Grupos, Anillos y Cuerpos

Inmaculada Fortes
Departamento de Matemática Aplicada
Universidad de Málaga

Operaciones binarias

Definición

Dados el conjunto A, llamamos operación binaria interna sobre A a cualquier función $*$ cuyo dominio es el producto cartesiano $A \times A$ y codominio A, esto es:

$$\begin{array}{rcl} *: A \times A & \longrightarrow & A \\ (a_1, a_2) & \longmapsto & a_1 * a_2 \end{array}$$

Ejemplo

La suma y el producto en los enteros modulares son operaciones internas.

$$+: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \qquad\qquad \cdot: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

Definición

Dados los conjuntos A, B y C llamamos operación binaria externa *es una función $*$ cuyo dominio es el producto cartesiano $A \times B$ y codominio C, esto es:*

$$\begin{array}{rcl} *\colon A \times B & \longrightarrow & C \\ (a_1, a_2) & \longmapsto & a_1 * a_2 \end{array}$$

Ejemplo

La función $*\colon \mathbb{N} \times \mathcal{P}(\mathbb{R}) \longrightarrow \mathcal{P}(\mathbb{R})$, definida para cada $n \in \mathbb{N}$ y $p(x) \in \mathcal{P}(\mathbb{R})$ como $*(n, p(x)) = n\ p(x)$ es una operación externa, donde $\mathcal{P}(\mathbb{R})$ es el conjunto de polinomios con coeficientes reales.

Ejemplo

La siguiente función también es una operación externa.

$$\begin{array}{rcl} *\colon \mathbb{Z} \times \mathcal{M}_{m\times n}(\mathbb{Z}) & \longrightarrow & \mathcal{M}_{m\times n}(\mathbb{Z}) \\ (\lambda, M) & \longmapsto & *(\lambda, M) = \lambda\ M \end{array}$$

Propiedades

Propiedad asociativa: Si para cada $a, b, c \in A$ se verifica que

$$(a * b) * c = a * (b * c)$$

Propiedad conmutativa: Si para cada $a, b \in A$ se verifica que

$$a * b = b * a$$

Leyes de cancelación: Cancelación a la izquierda si para cada $a, b, c \in A$ se verifica que

$$\text{si} \qquad a * b = a * c \qquad \text{entonces} \qquad b = c$$

Si tenemos una segunda operación $\star$
Propiedad distributiva: Si para cada $a, b, c \in A$ se verifica que

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

Por otro lado, algunos elementos del conjunto A se pueden comportar de forma notable con respecto a una operación $*$.

Elemento neutro $e \in A$ **:** Si para cada $a \in A$ se verifica que

$$a * e = e * a = a$$

Elemento absorbente $z \in A$**:** Si para cada $a \in A$ se verifica que

$$a * z = z * a = z$$

Elemento idempotente $a \in A$**:** Si se verifica que

$$a * a = a$$

Elemento simétrico $a \in A$**:** Si existe un elemento $a' \in A$ tal que

$$a * a' = a' * a = e$$

Ejemplo

Comprobar qué propiedades cumplen las operaciones siguientes.

- $*\colon \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ *definida como* $p * q = p$, *para todo* $p, q \in \mathbb{A}$.
- $\star\colon (\mathbb{Z}_n \times \mathbb{Z}_n) \times (\mathbb{Z}_n \times \mathbb{Z}_n) \to \mathbb{Z}_n$ *definida como*

$$(n, m) \star (s, t) = (n + s, m + t)$$

para todo $(n, m), (s, t) \in \mathbb{Z}_n \times \mathbb{Z}_n$.

Ejemplo

Dado un conjunto A, *sobre el que definimos la operación:*

$$\Delta\colon \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}; \qquad x \Delta y = x + y + 1$$

¿Qué propiedades cumple?

Estructuras algebraicas

Cuando tenemos uno o más conjuntos con una o varias operaciones binarias, con unas determinadas propiedades y unos determinados elementos notables, tenemos una estructura algebraica.

Si $A = \{a_1, a_2, \ldots, a_n\}$ es posible representar dicha operación mediante una tabla de la forma

$$\begin{array}{c|ccccc}
* & a_1 & \cdots & a_j & \cdots & a_n \\
\hline
a_1 & & & \vdots & & \\
\vdots & & & \vdots & & \\
a_i & \cdots & \cdots & a_i * a_j & \cdots & \cdots \\
\vdots & & & \vdots & & \\
a_n & & & \vdots & &
\end{array}$$

Las estructuras se presentan agrupando bajo un paréntesis el conjunto y las operaciones que actúan sobre él, como por ejemplo $(A, *)$, $(A, *, \star)$

Enteros modulares

El conjunto $\mathbb{Z}_n$ se define mediante una relación de equivalencia en $\mathbb{Z}$ llamada de congruencia módulo n, se dice que

$$a \equiv b \pmod{n} \iff b - a \quad \text{es múltiplo entero de } n$$

Una de las operaciones internas que se pueden definir sobre este conjunto, se representa por $+$, y viene dada por

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

Obteniendo que $(\mathbb{Z}_n, +)$ es una estructura algebraica. Dado que $\mathbb{Z}_n$ es finito, se puede representar dicha operación mediante una tabla.

Por ejemplo podemos observar las dadas para $\mathbb{Z}_2$ y $\mathbb{Z}_5$ con la suma:

$+$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$+$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

Escribe las tablas para $\mathbb{Z}_4$ y $\mathbb{Z}_5$ con el producto, y analiza las diferencias.

Morfismos

Definición

Dadas dos estructuras algebraicas similares (con las mismas propiedades) se llama homomorfismo entre las estructuras a una función entre los conjuntos que respeta la estructura. Por ejemplo, si $(A, *)$ y $(B, \star)$ son dos estructuras algebraicas, un homomorfismo entre ambas es una función $f : A \to B$ que verifica

$$f(a * b) = f(a) \star f(b)$$

para cada par de elementos a, b de A.

Cuando los homomorfismos son inyectivos o sobreyectivos reciben nombres especiales:

- Monomorfismo: si es inyectivo.
- Epimorfismo: si es sobreyectivo.
- Isomorfismo: si es biyectivo.

Definición

Decimos que dos estructuras algebraicas son isomorfas si existe un isomorfismo entre ambas.

Ejemplo

Dados los conjuntos $A = \{a, b, c\}$ *y* $B = \{1, 2, 3\}$ *con operaciones definidas mediante las tablas*

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

$\star$	1	2	3
1	1	1	1
2	1	2	3
3	1	3	1

se observa que son estructuras isomorfas, puesto que la función $f : A \to B$ *definida como* $f(a) = 2$, $f(b) = 1$ *y* $f(c) = 3$ *es un isomorfismo.*

Definición

Dado un conjunto G y una operación interna $*\colon G \times G \to G$ que verifica las propiedades:

1. *Asociativa*: $(a * b) * c = a * (b * c)$ *para cada* $a, b, c \in G$;
2. *Existencia de elemento neutro: existe un elemento* $e \in G$ *que cumple que* $a * e = e * a = a$ *para cualquier* $a \in G$, *que llamamos elemento neutro;*
3. *Existencia de elemento simétrico: para cada* $a \in G$, *existe un elemento* $a' \in G$ *tal que* $a * a' = a' * a = e$, *que llamamos elemento simétrico de* a;

se dice que el par $(G, *)$ *forma un grupo.*

Si la operación interna cumple la propiedad conmutativa , se dice que el grupo es conmutativo, o abeliano en honor al matemático noruego Niels Henrik Abel (1802–1829).

Ejemplo

- *Los pares* $(\mathbb{Z},+)$, $(\mathbb{Q},+)$ *y* $(\mathbb{R},+)$ *son grupos abelianos (aditivos), mientras que el par* $(\mathbb{N},+)$ *no lo es. Esto último debido a que no se cumple la propiedad de elemento simétrico.*

- *Ninguno de los pares* $(\mathbb{N},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$ *y* $(\mathbb{R},\cdot)$ *es grupo. Todos fallan, al menos, en que el simétrico de* 0 *no es un elemento del conjunto considerado. Sin embargo, los conjuntos* $(\mathbb{Q}^*,\cdot)$ *y* $(\mathbb{R}^*,\cdot)$, *donde* $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ *y* $\mathbb{R}^* = \mathbb{R} - \{0\}$, *son grupos abelianos (multiplicativos).*

- *Si p es primo,* $(\mathbb{Z}_p^*,\cdot)$, *es un grupo abeliano.*

- *Si consideramos un conjunto A, el formado por todas las aplicaciones biyectivas de A en A, denotado por* $S(A)$, *junto con la operación composición de funciones forman un grupo.*

- *Estudiar las propiedades que cumplen las estructuras* $(\mathcal{P}(A),\cup)$ *y* $(\mathcal{P}(A),\cap)$.

Notación Multiplicativa

Dado un grupo $(G, *)$, la notación habitual es la multiplicativa, entonces se representa por $(G, \cdot)$, y se adoptan los siguientes convenios, donde $a \in G$.

- El elemento neutro se representa por 1.
- El elemento simétrico de a se representa por a^{-1} y se llama inverso de a
-
  - Si $n \in \mathbb{Z}^+$, se define $a^n = \overbrace{a \cdot a \cdots a}^{n \text{ veces}}$;
  - si $n = 0$, se define $a^0 = 1$
  - si $n \in \mathbb{Z}^+$, se define $a^{-n} = (a^{-1})^n = (a^n)^{-1}$
- Para cualesquiera $n, m \in \mathbb{Z}$ se tiene que

$$\begin{aligned} a^{m+n} &= a^m \cdot a^n \\ a^{m-n} &= a^m \cdot a^{-n} \\ a^{mn} &= (a^m)^n \end{aligned}$$

Notación Aditiva

De forma análoga, dado un grupo $(G, *)$, si es conmutativo se suele usar la notación aditiva, entonces se representa por $(G, +)$, y se adoptan los siguientes convenios, donde $a \in G$.

- El elemento neutro se representa por 0.
- El elemento simétrico de a se representa por $-a$ y se llama opuesto de a
-
  - Si $n \in \mathbb{Z}^+$, se define $na = \overbrace{a + a + \cdots + a}^{n \text{ veces}}$;
  - si $n = 0$, se define $0a = 0$
  - si $n \in \mathbb{Z}^+$, se define $(-n)a = n(-a) = -(na)$
- Para cualesquiera $n, m \in \mathbb{Z}$ se tiene que

$$
\begin{aligned}
(m+n)a &= ma + na \\
(m-n)a &= ma + (-na) \text{ (que se podrá denotar por } ma - na) \\
(mn)a &= m(na)
\end{aligned}
$$

Teorema

En un grupo $(G,*)$*, el elemento simétrico de cualquier* $a \in G$ *es único.*

Teorema

En un grupo $(G,*)$*, se cumplen las leyes de cancelación. Esto es, para cualesquiera* $a, b, c \in G$ *se tiene que:*

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

Teorema

Dado un grupo $(G, *)$ *y* $a, b \in G$*, se tiene que:*

1. *El elemento simétrico del neutro es él mismo:* $e' = e$.
2. *El simétrico del simétrico de un elemento* a *es el propio* a*:* $(a')' = a$.
3. $(a * b)' = b' * a'$
4. *Las ecuaciones del tipo:* $a * x = b$ *y* $x * a = b$*, tienen solución única.*

De forma usual, se representará la operación de un grupo abeliano cualquiera por $+$ (notación aditiva). Para el resto de grupos, se denotará la operación interna por $\cdot$ (notación multiplicativa).

Ejemplo

Sobre el conjunto $\mathbb{Z}_n$*, se define la operación interna dada por* $[a] \cdot [b] = [ab]$*. ¿Es* $(\mathbb{Z}_n, \cdot)$ *un grupo? ¿Qué ocurre con* $(\mathbb{Z}_n^*, \cdot)$*?*

Grupos Simétricos

Ya hemos visto que dado A, el conjunto $S(A)$ de las aplicaciones biyectivas es un grupo. Si A es finito entonces a las aplicaciones biyectivas, de A en A, se les llama permutaciones y al grupo de las permutaciones $S(A)$ se le suele representar como S_n (donde n es el cardinal de A) y se le conoce como el *grupo simétrico* en n letras o n símbolos.
Se puede considerar que los elementos de A son de la forma 1, 2, ... y n, en lugar de a_1, a_2, ... y a_n; por tanto, tenemos que $A = \{1, 2, \ldots, n\}$.
Si $\sigma \in S_n$ y $\sigma(i) = s_i$, se acostumbra a usar la siguiente notación para representarla:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ s_1 & s_2 & \ldots & s_n \end{pmatrix}$$

Llamamos *producto de permutaciones* a la composición como funciones, es decir $\sigma\tau = \tau \circ \sigma$.

Ejemplo

En el grupo simétrico S_4 si

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

entonces

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Bajo esta notación el elemento neutro será la permutación identidad

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

Teorema

El grupo simétrico S_n tiene $n!$ elementos.

Ejemplo

El grupo simétrico S_3 *tiene* $3! = 6$ *elementos que son:*

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

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

donde e actúa como elemento neutro y la tabla para este grupo queda de la forma:

	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_2	μ_3	μ_1
ρ_2	ρ_2	e	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	e	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	e	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	e

Subgrupos

Definición

Decimos que un subconjunto H de un grupo $(G,\cdot)$ es un subgrupo si es grupo con la restricción de la operación G en H, y se representa por $H \leq G$.

Por tanto, que H es subgrupo si verifica:

1. Es cerrado para la operación: si $a, b \in H$, entonces $a \cdot b \in H$.
2. Contiene al elemento neutro: $e \in H$.
3. Es cerrado para el inverso: si $a \in H$, entonces $a^{-1} \in H$. [1]

Ejemplo

Dado cualquier grupo $(G,\cdot)$, los subconjuntos $\{e\}$ y el propio G son subgrupos de $(G,\cdot)$, y reciben el nombre de subgrupos triviales. Los subgrupos que no son triviales se denominan subgrupos propios.

[1] Obsérvese que las propiedades 2) y 3) implican la propiedad 1)

Ejemplo

El par $(\mathbb{R}^+, \cdot)$ *forma un subgrupo de* $(\mathbb{R}^*, \cdot)$, *mientras que* $(\mathbb{R}^-, \cdot)$ *no lo es.*

Ejemplo

Buscar un subgrupo de $(\mathbb{Z}_4, +)$.

El siguiente teorema, proporciona una caracterización del concepto de subgrupo.

Teorema

Dado un grupo $(G, \cdot)$, *una condición necesaria y suficiente para que un subconjunto* $H \subseteq G, H \neq \varnothing$ *sea subgrupo es que*

$$\text{para todo } \; a, b, \in H \text{ se tiene que } \; ab^{-1} \in H$$

Ejemplo

Los subgrupos del grupo $(\mathbb{Z}, +)$ *son los subconjuntos de la forma* $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ *siendo* $n \in \mathbb{N}$.

Ejemplo

Probar que para el grupo multiplicativo $(Q^*, \cdot)$, *el conjunto* $\{1, 2, 1/2, 2^2, 1/2^2, \ldots, 2^n, 1/2^n, \ldots\}$ *es un subgrupo.*

Ejemplo

Comprobar que $(\mathbb{Z}^*, \cdot)$ *no es un subgrupo de* $(\mathbb{Q}^*, \cdot)$, *esto es,* $(\mathbb{Z}^*, \cdot) \not\leq (\mathbb{Q}^*, \cdot)$.

En el caso de considerar un subconjunto finito, el teorema de caracterización se simplifica del siguiente modo:

Teorema

Si $H \neq \varnothing$ *es un subconjunto finito de un grupo* $(G, \cdot)$, *entonces* H *es subgrupo si y solo si es cerrado para la operación del grupo.*

Si el subgrupo H es finito llamamos orden del subgrupo al número de elemento que posee.

Morfismos de grupos

Definición

Dados los grupos $(G, *)$ *y* $(G', \star)$, *decimos que una función* $f : (G, *) \to (G', \star)$ *es un homomorfismo de grupos si*

$$f(a * b) = f(a) \star f(b) \quad \text{para todo} \ \ a, b \in G$$

se mantiene la terminología de monomorfismo, epimorfismo e isomorfismo.

Teorema

Si $f : (G, *) \to (G', \star)$ *es un homomorfismo de grupos, entonces:*

1. *Si* e *y* e' *son los elementos neutros de* $(G, *)$ *y* $(G', \star)$ *respectivamente, entonces* $f(e) = e'$.
2. *Para cada* $a \in G$ *se cumple* $f(a^{-1}) = (f(a))^{-1}$.
3. *Para cada entero* n *y cada* $a \in G$ *se cumple* $f(a^n) = (f(a))^n$.
4. $(f(G), \star)$ *es un subgrupo y se denota por* $Im(f)$.

Ejemplo

Probemos que la función $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ *definida por* $f(x) = e^x$ *es un isomorfismo.*

- *Si* $f(a) = f(b)$, *de modo que* $e^a = e^b$, *entonces* $a = b$. *Por lo tanto,* f *es inyectiva.*
- *Si* $c \in \mathbb{R}^+$, *entonces* $ln(c) \in \mathbb{R}$ *y* $f(ln(c)) = e^{ln(c)} = c$, *por lo tanto* f *es sobreyectiva.*
- $f(a + b) = e^{a+b} = e^a e^b = f(a)f(b)$, *por lo tanto* f *es un isomorfismo.*

Ejemplo

Si consideramos un grupo $(G, \cdot)$ *y un elemento* $a \in G$, *la función* $f : (G, \cdot) \to (G, \cdot)$, *definida como* $f(x) = a^{-1}xa$, *para cada* $x \in G$ *y donde* a^{-1} *es el inverso de* a, *es un isomorfismo de grupos.*

Orden de un elemento

Definición

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

- $a^0 = e$
- $a^{n+1} = a * a^n$

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* $(\mathbb{Z}_6, +)$ *se tiene* $[4] + [4] + [4] = [0] \Rightarrow o([4]) = 3$ *y* $[5] + \cdots + [5] = [0] \Rightarrow o([5]) = 6$
- *En el grupo* $(\mathbb{Z}_7, \cdot)$ *se tiene* $[2] \cdot [2] \cdot [2] = [1] \Rightarrow o([2]) = 3$ *y* $[6] \cdot [6] = [1] \Rightarrow o([6]) = 2$

Grupos cíclicos

Teorema

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

Ejemplo

En el grupo $(\mathbb{Z}_7^*, \cdot)$ *el subgrupo generado por* $[4]$ *es* $< [4] >= \{[1], [2], [4]\}$.

Definición

Se dice que un grupo G *es* **cíclico** *si existe un elemento* $c \in G$ *tal que* $< c >= G$.

Ejemplo

$(\mathbb{Z}_7^*, +)$ *es cíclico y está generado por* $< [4] >= \{[0], [4], [1], [5], [2], [6], [3]\}$

Teorema

Si $(G, *)$ *es un grupo cíclico entonces es abeliano.*

Definición

Sea H un subgrupo de $(G, *)$ un grupo 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 $Ha = \{h * a, h \in H\}$*

Lema

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

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

Subgrupos normales

Definición

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

Lema

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

Teorema (de Lagrange)

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

Anillos y Cuerpos

Definición

Dado un conjunto A con dos operaciones internas que denotamos por $+$ y $\cdot$, decimos que $(A, +, \cdot)$ es un anillo si verifica:

1. $(A, +)$ *es un grupo abeliano.*
2. $(A, \cdot)$ *es un semigrupo.*
3. *Para cualesquiera $a, b, c \in A$ se cumplen:*
   - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
   - $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Cuando $(A, \cdot)$ es un monoide se dice que A es un anillo unitario *o* anillo con unidad. *Denotaremos al elemento neutro de $(A, \cdot)$ por 1.*

Cuando $(A, \cdot)$ es un semigrupo conmutativo, se dice que R es un anillo conmutativo.

Ejemplo

Los conjuntos numéricos con las operaciones habituales $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ *y* $(\mathbb{R}, +, \cdot)$ *son anillos conmutativos unitarios.* $(\mathbb{N}, +, \cdot)$ *no es un anillo por no ser* $(\mathbb{N}, +)$ *un grupo.*

Ejemplo

Para cada entero positivo n*:*

- *el conjunto* $\mathbb{Z}_n$ *junto con la suma y el producto usuales es un anillo conmutativo y unitario.*
- *el conjunto* $\mathcal{M}_n(A)$ *de matrices cuadradas con coeficientes en un anillo* $(A, +, \cdot)$*, junto con las operaciones de suma y producto de matrices, forman un anillo.*

Teorema

Si A es un anillo, con elemento neutro aditivo 0, entonces para cualesquiera elementos $a, b \in A$ se tiene:

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

Muchas de las propiedades de los anillos son reformulaciones de las propiedades correspondientes a los grupos, por ejemplo:

- Si $m, n \in \mathbb{Z}, a \in \mathbb{R} \left\{ \begin{array}{c} ma + na = (m+n)a \\ m(na) = (mn)a \end{array} \right.$
- Si $m, n \in \mathbb{N}, a \in \mathbb{R} \left\{ \begin{array}{c} a^m a^n = a^{m+n} \\ (a^m)^n = a^{mn} \end{array} \right.$

Al ser una estructura más rica que la de grupo, se tienen expresiones completamente nuevas basadas en la propiedad distributiva.

Subanillos

Definición

Dado un anillo $(A, +, \cdot)$, $S \subseteq A$ *es un subanillo de* $(A, +, \cdot)$ *si forma un anillo junto con las operaciones definidas en* A, *es decir:*

$$Dados\ x, y \in S \Rightarrow x - y \in S \ y \ x \cdot y \in S$$

Dominios de integridad

Definición

Si a y b son elementos distintos de cero de un anillo $(A, +, \cdot)$ tal que $a \cdot b = 0$, entonces se dice que a y b son divisores de cero.

Ejemplo

- *Los elementos $[2]$ y $[3]$ de $\mathbb{Z}_6$ son dos divisores de cero.*
- *Los divisores de cero del anillo $(\mathbb{Z}_n, +, \cdot)$ son aquellas clases cuyos elementos no son primos relativos con n.*

Teorema

Si $(A, +, \cdot)$ es un anillo, entonces son válidas las leyes de cancelación para $(A, \cdot)$ si y solo si no tiene divisores de cero.

Definición

Llamamos *dominio de integridad* *a un anillo conmutativo unitario que no contiene divisores de cero.*

Ejemplo

- *Los anillos numéricos* $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$*y* $(\mathbb{R}, +, \cdot)$ *son dominios de integridad.*
- *El anillo* $(\mathcal{M}_n, +\cdot)$ *de matrices cuadradas de orden n, con* $n \geq 2$ *no son dominios de integridad.*

Cuerpos

Definición

Llamamos cuerpo a un anillo conmutativo unitario $(K, +, \cdot)$ *donde cada elemento distinto de cero es inversible, es decir: si* $a \in K, a \neq 0$, *existe* a^{-1} *tal que* $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Ejemplo

$\mathbb{Z}$, *con las operaciones usuales de suma y producto, no es un cuerpo, puesto que los únicos elementos inversibles son* 1 *y* -1. *En cambio sí son cuerpos las estructuras* $(\mathbb{Q}, +, \cdot)$ *y* $(\mathbb{R}, , +, \cdot)$

Teorema

Todo cuerpo es un dominio de integridad.

El inverso de este teorema no es cierto, en general, tenemos dominios de integridad que no son cuerpos y $(\mathbb{Z}, +, \cdot)$ es un ejemplo de ello. En cambio si el conjunto considerado es finito.

Teorema

Todo dominio de integridad finito es un cuerpo.

Este teorema nos permite identificar los cuerpos finitos.

Corolario

Si p es un entero positivo primo, $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.

Se puede probar que todo cuerpo finito contiene un subcuerpo que es isomorfo a un cierto $(\mathbb{Z}_p, +, \cdot)$, es más, se prueba también que todos los cuerpos infinitos contienen un subcuerpo isomorfo a $(\mathbb{Q}, +, \cdot)$.