (a \star b)^{-1}$$

□

## Reglas de cancelación

**Proposición 1.1.2.** Sea  $G$  un grupo y  $a, b, c \in G$ , tendremos que:

$$\begin{aligned}a \star b = a \star c &\implies b = c \\ b \star a = c \star a &\implies b = c\end{aligned}\tag{1.1.3}$$

*Demostración.* Si tomamos en cuenta que  $a \star b = a \star c$ :

$$b = e \star b = \left(a^{-1} \star a\right) \star b = a^{-1} \star (a \star b) = a^{-1} \star (a \star c) = \left(a^{-1} \star a\right) \star c = e \star c = c$$

de la misma manera para  $b \star a = c \star a$ :

$$b = b \star e = b \star \left(a \star a^{-1}\right) = (b \star a) \star a^{-1} = (c \star a) \star a^{-1} = c \star \left(a \star a^{-1}\right) = c \star e = c$$

□

## Subgrupos

**Definición 1.1.4.** Un subconjunto no vacío  $H$  de un grupo  $G$  se llama subgrupo si  $H$  mismo forma un grupo respecto a la operación de  $G$ . Cuando  $H$  es subgrupo de  $G$  se denota  $H < G$  o  $G > H$ .

*Observación 1.1.1.* Todo grupo  $G$  tiene automáticamente dos subconjuntos triviales, el mismo  $G$  y la identidad  $\{e\}$ .

**Proposición 1.1.3.** Un subconjunto no vacío  $H \subset G$  es un subgrupo de  $G$  si y solo si  $H$  es cerrado respecto a la operación de  $G$  y  $a \in H \implies a^{-1} \in H$ .

*Demostración.* Teniendo que  $H$  es un subgrupo de  $G$  tenemos que  $H$  es un grupo, por lo que automáticamente se cumple la cerradura y la existencia del inverso dentro del subgrupo. Teniendo que  $H$  es cerrado, no vacío y  $a^{-1} \in H \quad \forall a \in H$ . Sabemos que  $a^{-1} \star a = e \in H$  debido a que  $H$  es cerrado. Además para  $a, b, c \in H$  sabemos que  $a \star (b \star c) = (a \star b) \star c$  debido a que se cumple en  $G$  y  $H$  hereda esta propiedad. Por lo que  $H$  es un grupo, y por lo tanto subgrupo de  $G$ . □

**Ejemplo 1.1.4.** Sea  $G = \mathbb{Z}$  con la suma usual y sea  $H$  el conjunto de los enteros pares, es decir:

$$H = \{2n | n \in \mathbb{Z}\}$$

¿Es  $H$  un subgrupo de  $G$ ?  
Empecemos con dos elementos  $a, b \in H$ , por lo que tenemos que:

$$\begin{aligned} a &= 2q \quad q \in \mathbb{Z} \\ b &= 2q' \quad q' \in \mathbb{Z} \end{aligned}$$

y al sumarlos tenemos que:

$$a + b = 2q + 2q' = 2(q + q') = 2q'' \quad q'' \in \mathbb{Z}$$

por lo que  $a + b \in H$ .  
Por otro lado, para  $a \in H$  existe un  $q \in \mathbb{Z}$  tal que  $a = 2q$ . Su inverso será:

$$-a = -2q = 2(-q)$$

por lo que existe  $q' = -q \in \mathbb{Z}$  tal que:

$$2q' = -a \in H$$

y por lo tanto  $H < \mathbb{Z}$ .

**Ejemplo 1.1.5.** Consideremos  $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$  con el producto usual, y un subconjunto  $\mathcal{U}$

$$\mathcal{U} = \{z \in \mathbb{C}^* \mid |z| = 1\}$$

¿Es  $\mathcal{U}$  un subgrupo de  $G$ ?

Dados dos elementos  $z_1, z_2 \in \mathcal{U}$  sabemos que  $|z_1| = |z_2| = 1$ , por lo tanto:

$$|z_1 z_2| = |z_1| |z_2| = 1$$

por lo que  $z_1 z_2 \in \mathcal{U}$ .

Por otro lado, para  $z \in \mathcal{U}$  tenemos que  $|z| = 1$ , y por lo tanto:

$$|z^{-1}| = |z|^{-1} = \frac{1}{|z|} = 1$$

por lo que  $z^{-1} \in \mathcal{U}$  y  $\mathcal{U} < \mathbb{C}^*$

**Ejemplo 1.1.6.** Sea  $G$  un grupo,  $a$  un elemento del grupo y  $C(a) = \{g \in G \mid g \star a = a \star g\}$  ¿Es  $C(a)$  subgrupo de  $G$ ?

Primero notamos que  $C(a)$  es no vacío debido a que al menos tiene a la identidad.

$$e \star a = a \star e \implies e \in C(a)$$

Ahora tomemos dos elementos  $g_1, g_2 \in C(a)$ , para los cuales:

$$g_1 \star a = a \star g_1$$

$$g_2 \star a = a \star g_2$$

Ahora, si operamos estos dos elementos tendremos:

$$(g_1 \star g_2) \star a = g_1 \star (g_2 \star a) = g_1 \star (a \star g_2) = (g_1 \star a) \star g_2 = (a \star g_1) \star g_2 = a \star (g_1 \star g_2)$$

por lo que  $g_1 \star g_2 \in C(a)$ .

Por último, podemos ver que:

$$a = a \star e = a \star (g \star g^{-1}) = (g \star a) \star g^{-1}$$

En donde para que el elemento inverso exista en  $C(a)$ , se debe de cumplir que  $g^{-1} \star a = a \star g^{-1}$ :

$$g^{-1} \star a = g^{-1} \star ((g \star a) \star g^{-1}) = g^{-1} \star (g \star a) \star g^{-1} = g^{-1} \star g \star a \star g^{-1} = e \star a \star g^{-1} = a \star g^{-1}$$

Por lo que  $C(a) < G$ .

**Ejercicio 1.1.5.** Sea  $X$  un conjunto no vacío. Consideremos  $G = \delta X$ . Sea  $a \in X$ ,  $H(a) = \{f \in \delta X \mid f(a) = a\}$ . Verificar que  $H \subset G$  es un subgrupo bajo la composición de funciones. Note que  $H(a)$  es no vacío, debido a que  $\text{id}_X \in H(a)$ .

**Definición 1.1.5.** Sea  $G$  un grupo y  $a \in G$ . El conjunto

$$A = \langle a \rangle = \left\{ a^i \mid i \in \mathbb{Z} \right\} \tag{1.1.4}$$

es un subgrupo de  $G$ .

$A$  es no vacío, puesto que  $a^0 = e \in A$ .

Por otro lado, para dos elementos  $a^i, a^j \in A$  tenemos que:

$$a^i a^j = a^{i+j} \in A$$

y para un elemento  $a^i \in A$ , tenemos que:

$$a^{-i} = \left(a^i\right)^{-1} = \left(a^{-1}\right)^i \in A$$

por lo que  $\langle a \rangle$  es un subgrupo. A este se le llama subgrupo cíclico de  $G$  generado por  $a$ .

**Definición 1.1.6.** Sea  $G$  un grupo, decimos que  $G$  es cíclico si  $G = \langle a \rangle$  para algún  $a \in G$ .

**Ejemplo 1.1.7.** Dado el grupo  $G = \{e\}$ , tenemos que el subgrupo cíclico generador de  $G$  es:

$$\langle e \rangle = \left\{ e^i \in G \mid i \in \mathbb{Z} \right\}$$

al operar este subgrupo tenemos:

$$\begin{aligned} e^1 &= e \\ e^2 &= e \star e = e \\ e^3 &= e \star e \star e = e \end{aligned}$$

por lo que obtenemos todos los elementos del grupo.

**Ejemplo 1.1.8.** Dado el grupo  $G = \{a, e\}$ , y la siguiente tabla para la operación del grupo:

$\star$	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

con esto, tenemos que el subgrupo ciclico generador de  $G$  es:

$$\langle a \rangle = \left\{ a^i \in G \mid i \in \mathbb{Z} \right\}$$

y al operar este subgrupo tenemos:

$$\begin{aligned} a^1 &= a \\ a^2 &= a \star a = e \end{aligned}$$

y obtenemos todos los elementos del grupo.

**Ejercicio 1.1.6.** Dado el grupo  $G = \{e, a, b\}$  y la operación:

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Encontrar el subgrupo cíclico generador.

**Ejercicio 1.1.7.** Dado el grupo  $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2 = \{[0], [1]\}$  con la operación  $[a] + [b]$ ; encontrar el subgrupo cíclico generador.

**Ejercicio 1.1.8.** Sea  $G$  un grupo en el que  $x^2 = e$  para todo  $x \in G$ . Verificar que  $G$  es abeliano, es decir  $a \star b = b \star a$ .

**Definición 1.1.7.** Sea  $G$  un grupo,  $H$  un subgrupo de  $G$  ( $H < G$ ), para  $a, b \in G$ , decimos que  $a$  es congruente con  $b$  mód  $H$ , denotado por:

$$a \cong b \text{ mód } H \quad (1.1.5)$$

si

$$a \star b^{-1} \in H \quad (1.1.6)$$

**Ejercicio 1.1.9.** Demostrar que  $\cong$  es una relación de equivalencia.

**Definición 1.1.8.** Si  $H$  es un subgrupo de  $G$  y  $a \in G$ , entonces

$$Ha = \{ha \mid h \in H\} \quad (1.1.7)$$

se llama clase lateral derecha de  $H$  en  $G$ .

**Lema 1.1.1.** Para todo  $a \in G$  se tiene que:

$$Ha = \{x \in G \mid a \cong x \text{ mód } H\} \quad (1.1.8)$$

**Demostración.** Sea un conjunto definido como  $[a] = \{x \in G \mid a \cong x \text{ mód } H\}$ , por verificar que  $Ha = [a]$ . Para verificar esto, tenemos que verificar que  $Ha \subseteq [a]$  y después que  $[a] \subseteq Ha$ .

Para verificar que  $Ha \subseteq [a]$  definimos un elemento  $h \in H$  y  $ha \in Ha$ , si ahora operamos  $a$  con  $(ha)^{-1}$  y verificamos que esta en  $H$ , podemos decir que  $a \cong ha \text{ mód } H$ :

$$a(ha)^{-1} = a(a^{-1}h^{-1}) = (aa^{-1})h^{-1} = h^{-1} \in H$$

por lo que podemos concluir que  $a \cong ha \text{ mód } H$ , lo que implica que  $ha \in [a]$ ; pero como  $ha$  es un elemento arbitrario de  $Ha$ , tenemos que:

$$Ha \subseteq [a]$$

Para verificar que  $[a] \subseteq Ha$  empezamos con un elemento  $x \in [a]$ , es decir  $a \cong x \pmod H$ , lo cual implica  $ax^{-1} \in H$ , en particular nos interesa:

$$(ax^{-1})^{-1} = xa^{-1} \in H$$

Por otro lado, sea  $h = xa^{-1} \in H$ , entonces tenemos que:

$$ha = (xa^{-1})a = x(a^{-1}a) = x \in Ha$$

por lo que podemos decir que:

$$[a] \subseteq Ha$$

y por lo tanto

$$[a] = Ha$$

□

**Teorema 1.1.1.** Sea  $G$  un grupo finito y  $H \subset G$ , entonces el orden de  $H$  divide al orden de  $G$

$$|H| \mid |G| \tag{1.1.9}$$

y esto implica que existe una  $k \in \mathbb{Z}$  tal que:

$$|G| = k|H| \tag{1.1.10}$$

A esto se le conoce como Teorema de Lagrange.

*Demostración.* Dado  $[a] = Ha$ , las clases de equivalencia forman una partición de  $G$ :

$$\begin{aligned} [a_1] \cup [a_2] \cup \dots \cup [a_k] &= G \\ [a_i] \cap [a_j] &= \emptyset \quad i \neq j \end{aligned}$$

Por otro lado, las clases laterales derechas forman una partición:

$$\begin{aligned} Ha_1 \cup Ha_2 \cup \dots \cup Ha_k &= G \\ Ha_i \cap Ha_j &= \emptyset \quad i \neq j \end{aligned}$$

Establezcamos una biyección:

$$\begin{aligned} Ha_i &\rightarrow H \\ ha_i &\rightarrow h \end{aligned}$$

es decir, el orden de  $Ha_i$  es el orden de  $H$

$$|Ha_i| = |H| \quad \forall 1 \leq i \leq k$$

entonces:

$$\begin{aligned} |G| &= |Ha_1| + |Ha_2| + \cdots + |Ha_k| \\ &= |H| + |H| + \cdots + |H| \\ |G| &= k|H| \end{aligned}$$

pero  $k \in \mathbb{Z}$ , entonces:

$$|H|/|G|$$

□

**Definición 1.1.9.** Si  $G$  es finito y  $H$  es un subgrupo de  $G$  llamamos  $\frac{|G|}{|H|}$  el índice de  $H$  en  $G$  y lo denotamos por  $i_G(H)$ .

**Definición 1.1.10.** Si  $G$  es finito y  $a \in G$ , llamamos orden de  $a$  al mínimo entero positivo  $n$  tal que  $a^n = e$  y lo denotamos por  $O(a)$ , por lo que se sigue que:

$$a^{O(a)} = e \tag{1.1.11}$$

**Proposición 1.1.4.** Si  $G$  es finito y  $a \in G$ , entonces el orden de  $a$  divide al orden de  $G$ :

$$O(a)/|G| \tag{1.1.12}$$

*Demostración.* Supongamos  $H = \langle a \rangle$ , entonces  $O(a) = |H|$ . Podemos ver ahora, por el teorema de Lagrange:

$$|H|/|G| \implies O(a)/|G|$$

□

**Corolario 1.1.1.** Si  $G$  es un grupo finito de orden  $n$ , entonces:

$$a^n = e \quad \forall a \in G \tag{1.1.13}$$

*Demostración.* Por la proposición anterior tenemos que:

$$O(a)/|G| = O(a)/n$$

esto equivale a decir que existe un  $k \in \mathbb{Z}$ , tal que  $n = kO(a)$ , entonces podemos decir:

$$a^n = a^{kO(a)} = \left(a^{O(a)}\right)^k = e^k = e \quad \forall a \in G$$

□

# Subgrupo Normal

**Definición 1.1.11.** Un grupo  $N$  de  $G$  se dice que es un subgrupo normal de  $G$  denotado por  $N \triangleleft G$ , si para todo  $g \in G$  y para todo  $n \in N$  se tiene que:

$$gng^{-1} \in N \quad (1.1.14)$$

**Lema 1.1.2.**  $N$  es un subgrupo normal de  $G$  si y solo si:

$$gNg^{-1} = N \quad \forall g \in G \quad (1.1.15)$$

*Demostración.* Si  $gNg^{-1} = N \quad \forall g \in G$ , entonces en particular tenemos que:

$$gNg^{-1} \subseteq N$$

por lo que se tiene que  $gng^{-1} \in N \quad \forall n \in N$ , por lo tanto  $N \triangleleft G$ .

Por otro lado, si  $N$  es un subgrupo normal de  $G$ , entonces tenemos que:

$$gng^{-1} \in N$$

para todo  $g \in G$  y para todo  $n \in N$ , esto implica que:

$$gNg^{-1} \subseteq N$$

Por ultimo, podemos ver que  $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subseteq N$ , ademas:

$$N = eNe = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$$

por lo tanto, podemos concluir que  $gNg^{-1} = N$  □

**Lema 1.1.3.** El subgrupo  $N$  de  $G$ , es un subgrupo normal de  $G$  ( $N \triangleleft G$ ), si y solo si toda clase lateral izquierda de  $N$  en  $G$  es una clase lateral derecha de  $N$  en  $G$ .

*Demostración.* Sea  $aH = \{ah \mid h \in H\}$  la clase lateral izquierda de  $H$ .

Si  $N$  es un subgrupo normal de  $G$ , para todo  $g \in G$  y para todo  $n \in N$ , tenemos que:

$$gNg^{-1} = N$$

entonces tenemos que:

$$gN = gNe = gN(g^{-1}g) = (gNg^{-1})g = Ng$$

por lo que toda clase lateral izquierda coincide con la clase lateral derecha.

Por otro lado, si ahora suponemos que las clases laterales coinciden, entonces:

$$gNg^{-1} = (gN)g^{-1} = Ngg^{-1} = N$$

por lo que podemos concluir que se trata de un subgrupo normal. □



**Definición 1.1.12.** Denotamos  $G/N$  a la colección de las clases laterales derechas de  $N$  en  $G$ .

$$G/N = \{Na \mid a \in G\} \tag{1.1.16}$$

**Teorema 1.1.2.** Si  $G$  es un grupo y  $N$  es un subgrupo normal de  $G$ , entonces  $G/N$  es tambien un grupo y se denomina grupo cociente.

*Demostración.* Para demostrar la existencia de identidad primero verificamos que para un elemento  $x \in G/N$ , el elemento tiene la forma  $x = Na \quad a \in G$ , por lo que podemos ver que:

$$\begin{aligned} xNe &= xN = NaN = NNa = Na = x \\ Nex &= Nx = NNa = Na = x \end{aligned}$$

□

Para demostrar la existencia de un inverso definimos un elemento  $x \in G/N$  y  $Na^{-1} \in G/N$ , y queremos demostrar que  $x^{-1} = Na^{-1}$  es el inverso de  $x = Na$ . Al operar estos elementos por la derecha y la izquierda tenemos:

$$\begin{aligned} xx^{-1} &= NaNa^{-1} = NNa^{-1} = Ne = N \\ x^{-1}x &= Na^{-1}Na = NNa^{-1}a = Ne = N \end{aligned}$$

por lo tanto  $Na^{-1} = x^{-1}$  es el inverso de  $x$ . Por lo tanto,  $G/N$  es un grupo.

## Homomorfismos de grupo

**Definición 1.1.13.** Sea una aplicación  $\varphi: G \rightarrow \tilde{G}$ ,  $G$  un grupo con operacion  $\circ$  y  $\tilde{G}$  un grupo con operación  $\diamond$ . Se dice que  $\varphi$  es un homomorfismo si para  $a, b \in G$  cualesquiera se tiene que:

$$\varphi(a \circ b) = \varphi(a) \diamond \varphi(b) \tag{1.1.17}$$

**Ejemplo 1.1.9.** Sea  $G = \mathbb{R}^+ \setminus \{0\}$ , bajo el producto usual y sea  $\tilde{G} = \mathbb{R}$  bajo la adición, definimos  $\varphi: G \rightarrow \tilde{G}$  como:

$$\begin{aligned} \varphi: \mathbb{R}^+ \setminus \{0\} &\rightarrow \mathbb{R} \\ r &\rightarrow \ln r \end{aligned}$$

Sean  $r_1, r_2 \in \mathbb{R}^+ \setminus \{0\}$  tal que:

$$\varphi(r_1 \cdot r_2) = \ln (r_1 \cdot r_2) = \ln r_1 + \ln r_2 = \varphi(r_1) + \varphi(r_2)$$

por lo que podemos asegurar que  $\varphi$  es un homomorfismo.

**Lema 1.1.4.** Supongamos que  $G$  es un grupo y que  $N$  es un subgrupo normal de  $G$ . Definamos la aplicación:

$$\begin{aligned}\varphi: G &\rightarrow G/N \\ x &\rightarrow Nx\end{aligned}$$

entonces  $\varphi$  es un homomorfismo.

*Demostración.* Sean  $x, y \in G$ , entonces  $\varphi(x) = Nx$  y  $\varphi(y) = Ny$ , por lo que podemos ver que:

$$\varphi(x \circ y) = Nxy = NNxy = NxNy = \varphi(x) \diamond \varphi(y)$$

por lo que  $\varphi$  es un homomorfismo. □

**Definición 1.1.14.** Si  $\varphi$  es un homomorfismo de  $G$  en  $\bar{G}$ , el nucleo de  $\varphi$ , denominado  $\ker \varphi$  se define:

$$\ker \varphi = \{x \in G \mid \varphi(x) = \bar{e}\} \tag{1.1.18}$$

donde  $\bar{e}$  es la identidad de  $\bar{G}$ .

**Lema 1.1.5.** Si  $\varphi$  es un homomorfismo de  $G$  en  $\bar{G}$ , entonces:

1.  $\varphi(e) = \bar{e}$
2.  $\varphi(x^{-1}) = \varphi(x)^{-1} \quad \forall x \in G$

*Demostración.* Para demostrar la primera parte tenemos un elemento  $x \in G$ , por lo que:

$$\varphi(x) \diamond \bar{e} = \varphi(x) = \varphi(x \circ e) = \varphi(x) \diamond \varphi(e)$$

por lo que  $\bar{e} = \varphi(e)$

Para demostrar la segunda parte, notamos que:

$$\begin{aligned}\bar{e} = \varphi(e) &= \varphi(x \circ x^{-1}) = \varphi(x) \diamond \varphi(x^{-1}) = \bar{e} \\ &= \varphi(x^{-1} \circ x) = \varphi(x^{-1}) \diamond \varphi(x) = \bar{e}\end{aligned}$$

por lo que  $\varphi(x)^{-1} = \varphi(x^{-1})$ . □

**Ejercicio 1.1.10.** Sea  $G$  un grupo abeliano, tenemos que:

$$\begin{aligned}\varphi: G &\rightarrow G \\ a &\rightarrow a^2\end{aligned}$$

Verificar que  $\varphi$  es un homomorfismo.

**Ejercicio 1.1.11.** Sea  $G$  y  $G'$  dos grupos y sea  $e'$  la identidad en  $G'$ , entonces:

$$\begin{aligned}\varphi: G &\rightarrow G' \\ g &\rightarrow e'\end{aligned}$$

verificar que  $\varphi$  es un homomorfismo.

**Ejercicio 1.1.12.** La identidad dada por:

$$\begin{aligned}\text{id}_G: G &\rightarrow G \\ g &\rightarrow g\end{aligned}$$

verificar que  $\text{id}_G$  es un homomorfismo.

**Ejercicio 1.1.13.** Sea  $G = \mathbb{Z}$  con la suma usual y  $G' = \{1, -1\}$  con el producto usual. Si definimos:

$$\begin{aligned}\varphi: \mathbb{Z} &\rightarrow \{1, -1\} \\ n &\rightarrow \begin{cases} 1 & \text{si } n \text{ es par} \\ -1 & \text{si } n \text{ es impar} \end{cases} \quad \forall n \in G\end{aligned}$$

¿Será  $\varphi$  un homomorfismo?

**Ejercicio 1.1.14.** Sean  $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$  con el producto correspondiente y  $G' = \mathbb{R}^+$  con el producto correspondiente. Entonces definimos:

$$\begin{aligned}\varphi: \mathbb{C}^* &\rightarrow \mathbb{R}^+ \\ z &\rightarrow |z|\end{aligned}$$

¿Será  $\varphi$  un homomorfismo?

**Ejercicio 1.1.15.** Definimos:

$$\begin{aligned}\varphi: \mathbb{Z} &\rightarrow \mathbb{Z}_n \\ a &\rightarrow [a]\end{aligned}$$

y sabemos que:

$$[a + b] = [a] + [b]$$

¿Será  $\varphi$  un homomorfismo?

**Definición 1.1.15.** Un homomorfismo  $\varphi: G \rightarrow G'$  se dice que es:

**Monomorfismo** si es inyectivo (1 - 1).

**Epimorfismo** si es suprayectivo (sobre).

**Isomorfismo** si es biyectivo (1 - 1 y sobre).

**Definición 1.1.16.** Si  $\varphi: G \rightarrow G'$  es un isomorfismo, decimos que  $G$  y  $G'$  son isomorfos y escribimos:

$$G \cong G' \quad (1.1.19)$$

**Proposición 1.1.5.** Si  $\varphi: G \rightarrow G'$  es un homomorfismo, entonces:

$$\text{im } \varphi < G' \quad (1.1.20)$$

donde:

$$\text{im } \varphi = \{x \in G, y \in G' \mid \varphi(x) = y\} \subset G' \quad (1.1.21)$$

*Demostración.* Para demostrar que  $\text{im } \varphi$  es un subgrupo de  $G'$ , tenemos que demostrar que esta contenido en  $G'$  y que es grupo, pero por definición sabemos que  $\text{im } \varphi \subset G'$ , por lo que solo nos queda demostrar que es un grupo. Para demostrar que es un grupo, pasamos a verificar la cerradura y la existencia de un inverso.

Para demostrar la propiedad de cerradura, tomamos dos elementos  $y_1, y_2 \in \text{im } \varphi$  tales que tienen la forma:

$$\begin{aligned} y_1 &= \varphi(x_1) \in G' & x_1 &\in G \\ y_2 &= \varphi(x_2) \in G' & x_2 &\in G \end{aligned}$$

por lo que al operarlos entre si tenemos:

$$y_1 y_2 = \varphi(x_1) \varphi(x_2) = \varphi(x_1 x_2) = y_1 y_2 \in \text{im } \varphi$$

Por otro lado, para demostrar la existencia de un inverso, operamos un elemento  $y = \varphi(x) \in \text{im } \varphi$  con el elemento  $\varphi(x^{-1})$ , el cual queremos demostrar es el inverso.

$$\begin{aligned} \varphi(x) \varphi(x^{-1}) &= \varphi(x x^{-1}) = \varphi(e) = e' \in G' \\ \varphi(x^{-1}) \varphi(x) &= \varphi(x^{-1} x) = \varphi(e) = e' \in G' \end{aligned}$$

por lo que se concluye que el inverso es:

$$\varphi(x)^{-1} = \varphi(x^{-1})$$

y por lo tanto  $\text{im } \varphi$  es subgrupo de  $G'$ . □

**Definición 1.1.17.** Sea  $\varphi: G \rightarrow G'$  un homomorfismo, el nucleo de  $\varphi$  es:

$$\ker \varphi = \{a \in G \mid \varphi(a) = e'\} \subset G \tag{1.1.22}$$

*Observación 1.1.2.*

$$\ker \varphi = \left\{ \varphi^{-1}(e') \mid a = \varphi^{-1}(e'), a \in G \right\} \tag{1.1.23}$$

son las preimagenes de  $e'$ .

**Proposición 1.1.6.** Sea  $\varphi: G \rightarrow G'$  un homomorfismo. Entonces  $\varphi$  es un monomorfismo, si y solo si:

$$\ker \varphi = \{0\} \tag{1.1.24}$$

es decir  $e = 0 \in G$ .

*Demostración.* Si suponemos que  $\ker \varphi = \{0\}$ , tenemos que para dos elementos  $\varphi(x_1)$  y  $\varphi(x_2)$  iguales:

$$\begin{aligned} \varphi(x_1) &= \varphi(x_2) \\ \varphi(x_1) - \varphi(x_2) &= 0 \\ \varphi(x_1 - x_2) &= 0 \end{aligned}$$

por lo que  $x_1 - x_2 \in \ker \varphi$ , lo cual implica que:

$$\begin{aligned} x_1 - x_2 &= 0 \\ x_1 &= x_2 \end{aligned}$$

por lo que podemos concluir que  $\varphi$  es un monomorfismo. □

**Teorema 1.1.3.** Si  $\varphi$  es un homomorfismo, entonces se satisface que:

1.  $\ker \varphi < G$
2.  $a^{-1} \ker \varphi a \subseteq \ker \varphi \quad \forall a \in G$

*Demostración.* Sabemos que  $\ker \varphi \neq \emptyset$ , ya que existe un  $e \in G$  tal que  $\varphi(e) = e'$ . Por lo que pasamos a comprobar que  $\ker \varphi$  es un grupo, ya que por definición  $\ker \varphi \subset G$ . Para comprobar que  $\ker \varphi$  definimos dos elementos  $x, y \in \ker \varphi$ , por lo que al operarlos entre si tenemos:

$$\varphi(xy) = \varphi(x)\varphi(y) = e'e' = e'$$

por lo que  $xy \in \ker \varphi$ .

Por otro lado, para un elemento  $x \in \ker \varphi$ , para el cual  $\varphi(x) = e'$ , tenemos que:

$$\varphi(x^{-1}) = \varphi(x^{-1})e' = \varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = e'$$

por lo que podemos ver que existe un inverso  $x^{-1} \in \ker \varphi$  y por lo tanto concluir que  $\ker \varphi < G$ .

Para comprobar la segunda proposición tomamos un elemento  $a \in G$  y un elemento  $g \in \ker \varphi$ , para el cual  $\varphi(g) = e'$ , por lo que queremos verificar que:

$$a^{-1}ga \in \ker \varphi \quad \forall g \in \ker \varphi$$

Sabemos que cualquier elemento en  $\ker \varphi$ , al evaluarlo en  $\varphi$ , obtendremos la identidad, por lo que procederemos a tratar de obtenerla:

$$\begin{aligned} \varphi(a^{-1}ga) &= \varphi(a^{-1})\varphi(g)\varphi(a) = \varphi(a^{-1})e'\varphi(a) \\ &= \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e' \end{aligned}$$

por lo que podemos concluir que:

$$\varphi(a^{-1}ga) \in \ker \varphi$$

□

**Observación 1.1.3.**  $\ker \varphi$  es un subgrupo normal de  $G$ .

**Ejercicio 1.1.16.** Sea  $\varphi$  definida como:

$$\begin{aligned} \varphi: \mathbb{Z} &\rightarrow \{-1, 1\} \\ n &\rightarrow \begin{cases} -1 & \text{si } n \text{ es par} \\ 1 & \text{si } n \text{ es impar} \end{cases} \quad \forall n \in \mathbb{Z} \end{aligned}$$

Verificar si  $\varphi$  es monomorfismo.

**Ejercicio 1.1.17.** Sea  $\varphi$  definida como:

$$\begin{aligned} \varphi: \mathbb{C}^* &\rightarrow \mathbb{C}^* \\ z &\rightarrow |z| \end{aligned}$$

¿Será  $\varphi$  un monomorfismo?

**Proposición 1.1.7.** Sea  $G$  un grupo y  $N$  un subgrupo normal de  $G$ . Existe un epimorfismo  $\varphi: G \rightarrow G/N$  cuyo nucleo es  $N$ .

**Demostración.** Sea  $\varphi$  definida como:

$$\begin{aligned} \varphi: G &\rightarrow G/N \\ a &\rightarrow [a] \end{aligned}$$

sean  $a, b \in G$  tales que al operarlos tenemos que:

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

por lo que podemos concluir que  $\varphi$  es un homomorfismo. Ahora, como  $\varphi$  es sobre por construcción, sabemos que  $\varphi$  es un epimorfismo, es decir, si  $[a] \in G/N$  existe un  $a \in G$  tal que  $\varphi(a) = [a]$ . Si ahora tenemos un elemento  $a \in \ker \varphi$ , esto implica que  $\varphi(a) = [e]$ , es decir:

$$a \cong e \pmod{N}$$

lo cual implica:

$$ae^{-1} \in N$$

$$ae \in N$$

$$a \in N$$

por lo que podemos concluir que  $\ker \varphi \subseteq N$ . □

## Teoremas de isomorfismos

**Teorema 1.1.4.** Sea  $\varphi$  definido por:

$$\begin{aligned} \varphi: G &\rightarrow G' \\ g &\rightarrow \varphi(g) \end{aligned}$$

un epimorfismo con nucleo  $K$ , entonces:

$$G/K \cong G' \tag{1.1.25}$$

**Demostración.** Para demostrar que  $G/K$  y  $G'$  son isomorfos, debemos demostrar que existe un isomorfismo entre los dos grupos. Empezamos definiendo un mapeo  $\bar{\varphi}$  definido por:

$$\begin{aligned} \bar{\varphi}: G/K &\rightarrow G' \\ Kg &\rightarrow \varphi(g) \end{aligned}$$

es decir  $\bar{\varphi}(Kg) = \varphi(g)$ .

Para demostrar que es un isomorfismo, debemos demostrar que es 1 - 1 y sobre. Para demostrar su inyectividad tomamos dos elementos  $g_1, g_2 \in G$  y al evaluarlos e igualarlos, tenemos que:

$$\bar{\varphi}(Kg_1) = \bar{\varphi}(Kg_2) \implies \varphi(g_1) = \varphi(g_2)$$

Por otro lado, si operamos  $g_1g_2^{-1}$  tenemos que:

$$\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_2)\varphi(g_2^{-1}) = \varphi(g_2g_2^{-1}) = \varphi(e) = e'$$

Esto es equivalente a decir que  $g_1g_2^{-1} \in K$ , lo cual implica que:

$$\begin{aligned} g_1 &\cong g_2 \text{ mód } K \\ g_2 &\cong g_1 \text{ mód } K \end{aligned}$$

es decir:

$$\begin{aligned} [g_1] &= [g_2] \\ Kg_1 &= Kg_2 \end{aligned}$$

por lo que podemos concluir que  $\bar{\varphi}$  es inyectiva.

Por otro lado,  $\bar{\varphi}$  es sobre por construcción, por lo que podemos afirmar que es una biyección.  $\square$

**Ejercicio 1.1.18.** Verificar que  $\varphi$  es un homomorfismo, es decir:

$$\bar{\varphi}(Kg_1Kg_2) = \bar{\varphi}(Kg_1)\bar{\varphi}(Kg_2)$$

**Teorema 1.1.5.** Sea  $G$  un grupo y  $H < G$  y  $N \trianglelefteq G$ , entonces:

$$HN < G \quad (1.1.26)$$

$$H \cap N \trianglelefteq H \quad (1.1.27)$$

$$N \trianglelefteq HN \quad (1.1.28)$$

y además:

$$HN/N \cong H/H \cap N \quad (1.1.29)$$

**Teorema 1.1.6.** Sea  $G$  un grupo,  $N \trianglelefteq G$  y  $K < N$  con  $K \trianglelefteq G$ , entonces:

$$G/K/N/K \cong G/N \quad (1.1.30)$$

Sea  $G_1, G_2, \dots, G_n$  grupos. Su producto directo o externo denotado por:

$$G_1 \times G_2 \times \cdots \times G_n \quad (1.1.31)$$

es el conjunto de  $n$ -adas  $(a_1, a_2, \dots, a_n)$ , donde cada  $a_i \in G_i$  para todo  $i \in \mathbb{N}$  y la operación en  $G_1 \times G_2 \times \cdots \times G_n$  se define componente a componente:

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n) \quad (1.1.32)$$

Tenemos que  $G = G_1 \times G_2 \times \cdots \times G_n$  es un grupo, cuyo elemento identidad es  $(e_1, e_2, \dots, e_n)$  y el inverso de  $(a_1, a_2, \dots, a_n)$  es  $(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$ .



## 1.2. Anillos

### Definiciones

**Definición 1.2.1.** Un conjunto no vacío  $R$  es un anillo si tiene definidas dos operaciones  $(+, \cdot)$ , tales que se cumplen las siguientes propiedades:

**Cerradura**  $a + b \in R \quad \forall a, b \in R$

**Asociatividad**  $a + (b + c) = (a + b) + c \quad \forall a, b, c \in R$

**Conmutatividad**  $a + b = b + a \quad \forall a, b \in R$

**Identidad**  $\exists 0 \in R \ni a + 0 = a \quad \forall a \in R$

**Inverso**  $\exists b \in R \ni a + b = 0 \quad \forall a \in R$

De estas propiedades podemos concluir que  $R$  es un grupo abeliano con respecto a  $(+)$ , pero aun tenemos lo siguiente:

**Cerradura**  $a \cdot b \in R \quad \forall a, b \in R$

**Asociatividad**  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

De estas propiedades podemos concluir que  $R$  es un semigrupo con respecto a  $(\cdot)$  y además:

**Distributividad**  $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$

**Definición 1.2.2.** Diremos que un anillo  $R$  es un anillo con identidad si existe un  $1 \in R$  diferente de  $0$  tal que:

$$a \cdot 1 = 1 \cdot a \quad \forall a \in R \tag{1.2.1}$$

**Definición 1.2.3.** Un anillo  $R$  es un anillo conmutativo si:

$$a \cdot b = b \cdot a \quad \forall a, b \in R \tag{1.2.2}$$

**Definición 1.2.4.** Sea  $R$  un anillo y  $a \in R$  con  $a \neq 0$ ; diremos que  $a$  es divisor de cero si existe un  $b \in R$  con  $b \neq 0$  tal que:

$$a \cdot b = 0 \tag{1.2.3}$$

a este se le llama divisor por la derecha, o bien si existe un  $c \in R$  con  $c \neq 0$  tal que:

$$c \cdot a = 0 \tag{1.2.4}$$

al que se le llama divisor por la izquierda.

**Definición 1.2.5.** Sea  $R$  un anillo con identidad. Diremos que  $R$  es un anillo con división si para todo  $a \in R$  existe un  $b \in R$  tal que:

$$a \cdot b = b \cdot a = 1 \tag{1.2.5}$$

**Definición 1.2.6.** Un campo es un anillo con división, que además es conmutativo. Un campo es un grupo abeliano con respecto a la suma y a la multiplicación.

**Definición 1.2.7.** Un anillo conmutativo con identidad es un dominio entero si:

$$a \cdot b = 0 \implies a = 0 \text{ o } b = 0 \tag{1.2.6}$$

es decir, no existen divisores de cero en el anillo.

**Observación 1.2.1.** Si  $p$  es primo, entonces  $\mathbb{Z}_p$  es campo.

**Ejercicio 1.2.1.** Sea  $\mathcal{M}_{2 \times 2}(\mathbb{R})$  definido como:

$$\mathcal{M}_{2 \times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \tag{1.2.7}$$

Verificar que  $\mathcal{M}_{2 \times 2}(\mathbb{R})$  es un anillo con identidad no conmutativo y ademas no es dominio entero.

**Proposición 1.2.1.** Sea  $R$  un anillo y sean  $a, b \in R$ , entonces se cumplen las siguientes propiedades:
 

- $a \cdot 0 = 0 \cdot a = 0$
- $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
- $(-a) \cdot (-b) = -(-a) \cdot b = ab$
- Si  $1 \in R \implies (-1) \cdot a = -a$

*Demostración.* Para la verificación de la primer proposición tenemos que:

$$a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

y cancelando  $a \cdot 0$  de ambos lados:

$$0 = a \cdot 0$$

Para la verificación de la segunda proposición tenemos que:

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot (0) = 0$$

si conservamos los extremos de este procedimiento y despejamos el segundo termino del lado izquierdo, tenemos:

$$a \cdot (-b) = -(a \cdot b)$$

Para la verificación de la tercer proposición tenemos que:

$$(-a) \cdot (-b) + (-a) \cdot (b) = (-a) \cdot (-b + b) = (-a) \cdot (0) = 0$$

de nuevo, despejando el segundo termino del lado izquierdo, tenemos:

$$(-a) \cdot (-b) = -(-a) \cdot (b) = (-(-a)) \cdot (b)$$

al operar de nuevo con el mismo termino tenemos:

$$(-(-a)) \cdot (b) - (a) \cdot (b) = (b) \cdot (-a - (-a)) = (b) \cdot (0) = 0$$

lo cual nos da que:

$$(-(-a)) \cdot (b) = (a) \cdot (b) = (a \cdot b)$$

Para la ultima proposición tenemos que:

$$(-1) \cdot a + (1) \cdot a = a \cdot (1 - 1) = a \cdot (0) = 0$$

por lo que tenemos que:

$$(-1) \cdot a = -(1) \cdot a = -a$$

□

## Homomorfismos de anillo

**Definición 1.2.8.** Una función  $\varphi: R \rightarrow R'$  es un homomorfismo si:

$$\varphi(a) + \varphi(b) = \varphi(a + b) \quad (1.2.8)$$

$$\varphi(a)\varphi(b) = \varphi(ab) \quad (1.2.9)$$

**Definición 1.2.9.** Sea  $\varphi: R \rightarrow R'$  homomorfismo de anillos, a parte se dice que es:

**Monomorfismo** si  $\varphi$  es inyectivo (1 - 1).

**Epimorfismo** si  $\varphi$  es suprayectivo (sobre).

**Isomorfismo** si  $\varphi$  es biyectivo (1 - 1 y sobre).

**Definición 1.2.10.** El nucleo de  $\varphi$  es:

$$\ker \varphi = \{x \in R \mid \varphi(x) = 0\} \quad (1.2.10)$$

**Proposición 1.2.2.** Sea  $\varphi$  un homomorfismo de anillos, entonces:

1.  $\ker \varphi$  es un subgrupo aditivo
2. Dados  $k \in \ker \varphi$  y  $r \in R$  se cumple que  $rk, kr \in \ker \varphi$ .

*Demostración.* Sean  $k \in \ker \varphi$  y  $r \in R$ , entonces tenemos que:

$$\begin{aligned}\varphi(rk) &= \varphi(r)\varphi(k) = \varphi(r) \cdot 0 = 0 \\ \varphi(kr) &= \varphi(k)\varphi(r) = 0 \cdot \varphi(r) = 0\end{aligned}$$

por lo que podemos concluir que:

$$kr, rk \in \ker \varphi$$

□

## Ideales

**Definición 1.2.11.** Sea  $R$  un anillo e  $I$  un subconjunto de  $R$ , se dice que  $I$  es un ideal de  $R$  si:

1.  $I$  es un subgrupo aditivo de  $R$
2. Dados  $r \in R$  y  $a \in I$ , tenemos que se cumple  $ra, ar \in I$ . A esto se le conoce como la propiedad de absorción.

**Corolario 1.2.1.** Si  $\varphi: R \rightarrow R'$  es un homomorfismo, entonces  $K = \ker \varphi$  es un ideal de  $R$ .

**Definición 1.2.12.** Sea  $R$  un anillo e  $I$  un ideal de  $R$ , entonces  $R/I$  es llamado anillo cociente y es un grupo, con la suma de clases de equivalencia:

$$(a + I) + (b + I) = (a + b) + I \quad (1.2.11)$$

para  $a, b \in R$ .

**Definición 1.2.13.** Definimos el producto como:

$$(a + I)(b + I) = ab + I \quad (1.2.12)$$

para  $a, b \in I$

**Observación 1.2.2.** Sea  $R$  un anillo, tenemos que  $\{0\}$  y  $R$  mismo son ideales triviales de  $R$ .

**Definición 1.2.14.** Si  $I$  es un ideal de  $R$  e  $I \neq R$ , decimos que  $I$  es un ideal propio.

**Proposición 1.2.3.** Sea  $R$  un anillo con identidad e  $I$  un ideal de  $R$  tal que  $1 \in I$ , entonces  $I = R$ .

*Demostración.* Para demostrar que  $I = R$  primero tenemos que demostrar que  $I \subseteq R$  y después que  $R \subseteq I$ . Por definición  $I \subseteq R$ , por lo que solo resta demostrar  $R \subseteq I$ .

Empecemos con un elemento general  $a \in R$ , entonces se cumple que:

$$a = a \cdot 1$$

en donde  $1 \in I$  y  $a \in R$ , por lo que por la propiedad de absorción de un ideal podemos decir que  $a \in I$ . Y como  $a$  es un elemento general de  $R$ , podemos concluir que:

$$R \subseteq I$$

□

**Ejemplo 1.2.1.** Sea  $R$  un anillo conmutativo con identidad. Dado un elemento  $a \in R$  tenemos que:

$$(a) = \{ax \mid x \in R\}$$

Verificar que  $(a)$  es un ideal.

Primero notamos que  $(a)$  es no vacío, ya que al menos existe un elemento:

$$a \cdot 0 = 0 \in (a)$$

Ahora, para comprobar la cerradura con respecto a  $(+)$  tenemos que tomar dos elementos  $ax_1, ax_2 \in (a)$  y operarlos, con lo que obtenemos:

$$ax_1 + ax_2 = a(x_1 + x_2)$$

y ya que  $x_1 + x_2 \in R$ , sabemos que el resultado esta en  $(a)$ .

Para comprobar la existencia del inverso, tenemos que:

$$-ax_1 + ax_1 = a(-x_1 + x_1) = a \cdot 0 = 0$$

por lo que se cumple la existencia del inverso, por lo que concluimos que  $(a)$  es un subgrupo con respecto a  $(+)$ . Ahora solo nos queda por comprobar la propiedad de absorción del ideal.

Si tomamos un elemento  $ax \in (a)$  y un elemento  $y \in R$  tendremos que:

$$axy = a(xy) = yax$$

pero  $xy \in R$ , por lo que concluimos que la operación sigue estando en  $(a)$ , por lo que tenemos que  $(a)$  es un ideal.

**Definición 1.2.15.** Sea  $R$  anillo conmutativo con identidad, un ideal principal es un ideal de la forma  $(a)$  para algun  $a \in R$ .

**Definición 1.2.16.** Sea  $R$  un dominio entero, diremos que  $R$  es un dominio de ideales principales, si todos los ideales de  $R$  son principales.

**Definición 1.2.17.** Sean  $I, J$  ideales del anillo  $R$ , definimos las operaciones de ideales como:

$$I + J = \{a + b \mid a \in I, b \in J\} \tag{1.2.13}$$

$$IJ = \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}, a_i \in I, b_i \in J \right\} \tag{1.2.14}$$

**Ejercicio 1.2.2.** Verificar que  $I + J$  es un ideal dado que  $I \cap J$  es un ideal de  $R$ .

**Proposición 1.2.4.** *Tenemos que  $R/I$  es un anillo con la suma y productos correspondientes:*

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

entonces la función:

$$\begin{aligned} \varphi: R &\rightarrow R/I \\ a &\rightarrow a + I \end{aligned}$$

es un epimorfismo.

**Demostración.** Primero debemos verificar que  $\varphi$  es un homomorfismo:

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

Tambien notamos que  $\varphi$  es sobre por construcción, por lo que podemos concluir que es un epimorfismo. □

**Ejercicio 1.2.3.** Verificar que el nucleo de  $\varphi$  definido como:

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0 + I\}$$

coincide con el ideal  $I$ .

## Teoremas de isomorfismos

**Teorema 1.2.1.** Sea  $\varphi: R \rightarrow R'$  un epimorfismo de anillos, y  $K = \ker \varphi$ , entonces  $R/K$  es isomorfo con  $R'$ , es decir:

$$R/K \cong R' \quad (1.2.15)$$

**Teorema 1.2.2.** Sea  $R$  anillo, sean  $A$  un subconjunto de  $R$  ( $A$  subanillo de  $R$ ) y  $B$  un ideal de  $R$ , entonces  $A + B$  es un subanillo de  $R$  y un ideal de  $A$ , ademàs:

$$A + B/B \cong A/A \cap B \quad (1.2.16)$$

**Teorema 1.2.3.** Sean  $I, J$  ideales del anillo  $R$ , con  $I \subseteq J$ , entonces  $I/I$  es ideal de  $R/I$ , ademàs:

$$R/I/I \cong R/J \quad (1.2.17)$$

**Ejemplo 1.2.2.** Sea  $n \in \mathbb{N}$ , con  $n > 1$  tenemos la aplicación:

$$\begin{aligned} \varphi: \mathbb{Z} &\rightarrow \mathbb{Z}' \\ a &\rightarrow [a] \end{aligned}$$

por lo que  $\varphi$  es un epimorfismo con:

$$\begin{aligned} [a + b] &= [a] + [b] \\ [ab] &= [a][b] \end{aligned}$$

y su nucleo es:

$$\begin{aligned} \ker \varphi &= \{a \in \mathbb{Z} \mid \varphi(a) = [a] = [0]\} \\ &= \{a \in \mathbb{Z} \mid a \cong 0 \text{ mód } n\} \\ &= \{a \in \mathbb{Z} \mid n/a\} \\ &= \{a \in \mathbb{Z} \mid a = nz, z \in \mathbb{Z}\} = n\mathbb{Z} \end{aligned}$$

por lo que podemos aplicar el primer teorema de isomorfismos y decir que:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}'$$

**Ejemplo 1.2.3.** Sea  $F$  un campo, es decir, un anillo conmutativo con división, entonces  $\{0\}$  es un ideal de  $F$ .

Sea  $I$  un ideal diferente a  $\{0\}$ . Tenemos un elemento  $a \in I$ , con  $a \neq 0$ , entonces  $1 = a^{-1}a$  con  $a^{-1} \in F$  y  $a \in I$ , por lo que:

$$1 = a^{-1}a \in I$$

Si ahora tomamos un elemento cualquiera  $r \in F$ , el cual obviamente puede ser escrito como  $r = 1 \cdot r$ , con  $1 \in I$  y  $r \in F$  tenemos que:

$$r = 1 \cdot r \in I$$

y por lo tanto:

$$F \subseteq I$$

y por definición sabemos que  $I \subseteq F$ , por lo que este ideal es el mismo que el campo.

$$F = I$$

**Ejercicio 1.2.4.** Sea  $R$  definido como:

$$R = \{f: [0, 1] \rightarrow \mathbb{R} \mid f \text{ es continua}\}$$

con las operaciones definidas como:

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

$$(f \cdot g)(x) = f(x)g(x)$$

¿Es  $R$  un anillo con identidad?

**Ejercicio 1.2.5.** Si definimos el nucleo como:

$$I = \left\{ f \in R \mid f\left(\frac{1}{2}\right) = 0 \right\}$$

y definimos una función  $\varphi$  como:

$$\begin{aligned} \varphi: R &\rightarrow R \\ f &\rightarrow f\left(\frac{1}{2}\right) \end{aligned}$$

¿Podemos decir que  $R/I$  y  $R$  son isomorfos?



### 1.3. Dominios Enteros

#### Definiciones

**Definición 1.3.1.** Se dice que  $a \in \mathbb{Z}$  divide a  $b \in \mathbb{Z}$  si existe un  $q \in \mathbb{Z}$  tal que:

$$b = qa \tag{1.3.1}$$

y se denota por  $a/b$

**Teorema 1.3.1.** Si  $a/b$  y  $a/c$ , entonces  $a/bx + cy \quad \forall x, y \in \mathbb{Z}$ .

*Demostración.* Como  $a/b$  sabemos que existe un  $q \in \mathbb{Z}$  tal que  $b = aq$  y como  $a/c$  sabemos que existe un  $q' \in \mathbb{Z}$  tal que  $c = aq'$ . Dados  $x, y \in \mathbb{Z}$  generales, al multiplicar estos enteros por las relaciones anteriores obtenemos:

$$\begin{aligned} bx &= aqx \\ cy &= aq'y \end{aligned}$$

y si sumamos ambas relaciones obtendremos:

$$bx + cy = aqx + aq'y = a(qx + q'y)$$

y como  $x, y, q, q' \in \mathbb{Z}$ , podemos establecer la siguiente relación:

$$bx + cy = a\bar{q} \quad \bar{q} \in \mathbb{Z}$$

por lo que es inmediato que:

$$a/bx + cy \tag{1.3.2}$$

□

**Definición 1.3.2.** Un entero  $p \neq 0$  se dice primo si y solo si sus únicos divisores son  $\pm 1$  y  $\pm p$

#### Máximo Común Divisor

**Definición 1.3.3.** Si  $a/b$  y  $a/c$  se dice que  $a$  es divisor común de  $b$  y  $c$ . Si además, todo divisor común de  $b$  y  $c$  también es divisor de  $a$ , se dice que  $a$  es el máximo común divisor de  $b$  y  $c$ , es decir:

$$a = (b, c) \tag{1.3.2}$$

**Ejemplo 1.3.1.** Calcular el máximo común divisor de 24 y 60, es decir  $(24, 60)$ .

24	60	2
12	30	2
6	15	3
2	5	

$$(24, 60) = 12$$

### mínimo común múltiplo

**Definición 1.3.4.** Aprovechando la definición dada del Máximo Común Divisor, simplemente damos una definición de la siguiente forma para el mínimo común múltiplo:

$$\frac{ab}{(a, b)} \tag{1.3.3}$$

**Ejemplo 1.3.2.** Calcular el mínimo común múltiplo de 24 y 60.

$$\frac{24 \cdot 60}{12} = 120$$

24	60	2
12	30	2
6	15	3
2	5	2
1	5	5
1	1	

**Ejemplo 1.3.3.**

**Ejemplo 1.3.4.**

**Ejercicio 1.3.1.** Calcular  $(0, c)$  con  $c \neq 0, c \in \mathbb{Z}$ .

### Algoritmo de la división de Euclides

**Definición 1.3.5.** Para cualesquiera enteros no nulos  $a, b$  existen  $q, r$  únicos, denominados cociente y residuo respectivamente, tales que:

$$a = bq + r \tag{1.3.4}$$

Si  $b/a$ , entonces  $r = 0$ , de lo contrario  $0 < r < |b|$ .

**Proposición 1.3.1.** Se puede verificar que un divisor común de  $a$  y  $b$  divide a  $r$  y un divisor común de  $b$  y  $r$  divide a  $a$ , es decir:

$$(a, b) = (b, r) \tag{1.3.5}$$

*Demostración.* Si  $b$  no divide a  $a$ , entonces tenemos que:

$$a = bq + r \quad 0 < r < |b|$$

Primero demostraremos la primera afirmación de la proposición, para lo que decimos que existe un divisor común para  $a$  y  $b$ , al cual llamamos  $c$ , esto es equivalente a decir que  $c/a$  y  $c/b$ , lo cual implica que existen  $\bar{q}, q' \in \mathbb{Z}$  tales que:

$$\begin{aligned} a &= c\bar{q} \\ b &= cq' \end{aligned}$$

lo cual implica que nuestro residuo se escribe como:

$$r = a - bq = c\bar{q} - cq'q = c(\bar{q} - q'q)$$

en donde  $\bar{q} - q'q \in \mathbb{Z}$ , por lo que podemos concluir que  $c/r$ .

Para demostrar la segunda afirmación, tenemos un divisor común de  $b$  y de  $r$  al que llamamos  $l$ , es decir,  $l/b$  y  $l/r$ , lo cual implica que existen  $\bar{m}, m' \in \mathbb{Z}$  tales que:

$$\begin{aligned} b &= l\bar{m} \\ r &= lm' \end{aligned}$$

lo cual implica que la ecuación original puede ser escrita como:

$$a = bq + r = l\bar{m}q + lm' = l(\bar{m}q + m')$$

en donde  $\bar{m}q + m' \in \mathbb{Z}$ , por lo que podemos concluir que  $l/a$ , y por lo tanto:

$$(a, b) = (b, r)$$

□

**Teorema 1.3.2.** *Para dos enteros no nulos  $(a, b)$  existen dos enteros únicos  $q, r$  tales que:*

$$a = bq + r \quad 0 \leq r < |b| \tag{1.3.6}$$

*A este teorema se le conoce como el algoritmo de la división de Euclides.*

*Demostración.* Definimos un conjunto de la forma:

$$S = \{a - bx \mid x \in \mathbb{Z}\} \tag{1.3.7}$$

es decir, el conjunto de los residuos en esta ecuación. Primero queremos verificar que este residuo  $r = a - bx \geq 0$ , lo que es equivalente a decir:

$$S \subset \mathbb{Z}^+ \cup \{0\}$$

1. Si  $b$  es negativo ( $b < 0$ ), entonces  $b \leq -1$

$$b|a| \leq -|a| \leq a$$

$$a - b|a| \geq 0$$

2. Si  $b$  es positivo ( $b > 0$ ), entonces  $b \geq 1$

$$b(-|a|) \leq -|a| \leq a$$

$$a - b(-|a|) \geq 0$$

por lo que podemos concluir que  $S \subset \mathbb{Z}^+ \cup \{0\}$  y por lo tanto que  $r = a - bx \geq 0$ . Ahora demostraremos que  $r < |b|$ .

Supongamos que  $r$  es el menor de estos enteros no negativos y  $r \in S$ , además supongamos que  $r \geq |b|$ , o bien:

$$r - |b| \geq 0$$

Como  $r \in S$ , existe un  $x = q \in \mathbb{Z}$  tal que  $r = a - bq$ , por lo que tenemos que:

$$r - |b| = a - bq - |b| = \begin{cases} a - b(q - 1) & \text{Si } b < 0 \\ a - b(q + 1) & \text{Si } b > 0 \end{cases}$$

Por otro lado, sabemos que los valores de  $r - |b|$  son:

$$r - |b| = r - b < r \text{ para } b > 0$$

$$r - |b| = r + b < r \text{ para } b < 0$$

pero asumimos que  $r$  es el menor de los enteros positivos en  $S$ , por lo que llegamos a una contradicción y por lo tanto:

$$r < |b|$$

Si bien hemos demostrado la veracidad de esta ecuación, aun no hemos demostrado que  $q$  y  $r$  sean únicos, por lo que ahora procederemos demostrando esto.

Empezaremos suponiendo que existen  $q'$  y  $r'$  enteros, además de  $q$  y  $r$  tales que:

$$a = bq + r$$

$$a = bq' + r'$$

en donde  $0 \leq r < |b|$  y  $0 \leq r' < |b|$ . Si estas expresiones las restamos entre si, obtendremos:

$$b(q - q') = r' - r$$

lo cual implica que  $b/r' - r$ , es decir, existe un  $t \in \mathbb{Z}$ , tal que:

$$r' - r = bt$$

Por otro lado, la expresión  $b(q - q') = r' - r$  puede ser expresada como:

$$b(q - q') + (r - r') = 0$$

$$b(q' - q) + (r' - r) = 0$$

lo cual, ya hemos comprobado que implica:

$$|r - r'| \leq |b|$$

o bien:

$$|bt| \leq |b|$$

Si tomamos en cuenta los valores que puede tomar  $t$ , nos daremos cuenta que:

1. Si  $t = 0$

$$r' = r \implies q' = q$$

2. Si  $t = -1$

$$|-b| \leq |b| \implies r' - r = -b \implies r' = r - b \geq 0 \implies r \geq b$$

lo cual es falso, por lo que  $t \neq -1$

3. Si  $t = 1$

$$|b| \leq |b| \implies r' - r = b \implies r = r' - b \geq 0 \implies r' \geq b$$

lo cual es falso, por lo que  $t \neq 1$

y como el caso en que  $t = 0$  es el único cierto, concluimos que  $q, r$  deben ser únicos. □



## Capítulo 2

# Álgebra lineal





## **Capítulo 3**

# **Ecuaciones diferenciales**