Grupos, Anillos y Cuerpos

Mariam Cobalea Vico

Universidad de Málaga
Dpto. de Matemática Aplicada

Curso 16/17

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**: $\forall a \in G,\ \exists a' \in G,\ \ a * a' = a' * a = e$

Se dice que es un **grupo abeliano** *si además se verifica la propiedad*

- **Conmutativa**: $\forall a, b \in G,\ a * b = b * a$

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

Grupos

Ejemplos

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

Teorema

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

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

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 (Cancelación)

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 $b = c$*

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 como $f(x) = a * x$ es biyectiva.*

Grupos

Propiedades de los grupos

Definición

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

La operación de un grupo finito se puede dar con una **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

Grupos

Propiedades de los grupos

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 es cierto.

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.

Grupos

Operación compatible con una relación de equivalencia

Definición

Sea A un conjunto con una relación de equivalencia $\sim$ y una operación binaria $*$. Se dice que $\sim$ y $*$ son **compatibles** *si para todo $a_1, a_2, b_1, b_2 \in A$ tales que $a_1 \sim a_2$ y $b_1 \sim b_2$, entonces se tiene que $a_1 * b_1 \sim a_2 * b_2$.*

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

Ejemplo

En $\mathbb{Z}$, la suma y el producto son compatibles con la relación de equivalencia congruencia módulo m, $\quad a \equiv b \ (\text{mód } m) \iff a - b = k \cdot m, \quad k \in \mathbb{Z}$

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

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

Grupos

Operación compatible con una relación de equivalencia

Ejemplo

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

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

- La operación $+_m$ es asociativa, 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.

Grupos

Operación compatible con una relación de equivalencia

Ejemplo

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

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

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

Grupos

Operación compatible con una relación de equivalencia

Ejemplos

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

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

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

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

Grupos

Producto directo

Teorema

Dados los grupos $(G, *)$ y $(H, \cdot)$, el **producto directo** *$(G \times H, \oplus)$ es un grupo, donde la operación $\oplus$ se define como $(g_1, h_1) \oplus (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$.*
Si G y H son finitos, entonces $|G \times H| = |G| \times |H|$.

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

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

Grupos

Subgrupos

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.*

Todo grupo G tiene, al menos, dos subgrupos impropios: $\{e\}$ y el mismo G.

Ejemplos

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

Teorema

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

1. *H es un subgrupo de G.*
2. *Si $h, k \in H$, entonces $h * k^{-1} \in H$.*

Grupos

Subgrupos

Teorema

Sea $(G,*)$ un grupo y sea $\varnothing \neq H \subseteq G$, H **finito**. *Si para cualesquiera $x, y \in H$ se tiene que $x * y \in H$ ($*$ es una operación cerrada en H) entonces $(H,*)$ es un subgrupo de $(G,*)$.*

Ejemplo

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

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

Grupos

Subgrupos

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 $(\mathbb{Z}_{11}^*, \cdot_{11})$.

Ejercicio

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 $(\mathcal{M}_2(\mathbb{R}), +)$.

Grupos

Unión e Intersección de Subgrupos

Teorema

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

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

Ejemplo

$2\mathbb{Z} \cap 3\mathbb{Z}$ es un subgrupo de $(\mathbb{Z}, +)$, que coincide con $6\mathbb{Z}$.

Sin embargo, $2\mathbb{Z} \cup 3\mathbb{Z}$ no es un subgrupo de $(\mathbb{Z}, +)$.

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 $2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Grupos

Subgrupos

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.

Grupos

Orden de un elemento

Definición

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

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

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**.

Ejemplos

En el grupo $\mathbb{H} = (\{1, i, -1, -i\}, \cdot)$ tenemos $o(-1) = 2$, y $o(-i) = 4$,

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

Grupos

Orden de un elemento

Ejemplos

- 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.

Grupos

Grupos cíclicos

Teorema

Sea $(G, *)$ un grupo y $c \in G$. El mínimo subgrupo de G que contiene a c es $\{c^n : n \in \mathbb{Z}\}$, y se denota $\langle c \rangle$.

Ejemplo

- 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 $c \in G$ tal que $\langle c \rangle = G$.*

Ejemplos

- El grupo $(\mathbb{Z}_7, +_7)$ es cíclico, y está generado por $[4]_7$, ya que
  $\langle [4]_7 \rangle = \{[4]_7, [1]_7, [5]_7, [2]_7, [6]_7, [3]_7, [0]_7\}$
  En general, todo $(\mathbb{Z}_m, +_m)$ es un grupo cíclico.
- $\mathbb{H} = (\{1, i, -1, -i\}, \cdot)$ es cíclico, pues $i = i^1$, $-1 = i^2, -i = i^3, 1 = i^4$.

Grupos

Grupos cíclicos

- 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

Grupos

Homomorfismos de grupos

Definición

Dados dos grupos $(G,*)$ y $(H,\cdot)$, una función $\psi\colon G \to H$ es un **homomorfismo de grupos** *si para todo $x, y \in G$, se tiene que $\psi(x*y) = \psi(x)\cdot\psi(y)$.*

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 $m, n \in \mathbb{Z}$,

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

Grupos

Homomorfismos de grupos

Teorema

Sea $\psi\colon G \to H$ un homomorfismo de grupos, entonces:

1. *ψ conserva el elemento neutro: $\psi(e_G) = e_H$*
2. *ψ conserva el elemento simétrico: $\psi(a^{-1}) = \big(\psi(a)\big)^{-1}$*
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.*

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

Grupos

Núcleo de un homomorfismo de grupos

Definición

El **núcleo** *de un homomorfismo* $\psi\colon G \to H$*, denotado* $\ker\psi$*, es el subconjunto de elementos de* G *cuya imagen es el elemento neutro de* H*.*

Observación

Por ser la preimagen del subgrupo trivial $\{e_h\}$, el núcleo de un homomorfismo de grupos $\psi\colon G \to H$ es un subgrupo de G.

Ejemplo

Para el homomorfismo $\psi\colon (\mathbb{Z},+) \to (\mathbb{C}^*,\cdot)$ definido por $\psi(n) = i^n$ se tiene que

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

Teorema

Sea $\psi\colon G \to H$ *un homomorfismo.* $\ker\psi = \{e_G\}$ *si y solo si* ψ *es inyectiva.*

Grupos

Imagen de un Homomorfismo de grupos

Definición

La **imagen** *de un homomorfismo* $\psi\colon G \to H$*, denotado* $\text{Im}\,\psi$*, es el subconjunto de elementos de* H *que son imagen de algún elemento de* G*.*

Ejemplo

La imagen del homomorfismo $\psi\colon (\mathbb{Z},+) \to (\mathbb{C}^*,\cdot)$ definido por $\psi(n) = i^n$ es

$$\text{Im}\,\psi = \{y \in \mathbb{C}^* \mid \exists m \in \mathbb{Z},\ \psi(m) = y\} = \{1, i, -1, -i\}$$

Observación

Por ser la imagen del grupo G, se tiene que $\text{Im}\,\psi$ es un subgrupo de H.

Grupos

Isomorfismo de grupos

Definición

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

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

Ejemplo

Sean los grupos $(\mathbb{Z}_4, +_4)$ y $(\mathbb{H}, \cdot)$. La función $f : \mathbb{Z}_4 \to \mathbb{H}$ definida abajo es un isomorfismo de grupos:

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

Grupos

Isomorfismo de grupos: Grupos cíclicos

Teorema

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

1. $(G, *)$ *es abeliano si y solo si* $(H, \cdot)$ *es abeliano.*
2. $(G, *)$ *es cíclico si y solo si* $(H, \cdot)$ *es cíclico.*
3. *Para todo* $c \in G$, *el orden de* c *coincide con el de* $\psi(c)$.
4. *La función inversa* $\psi^{-1}\colon H \to G$ *es un isomorfismo de* $(H, \cdot)$ *en* $(G, *)$.

Ejemplo

Son isomorfismos de grupos las funciones

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

Grupos

Isomorfismo de grupos: Grupos cíclicos

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 $(\mathbb{Z},+)$.

Subgrupos normales

Clases laterales

Definición

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

- *La* **clase lateral izquierda** *del elemento a respecto del subgrupo H es el conjunto $aH = \{a * h,\ h \in H\}$.*
- *La* **clase lateral derecha** *del elemento a respecto del subgrupo H es el conjunto $Ha = \{h * a,\ h \in H\}$.*

Observación

Para que las clases laterales sean distintas, el grupo no puede ser conmutativo.

Lema

Un subgrupo H de $(G,*)$ induce dos particiones de G usando las clases laterales

$$G/H = \{aH,\ a \in G\} \qquad G\backslash H = \{Ha,\ a \in G\}$$

Subgrupos normales

Grupo cociente

Definición

Sea H un subgrupo de un grupo $(G, *)$. Se dice que H es un **subgrupo normal** *si para cada $a \in G$ se tiene que $aH = Ha$.*

Ejemplo

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

Un subgrupo normal permite definir el *grupo cociente*, de forma análoga al *conjunto cociente* respecto de una relación de equivalencia:

- $G/H = G\backslash H$, por definición.
- Podemos definir la operación $aH \cdot bH = (a * b)H$

Teorema

Si H es subgrupo normal de G, entonces G/H es un grupo con la operación anterior.

Teorema de Lagrange

Lema

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

Teorema (Lagrange)

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

Corolario

1. *Dado $c \in G$, el orden de c 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.

Introducción a la Teoría de la Codificación

- Nos planteamos la **transmisión** segura de un **mensaje** sobre un canal de comunicación que puede estar afectado por **ruido**.
- El resultado es que **el mensaje recibido o leido puede ser diferente del enviado o almacenado originalmente**. En este caso decimos que ha habido **error** en la transmisión.
- Para que el mensaje original se pueda recuperar con un cierto grado de certeza, el mensaje que se transmite lleva información **redundante**.
- La **teoría de codificación** ha desarrollado técnicas para introducir en los datos transmitidos información redundante que ayude a **detectar** (e incluso a **corregir**) los errores.
- Algunas de éstas técnicas utilizan la **teoría de grupos**.

Codificación de la información y detección de errores

Definición

- *Se llama* **palabra** *a una cadena de símbolos de un alfabeto.*
- *Un* **código** *es una colección de palabras usadas para representar mensajes. Una palabra de un código se llama también* **palabra clave**.
- *Un* **código de bloques** *está formado por palabras con la misma longitud.*

1. Trabajaremos en binario, con el alfabeto $\{0, 1\}$.
2. Las palabras de longitud m se pueden considerar como elementos del grupo $(\mathbb{Z}_2^m, \oplus)$, escritos sin paréntesis ni corchetes.

Codificación de la información y detección de errores

Definiciones

- Si nuestro mensaje original está compuesto por palabras de longitud m, entonces se elige un entero $n > m$ y una función inyectiva $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ que se llama **función de codificación** (m, n).
- Cada palabra de $\mathbb{Z}_2^m$ se representa mediante una palabra de $\mathbb{Z}_2^n$.
- De esta forma, si $x \in \mathbb{Z}_2^m$, entonces $\mathcal{C}(x)$ es la **palabra codificada** que representa a x.
- Al conjunto Im $\mathcal{C}$ se le denota $\mathcal{W}$ y se le llama también **código** o conjunto de **palabras clave**.

Codificación de la información y detección de errores

Ejemplos

1. Función de codificación de **control de paridad** $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^{m+1}$

$$\mathcal{C}(x) = xc, \text{ donde } c = \begin{cases} 0, & \text{si hay una cantidad par de unos en } x \\ 1, & \text{si hay una cantidad impar de unos en } x \end{cases}$$

   El último dígito es un dígito de control de paridad: cualquier palabra transmitida correctamente tiene un número par de unos.

2. Función de codificación de **triple repetición** $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^{3m}$

$$\mathcal{C}(x) = xxx$$

   Supongamos que xxx es la palabra enviada y abc es la palabra recibida. Si no ha habido errores,

$$a = b = c = x$$

Codificación de la información y detección de errores

Definiciones

- Se llama **peso** de una palabra x, y se denota $|x|$, al número de unos de x.
- Dadas dos palabras de la misma longitud, u y v, se define $\delta(u, v)$, la **distancia** entre u y v, como el número de posiciones en que difieren. Este número coincide con el peso de su diferencia, esto es, $\delta(u, v) = |u \oplus v|$.

Ejemplo

$|10001| = 2, \quad \delta(11011, 10101) = 3$

- Una **buena** función de codificación será aquella que **maximice** las distancias entre palabras clave.

Teorema (Propiedades de la distancia)

Para cualesquiera $x, y, z \in \mathbb{Z}_2^m$ se cumplen las siguientes propiedades:

1. $\delta(x, y) = \delta(y, x)$
2. $\delta(x, y) \geq 0$
3. $\delta(x, y) = 0 \iff x = y$
4. $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$

Codificación de la información y detección de errores

Definiciones

Sea $\mathcal{C}$ una función de codificación (m, n).

- Se dice que la palabra clave $\mathcal{C}(x)$ se ha transmitido con k **errores** a lo sumo si la palabra enviada $\mathcal{C}(x)$ y la palabra recibida v difieren entre 1 y k posiciones. Es decir, si $1 \leq \delta(\mathcal{C}(x), v) \leq k$.
- Se dice que $\mathcal{C}$ **detecta** a lo sumo k errores si siempre que $\mathcal{C}(x)$ se transmite con a lo sumo k errores, la palabra recibida v no es una palabra clave.
- La **mínima distancia** de una función de codificación $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ es

$$\text{mín}\{\delta(\mathcal{C}(x), \mathcal{C}(y)) \mid x, y \in \mathbb{Z}_2^m, \quad x \neq y\}$$

Codificación de la información y detección de errores

Teorema

Sea $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *una función de codificación* (m, n)*, entonces:*

1. $\mathcal{C}$ *permite* **detectar** *a lo sumo* k *errores si y solo si la mínima distancia de* $\mathcal{C}$ *es al menos* $k+1$.
2. $\mathcal{C}$ *permite* **corregir** k *errores a lo sumo si y solo si la mínima distancia de* $\mathcal{C}$ *es al menos* $2k+1$.

Ejemplo

Para la función de codificación $\mathcal{C}: \mathbb{Z}_2^4 \to \mathbb{Z}_2^9$ definida como $\mathcal{C}(x) = xxc$, donde $c = \begin{cases} 0, & |x| \text{ es par} \\ 1, & |x| \text{ es impar} \end{cases}$, la mínima distancia es 3.

Según el teorema anterior, con $\mathcal{C}$ se pueden detectar hasta dos errores, pero solo se podrá corregir uno.

Códigos de grupo

Usando la teoría de grupos, se puede calcular la mínima distancia de una función de codificación de una manera relativamente simple.

Definición

Una función de codificación $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *es un* **código de grupo** *(o* **lineal***) si* $Im\ \mathcal{C} = \mathcal{W}$ *es un subgrupo de* $\mathbb{Z}_2^n$.

Teorema

Sea $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *un código de grupo, entonces la mínima distancia de* $\mathcal{C}$ *coincide con el mínimo peso de las palabras clave no nulas. Esto es,*

$$\text{mín}\{\delta(\mathcal{C}(x), \mathcal{C}(y)), \mid x, y \in \mathbb{Z}_2^m, x \neq y\} = \text{mín}\{|\mathcal{C}(x)| \mid 0 \neq x \in \mathbb{Z}_2^m\}$$

En el último ejemplo bastará con calcular los pesos de 15 palabras en vez de hallar las 104 distancias entre parejas de palabras clave distintas.

Códigos de grupo

- Como $(\mathbb{Z}_2^m, \oplus)$ y $(\mathbb{Z}_2^n, \oplus)$ son grupos, obtendremos un código de grupo siempre que la función de codificación sea homomorfismo de grupos.

Definición (Matriz generadora $\mathcal{G}$)

Sean $m, n \in \mathbb{Z}$, con $m < n$. Una **matriz generadora** *$\mathcal{G}$ es una matriz $m \times n$ con entradas en $\mathbb{Z}_2$ tal que las primeras m columnas forman la matriz identidad I_m. Luego, se tiene que $\mathcal{G} = \begin{pmatrix} I_m & A \end{pmatrix}$ donde A es una matriz $m \times (n-m)$.*

Teorema

Sea $\mathcal{G}$ una matriz generadora. Entonces $\mathcal{C}_\mathcal{G} : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ definido como $\mathcal{C}_\mathcal{G}(x) = x\mathcal{G}$ nos da un código de grupo.

Códigos de grupo

Ejemplo

Sea la función de codificación $\mathcal{C}_\mathcal{G} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^4$ dada por la matriz generadora

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} \mathcal{C}_\mathcal{G}(00) &= 0000 \\ \mathcal{C}_\mathcal{G}(01) &= 0101 \\ \mathcal{C}_\mathcal{G}(10) &= 1011 \\ \mathcal{C}_\mathcal{G}(11) &= 1110 \end{aligned}$$

$$\text{Im } \mathcal{C} = \mathcal{W} = \{0000, 0101, 1011, 1110\}$$

La mínima distancia entre palabras clave es 2, por eso el código puede detectar un error, pero no puede corregir errores.

Códigos de grupo

Ejemplo

Sea la función de codificación $\mathcal{C}_\mathcal{G}: \mathbb{Z}_2^2 \to \mathbb{Z}_2^5$ dada por la matriz generadora

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\begin{aligned} \mathcal{C}_\mathcal{G}(00) &= 00000 \\ \mathcal{C}_\mathcal{G}(01) &= 01011 \\ \mathcal{C}_\mathcal{G}(10) &= 10110 \\ \mathcal{C}_\mathcal{G}(11) &= 11101 \end{aligned}$$

$$\text{Im } \mathcal{C} = \mathcal{W} = \{00000, 01011, 10110, 11101\}$$

La mínima distancia es 3, por eso el código puede detectar 2 errores y corregir 1.

Ejercicio

Sea $\mathcal{C} \subseteq \mathbb{Z}_2^5$ un código de grupo de cuatro elementos. Sabiendo que 10101 y 11010 son elementos de $\mathcal{C}$, determina los restantes elementos de $\mathcal{C}$ y una matriz generadora del código.

Códigos de grupo

Ejemplo

Sea la función de codificación $\mathcal{C}_\mathcal{G}: \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$ dada por la matriz generadora

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{aligned} \mathcal{C}_\mathcal{G}(000) &= 000000 \\ \mathcal{C}_\mathcal{G}(001) &= 001111 \\ \mathcal{C}_\mathcal{G}(010) &= 010101 \\ \mathcal{C}_\mathcal{G}(011) &= 011010 \\ \mathcal{C}_\mathcal{G}(100) &= 100111 \\ \mathcal{C}_\mathcal{G}(101) &= 101000 \\ \mathcal{C}_\mathcal{G}(110) &= 110010 \\ \mathcal{C}_\mathcal{G}(111) &= 111101 \end{aligned}$$

$$\mathcal{W} = \{000000, 001111, 010101, 011010, 100111, 101000, 110010, 111101\}$$

La mínima distancia entre palabras clave es 2, por eso el código puede detectar 1 error, pero no puede corregir ni siquiera un simple error.

Detección y corrección de errores

- Sea $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ un código de grupo y sea $\mathcal{W}$ el conjunto de palabras clave (que es un subgrupo de $\mathbb{Z}_2^n$).
- Se envía la palabra $\mathcal{C}(x) = w$, pero ocurre algún error y se recibe v. Nuestro problema es identificar la palabra $\mathcal{C}(x) = w$ del mensaje original.
- Si al enviar w ocurre un error en el último dígito, por ejemplo, y se recibe la palabra v, entonces v coincide con w en todos los dígitos excepto en el último; por lo tanto, $v = e_n \oplus w$, donde $e_n = 0\ldots01$
- Así pues, el conjunto de palabras que se pueden recibir como resultado de un simple error en el último dígito es la **clase lateral de e_n respecto de $\mathcal{W}$**, $e_n \oplus \mathcal{W}$.
- Análogamente, para un error en el dígito j, obtendremos una palabra de la clase lateral $e_j \oplus \mathcal{W}$ del elemento e_j respecto al subgrupo $\mathcal{W}$.

Detección y corrección de errores

Tabla de descodificación

Es posible agrupar todos los cálculos mediante una tabla que muestre la partición determinada por las clases laterales.

Tabla de descodificación

Se construye siguiendo los pasos:

1. Se escriben los elementos de $\mathcal{W}$ en la primera fila.
2. Se busca una palabra de peso mínimo e que no esté en $\mathcal{W}$.
3. Se escribe la palabra $e \oplus w$ bajo cada palabra clave.
4. Se busca una palabra de peso mínimo e' que todavía no esté escrita y se escribe la clase lateral $e' \oplus \mathcal{W}$ en la siguiente línea.

Se repite este procedimiento hasta que hayan aparecido todos los elementos de $\mathbb{Z}_2^n$.

Detección y corrección de errores

Tabla de descodificación

Ejemplo

Sea la función de codificación $\mathcal{C}_\mathcal{G}: \mathbb{Z}_2^2 \to \mathbb{Z}_2^5$ dada por la matriz generadora

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\begin{aligned} \mathcal{C}_\mathcal{G}(00) &= 00000 \\ \mathcal{C}_\mathcal{G}(01) &= 01011 \\ \mathcal{C}_\mathcal{G}(10) &= 10110 \\ \mathcal{C}_\mathcal{G}(11) &= 11101 \end{aligned}$$

Una tabla de decodificación es

00000	01011	10110	11101
00001	01010	10111	11100
00010	01001	10100	11111
00100	01111	10010	11001
01000	00011	11110	10101
10000	11011	00110	01101
10001	11010	00111	01100
00101	01110	10011	11000

Códigos de grupo

¿Cómo detectar y corregir errores en un mensaje recibido?

Al recibir una palabra v, buscamos dónde está situada en la tabla.

Una vez encontrada, la reemplazamos por la palabra clave que está en la primera fila de su columna:

$$v = e \oplus w \implies (-e) \oplus v = (-e) \oplus e \oplus w \implies w = -e \oplus v = e \oplus v$$

Este procedimiento se resumen en:

1. Se determinan todas las clases laterales respecto de $\mathcal{W}$.
2. En cada clase se elige una palabra de peso mínimo (**representante** de la clase).
3. Para una palabra recibida v, la palabra transmitida (con mayor probabilidad) es $e \oplus v$, donde e es el representante de la clase a la que pertenece v.

Detección y corrección de errores

Tabla de descodificación

Ejemplo

Se quiere enviar el mensaje 00 01 10 11 11 01 00

Se codifica usando la matriz $\mathcal{G}$ del ejemplo anterior y se envía,

00000 01011 10110 11101 11101 01011 00000

pero se recibe

00000 0**0**011 1**11**0 11101 1**0**101 **111**0**1** 0**1**000

Al aplicar la tabla de descodificación se obtiene

00000 01010 11101 11101 11101 11101 00000

Por último, extrayendo los dos primeros dígitos de cada palabra, nos queda

00 01 **11** 11 11 **11** 00

Hemos corregido los errores simples, aunque no los dobles ni los triples.

Matriz de verificación de paridad

Es posible evitar calcular la tabla de descodificación usando algo más de álgebra.

Definición

Dada una matriz generadora $\mathcal{G} = \begin{pmatrix} I_m & A \end{pmatrix}$, *su* **matriz de verificación de paridad** *asociada es la matriz* $\mathcal{H} = \begin{pmatrix} A \\ I_{n-m} \end{pmatrix}$.

El **síndrome** *de una palabra* $v \in \mathbb{Z}_2^n$, *se define como* $v\mathcal{H}$.

Ejemplo

Tenemos $m = 2, n = 5, n - m = 3$

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad \mathcal{H} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

El síndrome de 01100 es $01100\mathcal{H} = 111$.

El síndrome de 11101 es $11101\mathcal{H} = 000$.

Matriz de verificación de paridad

Teorema

Sea $\mathcal{H}$ una matriz de verificación de paridad asociada a una matriz $\mathcal{G}$ generadora de un código de grupo. Entonces w es una palabra clave si y sólo si su síndrome $w\mathcal{H}$ es el elemento neutro de $\mathbb{Z}_2^{n-m}$.

Corolario

Dos palabras están en la misma fila de la tabla de descodificación si y sólo si tienen el mismo síndrome.

Del corolario se deduce que existe una biyección entre los síndromes y las clases laterales (las filas de la tabla de descodificación).
Conociendo esta biyección podemos usar la capacidad de corrección del código sin necesidad de la tabla.

Códigos de grupo

Matriz $\mathcal{H}$ de verificación de paridad

Ejemplo

Sea un código de grupo dado por

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Usando la equivalencia

000	001	010	011	100	101	110	111
A	C	E	N	O	R	S	T

se codifica y envía un mensaje que se recibe

101110 100001 101011 111011 010011 011110 111000 100001

¿Qué información se quiere transmitir?

Códigos de grupo

Matriz $\mathcal{H}$ de verificación de paridad

Solución

Usamos la matriz de verificación de paridad $\mathcal{H}$, para establecer la biyección entre los síndromes y cada uno de los representantes (*líderes*) de cada clase lateral.

$$\mathcal{H} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Líderes	Síndromes
000000	000
000001	001
000010	010
000100	100
001000	110
010000	011
100000	101
100010	111

Códigos de grupo

Matriz $\mathcal{H}$ de verificación de paridad

Solución

1. Calculamos el síndrome $v\mathcal{H}$ de cada palabra v recibida:

   101 100 000 011 000 011 000 100

2. Hallamos los líderes e asociados usando la biyección:

   100000 000100 000000 010000 000000 010000 000000 000100

3. Se corrige el mensaje haciendo $w = e \oplus v$

   001110 100**1**01 101011 **1**01011 010011 0**0**1110 111000 100**1**01

4. Ignorando la información redundante, se obtiene el mensaje inicial

   $\underbrace{001}_{\mathbf{C}}110$ $\underbrace{100}_{\mathbf{O}}101$ $\underbrace{101}_{\mathbf{R}}011$ $\underbrace{101}_{\mathbf{R}}011$ $\underbrace{010}_{\mathbf{E}}011$ $\underbrace{001}_{\mathbf{C}}110$ $\underbrace{111}_{\mathbf{T}}000$ $\underbrace{100}_{\mathbf{O}}101$

Anillos

Estructuras algebraicas con dos operaciones

Para resolver en $\mathbb{Z}$ una ecuación tal como

$$2(x+3)+4(x-5)=28$$

procedemos de la siguiente manera:

- Se aplica la propiedad distributiva del producto respecto a la suma
$$(2x+2\cdot 3)+(4x+4(-5))=28$$
- Se aplican las propiedades asociativa y conmutativa de la suma
$$(2x+4x)+(6-20)=28$$
- Se aplica la propiedad distributiva del producto respecto a la suma y se suma 14 en ambos miembros
$$((2+4)x+(-14))+14=28+14$$
- Se aplica la propiedad asociativa de la suma
$$6x+((-14)+14)=42$$

Anillos

Estructuras algebraicas con dos operaciones

- Se aplica la propiedad del opuesto
$$6x+(0)=42$$
- Se usa la propiedad de identidad del neutro de la suma
$$6x=42$$
- Se aplica la propiedad de simplificación del producto
$$6x=6\cdot 7 \implies x=7$$

En este ejemplo, además de usar que la suma y el producto son operaciones binarias en el conjunto de los enteros, se aplican otras propiedades.

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

Anillos

Estructuras algebraicas con dos operaciones

Definición

Se dice que $(A,+,\cdot)$ *es un* **anillo** *si* $+$ *y* $\cdot$ *dos operaciones binarias en* A *tales que:*

1. $(A,+)$ *es grupo abeliano.*
2. *La operación* $\cdot$ *es asociativa:* $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
3. *La operación* $\cdot$ *es distributiva respecto de* $+$ $\begin{cases} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (b+c)\cdot a &= b\cdot a + c\cdot a \end{cases}$

Ejemplos (de anillos)

1. $(\mathbb{Z},+,\cdot),(m\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$
2. Los enteros módulo m $(\mathbb{Z}_m,+_m,\cdot_m)$, para $1<m\in\mathbb{N}$
3. Las matrices cuadradas $(\mathcal{M}_{n\times n}(\mathbb{R}),+,\cdot)$
4. El conjunto $\mathcal{F}(\mathbb{R})=\{f: D\subseteq\mathbb{R}\to\mathbb{R}\}$ con la suma y el producto usuales

Anillos

Teorema

Sea $(A,+,\cdot)$ *un anillo. Para todo* $a,b\in A$ *se verifica:*

1. $a\cdot 0 = 0\cdot a = 0$
2. $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$
3. $(-a)\cdot(-b) = a\cdot b$

Definición

$(A,+,\cdot)$ es un **anillo unitario** si tiene elemento unidad para el producto.

Ejemplos

1. Los ejemplos anteriores de anillo son unitarios, salvo $m\mathbb{Z}$.
2. En $(\mathcal{F}(\mathbb{R}),+,\cdot)$, el elemento unidad es la función constante 1.
3. En el anillo de matrices $(\mathcal{M}_{n\times n}(\mathbb{R}),+,\cdot)$, la unidad es la matriz identidad

Anillos

Definiciones adicionales

Definición

- $(A, +, \cdot)$ es **anillo conmutativo** si la operación $\cdot$ es conmutativa.
- Dos elementos $a, b \in A$ son **permutables** si $a \cdot b = b \cdot a$

Ejemplo

- $(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \cdot)$ es un anillo no conmutativo, ya que

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 11 & 16 \end{pmatrix} \neq \begin{pmatrix} 4 & 7 \\ 8 & 15 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$$

- Sin embargo, $\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$ y $\begin{pmatrix} -3 & 1 \\ 2 & 0 \end{pmatrix}$ son permutables.

☛ En los anillos no conmutativos, en general

$$(a+b)^2 = a^2 + ab + ba + b^2 \neq a^2 + 2ab + b^2$$

Anillos

Definiciones adicionales

Definición

1. Los elementos **inversibles** de $(A, +, \cdot, 1)$ son aquellos elementos $a \in A$ que tienen simétrico (inverso) a^{-1} respecto a la segunda operación.

Ejemplos

1. En $(\mathbb{Z}_9, +_9, \cdot_9)$, son inversibles $[1], [2], [4], [5], [7], [8]$
2. En $(\mathcal{M}_2(\mathbb{Z}_2), +, \cdot)$, son inversibles:

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\}$$

Teorema

Dado $(A, +, \cdot, 1)$ sea A^* el subconjunto de todos los inversibles de A. Entonces $(A^*, \cdot)$ es un grupo (el **grupo multiplicativo** *de $(A, +, \cdot)$).*

Anillos

Definiciones adicionales

Definición

Un elemento no nulo $a \in A$ se dice que es **divisor de cero** en un anillo $(A, +, \cdot)$ si existe $b \neq 0$ tal que $a \cdot b = 0$ o bien $b \cdot a = 0$.

Ejemplos

- En el anillo $(\mathbb{Z}_{36}, +_{36}, \cdot_{36})$ la clase $[4]_{36}$ es un divisor de cero ya que existe la clase $[9]_{36} \neq [0]_{36}$ tal que $[4]_{36} \cdot_{36} [9]_{36} = [36]_{36} = [0]_{36}$
- En el anillo $(\mathcal{M}_2(\mathbb{Z}_2), +, \cdot)$ son divisores de cero las matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ y $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, ya que $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

  ¿Es divisor de cero la matriz $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$?

Anillos

Definiciones adicionales

Teorema

En todo anillo $(A, +, \cdot)$ un elemento $0 \neq c \in A$ es simplificable si y sólo si c no es divisor de cero.

☛ Los divisores de cero son elementos que **no** se pueden simplificar.

1. Si en un anillo no existen divisores de cero, entonces es válida para el producto la simplificación.
2. Si un elemento es inversible, entonces es simplificable. Por tanto, ningún elemento inversible es divisor de cero.

$$\text{INVERSIBLE} \implies \text{SIMPLIFICABLE} \iff \text{NO DIVISOR DE CERO}$$

3. Equivalentemente, si un elemento es divisor de cero, entonces es elemento no simplificable y, por tanto, no es inversible.

$$\text{NO INVERSIBLE} \impliedby \text{NO SIMPLIFICABLE} \iff \text{DIVISOR DE CERO}$$

Anillos

Subanillos. Ideales

Definición

Sea el anillo $(A, +, \cdot)$ y sea $\varnothing \neq B \subseteq A$. Se dice que B es **subanillo** *de A si B es anillo con las mismas operaciones que A.*

Se deduce que B es subanillo de A si y sólo si

$$\begin{cases} (B, +) \text{ es subgrupo de } A \\ \cdot \text{ es operación cerrada en } B \end{cases}$$

Aplicando lo estudiado en grupos, podemos afirmar que:

En un anillo $(A, +, \cdot)$, un subconjunto no vacío B es un subanillo de A si y sólo si para todo $a, b \in B$

1. $a - b \in B$
2. $a \cdot b \in B$

Anillos

Subanillos. Ideales

Ejemplos

- Para todo anillo A son subanillos $\{0\}$ y A.
- $\mathbb{Z}$ es subanillo de $\mathbb{Q}$; $\mathbb{Q}$ es subanillo de $\mathbb{R}$; $\mathbb{R}$ es subanillo de $\mathbb{C}$.
- Para todo entero $m > 1$, $m\mathbb{Z}$ es subanillo de $\mathbb{Z}$. Además, $\mathbb{Z}$ sólo admite subanillos del tipo $m\mathbb{Z}$.
- $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$ es subanillo de $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$.
- $\mathcal{J}(i) = \left\{ a + bi \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z} \right\}$ (Enteros de Gauss) es subanillo de $\mathbb{C}$.

Anillos

Subanillos. Ideales

Observaciones

- Si un anillo es conmutativo, lo son todos sus subanillos.
- La unidad no se conserva en subanillos.

Ejemplo

En el anillo unitario $\mathbb{Z}$ ninguno de los subanillos $m\mathbb{Z}$ son unitarios.
Y el anillo $\mathbb{Z}^3$ es unitario con unidad $(1,1,1)$, pero el elemento unidad del subanillo $\{(n,0,0)|n \in \mathbb{Z}\}$ es $(1,0,0)$.

- Los divisores de cero no se conservan en subanillos (sí al revés).Los divisores de cero del subanillo lo son del anillo. Sin embargo, puede ocurrir que un elemento sea divisor de cero en el anillo y no lo sea en el subanillo.

Ejemplo

$(2,0,0)$ es divisor de cero en el anillo $\mathbb{Z}^3$, pero no lo es en el subanillo $\{(n,0,0)|n \in \mathbb{Z}\}$.

Anillos

Subanillos. Ideales

Ejercicio

En el anillo unitario $(\mathbb{Z}_{15}, +_{15}, \cdot_{15})$ se considera el subconjunto

$$S = \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}$$

1. Estudia si S es un anillo unitario.
2. En caso afirmativo, señala el elemento unidad.

Anillos

Subanillos. Ideales

Definición

Dado un anillo $(A, +, \cdot)$, *un* **ideal** *es una parte no vacía* $J \subset A$ *tal que*

- *Para cualesquiera* $i, j \in J$ *se tiene* $i - j \in J$.
- *Para cualesquiera* $i \in J$ *y* $x \in A$ *se tiene que* $i \cdot x \in J$ *y* $x \cdot i \in J$.

Ejemplo

Para todo entero $m > 1$, $m\mathbb{Z}$ es un ideal del anillo $\mathbb{Z}$.

- Todo ideal es subanillo (pero no se verifica el recíproco).
- Los ideales de un anillo hacen el mismo papel que los subgrupos normales, nos permiten definir la estructura de anillo cociente.

Anillos

Homomorfismos de anillos

Definición

Dados dos anillos $(A, +, \cdot)$ *y* $(B, *, \bullet)$, *un* **homomorfismo de anillos** *es toda aplicación* $\varphi\colon A \to B$ *tal que para cualesquiera* $a_1, a_2 \in A$

$$\varphi(a_1 + a_2) = \varphi(a_1) * \varphi(a_2) \qquad \varphi(a_1 \cdot a_2) = \varphi(a_1) \bullet \varphi(a_2)$$

Ejemplo

Dados a y b números reales fijos, definimos $\varphi\colon (\mathcal{F}(\mathbb{R}), +, \cdot) \to (\mathbb{R}^2, +, \cdot)$ de la siguiente manera $\varphi(f) = (f(a), f(b))$

Veamos que φ es homomorfismo de anillos:

- $\varphi(f+g) = ((f+g)(a), (f+g)(b)) = (f(a) + g(a), f(b) + g(b))$
  $= (f(a), f(b)) + (g(a), g(b))$
- $\varphi(f \cdot g) = ((f \cdot g)(a), (f \cdot g)(b)) = (f(a) \cdot g(a), f(b) \cdot g(b))$
  $= (f(a), f(b)) \cdot (g(a), g(b))$

Anillos

Homomorfismos de anillos

Teorema

Sea $\varphi\colon (A,+,\cdot) \to (B,+,\cdot)$ un homomorfismo de anillos. Entonces:

1. $\varphi(0) = 0$
2. *Para todo* $a \in A$, $\varphi(-a) = -\varphi(a)$.
3. *Si A_1 es subanillo de A, entonces $\varphi(A_1)$ es subanillo de B.*
4. *Si B_1 es subanillo de B, entonces $\varphi^{-1}(B_1)$ es subanillo de A.*
5. *Si φ es isomorfismo, entonces φ^{-1} es también isomorfismo.*

Anillos

Núcleo e imagen de un homomorfismo

Definiciones

Sea $\varphi\colon (A,+,\cdot) \to (B,+,\cdot)$ un homomorfismo de anillos:

- Se llama **núcleo** de φ al conjunto $\ker\varphi = \{a \in A \mid \varphi(a) = 0\} = \varphi^{-1}(\{0\})$
- Se llama **imagen** de φ al conjunto $\text{Im}\ \varphi = \{\varphi(a) \mid a \in A\}$.

Lema

- *Un homomorfismo de anillos es inyectivo si y solo si* $\ker\varphi = \{0\}$
- *Un homomorfismo de anillos es sobreyectivo si y solo si* $\text{Im}\ \varphi = B$

Anillos

Núcleo e imagen de un homomorfismo

Ejemplo

Dados a y b números reales fijos, sea el homomorfismo

$$\varphi\colon (\mathcal{F}(\mathbb{R}),+,\cdot) \to (\mathbb{R}^2,+,\cdot)$$

definido

$$\varphi(f) = (f(a), f(b))$$

El núcleo de este homomorfismo es

$$\mathcal{K}er\varphi = \{f \in \mathcal{F}(\mathbb{R}) | f(a) = f(b) = 0\}$$

el conjunto de funciones que se anulan simultáneamente en a y b.

Anillos

Núcleo e imagen de un homomorfismo

Teorema

- $\ker\varphi$ *es un ideal de* A.
- *Im* φ *es un subanillo de* B.
- *Si* A *es unitario, entonces Im* φ *es unitario, y* $\varphi(1_A) = 1_{Im\,\varphi}$.

Observación

Cuando φ no sea sobreyectiva, el elemento unidad de B generalmente no coincidirá con el elemento unidad $\varphi(1)$ de Im φ.

Ejemplo

Sea $\varphi\colon (\mathbb{Z}^3,+,\cdot) \to (\mathbb{Z}^3,+,\cdot)$, definido como $\varphi(a_1,a_2,a_3) = (a_1,a_2,0)$.
El elemento unidad de $(\mathbb{Z}^3,+,\cdot)$ es $(1,1,1)$ y, sin embargo, el elemento unidad de Im φ es $(1,1,0)$.

Cuerpos

Definición

Un anillo $(K, +, \cdot)$ se dice que es un **cuerpo** *si*

1. *es conmutativo*
2. *es unitario y su elemento unidad es distinto del cero*
3. *todos sus elementos (excepto el cero) son inversibles.*

Equivalentemente, $(K, +, \cdot)$ es un cuerpo si

- $(K, +)$ es grupo abeliano.
- $(K \setminus \{0\}, \cdot)$ es grupo abeliano.
- La operación $\cdot$ es distributiva respecto a $+$.

Ejemplo

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son cuerpos con la suma y el producto usuales.
- $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es cuerpo con la suma y el producto usuales.

Cuerpos

Subcuerpos

Definición (Subcuerpo)

Sea el cuerpo $(K, +, \cdot)$ y sea $\varnothing \neq H \subseteq K$. Se dice que H es un **subcuerpo** *de K si H es cuerpo con las mismas operaciones que K.*

Aplicando lo estudiado anteriormente, podemos afirmar que:

H es subcuerpo de $(K, +, \cdot)$ si y sólo si

1. H es subanillo de $(K, +, \cdot)$
2. el inverso de todo elemento de H pertenece a H

Ejemplos

- $\mathbb{Q}$ es subcuerpo de $\mathbb{R}$, y $\mathbb{R}$ es subcuerpo de $\mathbb{C}$
- $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es subcuerpo de $\mathbb{R}$.

Cuerpos

Propiedades de los cuerpos

Teorema

1. *Todo anillo* **finito** *conmutativo, unitario, y sin divisores de cero, es un cuerpo.*
2. *Los únicos ideales que existen en un cuerpo K son $\{0\}$ y K.*
3. *$(\mathbb{Z}_p, +_p, \cdot_p)$ es un cuerpo si y solo si p es un número primo.*
4. *Para cada p primo y $n \in \mathbb{Z}^+$, salvo isomorfismo, existe exactamente un cuerpo finito de dimensión p^n.*

No todos los cuerpos finitos son de la forma $\mathbb{Z}_p$.

Ejemplo

Sea $\mathcal{A}_2(K)$ el conjunto de las matrices $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ con $x, y \in K$.

Se tiene que $\mathcal{A}_2(K)$ es un cuerpo si $K = \mathbb{Z}_3$, pero no lo es si $K = \mathbb{Z}_5$.

Bibliografía

Matemática Discreta N.L.Biggs (Ed. Vicens Vives)

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

Matemática Discreta R. Johnsonbaugh (Ed. Prentice Hall)

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

2000 Problemas resueltos de Matemática Discreta
S. Lipschutz y M. Lipson (Ed. McGraw Hill)

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

Matemática Discreta y sus aplicaciones K. Rosen (Ed. McGraw Hill)