Infierno y Purgatorio
Saga de la Divina comedia

Jesús González Abril

Curso 2025-2026

Índice general

Capítulo 1

Grupos

1.1. Operaciones binarias

Definición 1.1.1: Operación binaria

Sea X un conjunto. Una operación binaria en X es una aplicación $* : X \times X \to X$. 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. Motivación del concepto de grupo

Sección sacada de [Arn09].

Una *transformación* de un conjunto es una aplicación biyectiva del conjunto sobre sí mismo.

Ejercicio 1.3

¿Cuál de las tres siguientes aplicaciones es una transformación?

$$1)\ \mathbb{R} \to \mathbb{R},\ \ x \mapsto e^x; \quad 2)\ \mathbb{R} \to \mathbb{R},\ \ x \mapsto x^3; \quad 3)\ \mathbb{C} \to \mathbb{C},\ \ z \mapsto z^2.$$

Respuesta: Solo la segunda.

El *producto* fg de las transformaciones f y g de un conjunto es la transformación obtenida aplicando primero g, luego f, es decir, $(fg)(x) = f(g(x))$.

Ejercicio 1.4

Dar un ejemplo en el que fg no sea igual a gf.

La transformación f^{-1} *inversa* de f se define por la condición de que si f lleva x a y, entonces f^{-1} lleva y a x.

Una colección de transformaciones de un conjunto se llama *grupo de transformaciones* si contiene la inversa de cada una de sus transformaciones y el producto de cualesquiera dos de sus transformaciones.

Ejercicio 1.5

¿Es el conjunto de las tres reflexiones sobre los vértices de un triángulo equilátero un grupo de transformaciones? ¿Cuántos elementos hay en el grupo de isometrías de un triángulo equilátero? ¿Y en el grupo de rotaciones de un tetraedro?

Respuesta: No, 6, 12.

El concepto de grupo de transformaciones es uno de los más fundamentales en toda la matemática y al mismo tiempo uno de los más simples: la mente humana piensa naturalmente en términos de invariantes de grupos de transformaciones (esto está conectado tanto con el aparato visual como con nuestro poder de abstracción).

Sea A un grupo de transformaciones en el conjunto X. La multiplicación y la inversión definen aplicaciones $A \times A \to A$ y $A \to A$ (el par (f, g) va a fg, y el elemento g a g^{-1}). Un conjunto A dotado de estas dos aplicaciones se llama *grupo*. Así, un *grupo* se obtiene de un *grupo de transformaciones* simplemente ignorando el conjunto que se transforma.

1.3. Definiciones y ejemplos

Definición 1.3.1: Grupo

Un grupo es una pareja $(G, \cdot)$, formada por un conjunto no vacío G junto con una operación binaria, que denotaremos por $\cdot$, que satisface los siguientes axiomas:

1. (Asociativa) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$.
2. (Neutro) Existe un elemento $e \in G$, llamado elemento neutro del grupo, tal que $e \cdot a = a = a \cdot e$, para todo $a \in G$.
3. (Inverso) Para todo $a \in G$ existe otro elemento $a^{-1} \in G$, llamado elemento inverso de a, tal que $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Si además se verifica el siguiente axioma se dice que el grupo es abeliano o conmutativo:

4. (Conmutativa) $a \cdot b = b \cdot a$, para todo $a, b \in G$.

Demostraremos ahora algunas propiedades de los grupos.

Lema 1.3.2: Propiedades básicas de grupos

Sea $(G, \cdot)$ un grupo.

1. (Unicidad del neutro) El neutro de G es único y lo denotaremos e. De hecho, si $a, b \in G$ satisfacen que $a \cdot b = a$ ó $b \cdot a = a$ entonces $b = e$.
2. (Unicidad del inverso) El inverso de un elemento a de G es único y lo denotaremos a^{-1}. De hecho, si e es el neutro de G y $a, b \in G$ satisfacen $a \cdot b = e$ ó $b \cdot a = e$ entonces $b = a^{-1}$.
3. (Propiedad Cancelativa) Todo elemento de G es cancelativo.
4. Para todo $a, b \in G$, las ecuaciones $a \cdot X = b$ y $X \cdot a = b$ tienen una única solución en G.
5. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demostración

1. Haremos solo el caso por la derecha, en efecto, si $a \cdot b = a$ entonces
$$b = e \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot a = e.$$
2. De nuevo hacemos solo el caso $a \cdot b = e$
$$a^{-1} = a^{-1} \cdot e = a^{-1} \cdot a \cdot b = e \cdot b = b.$$
3. Sea $x \in G$, entonces x debe ser cancelable puesto que en caso contrario existirían $a, b \in G$

con $a \neq b$ tales que $x \cdot a = x \cdot b$, pero entonces

$$a = e \cdot a = x^{-1} \cdot x \cdot a = x^{-1} \cdot x \cdot b = e \cdot b = b$$

una contradicción.

4. Sean $a, b \in G$ arbitrarios y x, y dos soluciones cualesquiera, entonces

$$x = e \cdot x = a^{-1} \cdot a \cdot x = a^{-1} \cdot b$$

y de igual manera

$$y = e \cdot y = a^{-1} \cdot a \cdot y = a^{-1} \cdot b$$

luego $x = y$. Para la otra ecuación se razona igual. Notemos que también hemos demostrado la existencia de una solución ($x = a^{-1} \cdot b$).

5. Basta realizar un sencillo cálculo y aplicar el apartado 2

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

■

Ejemplo

Sea X un conjunto y consideremos la aplicación identidad $id : X \to X$ tal que $id(x) = x$ para todo $x \in X$. Entonces el conjunto $T = \{id\}$ con la operación de composición es un grupo $(T, \circ)$ que llamaremos el grupo trivial (lo denotaremos 1).
En general, podríamos haber definido este grupo como un único elemento $\{x\}$ con la operación descrita por $x \cdot x = x$.

En términos de grupos de transformaciones, el grupo trivial de X es el grupo de transformaciones más pequeño que podemos construir. Que en efecto se trata de un grupo es inmediato.

Ejemplo

Sean X un conjunto y S_X el conjunto de todas las biyecciones de X en sí mismo. Entonces $(S_X, \circ)$ es un grupo, llamado grupo simétrico o grupo de las permutaciones de X.

En términos de grupos de transformaciones, el grupo de permutaciones de X es el grupo de transformaciones más grande que podemos construir. Probemos ahora que en efecto es un grupo.

Demostración

Prescindiremos del uso de $\circ$ para simplificar la notación.

1. Asociativa: sean f, g, h biyecciones, dado $x \in X$ cualquiera

$$((fg)h)x = (fg)(h(x)) = f(g(h(x))) = f(gh(x)) = (f(gh))x \implies (fg)h = f(gh)$$

2. Neutro: basta considerar la aplicación identidad $id(x) = x$.
3. Inverso: claramente el inverso de una biyección cualquiera f es su inversa f^{-1}, que verifica

$$(ff^{-1})(x) = f(f^{-1}(x)) = x$$

luego $ff^{-1} = id$.

Nota

En general S_X no es un grupo abeliano.

Ejemplo

Si $(G, *)$ y $(H, *)$ son dos grupos, entonces el producto directo $G \times H$ es un grupo en el que la operación viene dada componente a componente:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 * h_2).$$

Más generalmente, si $(G_i)_{i \in I}$ es una familia arbitraria de grupos, entonces el producto directo $\prod_{i \in I} G_i$ tiene una estructura de grupo en el que el producto se realiza componente a componente. Para más información ver la Definición A.5.1.

Probemos que el producto directo de dos grupos es un grupo:

Demostración

1. Asociativa:

$$\begin{aligned}((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) = (g_1 * g_2, h_1 * h_2) \cdot (g_3, h_3) = (g_1 * g_2 * g_3, h_1 * h_2 * h_3) = \\ = (g_1, h_1) \cdot (g_2 * g_3, h_2 * h_3) = (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3))\end{aligned}$$

donde hemos usado la asociatividad de los grupos G, H.

2. Neutro: basta considerar el elemento (e_G, e_H) donde e_G es el neutro de G y e_H el de H.
3. Inverso: claramente el inverso de un elemento cualquiera (g_1, h_1) es (g_1^{-1}, h_1^{-1}), que verifica

$$(g_1, h_1) \cdot (g_1^{-1}, h_1^{-1}) = (g_1 * g_1^{-1}, h_1 * h_1^{-1}) = (e_G, e_H).$$

Ejemplo

Para cada número natural positivo n definimos un grupo C_n formado por n elementos

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\},$$

donde a es un símbolo, y en el que la multiplicación viene dada por la siguiente regla:

$$a^i a^j = a^{[i+j]_n}$$

donde $[x]_n$ denota el resto de dividir x entre n. Este grupo se llama cíclico de orden n.
También definimos el grupo cíclico infinito como el conjunto $C_\infty = \{a^n : n \in \mathbb{Z}\}$, donde a es un símbolo y consideramos $a^n = a^m$ si y solo si $n = m$, y en el que el producto viene dado por $a^n \cdot a^m = a^{n+m}$.

Nota

Es fácil notar la similitud entre C_n y $\mathbb{Z}_n$, así como entre C_∞ y $\mathbb{Z}$. Más tarde formalizaremos esta intuición probando que estos grupos son equivalentes (isomorfos).

Ejemplo

Para cada número natural positivo n definimos un grupo formado por $2n$ elementos

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$$

en el que la multiplicación viene dada por la siguiente regla:

$$(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{[i_1+(-1)^{j_1}i_2]_n}b^{[j_1+j_2]_2}$$

con notación como en el ejemplo anterior. Este grupo se llama grupo diédrico de orden $2n$.
El grupo diédrico infinito D_∞ está formado por elementos de la forma a^nb^m, con $n \in \mathbb{Z}$ y $m = 0, 1$ con el producto $(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{i_1+(-1)^{j_1}i_2}b^{[j_1+j_2]_2}$.

Capítulo 2

Anillos

2.1. Anillos

Definición 2.1.1: 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

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

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. El termino divisor de

cero se justifica por lo siguiente. Supongamos que $x \in A$ no es cancelable respecto al producto, en tal caso existen dos elementos distintos $a \neq b$ tales que $ax = bx$. Pero entonces es inmediato que

$$(a-b)x = 0$$

sin embargo, ni $(a-b)$ ni x son cero, por lo que podemos interpretar que ambos son «divisores del cero».

2.1.1. 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

Demostrar que se trata de anillos conmutativos es muy sencillo, basta comprobar que se verifican todas las propiedades pertinentes.

Probaremos que en $\mathbb{C}$ todos los elementos salvo el 0 son invertibles, el resto de afirmaciones quedan como ejercicio. 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 $f : X \to \cup_{i\in X} A_i$, es decir, el conjunto de funciones $f : X \to A$, luego A^X es un anillo correspondiente a un producto «infinito» del anillo A consigo mismo. Para más información ver la Definición A.5.1.

Ejemplo

Dado un anillo A, un polinomio en una indeterminada es una expresión:

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

donde $n \geq 0$ y $a_i \in A$ para todo i. El conjunto de polinomios con coeficientes en A se denota $A[X]$. La suma y producto en $A[X]$ se definen de la forma usual.

Ejemplo

Dado un anillo A, denotamos por $A[[X]]$ el conjunto de sucesiones $(a_0, a_1, a_2, \ldots)$ de elementos de A. Con las operaciones:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (a_0b_0, a_0b_1 + a_1b_0, \ldots),$$

$A[[X]]$ es un anillo llamado anillo de series de potencias con coeficientes en A.

2.1.2. Propiedades de los anillos

Lema 2.1.2

Sea A un anillo y sean $a, b, c \in A$. Se verifican las siguientes propiedades

1. Todo elemento de A es cancelable respecto de la suma.
2. Todo elemento invertible de A es regular en A.
3. Si $b + a = a$ entonces $b = 0$. Si $ba = a$ para todo a, entonces $b = 1$. En particular, el cero y uno son únicos.
4. El opuesto de a es único y si a es invertible, entonces a tiene un único inverso.
5. $0a = 0 = a0$.
6. $a(-b) = (-a)b = -(ab)$.
7. $a(b - c) = ab - ac$.
8. a y b son invertibles si y solo si ab y ba son invertibles. En tal caso $(ab)^{-1} = b^{-1}a^{-1}$.
9. Si $0 = 1$ entonces $A = \{0\}$.

Demostración

1. Como A es un grupo respecto de la suma todo elemento tiene inverso, y por la Proposición 1.1.5 todo elemento invertible (respecto a la suma) es cancelable (respecto a la suma).
2. De nuevo por la Proposición 1.1.5 todo elemento invertible (respecto al producto) es cancelable (respecto al producto).
3. Si $b + a = a$ entonces como a es cancelable por el apartado 1, tenemos $b = 0$. Si $ba = a$ para todo a, entonces como el neutro es único $b = 1$.
4. De nuevo se sigue de la Proposición 1.1.5.
5. Basta aplicar un pequeño truco
$$0a = (0 + 0)a = 0a + 0a \implies 0 = 0a$$
para el caso $a0$ se procede igual.
6. Basta notar que
$$ab + a(-b) = a(b - b) = 0, ab + (-a)b = (a - a)b = 0 \implies -(ab) = a(-b) = (-a)b$$
ya que los opuestos son únicos.
7. $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac$.

8. En primer lugar si a, b son invertibles entonces existen a^{-1}, b^{-1} y es fácil ver que

$$ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab, ba(a^{-1}b^{-1}) = e = (a^{-1}b^{-1})ba$$

luego ab, ba son invertibles. Para el recíproco, si ab, ba son invertibles entonces

$$a(b(ab)^{-1}) = ab(ab)^{-1} = e, ((ba)^{-1}b)a = (ba)^{-1}ba = e$$

por tanto, por la Proposición 1.1.5 ambos simétricos $b(ab)^{-1}, (ba)^{-1}b$ son iguales (ambos son a^{-1}) y a es invertible. Para ver que b es invertible se procede igual.

9. Si $0 = 1$ entonces dado $x \in A$ tenemos

$$x = x1 = x0 = 0 \implies A = \{0\}.$$

Dados un anillo A, un elemento $a \in A$ y un entero positivo n, la notación na (respectivamente a^n) representa el resultado de sumar (respectivamente multiplicar) a consigo mismo n veces, y si $n = 0$ convenimos que $0a = 0$ y $a^0 = 1$. Más rigurosamente, a partir de estas últimas igualdades se definen na y a^n de forma recurrente poniendo $(n+1)a = a + na$ y $a^{n+1} = aa^n$ para $n \geq 0$. Por último, si $n \geq 1$ se define $(-n)a = -(na)$, y si además a es invertible se define $a^{-n} = (a^{-1})^n$.

Lema 2.1.3

Sea A un anillo, $a, b \in A$, y $m, n \in \mathbb{Z}$. Se verifican:

1. $n(a + b) = na + nb$.
2. $(n + m)a = na + ma$.
3. Si $n, m \geq 0$, entonces $a^{n+m} = a^n a^m$. Si a es invertible, la igualdad vale para n, m arbitrarios.
4. Si A es conmutativo y $n \geq 0$, entonces $(ab)^n = a^n b^n$. Si a y b son invertibles, la igualdad vale para todo n.

Demostración

1. Por inducción: el caso base $n = 0$ es inmediato, si lo suponemos para n entonces

$$(n + 1)(a + b) = (a + b) + na + nb = (n + 1)a + (n + 1)b.$$

2. Basta aplicar recursivamente que $(n + 1)a = a + na$.
3. Basta aplicar recursivamente que $a^{n+1} = aa^n$. Si a es invertible entonces podemos usar que $a^{-n} = (a^{-1})^n$ distinguiendo casos. Por ejemplo si $n > 0, m < 0, n > m$ entonces

$$a^n a^m = a^n (a^{-1})^{-m} = a^{n+m} a^{-m} (a^{-1})^{-m} = a^{n+m}.$$

4. Por inducción: el caso base $n = 0$ es inmediato, si lo suponemos para n entonces

$$(ab)^{n+1} = ab(ab)^n = aba^n b^n = aa^n bb^n = a^{n+1}b^{n+1}.$$

Cuando a y b son invertibles, si $n < 0$

$$(ab)^n = ((ab)^{-1})^{-n} = (b^{-1}a^{-1})^{-n} = (b^{-1})^{-n}(a^{-1})^{-n} = b^n a^n.$$

2.2. Subanillos

Nota

A partir de ahora supondremos que todos los anillos serán conmutativos, con lo que por defecto cada vez que digamos anillo estaremos suponiendo que se trata de un anillo conmutativo.

Sea una operación en un conjunto A y sea B un subconjunto de A. Decimos que B es cerrado con respecto a si para todo $a, b \in B$ se verifica que $ab \in B$. En tal caso podemos considerar como una operación en B que se dice inducida por la operación en A.

Un subsemigrupo de un semigrupo es un subconjunto suyo que con la misma operación es un semigrupo. Un subgrupo de un grupo es un subconjunto suyo que con la misma operación es un grupo. Un submonoide de un monoide es un subconjunto suyo que con la misma operación es un monoide con el mismo neutro.

Definición 2.2.1: Subanillo

Un subanillo de un anillo es un subconjunto suyo que con la misma suma y producto es un anillo con el mismo uno.

Proposición 2.2.2: Caracterización de subanillos

Las siguientes condiciones son equivalentes para $B \subseteq A$:

1. B es un subanillo de A.
2. B contiene al 1 y es un anillo, luego es cerrado para sumas, productos y opuestos.
3. B contiene al 1 y es cerrado para restas y productos.

Demostración

(1) $\implies$ (2): Si B es un subanillo, contiene al 1 y es cerrado para sumas y productos. Además, el cero de B coincide con el de A, y los opuestos en B coinciden con los de A.
(2) $\implies$ (3): Inmediato.
(3) $\implies$ (1): Si B contiene al 1 y es cerrado para restas, entonces $0 = 1 - 1 \in B$, y para $b \in B$, $-b = 0 - b \in B$. Además, $a + b = a - (-b) \in B$, luego B es cerrado para sumas.

2.3. Homomorfismos de anillos

Definición 2.3.1: Homomorfismo de anillos

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

2.4. Ideales y anillos cociente

Definición 2.4.1: 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 2.4.2: Congruencia módulo un ideal

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

Definición 2.4.3: Anillo cociente

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

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (a \cdot b) + I$$

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

2.5. Teoremas de isomorfía

Teorema 2.5.1: Primer teorema de isomorfía

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

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

Demostración

Teorema 2.5.2: 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 2.5.3: 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

Teorema 2.5.4: Teorema chino de los restos

Sea A un anillo y $I_1, \ldots, I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces:

$$\frac{A}{I_1 \cap \cdots \cap I_n} \cong \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$$

Demostración

Apéndice A

Teoría de conjuntos

A.1. Conjuntos y clases

Introducimos de manera informal en esta sección la teoría de conjuntos de von Neumann-Bernays-Gödel (denotada NBG). Para más información consultar [Wik25]. Las nociones primitivas en esta teoría son las de clase, pertenencia e igualdad. Intuitivamente consideramos que una clase es una colección A de objetos tal que dado un objeto cualquiera x podemos determinar si este pertenece a la clase ($x \in A$) o no ($x \notin A$).

Los axiomas de la teoría se formulan en terminos de estas nociones primitivas y del cálculo de predicados lógicos de primer orden (es decir, las afirmaciones construidas usando conectores de tipo *y, o, negación, implica*, y cuantificadores $\forall, \exists$). Por ejemplo, se asume que la igualdad tiene las siguientes propiedades para cualesquiera clases A, B, C:

$$A = A, \quad A = B \implies B = A, \quad (A = B) \wedge (B = C) \implies A = C, \quad (A = B) \wedge (x \in A) \implies x \in B.$$

Por otro lado, el **axioma de extensionalidad** afirma que dos clases con los mismos elementos son iguales:

$$(x \in A \iff x \in B) \implies A = B.$$

Una clase A es un conjunto si y solo si existe una clase B tal que $A \in B$. Por tanto, un conjunto es un tipo particular de clase. Una clase que no es un conjunto se llama una clase propia. Informalmente un conjunto es una clase «pequeña», mientras que una clase propia es «grande». El **axioma de formación** de clases asegura que para cualquier enunciado $P(y)$ de primer orden involucrando a la variable y existe una clase A tal que

$$x \in A \iff (x \text{ es un conjunto} \wedge x \text{ es verdadero})$$

en tal caso denotamos a la clase A como $\{x : P(x)\}$, llamada clase de todos los x tal que se cumple $P(x)$. En ocasiones podemos describir una clase listando sus elementos: $\{a, b, c\}$.

Ejemplo

> Consideremos la clase $M = \{X : X \text{ es un conjunto y } X \notin X\}$. La afirmación $X \notin X$ tiene sentido como predicado, de hecho muchos conjuntos la satisfacen (por ejemplo, el conjunto de todos los libros no es un libro). Veamos que M es una clase propia. En efecto, si M fuera un conjunto, entonces tendríamos que $M \in M$ o $M \notin M$. Pero por la definición de M, $M \in M$ implica $M \notin M$ y $M \notin M$ implica $M \in M$. Así, en ambos casos, la suposición de que M es un conjunto lleva a una contradicción: $M \in M$ y $M \notin M$.

Una clase A es una subclase de una clase B, $A \subset B$ si

$$\forall x \in A, x \in A \implies x \in B$$

por el axioma de extensionalidad y las propiedades de la igualdad tenemos

$$A = B \iff (A \subset B) \wedge (B \subset A).$$

Una subclase A de un conjunto B es un conjunto en sí misma, y en tal caso decimos que es un subconjunto.

El conjunto vacío $\emptyset$ es el conjunto sin elementos, es decir, $\forall x, x \notin \emptyset$. Como la afirmación $x \in \emptyset$ es siempre falsa tenemos de manera trivial que $\emptyset \subset B$ para cualquier clase B. Se dice entonces que A es una subclase propia de B si $A \subset B$ pero $A \neq \emptyset, A \neq B$.

El **axioma de partes** establece que para cualquier conjunto A la clase $\mathcal{P}(A)$ de todos sus subconjuntos es ella misma un conjunto, que usualmente llamamos las partes de A.

A.2. Uniones, intersecciones, complementos

Una familia de conjuntos indexada por una clase (no vacía) I es una colección de conjuntos $\{A_i : i \in I\}$. Dada una familia su unión e intersección son las clases:

$$\cup_{i \in I} A_i = \{x : x \in A_i \text{ para algún } i \in I\}$$
$$\cap_{i \in I} A_i = \{x : x \in A_i \text{ para todo } i \in I\}$$

Si I es un conjunto entonces las construcciones anteriores son conjuntos.

Si A y B son clases su diferencia es la subclase de B

$$B \setminus A = \{x : x \in B, x \notin A\}.$$

A.3. Aplicaciones

Dadas dos clases A, B la definición de aplicación es idéntica a la ya conocida para conjuntos. Se dan por conocidos los conceptos ya conocidos de dominio, rango, restricciones, etc. Dos aplicaciones son iguales si tienen el mismo dominio, rango y asignan el mismo valor a cada elemento de su dominio común.

Dada una clase A la aplicación identidad en A (denotada $1_A : A \to A$) es la aplicación dada por $a \mapsto a$. Si $S \subseteq A$, la aplicación $1_A|_S : S \to A$ se llama la aplicación inclusión de S en A.

Sean $f : A \to B$ y $g : B \to C$ aplicaciones. La composición de f y g es la aplicación $A \to C$ dada por

$$a \mapsto g(f(a)), \quad a \in A.$$

La aplicación compuesta se denota $g \circ f$ o simplemente gf. Si $h : C \to D$ es una tercera aplicación, es fácil verificar que $h(gf) = (hg)f$. Si $f : A \to B$, entonces $f \circ 1_A = f = 1_B \circ f : A \to B$.

Un diagrama:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h}\downarrow & \swarrow{\scriptstyle g} & \\ C & & \end{array}$$

se dice que es conmutativo si $gf = h$. De manera similar, el diagrama:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[k]{} & D \end{array}$$

es conmutativo si $kh = gf$. Frecuentemente se trabaja con diagramas más complicados compuestos por varios triángulos y cuadrados como los anteriores. Tal diagrama se dice conmutativo si todo triángulo y cuadrado en él es conmutativo.

Las nociones de inyectividad y sobreyectividad son las usuales. Una aplicación $f : A \to B$ se dice inyectiva si

$$\forall a, a' \in A, \quad a \neq a' \implies f(a) \neq f(a').$$

Una aplicación f es sobreyectiva si $f(A) = B$; es decir,

$$\forall b \in B, \quad b = f(a) \text{ para algún } a \in A.$$

Una aplicación f se dice biyectiva si es a la vez inyectiva y sobreyectiva. Se sigue inmediatamente de estas definiciones que, para cualquier clase A, la aplicación identidad $1_A : A \to A$ es biyectiva.

Enunciamos ahora el siguiente teorema que permite caracterizar las nociones anteriores en aplicación de inversas por la derecha e izquierda.

Teorema A.3.1

Sea $f : A \to B$ una aplicación, con $A \neq \emptyset$.

1. f es inyectiva si y solo si existe una aplicación $g : B \to A$ tal que $gf = 1_A$.
2. Si A es un conjunto, entonces f es sobreyectiva si y solo si existe una aplicación $h : B \to A$ tal que $fh = 1_B$.

La aplicación g del teorema anterior se llama una inversa por la izquierda de f, y h se llama una inversa por la derecha de f. Si una aplicación $f : A \to B$ tiene inversas por ambos lados entonces

$$g = g1_B = g(fh) = (gf)h = 1_A h = h$$

y la aplicación $g = h$ se llama la inversa de f. Este argumento también muestra que la inversa de una aplicación (si existe) es única. Por el Teorema A.3.1, si A es un conjunto y $f : A \to B$ una aplicación, entonces

$$f \text{ es biyectiva} \iff f \text{ tiene inversa por ambos lados}$$

La única inversa de una biyección f se denota f^{-1}; claramente f es una inversa de f^{-1}, por lo que f^{-1} también es una biyección.

Nota

> La caracterización de biyectividad como existencia de una inversa es válida incluso cuando A es una clase propia

A.4. Relaciones

El **axioma de formación de pares** establece que para dos conjuntos (elementos) a, b, existe un conjunto $P = \{a, b\}$ tal que $x \in P$ si y solo si $x = a$ o $x = b$; si $a = b$, entonces P es el conjunto unitario $\{a\}$. El par ordenado (a, b) se define como el conjunto $\{\{a\}, \{a, b\}\}$; su primera componente es a y su segunda componente es b. Es fácil verificar que $(a, b) = (a', b')$ si y solo si $a = a'$ y $b = b'$. El producto cartesiano de las clases A y B es la clase

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Nótese que $A \times \emptyset = \emptyset = \emptyset \times B$.

Una subclase R de $A \times B$ se llama una relación en $A \times B$. Por ejemplo, si $f : A \to B$ es una aplicación, el grafo de f es la relación $R = \{(a, f(a)) : a \in A\}$. Como f es una aplicación, R tiene la propiedad especial:

$$\text{cada elemento de } A \text{ es la primera componente de uno y solo un par ordenado en } R. \qquad (*)$$

Recíprocamente, cualquier relación R en $A \times B$ que satisfaga $(*)$ determina una única aplicación $f : A \to B$ cuyo grafo es R (definiendo $f(a) = b$, donde (a, b) es el único par ordenado en R con primera componente a). Por esta razón es habitual identificar una aplicación con su grafo, es decir, definir una aplicación como una relación que satisface $(*)$.

Otra ventaja de este enfoque es que permite definir funciones con dominio vacío. Dado que $\emptyset \times B = \emptyset$ es el único subconjunto de $\emptyset \times B$ y satisface trivialmente $(*)$, existe una única aplicación $\emptyset \to B$. También es claro por $(*)$ que solo puede haber una aplicación con rango vacío si el dominio también es vacío.

A.5. Productos

En esta sección solo tratamos con conjuntos. No hay clases propias involucradas.

Consideremos el producto cartesiano de dos conjuntos $A_1 \times A_2$. Un elemento de $A_1 \times A_2$ es un par (a_1, a_2) con $a_i \in A_i$, $i = 1, 2$. Así, el par (a_1, a_2) determina una aplicación $f : \{1, 2\} \to A_1 \cup A_2$ mediante: $f(1) = a_1$, $f(2) = a_2$. Recíprocamente, toda aplicación $f : \{1, 2\} \to A_1 \cup A_2$ con la propiedad de que $f(1) \in A_1$ y $f(2) \in A_2$ determina un elemento $(a_1, a_2) = (f(1), f(2))$ de $A_1 \times A_2$. Por lo tanto, no es difícil ver que hay una correspondencia biyectiva entre el conjunto de todas las aplicaciones de este tipo y el conjunto $A_1 \times A_2$. Este hecho nos lleva a generalizar la noción de producto cartesiano como sigue.

Definición A.5.1: Producto

Sea $\{A_i : i \in I\}$ una familia de conjuntos indexada por un conjunto (no vacío) I. El producto (cartesiano) de los conjuntos A_i es el conjunto de todas las aplicaciones $f : I \to \bigcup_{i \in I} A_i$ tales que $f(i) \in A_i$ para todo $i \in I$. Se denota $\prod_{i \in I} A_i$.

Si $I = \{1, 2, \ldots, n\}$, el producto $\prod_{i \in I} A_i$ a menudo se denota por $A_1 \times A_2 \times \cdots \times A_n$ y se identifica con el conjunto de todas las n-tuplas ordenadas $(a_1, a_2, \ldots, a_n)$, donde $a_i \in A_i$ para $i = 1, 2, \ldots, n$, como en el caso mencionado anteriormente donde $I = \{1, 2\}$. Una notación similar es a menudo conveniente cuando I es infinito. A veces denotaremos la aplicación $f \in \prod_{i \in I} A_i$ por $(a_i)_{i \in I}$ o simplemente (a_i), donde $f(i) = a_i \in A_i$ para cada $i \in I$.

Si algún $A_i = \emptyset$, entonces $\prod_{i \in I} A_i = \emptyset$, ya que no puede haber una aplicación $f : I \to \bigcup A_i$ tal que $f(i) \in A_i$. Si $\{A_i : i \in I\}$ y $\{B_i : i \in I\}$ son familias de conjuntos tales que $B_i \subset A_i$ para cada $i \in I$, entonces toda aplicación $I \to \bigcup B_i$ puede considerarse como una aplicación $I \to \bigcup_{i \in I} A_i$. Por lo tanto, consideramos $\prod_{i \in I} B_i$ como un subconjunto de $\prod_{i \in I} A_i$.

A.5.1. Caracterización del producto

Sea $\prod_{i \in I} A_i$ un producto cartesiano. Para cada $k \in I$, definamos una aplicación $\pi_k : \prod_{i \in I} A_i \to A_k$ mediante $f \mapsto f(k)$, o en la otra notación, $(a_i) \mapsto a_k$. π_k se llama la proyección canónica del producto sobre su k-ésima componente. Se deja como ejercicio probar que si cada A_i es no vacío, entonces cada π_k es sobreyectiva.

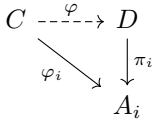
El producto $\prod_{i \in I} A_i$ y sus proyecciones son precisamente lo que necesitamos para el siguiente teorema

Teorema A.5.2: Propiedad universal del producto

Sea $\{A_i : i \in I\}$ una familia de conjuntos indexada por I. Entonces existe un conjunto D, junto con una familia de aplicaciones $\{\pi_i : D \to A_i : i \in I\}$, con la siguiente propiedad: para cualquier conjunto C y familia de aplicaciones $\{\varphi_i : C \to A_i : i \in I\}$, existe una única aplicación $\varphi : C \to D$ tal que $\pi_i \varphi = \varphi_i$ para todo $i \in I$. Además, D está determinado de manera única salvo biyección.

La última frase significa que si D' es un conjunto y $\{\pi_i' : D' \to A_i : i \in I\}$ una familia de aplicaciones que tienen la misma propiedad que D y $\{\pi_i\}$, entonces existe una biyección $D \to D'$.

Nótese que el enunciado del Teorema A.5.2 no menciona elementos; involucra solo conjuntos y aplicaciones. Establece que el producto $\prod_{i\in I} A_i$ se caracteriza por una cierta propiedad universal que cumplen todas las aplicaciones. Esta propiedad se resume en el siguiente diagrama conmutativo:



Bibliografía

[Hun74] Thomas W. Hungerford. *Algebra*. Springer, 1974. ISBN: 0-387-90518-9.

[Arn09] Vladimir I. Arnold. *Ordinary Differential Equations*. Springer Berlin Heidelberg, 2009. ISBN: 9783540862000.

[Wik25] Wikipedia contributors. *Von Neumann–Bernays–Gödel set theory — Wikipedia, The Free Encyclopedia*. [Online; accessed 13-August-2025]. 2025. URL: `https://en.wikipedia.org/w/index.php?title=Von_Neumann%E2%80%93Bernays%E2%80%93G%C3%B6del_set_theory&oldid=1281064703`.