

Infierno
Saga de la Divina comedia

Jesús González Abril

Curso 2025-2026

Índice general

Capítulo 1

Anillos

1.1. Operaciones binarias

Definición 1.1.1: Operación binaria

Sea X un conjunto. Una operación binaria en X es una aplicación $*$: $X \times X \rightarrow X$. Por lo general escribimos $*(a, b) = a * b$.

Nota

En general si por el contexto se sobreentiende que una operación es binaria se simplifica el lenguaje hablando simplemente de operaciones. De igual manera normalmente se omite el conjunto sobre el que está definida la operación.

Definición 1.1.2: Tipos de operaciones

Una operación $*$ se dice

- **Conmutativa** si $x * y = y * x$ para todo $x, y \in X$.
- **Asociativa** si $x * (y * z) = (x * y) * z$ para todo $x, y, z \in X$.

Definición 1.1.3: Terminología sobre elementos

Un elemento $x \in X$ se dice que es:

- **Neutro por la izquierda (neutro por la derecha)** si $x * y = y$ para todo $y \in X$ ($y * x = y$ para todo $y \in X$).
- **Cancelable por la izquierda (cancelable por la derecha)** si para cada dos elementos distintos $a \neq b$ de X se verifica $x * a \neq x * b$ ($a * x \neq b * x$).
- **Neutro** si es neutro por la derecha y por la izquierda.
- **Cancelable** si es cancelable por la izquierda y por la derecha.

Supongamos que e es un elemento neutro de X con respecto a $*$. Sean x e y elementos de X . Decimos que x es simétrico de y por la izquierda y que y es simétrico de x por la derecha con respecto a $*$ si se verifica $x * y = e$. En este contexto decimos que x es:

- **Simétrico** de y si lo es por ambos lados. En tal caso decimos que x es invertible, siendo y su inverso ($y = x^{-1}$ si el inverso es único).

Ejemplo

Si x es cancelable por la izquierda entonces para cualesquiera $a, b \in X$ se tiene

$$x * a = x * b \implies a = b$$

Demostración

Supongamos que $x * a = x * b$, si $a = b$ ya hemos terminado. En caso contrario a y b son elementos distintos, y como x es cancelable por la izquierda entonces debe ser $x * a \neq x * b$, pero eso contradice la suposición inicial, luego ha de ser $a = b$. ■

Ejercicio 1.1

Probar que si x es cancelable por la derecha entonces para cualesquiera $a, b \in X$ se tiene

$$a * x = b * x \implies a = b$$

Nota

Notemos que esta caracterización no es más que el contrarrecíproco de la primera definición que hemos dado de elemento cancelable.

Definición 1.1.4: Tipos de conjuntos con operaciones

Un par $(X, *)$ formado por un conjunto y una operación $*$ decimos que es un:

- **Semigrupo** si $*$ es asociativa.
- **Monoide** si es un semigrupo que tiene un elemento neutro con respecto a $*$.
- **Grupo** si es un monoide y todo elemento de X es invertible con respecto a $*$.
- **Grupo abeliano** si es un grupo y $*$ es conmutativa.

Ejemplo

Si tomamos la suma de elementos sobre distintos conjuntos de números obtenemos un ejemplo de cada uno de los tipos de conjuntos con operaciones:

1. $(\mathbb{N}, +)$ es un semigrupo.
2. $(\mathbb{Z}_{\geq 0}, +)$ es un monoide.
3. $(\mathbb{Z}, +)$ es un grupo abeliano.

Ejemplo

Un ejemplo de grupo no abeliano es $GL_n(\mathbb{R})$ si $n \geq 2$. $GL_n(\mathbb{R})$ es el grupo de las matrices invertibles $n \times n$ con entradas reales, donde la operación es la multiplicación de matrices.

Demostración

En primer lugar es inmediato que la operación es asociativa. También es fácil ver que tiene elemento neutro, la matriz identidad I_n . Si tomamos una matriz cualquiera $A \in GL_n(\mathbb{R})$ entonces ha de ser invertible, por lo que su elemento inverso es A^{-1} que claramente pertenece a $GL_n(\mathbb{R})$.

Finalmente, para ver que el grupo no es conmutativo notemos que para $n = 2$ podemos tomar las matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

ambas invertibles por tener determinante no nulo, que verifican

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$

En el caso de que sea $n > 2$ podemos tomar matrices de la forma

$$A' = \begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix}, B' = \begin{pmatrix} B & 0 \\ 0 & I_{n-2} \end{pmatrix}$$

cuyo producto no conmuta por las propiedades de la multiplicación de matrices por bloques. ■

Ejercicio 1.2

Sean A un conjunto y sea $X = A^A$, el conjunto de las aplicaciones de A en A . Probar que la composición de aplicaciones define una operación asociativa en X para la que la identidad 1_X es neutro. Por tanto (A^A, \circ) es un monoide.

Proposición 1.1.5

Sea $*$ una operación en un conjunto X .

1. Si e es un neutro por la izquierda y f es un neutro por la derecha de X con respecto a $*$, entonces $e = f$. En particular, X tiene a lo sumo un neutro.
2. Supongamos que $(X, *)$ es un monoide y sea $a \in X$.
 - a) Si x es un simétrico por la izquierda de a e y es un simétrico por la derecha de a , entonces $x = y$. Por tanto, en tal caso a es invertible y tiene a lo sumo un simétrico.
 - b) Si a tiene un simétrico por un lado entonces es cancelable por ese mismo lado. En particular, todo elemento invertible es cancelable.

Demostración

(1) Como e es neutro por la izquierda y f es neutro por la derecha tenemos

$$f = e * f = e.$$

(2a) Ahora suponemos que $(X, *)$ es un monoide. Por (1), $(X, *)$ tiene un único neutro que vamos a denotar por e . Como x es inverso por la izquierda de a e y es inverso por la derecha de a , usando la propiedad asociativa, tenemos que

$$y = e * y = (x * a) * y = x * (a * y) = x * e = x.$$

(2b) Supongamos que a es un elemento de X que tiene un inverso por la izquierda b y que $a * x = a * y$ para $x, y \in X$. Usando la asociatividad una vez más concluimos que

$$x = e * x = (b * a) * x = b * (a * x) = b * (a * y) = (b * a) * y = e * y = y.$$

Nota

Por la proposición anterior si X es un monoide cada elemento invertible a tiene un único inverso que denotaremos a^{-1} .

1.2. Anillos

Definición 1.2.1: Anillo

Un anillo es una terna $(A, +, \cdot)$ formada por un conjunto no vacío A y dos operaciones $+$ (suma) y \cdot (producto) en A que verifican:

1. $(A, +)$ es un grupo abeliano.
2. (A, \cdot) es un monoide.
3. Distributiva del producto respecto de la suma: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ para todo $a, b, c \in A$.

Si además \cdot es conmutativo en A , decimos que $(A, +, \cdot)$ es un anillo conmutativo.

Nota

- El neutro de A con respecto a $+$ se llama **cero** y se denota 0 .
- El neutro de A con respecto a \cdot se llama **uno** y se denota 1 .
- El simétrico de un elemento a con respecto a $+$ se llama **opuesto** y se denota $-a$.
- Si a es invertible con respecto a \cdot , su simétrico se llama **inverso** y se denota a^{-1} .
- En general para $+$ y \cdot usamos la notación usual para sumas y productos

$$a \cdot (b + c) = a(b + c) = ab + ac.$$

Nota

Como $(A, +)$ es un grupo, todo elemento de A es invertible respecto de la suma y por tanto cancelable. Diremos que un elemento de A es regular en A si es cancelable con respecto al producto. En caso contrario decimos que el elemento es singular en A o divisor de cero.

1.2.1. Ejemplos de anillo

Ejemplo

Los conjuntos \mathbb{Z} , \mathbb{Q} , \mathbb{R} y \mathbb{C} son anillos conmutativos con la suma y el producto usuales. Notemos que todo elemento no nulo de \mathbb{Q} , \mathbb{R} o \mathbb{C} es invertible. Sin embargo en \mathbb{Z} solo hay dos elementos invertibles (1 y -1) aunque todos los elementos son regulares menos el 0.

Demostración

Probaremos que en \mathbb{C} todos los elementos salvo el 0 son invertibles. Sea $z = a + bi$ un número

complejo cualquiera no nulo, en tal caso el número $w = \frac{a-bi}{a^2+b^2}$ verifica

$$zw = \frac{(a+bi)(a-bi)}{a^2+b^2} = \frac{a^2 - abi + abi - b(-1)}{a^2+b^2} = \frac{a^2+b^2}{a^2+b^2} = 1$$

luego $w = z^{-1}$. ■

Ejemplo

Sean A y B dos anillos. Entonces el producto cartesiano $A \times B$ tiene una estructura de anillo con las operaciones definidas componente a componente:

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

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

Obsérvese que $A \times B$ es conmutativo si y solo si lo son A y B , y que esta construcción se puede generalizar a productos cartesianos de cualquier familia (finita o no) de anillos.

Ejemplo

Dados un anillo A y un conjunto X , el conjunto A^X de las aplicaciones de X en A es un anillo con las siguientes operaciones:

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

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

Si definimos la familia de conjuntos $\{A_i = A : i \in X\}$ entonces es inmediato que $\cup_{i \in X} A_i = A$. Recordemos ahora que el producto $\prod_{i \in X} A_i$ es el conjunto de funciones $f : X \rightarrow \cup_{i \in X} A_i$, es decir, el conjunto de funciones $f : X \rightarrow A$, luego A^X es un anillo correspondiente a un producto «infinito» del anillo A consigo mismo.

1.3. Subanillos

Definición 1.3.1: Subanillo

Un subconjunto B de un anillo A es un **subanillo** de A si:

1. B contiene al 1.
2. B es cerrado para sumas, productos y opuestos.

Equivalentemente, B es un subanillo si contiene al 1 y es cerrado para restas y productos.

1.4. Homomorfismos de anillos

Definición 1.4.1: Homomorfismo de anillos

Sean A y B dos anillos. Un **homomorfismo de anillos** entre A y B es una aplicación $f : A \rightarrow B$ que satisface:

1. $f(x + y) = f(x) + f(y)$
2. $f(x \cdot y) = f(x) \cdot f(y)$
3. $f(1) = 1$

Un **isomorfismo** es un homomorfismo biyectivo. Dos anillos A y B son **isomorfos** ($A \cong B$) si existe un isomorfismo entre ellos.

1.5. Ideales y anillos cociente

Definición 1.5.1: Ideal

Un subconjunto I de un anillo A es un **ideal** si:

1. $I \neq \emptyset$
2. Para todo $x, y \in I$ y $a \in A$, se verifica que $x + y \in I$ y $a \cdot x \in I$.

Definición 1.5.2: Congruencia módulo un ideal

Sea I un ideal de un anillo A . Decimos que $a, b \in A$ son **congruentes módulo I** ($a \equiv b \pmod{I}$) si $b - a \in I$.

Definición 1.5.3: Anillo cociente

Dado un anillo A y un ideal I , el conjunto $A/I = \{a + I : a \in A\}$ con las operaciones:

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

es un anillo llamado **anillo cociente** de A módulo I .

1.6. Teoremas de isomorfía

Teorema 1.6.1: Primer teorema de isomorfía

Sea $f : A \rightarrow B$ un homomorfismo de anillos. Entonces existe un isomorfismo:

$$A/\ker f \cong \operatorname{Im} f$$

Demostración

Teorema 1.6.2: Segundo teorema de isomorfía

Sea A un anillo y $I \subseteq J$ ideales de A . Entonces:

$$\frac{A/I}{J/I} \cong \frac{A}{J}$$

Demostración

Teorema 1.6.3: Tercer teorema de isomorfía

Sea A un anillo, B un subanillo de A e I un ideal de A . Entonces:

$$\frac{B}{B \cap I} \cong \frac{B + I}{I}$$

Demostración

Bibliografía

- [Lam94] Leslie Lamport. “LaTeX: A Document Preparation System”. En: *Addison-Wesley* (1994). URL: <https://www.latex-project.org/help/documentation/latex2e/>.
- [Knu97] Donald E. Knuth. *The Art of Computer Programming, Volume 1: Fundamental Algorithms*. 3rd. Addison-Wesley, 1997. ISBN: 978-0201896831. URL: <https://www.pearson.com/store/p/the-art-of-computer-programming-volume-1-fundamental-algorithms/P100000001007/9780201896831>.