Índice general

Capítulo 1

Anillos

1.1. Operaciones binarias

Sea X un conjunto. Una *operación binaria* en X es una aplicación $* : X \times X \to X$. La imagen de (a, b) la denotamos por $a * b$. Decimos que $*$ es:

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

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

- *Neutro por la izquierda (neutro por la derecha)* de X con respecto a $*$ 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)* en X respecto a $*$ si para cada dos elementos distintos a y b de X se verifica $x * a \neq x * b$ ($a * x \neq b * x$).
- 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 que $x * y = e$.

Decimos que x es

- *Neutro* de X con respecto a $*$ si es neutro por la izquierda y por la derecha de X con respecto a $*$.
- *Cancelable* en X con respecto a $*$ si es cancelable en X con respecto a $*$ por los dos lados.
- *Simétrico* de y con respecto a $*$ si es simétrico de y con respecto a $*$ por los dos lados. En tal caso decimos que x es *invertible* de X respecto a $*$.

Un par $(X, *)$ formado por un conjunto y una operación binaria $*$ 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.

En el futuro simplificaremos la terminología y en lugar de decir "operación binaria" diremos simplemente "operación". Por otro lado nos ahorraremos los "con respecto a" cuando la operación esté clara por el contexto y los "de X" o "en X" cuando el conjunto X esté claro por el contexto o diremos que e es neutro, neutro por un lado, inverso, invertible o cancelable en $(X, *)$.

Veamos algunos ejemplos.

Ejemplos 1.1. *Operaciones*

(1) La suma es una operación en los conjuntos $\mathbb{N}$ de los números naturales, $\mathbb{Z}^{\geq 0}$ de los enteros no negativos, $\mathbb{Z}$ de los números enteros, $\mathbb{Q}$ de los números racionales, $\mathbb{R}$ de los números reales y $\mathbb{C}$ de los números complejos. En todos los casos se trata de una operación conmutativa y asociativa. Además 0 es neutro. Todo elemento a de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es cancelable y es invertible con respecto a la suma y su simétrico es su opuesto $-a$. Por tanto $(\mathbb{N}, +)$ es un semigrupo conmutativo, $(\mathbb{Z}^{\geq 0}, +)$ es un monoide conmutativo, y $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos abelianos.

(2) Otra operación conmutativa y asociativa en $\mathbb{N}$, $\mathbb{Z}^{\geq 0}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es el producto. En este caso el 1 es el neutro y todo elemento $a \neq 0$ de $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es invertible y su simétrico es su inverso a^{-1}. Sin embargo, en $\mathbb{Z}$ solamente 1 y -1 son invertibles respecto del producto mientras que 1 es el único elemento invertible de $\mathbb{N}$ y $\mathbb{Z}^{\geq 0}$. Por tanto, el producto define en todos estos conjuntos una estructura de monoide conmutativo y define una estructura de grupo abeliano en $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$ y $\mathbb{C} - \{0\}$. El único elemento de estos conjuntos que no es cancelativo con respecto al producto es el cero.

(3) Sea A un conjunto y sea $X = A^A$, el conjunto de las aplicaciones de A en A. 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. Sin embargo, esta operación no es conmutativa si A tiene al menos dos elementos.

(4) Sea A un conjunto y sea $X = \mathbb{R}^A$ el conjunto de las aplicaciones de A en $\mathbb{R}$. Definimos la suma en X poniendo

$$(f + g)(a) = f(a) + g(a), \quad a \in A$$

Esta es una operación conmutativa y asociativa, la aplicación 0 dada por $0(a) = 0$ para todo $a \in A$ es un neutro y para toda aplicación $f : A \to \mathbb{R}$, el simétrico de f con respecto a $+$ es la aplicación $-f$ dada por $(-f)(a) = -f(a)$. Por tanto, $(\mathbb{R}^A, +)$ es un grupo abeliano.

Definimos ahora el producto $\cdot$ en X poniendo

$$(f \cdot g)(a) = f(a)g(a), \quad a \in A$$

Esta operación también es conmutativa y asociativa y tiene por neutro la aplicación 1 dada por $1(a) = 1$ para todo $a \in A$. Para que un elemento f de X sea invertible es necesario y suficiente que $f(a) \neq 0$ para todo $a \in A$. En tal caso el simétrico de f con respecto a $\cdot$ es la aplicación g dada por $g(a) = g(a)^{-1}$. Luego $(\mathbb{R}^A, \cdot)$ es un monoide conmutativo.

Veamos ahora algunas propiedades básicas de las definiciones dadas más arriba.

1.2. Ideales y anillos cociente

Teorema 1.1 (Teorema de la Correspondencia). *Si I es un ideal de un anillo A, las asignaciones $J \mapsto J/I$ y $X \mapsto \pi^{-1}(X)$ definen aplicaciones biyectivas (una inversa de la otra) que conservan la inclusión entre el conjunto de los ideales de A que contienen al I y el conjunto de los ideales de A/I.*

Demostración.

(1) Si J es un ideal de A que contiene a I entonces J/I es un ideal de A/I y $\pi^{-1}(J/I) = J$.

(2) Si X es un ideal de A/I entonces $\pi^{-1}(X)$ es un ideal de A que contiene a I y $\pi^{-1}(X)/I = X$.

(3) Si $J \subseteq K$ son ideales de A que contienen a I entonces entonces $J/I \subseteq K/I$.

(4) Si $X \subseteq Y$ son ideales de A/I entonces $\pi^{-1}(X) \subseteq \pi^{-1}(Y)$.

□

1.3. Operaciones con ideales

Sea A un anillo. Recordemos que X es un subconjunto de A entonces llamamos *ideal* de A *generado* por X al menor ideal de A que contiene a X y que

$$(X) = \left\{ \sum_{i=1}^{n} a_i x_i : n \geq 0, a_i \in A, x_i \in X \right\}$$

Es fácil ver que la intersección de una familia de ideales de A es un ideal de A. Eso implica que (X) es también la intersección de todos los ideales de A que contienen a X.

Si I y J son dos ideales de A entonces la suma y el producto de A son los conjuntos

$$\begin{aligned} I + J &= \{x + y : x \in, y \in J\} \\ IJ &= \{x_1 y_1 + \cdots x_n y_n : x_1 \cdots, x_n \in I, y_1, \cdots, y_n \in J\} \end{aligned}$$

Más generalmente, si $I_1, \ldots, I_n$ son ideales, entonces la suma de estos ideales es

$$I_1 + \cdots + I_n = \{x_1 + \cdots + x_n : x_1 \in I_1, \ldots, x_n \in I_n\}$$

y el producto $I_1 \cdots I_n$, es el ideal formado por las sumas de productos de la forma $x_1 \cdots x_n$ donde $x_1 \in I_1, \ldots, x_n \in I_n$.

Aún más general, si $\{I_x : x \in X\}$ es una familia de ideales de A entonces

$$\sum_{x \in X} I_x = \left\{ \sum_{x \in X} a_x : a_x \in I_x \text{ para todo } x \in X \text{ y } a_x = 0 \text{ para casi todo } x \in X \right\}$$

y $\prod_{x \in X} I_x$ es el ideal formado por las sumas de productos de la forma $\prod_{x \in X} a_x$ donde $a_x \in I_x$ para todo $x \in X$ y $a_x = 1$ para casi todo $x \in X$.

Proposición 1.1. *Si $\{I_x : x \in X\}$ es una familia de ideales de un anillo A entonces:*

(1) $\sum_{x \in X} I_x$ es el menor ideal de A que contiene a todos los I_x, o sea el ideal generado por $\cup_{x \in X} I_x$.

(2) Si $I_1, \ldots, I_n$ son ideales de A entonces $I_1 \cdots I_n$ es el menor ideal de A generado por los productos $x_1 \cdots x_n$ con $x_1 \in I_1, \ldots, x_n \in I_n$.

Ejemplo 1.1. *Operaciones con ideales*

(1) Sean n y m dos números enteros y consideremos los ideales (n) y (m) de $\mathbb{Z}$. Claramente $(n)(m) = (nm)$. Por otro lado, $(n) \cap (m)$ está formado por los números enteros que son múltiplos de n y m. Esos son precisamente los múltiplos del mínimo común múltiplo de n y de m. Finalmente, $(n)+(m)$ es el menor ideal (d) de $\mathbb{Z}$ que contiene a (n) y (m), $(d) = (n)+(m)$ si y solo si d divide a n y a m y es múltiplo de todos los divisores comunes de n y m. O sea, d es el máximo común divisor de n y m. En resumen:

$$(n)(m) = (nm), \quad (n) \cap (m) = (\mathrm{mcm}\,(n,m)), \quad (n) + (m) = (\mathrm{mcd}\,(n,m))$$

(2) Consideremos ahora el anillo $\mathbb{Z}[X]$ de los polinomios con coeficientes enteros. Entonces $(2) + (X)$ está formado por los polinomios cuyo término independiente es par. Vamos a ver que este ideal no es principal. Supongamos por reducción al absurdo que $(2) + (X) = (a)$ para algún $a \in \mathbb{Z}[X]$. Entonces $2 = ab$ para algún polinomio b, lo que que implica que $a \in \mathbb{Z}$. Además, como $a \in (2, X)$, necesariamente a es par, lo que implica $X \notin (a) = (2) + (X)$, una contradicción.

1.4. Los Teoreamas de Isomorfía y Chino de los Restos

Teorema 1.2 (**Primer teorema de isomorfía**). *Sea $f : A \to B$ un homomorfismo de anillos. Entonces existe un único isomorfismo de anillos $\overline{f} : A/\operatorname{Ker} f \to \operatorname{Im} f$ que hace conmutativo el diagrama*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "p"'] & B \\
A/\operatorname{Ker} f \arrow[r, dashed, "\overline{f}"] & \operatorname{Im} f \arrow[u, "i"']
\end{tikzcd}$$

es decir, $i \circ \overline{f} \circ p = f$, donde i es la inclusión y p es la proyección. En particular,

$$A/\operatorname{Ker} f \simeq \operatorname{Im} f$$

Demostración. Sean $K = \operatorname{Ker} f$ e $I = \operatorname{Im} f$. La aplicación $\overline{f} : A/K \to I$ dada por $\overline{f}(x+K) = f(x)$ está bien definida (no depende de representantes) pues si $x + K = y + K$ entonces $x - y \in K$ y por lo tanto $f(x) - f(y) = f(x - y) = 0$, es decir, $f(x) = f(y)$. Además es elemental ver que es un homomorfismo de anillos y que es suprayectiva. Para ver que es inyectiva, veamos que su nucleo es nulo. Si $x + K$ está en el núcleo de $\overline{f}$ entonces $0 = \overline{f}(x + K) = f(x)$, de modo que $x \in K$ y así $x+K = 0+K$. Es decir $\operatorname{Ker} \overline{f} = 0$ y por lo tanto f es inyectiva. En conclusión, $\overline{f}$ es un isomorfismo, y hace conmutativo el diagrama porque, para cada $x \in A$, se tiene

$$i\left(\overline{f}\,(p(x))\right) = \overline{f}(x + K) = f(x)$$

En cuanto a la unicidad, supongamos que otro homomorfismo $\widehat{f} : A/K \longrightarrow I$ verifica que $i \circ \widehat{f} \circ p = f$; entonces para cada $x \in A$ se tiene $\widehat{f}(x + K) = i(\widehat{f}(p(x))) = f(x) = \overline{f}(x + K)$, y por lo tanto $\widehat{f} = \overline{f}$. □

Teorema 1.3 (**Segundo teorema de isomorfía**). *Sea A un anillo y sean I y J dos ideales tales $I \subseteq J$. Entonces J/I es ideal de A/I y existe un isomorfismo de anillos*

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

Demostración. Por el teorema de la correspondencia 1.1, J/I es un ideal de A/I. Sea $f : A/I \to A/J$ la aplicación definida por $f(a+I) = a+J$. Es elemental ver que f está bien definida, que es un homomorfismo suprayectivo de anillos y que $\operatorname{Ker} f = J/I$. Entonces el isomorfismo buscado se obtiene aplicando el primer teorma de isomorfía. □

Teorema 1.4 (**Tercer teorema de isomorfía**). *Sea A un anillo con un subanillo B y un ideal I. Entonces:*

(1) $B \cap I$ es un ideal de B.

(2) $B + I$ es un subanillo de A que contiene a I como ideal.

(3) Se tiene el isomorfismo de anillos

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

Demostración. Los dos primeros apartados se dejan como ejercicio. En cuanto al último, sea $f : B \to A/I$ la composición de la inclusión $j : B \to A$ con la proyección $p : A \to A/I$. Es claro que $\operatorname{Ker} f = B \cap I$ y que $\operatorname{Im} f = (B+I)/I$, por lo que el resultado se sigue del primer teorema de isomorfía. □