Estructuras Algebraicas para la Computación

Mariam Cobalea

Universidad de Málaga
Dpto. de Matemática Aplicada

Tema 3: Grupos, anillos y cuerpos

- Grupos y subgrupos. Clases laterales y teorema de Lagrange.
- Introducción a la teoría de la codificación.
- Anillos. Elementos inversibles y divisores de cero. Cuerpos.

Grupos

Introducción

Para resolver la ecuación $a+x=b$ en $\mathbb{Z}$ procedemos del siguiente modo:

1. Se suma $(-a)$ en ambos miembros,
$$(-a)+(a+x)=(-a)+b$$
2. Se aplica la propiedad asociativa
$$((-a)+a)+x=(-a)+b$$
3. Se aplica la propiedad del opuesto y obtenemos
$$0+x=(-a)+b$$
4. Usando la propiedad de identidad del neutro nos queda
$$x=(-a)+b$$
5. Sabemos que la suma de dos enteros siempre es un entero, de modo que $(-a)+b$ es un entero.

Grupos

Introducción

Así, para todo a y b de $\mathbb{Z}$, se tiene que $x=(-a)+b$ es el único entero que satisface la ecuación $a+x=b$.

En este ejemplo, aparte de usar el hecho de que la suma es una operación binaria en el conjunto de los enteros, se aplican otras tres propiedades de la suma:

- propiedad **asociativa**,
- propiedad de **elemento neutro** y
- propiedad del **simétrico**.

Estas propiedades se usan para definir la estructura algebraica de **grupo**.

Grupos

Definición

Sea $*$ *una operación binaria definida en un conjunto* G. *Se dice que* $(G, *)$ *es un* ***grupo*** *si se verifican las siguientes propiedades:*

1. ***Asociativa:*** $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$
2. ***Elemento neutro:*** $\exists e \in G,\ \forall a \in G,\ a * e = e * a = a$
3. ***Elemento simétrico:*** $\forall a \in G,\ \exists a' \in G,\ a * a' = a' * a = e$

Si además se verifica la propiedad

$$\textbf{Conmutativa:}\quad \forall a, b \in G,\ a * b = b * a$$

se dice que $(G, *)$ *es un* ***grupo abeliano****.*

Grupos

Notación

	Elemento neutro	Elemento simétrico
Operación aditiva	*Cero* 0	*Opuesto* $(-a)$
Operación multiplicativa	*Unidad* $1, \mathrm{I}$	*Inverso* a^{-1}

Grupos

Ejemplos

- $(\mathbb{Z}, +)$ es un grupo. El elemento neutro es 0 y para cada $x \in \mathbb{Z}$ su opuesto es $-x$. Además, $(\mathbb{Z}, +)$ es abeliano, ya que se verifica la propiedad conmutativa.
- $(\mathbb{Q}, +)$ es un grupo. El elemento neutro es 0 y para cada $x \in \mathbb{Q}$ su opuesto es $-x$. Además, $(\mathbb{Q}, +)$ es abeliano, ya que se verifica la propiedad conmutativa.
- $(\mathbb{R}^+, \cdot)$ es un grupo. El elemento neutro es 1 y para cada $x \in \mathbb{R}$ el inverso es $\frac{1}{x}$. Además, $(\mathbb{R}^+, \cdot)$ es abeliano ya que se verifica la propiedad conmutativa.
- $(\mathbb{Z}^+, \cdot)$ no es grupo, ya que 2 no tiene inverso.

Grupos

Ejercicios

1. En el conjunto $\mathbb{Z}$ se define la operación

   $$x * y = x + y + 1$$

   Estudia si $(\mathbb{Z}, *)$ es un grupo.
2. En el conjunto $\mathbb{R} - \{0\}$ se define la operación binaria

   $$x * y = \frac{x \cdot y}{2}$$

   Estudia si $(\mathbb{R} - \{0\}, *)$ es un grupo.
3. En el conjunto $\mathbb{Q} - \{1\}$ se define la operación $*$

   $$x * y = x + y - xy$$

   Estudia si $(\mathbb{Q} - \{1\}, *)$ es un grupo.

Grupos
Propiedades de los grupos

Teorema

Sea $(G, *)$ *un grupo. Entonces:*

- *El elemento neutro* e *es único.*
- *El elemento simétrico* a^{-1} *de cada elemento* $a \in G$ *es único.*
- $(a^{-1})^{-1} = a$

Teorema

Sea $(G, *)$ *un grupo y sean* $a, b \in G$. *Entonces:*

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

Teorema (Propiedad de simplificación)

Sea $(G, *)$ *un grupo y sean* $a, b, c \in G$. *Se verifican:*

- *Si* $a * b = a * c$, *entonces* $b = c$
- *Si* $b * a = c * a$, *entonces* $b = c$

Grupos
Propiedades de los grupos

Teorema

Sea $(G, *)$ *un grupo y sean* $a, b \in G$, *entonces*

- *la ecuación* $a * x = b$ *tiene solución única* $x = a^{-1} * b$
- *la ecuación* $y * a = b$ *tiene solución única* $y = b * a^{-1}$
- *fijado un elemento* $a \in G$, *la función* $f : G \to G$, *definida*

$$f(x) = a * x$$

es biyectiva.

Demostración: **Ejercicio**

Grupos
Propiedades de los grupos

Ejercicio: En el conjunto $G = \mathbb{R} - \{-1\}$ se define la operación $*$

$$\begin{aligned} *: \quad G \times G &\longrightarrow G \\ (x, y) &\longmapsto x * y = x + y + xy \end{aligned}$$

1. Demuestra que $(G, *)$ es grupo.
2. Encuentra el valor de $x \in G$ tal que $2 * x * 3 = 35$

Grupos
Propiedades de los grupos

Ejercicios: Demuestra que:

1. Si $(G, *)$ es un grupo tal que para todo $a \in G$, se verifica $a^2 = e$, entonces $(G, *)$ es abeliano.
2. Si $(G, *)$ es un grupo tal que para todo $a, b \in G$,

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

entonces $(G, *)$ es abeliano.

Definición

*El **orden** de un grupo $(G,*)$ es el cardinal del conjunto G.*
*Se dice que el grupo $(G,*)$ es **finito** si tiene orden finito.*

La operación de un grupo finito se puede especificar mediante una tabla, llamada **tabla de Cayley**.

Ejemplo El grupo $(H,\cdot)$, donde $H=\{1,i,-1,-i\}$, donde $i=\sqrt{-1}$.
La tabla de Cayley de la operación $\cdot$ es:

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

Teorema

Si $(G,*)$ es un grupo finito, entonces su tabla de Cayley es tal que cada elemento de G aparece exactamente una vez en cada fila y en cada columna.

☛ El recíproco no se verifica.

Ejercicio En el conjunto $S=\{a,b,c,d,e\}$ se define la operación $*$ dada por la tabla

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

Demuestra que no se verifica el recíproco del teorema anterior.

Ejercicio En el conjunto $G=\{e,a,b,c,d,f\}$ se considera una operación binaria $*$ dada por

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a		e	f	c	d
b	b	e	a			
c	c				a	
d	d	f				
f	f	c		a		

Completa la tabla anterior para que $(G,*)$ sea un grupo. ¿Es abeliano?

Ejercicio Se considera el conjunto $G=\{i,s_0,s_1,s_2\}$, cuyos elementos son transformaciones del plano provisto de dos ejes de referencia perpendiculares.

- i : identidad
- s_0 : simetría respecto al origen de coordenadas
- s_1 : simetría respecto al eje de abcisas
- s_2 : simetría respecto al eje de ordenadas

En G definimos la operación $\circ$ composición de funciones.

- Escribe la tabla de la operación $\circ$
- Demuestra que $(G,\circ)$ es un grupo.

(Este grupo es conocido como **grupo de Kleinn**)

Definición

Sea A un conjunto en el que hay definidas una relación de equivalencia $\sim$ y una operación binaria $*$. Se dice que $\sim$ y $*$ son ***compatibles*** *si para todo $a_1, a_2, b_1, b_2 \in A$ se verifica*

$$\left.\begin{array}{l} a_1 \sim a_2 \\ b_1 \sim b_2 \end{array}\right\} \Longrightarrow a_1 * b_1 \sim a_2 * b_2$$

Ejemplo: En $\mathbb{Z}$, la suma y el producto son compatibles con la relación de equivalencia congruencia módulo m

$$a \equiv b \pmod{m} \iff a - b = k \cdot m, \quad k \in \mathbb{Z}$$

Para todo $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ se verifica:

$$\left.\begin{array}{l} a_1 \equiv a_2 \ mod(m) \\ b_1 \equiv b_2 \ mod(m) \end{array}\right\} \Longrightarrow \left\{\begin{array}{lcll} a_1 + b_1 & \equiv & a_2 + b_2 & mod(m) \\ a_1 \cdot b_1 & \equiv & a_2 \cdot b_2 & mod(m) \end{array}\right\}$$

Teorema

Si $\sim$ y $*$ son compatibles, entonces en el conjunto cociente $A/_\sim$ se puede definir una operación $\circledast$

$$\begin{array}{rccc} \circledast : & A/_\sim \times A/_\sim & \longrightarrow & A/_\sim \\ & [x] \circledast [y] & = & [x * y] \end{array}$$

Ejemplo: En el conjunto $\mathbb{Z}_5$ se definen las operaciones:

$$\begin{array}{rccc} +_5 : & \mathbb{Z}_5 \times \mathbb{Z}_5 & \longrightarrow & \mathbb{Z}_5 \\ & [x]_5 + {}_5 [y]_5 & = & [x+y]_5 \end{array} \qquad \begin{array}{rccc} \cdot_5 : & \mathbb{Z}_5 \times \mathbb{Z}_5 & \longrightarrow & \mathbb{Z}_5 \\ & [x]_5 \cdot {}_5 [y]_5 & = & [x \cdot y]_5 \end{array}$$

Dada una estructura algebraica $(A, *)$, si la relación de equivalencia $\sim$ es compatible con la operación $*$, la estructura cociente $(A/_\sim, \circledast)$ ''hereda'' algunas propiedades de la estructura $(A, *)$.

Más exactamente,

- si $*$ es asociativa o conmutativa en A, entonces la operación $\circledast$ también es asociativa en $A/_\sim$;
- si e es el elemento neutro de $(A, *)$, entonces $[e]$ es el neutro de $(A/_\sim, \circledast)$;
- si $x' \in A$ es el simétrico de $x \in A$ en $(A, *)$, entonces $[x']$ es la clase simétrica de la clase $[x]$ en $(A/_\sim, \circledast)$.

Ejemplo: Para todo $m > 1$, en el conjunto cociente $\mathbb{Z}_m$ la operación

$$\begin{array}{rccc} +_m : & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m \\ & [x]_m +_m [y]_m & = & [x+y]_m \end{array}$$

verifica:

- $+_m$ es asociativa, es conmutativa, tiene elemento neutro $[0]_m$ y cada clase $[x]_m$ tiene su opuesto $-[x]_m = [-x]_m$.

Así, para todo $m > 1$, se verifica que $(\mathbb{Z}_m, +_m)$ tiene estructura de grupo abeliano.

Ejemplo: Para todo $m > 1$, en el conjunto cociente $\mathbb{Z}_m$ también podemos definir

$$\begin{array}{rccc} \cdot_m\colon & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m \\ & [x]_m \cdot_m [y]_m & = & [x \cdot y]_m \end{array}$$

- La operación $\cdot_m$ es asociativa, $[1]_m$ es el elemento neutro y es conmutativa.
- Así, para todo $m > 1$, se tiene que $(\mathbb{Z}_m, \cdot_m)$ es un monoide conmutativo.
- Además, cuando $m = p$ (siendo p un número primo) se verifica que cada elemento no nulo tiene inverso.
- Por lo tanto, para p primo, $(\mathbb{Z}_p - \{[0]_p\}, \cdot_p)$ es también un grupo.

Ejemplo: En particular, para $m = 4$ y $m = 5$, tenemos

$$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\} \qquad \mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$$

$+_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\cdot_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Definición

Dados los grupos $(G, *)$ y $(H, \bullet)$, el **producto directo** *$G \times H$ es el conjunto de pares ordenados (g, h) con $g \in G$ y $h \in H$, equipado con la operación $\perp$*

$$(g_1, h_1) \perp (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2)$$

Ejemplo:

- $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

- $(\mathbb{R} \times \mathbb{R}, +)$

Teorema

Sean los grupos $(G, *)$ y $(H, \bullet)$. El producto directo $(G \times H, \perp)$ es un grupo. Si G y H son finitos, entonces el orden de este grupo es el producto de los órdenes de G y H.

Ejemplo: Son grupos:

- $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$.
- $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$, en general $(\mathbb{Z}_n \times \mathbb{Z}_m, \oplus)$.
- $(\mathbb{R} \times \mathbb{R}, +)$,
- $(\mathbb{R} \times \cdots \times \mathbb{R}, +)$

Definición

Sea $(G,*)$ *un grupo y sea* $a \in G$. *Se define:*

1. $a^0 = e$
2. $a^{n+1} = a * a^n, \quad n \geq 0$

Definición

El ***orden*** *de un elemento* $a \in G$ *es el menor entero positivo* n *tal que*

$$a^n = e$$

Si no existe tal entero, se dice que el elemento a *tiene* ***orden infinito***.

Ejemplo: En el grupo $(H = \{1, i, -1, -i\}, \cdot)$ tenemos

- $(-1)(-1) = 1 \implies o(-1) = 2$
- $(-i)(-i)(-i)(-i) = 1 \implies o(-i) = 4$

Ejemplo:

- En el grupo $(\mathbb{Z}_6, +_6)$ el elemento neutro es $[0]_6$.
  - $[4]_6 \ +_6 \ [4]_6 \ +_6 \ [4]_6 = [12]_6 = [0]_6 \implies o([4]_6) = 3$
  - $[5]_6 \ +_6 \ \ldots \ +_6 \ [5]_6 = [30]_6 = [0]_6 \implies o([5]_6) = 6$
- En el grupo $(\mathbb{Z}_7^*, \cdot_7)$, el elemento neutro es $[1]_7$.
  - $[2]_7 \ \cdot_7 \ [2]_7 \ \cdot_7 \ [2]_7 = [8]_7 = [1]_7 \implies o([2]_7) = 3$
  - $[6]_7 \ \cdot_7 \ [6]_7 = [36]_7 = [1]_7 \implies o([6]_7) = 2$
- Si consideramos el grupo $(\mathcal{M}_{2\times 2}^*(\mathbb{Z}_p), \cdot)$ de las matrices inversibles de tamaño 2×2 con coeficientes en $\mathbb{Z}_p$, p primo, la matriz $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ tiene orden p.

Definición

Sea $(G,*)$ *un grupo y sea* $\varnothing \neq H \subseteq G$. *Se dice que* H *es un* ***subgrupo*** *de* $(G,*)$ *si* $(H,*)$ *es grupo.*

Ejemplos:

- $(2\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Z}, +)$.
- $(\mathbb{Z}, +)$ es subgrupo de $(\mathbb{R}, +)$.
- $(\{[0]_6, [2]_6, [4]_6\}, +_6)$ es subgrupo de $(\mathbb{Z}_6, +_6)$.

Ejercicio: Demuestra o refuta:

- El subconjunto de los enteros impares es un subgrupo de $(\mathbb{Z}, +)$.
- $(\mathbb{Z}_4, +_4)$ es un subgrupo de $(\mathbb{Z}_{12}, +_{12})$.
- $(\{[1]_{11}, [3]_{11}, [4]_{11}, [5]_{11}, [9]_{11}\}, \cdot_{11})$ es subgrupo de $(\mathbb{Z}_{11}^*, \cdot_{11})$.

En todo grupo G encontramos, al menos, dos subgrupos:

$$\{e\} \quad \text{y el mismo} \quad G.$$

Estos dos subgrupos se llaman ***subgrupos triviales*** o *impropios*; a los demás se les llama ***subgrupos propios***.

Teorema

Sea $(G,*)$ *un grupo y sea* $\varnothing \neq H \subseteq G$. *Son equivalentes:*

1. H *es un subgrupo de* G.
2. H *verifica las condiciones:*
   - *si* $h, k \in H$, *entonces* $h * k \in H$.
   - *si* $h \in H$, *entonces* $h^{-1} \in H$.
3. *Si* $h, k \in H$, *entonces* $h * k^{-1} \in H$.

Ejercicios: Demuestra que:

1. $(\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}, +_{12})$ es un subgrupo de $(\mathbb{Z}_{12}, +_{12})$.
2. El conjunto de matrices

$$\left\{A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad a, b \in \mathbb{R}\right\}$$

es un subgrupo del grupo de matrices $(\mathcal{M}_2(\mathbb{R}), +)$.

Teorema

Sea $(G, *)$ un grupo y sea $\varnothing \neq H \subseteq G$, H finito. Si $*$ es una operación cerrada en H, entonces $(H, *)$ es un subgrupo de $(G, *)$.

$$\forall x, y \in H, \quad x * y \in H \implies H \text{ es un } \textbf{subgrupo} \text{ de } (G, *)$$

Ejemplo: $(\{[1]_7, [2]_7, [4]_7\}, \cdot_7)$ es subgrupo de $(\mathbb{Z}_7^*, \cdot_7)$, ya que

$\cdot_7$	$[1]_7$	$[2]_7$	$[4]_7$
$[1]_7$	$[1]_7$	$[2]_7$	$[4]_7$
$[2]_7$	$[2]_7$	$[4]_7$	$[1]_7$
$[4]_7$	$[4]_7$	$[1]_7$	$[2]_7$

Teorema

Sea $(G, *)$ un grupo y sean H y K dos subgrupos de G. Entonces $H \cap K$ es un subgrupo de G.

Demostración: ***Ejercicio***

Ejemplo: Sea el grupo $(\mathbb{Z}, +)$ y los subgrupos $(2\mathbb{Z}, +)$ y $(3\mathbb{Z}, +)$. Entonces $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.

☛ La **unión** de dos subgrupos, en general no es subgrupo.

Como **contraejemplo** nos sirve el ejemplo anterior. La unión $2\mathbb{Z} \cup 3\mathbb{Z}$, es un subconjunto que no es cerrado para la suma:

$2 + 3 = 5$, pero $5 \notin 2\mathbb{Z}$, ni $5 \notin 3\mathbb{Z}$. Luego $2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Ejercicio Sea S_3 el conjunto de las permutaciones de 3 elementos.

$$S_3 = \{id, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$$

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

- Demuestra que $(S_3, \circ)$ es un grupo de orden 6 no conmutativo.
- Halla un subgrupo de S_3 que sea conmutativo.

Ejercicio Sea el conjunto de funciones $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, donde cada $f_i : \mathbb{R} - \{0,1\} \to \mathbb{R} - \{0,1\}$ para $i : 1, 2, ..., 6$, está definida

$$f_1(x) = x, \qquad f_2(x) = \frac{1}{x}, \qquad f_3(x) = 1 - x,$$

$$f_4(x) = \frac{1}{1-x}, \qquad f_5(x) = \frac{x-1}{x}, \qquad f_6(x) = \frac{x}{x-1}$$

Demuestra que $(\mathbf{F}, \circ)$ es un grupo y determina un subgrupo.

Dado un grupo $(G, *)$ y un elemento $a \in G$, nos preguntamos cuál es el mínimo subgrupo H tal que $a \in H$.

Teorema

Sea $(G, *)$ un grupo y sea $a \in G$. Sea $H = \{a^n : n \in \mathbb{Z}\}$. Entonces $(H, *)$ es un subgrupo de $(G, *)$ y, si $(H', *)$ es otro subgrupo tal que $a \in H'$, entonces $H \subseteq H'$.

Demostración:

- ✓ Claramente, si $a \in H$, entonces también $a^2, a^3, ... \in H$.
- ✓ El elemento neutro, a^0, también debe estar en H.
- ✓ Y ya que $a \in H$, también $a^{-1} \in H$.
- ✓ Además, $(a^{-1})^2 = a^{-2} \in H$, $(a^{-1})^3 = a^{-3} \in H$, ...
- ✓ En resumen, cualquier subgrupo H de $(G, *)$ tal que $a \in H$, debe contener al menos todos los elementos de la forma a^n donde $n \in \mathbb{Z}$.

El mínimo subgrupo de G que contiene al elemento a se denota $\langle a \rangle$.

Ejemplos:

- En el grupo $(\mathbb{Z}_7, +_7)$ el subgrupo generado por $[4]_7$ es

$$\langle [4]_7 \rangle = \{[4]_7, [1]_7, [5]_7, [2]_7, [6]_7, [3]_7, [0]_7\}$$

- En el grupo $(\mathbb{Z}_7^*, \cdot_7)$ el subgrupo generado por $[4]_7$ es

$$\langle [4]_7 \rangle = \{[4]_7, [2]_7, [1]_7\}$$

Definición

*Se dice que un grupo G es **cíclico** si existe un elemento $a \in G$ tal que $\langle a \rangle = G$.*

Ejemplos:

- $(G = \{1, i, -1, -i\}, \cdot)$ es cíclico, pues $i = i^1$, $-1 = i^2, -i = i^3, 1 = i^4$
- $(\mathbb{Z}_4, +_4)$ es cíclico, pues $[1]_4 = [1]_4$, $[1]_4 +_4 [1]_4 = [2]_4$, $[1]_4 +_4 [1]_4 +_4 [1]_4 = [3]_4$, $[1]_4 +_4 [1]_4 +_4 [1]_4 +_4 [1]_4 = [0]_4$

  En general, todo $(\mathbb{Z}_m, +_m)$ es un grupo cíclico.
- El grupo $(\mathbb{Z}_8, +_8)$ es cíclico, ya que el subgrupo $\langle [3]_8 \rangle = (\mathbb{Z}_8, +_8)$.
- El grupo $(\mathbb{Z}_5^*, \times_5)$ es cíclico, ya que el subgrupo $\langle [3]_5 \rangle = (\mathbb{Z}_5^*, \times_5)$.

- Evidentemente, todo grupo cíclico es abeliano. ¿Por qué?
- Sin embargo, el recíproco no es cierto.
- Un contraejemplo es el grupo $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ que es un grupo abeliano, pero no es cíclico. ¿Por qué?

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{00, 01, 10, 11\}$$

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Dado un grupo $(G, *)$ y un subconjunto $S \subseteq G$, nos preguntamos cuál es el mínimo subgrupo H que contiene al subconjunto S.

Definición

Sea S un subconjunto no vacío de un grupo $(G, *)$. El **subgrupo generado por** *S, denotado por $\langle S \rangle$, se define recursivamente*

(B) $S \subseteq \langle S \rangle$.

(R_1) *Si* $x, y \in S$, *entonces* $x * y \in \langle S \rangle$.

(R_2) *Si* $x \in S$, *entonces* $x^{-1} \in \langle S \rangle$.

Ejemplos:

1. Dado el grupo $(\mathbb{Z}, +)$, el subgrupo generado por $\{4\}$ es $\langle\{4\}\rangle = 4\mathbb{Z}$
2. Dado el grupo $(\mathbb{Z}, +)$, el subgrupo generado por $\{4, -6\}$ es $\langle\{4, -6\}\rangle = 2\mathbb{Z}$

Teorema

Sea S un conjunto no vacío del grupo $(G, *)$. Entonces $\langle S \rangle$ consta de todos los productos formados con los elementos de S y sus simétricos (opuesto o inversos).

- Si $S = \{x\}$, generalmente escribiremos $\langle x \rangle$ en lugar de $\langle\{x\}\rangle$.
- El subgrupo $\langle x \rangle$ consta de todos los productos de x y x^{-1}.
  Y cada producto será igual a una potencia de x o de x^{-1}, ya que podemos cancelar una x con una x^{-1}. Por lo tanto,

$$\langle x \rangle = \{x^k | k \in \mathbb{Z}\}$$

Definición

Sea $(G, *)$ un grupo y sea S un subconjunto de G. Se dice que S es un conjunto de **generadores** *de G o que* **genera** *a G, si $\langle S \rangle = G$.*

Ejercicio Sea $(G, *)$ el grupo generado por los elementos a y b tales que $a^3 = b^2 = 1$ y $b * a = a^2 * b$.
Calcula $(b * a)^2$ y escribe la tabla de Cayley de la operación.

Definición

Sean los grupos $(G,*)$ *y* $(H,\perp)$. *Se dice que una función* $\psi\colon G\to H$ *es un* ***homomorfismo de grupos*** *si para todo* $x,y\in G$,

$$\psi(x*y)=\psi(x)\perp\psi(y)$$

Ejemplo: Sean los grupos $(\mathbb{Z},+)$ y $(\mathbb{C}^*,\cdot)$ y la función $\psi\colon\mathbb{Z}\to\mathbb{C}^*$ definida

$$\psi(n)=i^n$$

donde $i=\sqrt{-1}$.

Claramente, ψ es un homomorfismo de grupos, ya que para todo $m,n\in\mathbb{Z}$,

$$\psi(n+m)\overset{(Def.\psi)}{=}i^{n+m}=i^n\cdot i^m\overset{(Def.\psi)}{=}\psi(n)\cdot\psi(m)$$

Teorema

Sea $\psi\colon G\to H$ *un homomorfismo de grupos.*

1. *Si* e_G *es el elemento neutro de* G *y* e_H *es el elemento neutro de* H, *entonces* $\psi(e_G)=e_H$.
2. *La imagen del elemento simétrico de* $a\in G$ *es el simétrico de la imagen de* a : $\psi(a^{-1})=(\psi(a))^{-1}$.
3. *La imagen de cada subgrupo de* G *es un subgrupo de* H.
4. *La preimagen de cada subgrupo de* H *es un subgrupo de* G.

Demostración*:*Ejercicio

Ejemplo: En el homomorfismo $\psi\colon(\mathbb{Z},+)\to(\mathbb{C}^*,\cdot)$ definido $\psi(n)=i^n$ tenemos que:

1. $\psi(0)=i^0=1$
2. $1\overset{(Prop.1)}{=}\psi(0)=\psi(n+(-n))\overset{(\psi\ es\ homomorf.)}{=}\psi(n)\cdot\psi(-n)$
   Por tanto, $\psi(-n)=(\psi(n))^{-1}$
3. La imagen del subgrupo $2\mathbb{Z}$ es el subgrupo $\{1,-1\}$.
4. La preimagen del subgrupo $\{1\}$ es el subgrupo $4\mathbb{Z}$.

Definición

Sea $\psi\colon G\to H$ *un homomorfismo de grupos. Se llama* ***núcleo*** *del homomorfismo* ψ *al subconjunto de elementos de* G *cuya imagen es el elemento neutro de* e_H. *Se denota* $\mathcal{K}er\psi$.

$$\mathcal{K}er\psi=\{x\in G\mid\psi(x)=e_H\}$$

Ejemplo:
El núcleo del homomorfismo $\psi\colon(\mathbb{Z},+)\to(\mathbb{C}^*,\cdot)$ definido $\psi(n)=i^n$ es

$$\mathcal{K}er\psi=\{x\in\mathbb{Z}\mid\psi(x)=1\}=\{\dots,-8,-4,0,4,8,\dots\}=4\mathbb{Z}$$

Grupos
Núcleo de un Homomorfismo de grupos

Teorema

El núcleo de un homomorfismo de grupos $\psi: G \to H$ *es un subgrupo de* G.

Demostración: ***Ejercicio***

Teorema

Sea $\psi: G \to H$ *un homomorfismo de grupos. Entonces,* $\mathcal{K}er\psi = \{e_G\}$ *si y sólo si* ψ *es inyectiva.*

Demostración: ***Ejercicio***

Grupos
Imagen de un Homomorfismo de grupos

Definición

Sea $\psi: G \to H$ *un homomorfismo de grupos. Se llama* ***imagen*** *del homomorfismo* ψ *al subconjunto de elementos de* H *que son imagen de algún elemento de* G. *Se denota* $\mathcal{I}m\psi$.

$$\mathcal{I}m\psi = \{y \in H \,|\, \exists x \in G,\ \psi(x) = y\}$$

Ejemplo: La imagen del homomorfismo $\psi: (\mathbb{Z}, +) \to (\mathbb{C}^*, \cdot)$ definido $\psi(n) = i^n$ es $\mathcal{I}m\psi = \{y \in \mathbb{C}^* \,|\, \exists m \in \mathbb{Z},\ \psi(m) = y\} = \{1, i, -1, -i\}$

Teorema

$\mathcal{I}m\psi$ *es un subgrupo de* H.

Demostración: ***Ejercicio***

Grupos
Isomorfismo de grupos

Definición

Sean los grupos $(G, *)$ *y* $(H, \perp)$. *Se dice que una función* $\psi: G \to H$ *es un* ***isomorfismo de grupos*** *si es biyectiva y para todo* $x, y \in G$,

$$\psi(x * y) = \psi(x) \perp \psi(y)$$

Ejemplo: Sean los grupos $(\mathbb{Z}_4, +_4)$ y $(H, \cdot)$, donde $H = \{1, i, -1, -i\}$. Un isomorfismo de grupos es la función

$$\begin{array}{rccc} f: & (\mathbb{Z}_4, +_4) & \to & (H, \cdot) \\ & [0]_4 & \mapsto & 1 \\ & [1]_4 & \mapsto & i \\ & [2]_4 & \mapsto & -1 \\ & [3]_4 & \mapsto & -i \end{array}$$

Grupos
Isomorfismo de grupos

Ejemplo:

$+_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

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

$$\begin{array}{rccc} f: & (\mathbb{Z}_4, +_4) & \to & (H, \cdot) \\ & [0]_4 & \mapsto & 1 \\ & [1]_4 & \mapsto & i \\ & [2]_4 & \mapsto & -1 \\ & [3]_4 & \mapsto & -i \end{array}$$

Ejemplo: Dados los grupos $(\mathbb{Z}_4, +_4)$ y $(\mathbb{Z}_5^*, \times_5)$, las funciones

$$f: \begin{array}{ccc} (\mathbb{Z}_4, +_4) & \to & (\mathbb{Z}_5^*, \times_5) \\ [0]_4 & \mapsto & [1]_5 \\ [1]_4 & \mapsto & [2]_5 \\ [2]_4 & \mapsto & [4]_5 \\ [3]_4 & \mapsto & [3]_5 \end{array} \qquad g: \begin{array}{ccc} (\mathbb{Z}_4, +_4) & \to & (\mathbb{Z}_5^*, \times_5) \\ [0]_4 & \mapsto & [1]_5 \\ [1]_4 & \mapsto & [3]_5 \\ [2]_4 & \mapsto & [4]_5 \\ [3]_4 & \mapsto & [2]_5 \end{array}$$

son isomorfismos de grupos.

Teorema

Si $\psi: G \to H$ *es un isomorfismo entre los grupos* $(G, *)$ *y* $(H, \bullet)$, *entonces:*

1. $(G, *)$ *es abeliano si y sólo si* $(H, \bullet)$ *es abeliano.*
2. $(G, *)$ *es cíclico si y sólo si* $(H, \bullet)$ *es cíclico.*
3. *Para todo* $a \in G$, $o(a) = o(\psi(a))$.
4. *La función inversa* $\psi^{-1}: H \to G$ *define un isomorfismo de* $(H, \bullet)$ *en* $(G, *)$.

Ejercicio:

- Demuestra que el grupo de Kleinn es isomorfo al grupo $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$, pero no es isomorfo al grupo $(\mathbb{Z}_4, +_4)$.
- Como consecuencia, $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ **no** es isomorfo a $(\mathbb{Z}_4, +_4)$.

Teorema

Sea $(G, *)$ *un grupo cíclico. Se verifica que*

1. *Si* G *es finito con* $|G| = m$, *entonces* $(G, *)$ *es isomorfo al grupo* $(\mathbb{Z}_m, +_m)$.
2. *Si* G *es infinito, entonces* $(G, *)$ *es isomorfo al grupo* $(\mathbb{Z}, +)$.

Ejemplo El grupo $(H = \{1, i, -1, -i\}, \cdot)$ es isomorfo al grupo $(\mathbb{Z}_4, +_4)$.

Ejercicio Se considera el conjunto de matrices

$$\mathcal{M}(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \ z \in \mathbb{Z} \right\}$$

Demuestra que:

1. $\mathcal{M}(\mathbb{Z})$ es un grupo con la operación multiplicación de matrices.
2. $(\mathcal{M}(\mathbb{Z}), \cdot)$ es isomorfo al grupo $(\mathbb{Z}, +)$.

Clases laterales

Definición

Sea H *un subgrupo de un grupo* $(G, *)$ *y sea* $a \in G$. *Se considera*

$$a * H = \{a * h,\ h \in H\}$$

Al subconjunto $a * H$ *se le llama* **clase lateral izquierda** *del elemento* a *respecto del subgrupo* H. *Análogamente, el subconjunto*

$$H * a = \{h * a,\ h \in H\}$$

se llama **clase lateral derecha** *del elemento* a *respecto del* **subgrupo** H.

Clases laterales

Ejemplo: Grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, Subgrupo $H_1 = \{f_1, f_2\}$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

- Clase lateral izquierda del elemento f_1

$$f_1 \circ H_1 = \{f_1 \circ f_1, f_1 \circ f_2\} = \{f_1, f_2\}$$

- Clase lateral izquierda del elemento f_2

$$f_2 \circ H_1 = \{f_2 \circ f_1, f_2 \circ f_2\} = \{f_2, f_1\}$$

Clases laterales

Ejemplo: Grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, Subgrupo $H_1 = \{f_1, f_2\}$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

- Clase lateral izquierda del elemento f_4

$$f_4 \circ H_1 = \{f_4 \circ f_1, f_4 \circ f_2\} = \{f_4, f_6\}$$

- Clase lateral izquierda del elemento f_6

$$f_6 \circ H_1 = \{f_6 \circ f_1, f_6 \circ f_2\} = \{f_6, f_4\}$$

Clases laterales

Ejemplo: Grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, Subgrupo $H_1 = \{f_1, f_2\}$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

- Clase lateral izquierda del elemento f_3

$$f_3 \circ H_1 = \{f_3 \circ f_1, f_3 \circ f_2\} = \{f_3, f_5\}$$

- Clase lateral izquierda del elemento f_5

$$f_5 \circ H_1 = \{f_5 \circ f_1, f_5 \circ f_2\} = \{f_5, f_3\}$$

Clases laterales

Ejemplo: Grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, Subgrupo $H_1 = \{f_1, f_2\}$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

- Clase lateral derecha del elemento f_1

$$H_1 \circ f_1 = \{f_1 \circ f_1, f_2 \circ f_1\} = \{f_1, f_2\}$$

- Clase lateral derecha del elemento f_2

$$H_1 \circ f_2 = \{f_1 \circ f_2, f_2 \circ f_2\} = \{f_2, f_1\}$$

Clases laterales

Ejemplo: Grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, Subgrupo $H_1 = \{f_1, f_2\}$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

- Clase lateral derecha del elemento f_3

$$H_1 \circ f_3 = \{f_1 \circ f_3, f_2 \circ f_3\} = \{f_3, f_4\}$$

- Clase lateral derecha del elemento f_4

$$H_1 \circ f_4 = \{f_1 \circ f_4, f_2 \circ f_4\} = \{f_4, f_3\}$$

Clases laterales

Ejemplo: Grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, Subgrupo $H_1 = \{f_1, f_2\}$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

- Clase lateral derecha del elemento f_5

$$H_1 \circ f_5 = \{f_1 \circ f_5, f_2 \circ f_5\} = \{f_5, f_6\}$$

- Clase lateral derecha del elemento f_6

$$H_1 \circ f_6 = \{f_1 \circ f_6, f_2 \circ f_6\} = \{f_6, f_5\}$$

Clases laterales

Veamos por qué se dan estos nombres. En G podemos definir dos relaciones $\sim_i$ y $\sim_d$

$$\forall a, b \in G, \quad a \sim_i b \iff a^{-1} \cdot b \in H$$

$$\forall a, b \in G, \quad a \sim_d b \iff a \cdot b^{-1} \in H$$

- Se demuestra que $\sim_i$ y $\sim_d$ son relaciones de equivalencia.
- Y para cada $a \in G$, denotamos

$[a]_i$ la clase para la relación $\sim_i$

$[a]_d$ la clase para la relación $\sim_d$

Clases laterales

Cada clase $[a]_i$ estará formada por todos los elementos $x \in G$ que se relacionan con a

$$x \in [a]_i \iff a \sim_i x \iff a^{-1} * x \in H \iff a^{-1} * x = h \in H$$

$$\iff x = a * h,\ h \in H \iff x \in a * H$$

Y análogamente

$$x \in [a]_d \iff a \sim_d x \iff x \sim_d a \iff x * a^{-1} \in H$$

$$\iff x * a^{-1} = h \in H \iff x = h * a,\ h \in H \iff x \in H * a$$

Clases laterales

Para cada elemento $x \in G$ tenemos

$$x \in [a]_i \iff x \in a * H$$

$$x \in [a]_d \iff x \in H * a$$

Así nos quedan las particiones

$$G_{/\sim_i} = \{[a]_i,\ a \in G\} = \{a * H,\ a \in G\}$$

$$G_{/\sim_d} = \{[a]_d,\ a \in G\} = \{H * a,\ a \in G\}$$

Clases laterales

Ejemplo: Para el grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ y el subgrupo $H_1 = \{f_1, f_2\}$, la partición correspondiente a la relación $\sim_i$ es

$$\Big\{\{f_1, f_2\}, \{f_3, f_5\}, \{f_4, f_6\}\Big\}$$

Y la partición correspondiente a la relación $\sim_d$ es

$$\Big\{\{f_1, f_2\}, \{f_3, f_4\}, \{f_5, f_6\}\Big\}$$

Definición

Sea H un subgrupo de un grupo $(G, *)$. Se dice que H es un **subgrupo normal** *o* **invariante** *si para cada $a \in G$ se verifica:*

$$a * H = H * a$$

Ejemplo: El subgrupo $H = \{f_1, f_4, f_5\}$ es un subgrupo normal del grupo $\mathbf{F} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$

Clases laterales

Observaciones

- ✓ La clase del elemento neutro es el subgrupo H

$$e * H = H$$

- ✓ $a \in a * H$, ¿por qué?
- ✓ El subconjunto $a * H$ no es subgrupo, a menos que $a \in H$.
- ✓ Si $b \in a * H$, entonces $b * H = a * H$.

Teorema

Sea H un subgrupo de un grupo $(G, *)$ y sean $a, b \in G$. Entonces $a * H = b * H$ ó bien $a * H \cap b * H = \varnothing$. Análogamente para las clases laterales a la derecha.

Demostración: Trivial por ser $\sim_i$ y $\sim_d$ relaciones de equivalencia.

Clases laterales

Teorema

Sea H un subgrupo del grupo $(G, *)$. Entonces cada clase lateral de H en G tiene el mismo cardinal que H.

Demostración:

- ✓ Para cada $a \in G$, la función $f : H \to H$, definida $f(h) = a * h$ es biyectiva.
- ✓ Por lo tanto, $|H| = |a * H|$.

Clases laterales

Teorema (Lagrange)

Sea H un subgrupo de un grupo finito $(G, *)$. Entonces el cardinal de H divide al cardinal de G.

Demostración: Por ser $\{a_1 * H, \cdots, a_k * H\}$ una partición de G,

$$|G| = \sum_{i=1}^{k} |a_i * H|$$

Aplicando el teorema anterior,

$$|G| = \sum_{i=1}^{k} |a_i * H| = |H| + |H| + \cdots + |H| = k|H|$$

Clases laterales

Corolario

1. *Sea $a \in G$. Entonces el orden del elemento a divide al orden de G.*
2. *Si G es un grupo de orden primo, entonces es cíclico.*

Ejercicio: Demuestra que:

- Si G es un grupo con siete elementos, entonces G es abeliano.

Bibliografía

Algebra lineal J. de Burgos (Ed. McGraw Hill)

Matemáticas discreta y combinatoria R.P. Grimaldi (Ed. Addison Wesley)

Estructuras de Matemáticas Discretas para la Computación
B. Kolman y R.C. Busby (Ed. Prentice Hall)

Estructuras de Matemáticas Discretas para la Computación
B. Kolman, R.C. Busby y S. Ross (Ed. Prentice Hall)

Elementos de Matemáticas Discretas C.L. Liu (Ed. McGraw Hill)