

Índice general

1. Anillos	1
1.1. Operaciones binarias	1
1.2. Ideales y anillos cociente	3
1.3. Operaciones con ideales	4
1.4. Los Teoremas de Isomorfía y Chino de los Restos	5

Capítulo 1

Anillos

1.1. Operaciones binarias

Sea X un conjunto. Una *operación binaria* en X es una aplicación $*$: $X \times X \rightarrow X$. 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 $f : A \rightarrow \mathbb{R}$, 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 $g(a) = f(a)^{-1}$. Luego (\mathbb{R}^A, \cdot) es un monoide conmutativo.

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

Proposición 1.1. *Sea $*$ una operación en un conjunto X .*

- (1) *Si $*$ es conmutativa entonces todo neutro por un lado, es neutro, todo elemento cancelativo por un lado es cancelativo y todo elemento que tenga simétrico por un lado es invertible.*

- (2) 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.
- (3) Supongamos que $(X, *)$ es un monoide y sea $a \in X$.
- (a) Si x es simétrico por la izquierda de a e y es un simétrico por la derecha de a entonces $x = y$.
- (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) Es obvio.
- (2) Como e es neutro por la izquierda y f es neutro por la derecha tenemos

$$f = e * f = e$$

- (3a) Ahora suponemos que $(X, *)$ es un monoide. Por (2), $(X, *)$ 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

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

- (3b) 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

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

□

Por la proposición 1.1, si $(X, *)$ es un monoide cada elemento invertible a sólo tiene un simétrico que habitualmente se denota por a^{-1} .

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 a 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

$$I + J = \{x + y : x \in I, y \in J\}$$

$$IJ = \{x_1 y_1 + \cdots + x_n y_n : x_1, \dots, x_n \in I, y_1, \dots, y_n \in J\}$$

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

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

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 $x_1 \in I_1, \dots, x_n \in I_n$.

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 1.2. 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 $\bigcup_{x \in X} I_x$.
- (2) Si I_1, \dots, 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 $x_1 \in I_1, \dots, x_n \in I_n$.

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:

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

- (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 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 Teoremas de Isomorfía y Chino de los Restos

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

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ p \downarrow & & \uparrow i \\ A/\text{Ker } f & \xrightarrow{\bar{f}} & \text{Im } f \end{array}$$

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

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

Demostración. Sean $K = \text{Ker } f$ e $I = \text{Im } f$. La aplicación $\bar{f} : A/K \rightarrow I$ dada por $\bar{f}(x + K) = f(x)$ 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 núcleo es nulo. Si $x + K$ está en el núcleo de \bar{f} entonces $0 = \bar{f}(x + K) = f(x)$, de modo que $x \in K$ y así $x + K = 0 + K$. Es decir $\text{Ker } \bar{f} = 0$ y por lo tanto \bar{f} es inyectiva. En conclusión, \bar{f} es un isomorfismo, y hace conmutativo el diagrama porque, para cada $x \in A$, se tiene

$$i(\bar{f}(p(x))) = \bar{f}(x + K) = f(x)$$

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

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 $f : A/I \rightarrow A/J$ 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 $\text{Ker } f = J/I$. Entonces el isomorfismo buscado se obtiene aplicando el primer teorema de isomorfía. \square

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 $f : B \rightarrow A/I$ la composición de la inclusión $j : B \rightarrow A$ con la proyección $p : A \rightarrow A/I$. Es claro que $\text{Ker } f = B \cap I$ y que $\text{Im } f = (B + I)/I$, por lo que el resultado se sigue del primer teorema de isomorfía. \square