

Anillos, Ideales y Cuerpos

11 de noviembre de 2018

Índice

1. Leyes de composición. Estructuras algebraicas.	1
2. Ejemplos	5
3. Reglas de cálculo	9
4. Homomorfismos	13
5. Subestructuras	16
6. Anillos cocientes	21
7. Dominios de integridad y cuerpos	23
8. El cuerpo de fracciones	25
Índice alfabético	27

1. Leyes de composición. Estructuras algebraicas.

Sean A, M conjuntos.

Definición 1.1. Una *operación binaria* o *ley de composición interna* en A es una aplicación

$$A \times A \rightarrow A \quad (a, b) \mapsto a * b.$$

Una *acción por la izquierda* o *ley de composición externa* de A sobre M es una aplicación

$$A \times M \rightarrow M \quad (a, x) \mapsto a * x.$$

De manera análoga se define una *acción por la derecha* como una aplicación

$$M \times A \rightarrow M \quad (x, a) \mapsto x * a.$$

Es costumbre escribir las leyes de composición como operadores “infijo”, es decir, con un símbolo entre los elementos. Se suelen usar los símbolos $+$, $-$, $*$, \cdot , \times , \div , \circ , \diamond , etc. O bien simplemente yuxtaponiendo los elementos combinados como ab o ax .

Ejemplo 1.2. La suma $a + b$ y el producto ab de números enteros son leyes de composición internas de \mathbb{Z} . También existen estas operaciones para los racionales \mathbb{Q} , los reales \mathbb{R} y los complejos \mathbb{C} .

Ejemplo 1.3. Sea $n > 0$ un entero fijo y sea \mathbb{Z}_n el conjunto de clases módulo n . Hemos definido las operaciones binarias suma y producto como $[a]_n + [b]_n = [a + b]_n$ y $[a]_n [b]_n = [ab]_n$.

En este caso también tenemos una acción $\mathbb{Z} \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ definida por $a[x]_n = [ax]_n$.

Ejemplo 1.4. Sea X un conjunto y sea $A = \{f : X \rightarrow X\}$ el conjunto de todas las aplicaciones de X en sí mismo. Podemos definir una operación $A \times A \rightarrow A$ por $(f, g) \mapsto fg$ donde $fg : X \rightarrow X$ viene dada por composición de aplicaciones, es decir que para todo $x \in X$ se define $(fg)(x) = f(g(x))$.

Ejemplo 1.5. Para cualquier K -espacio vectorial V la multiplicación de un escalar por un vector define una acción $K \times V \rightarrow V$.

Ejemplo 1.6. Sea $M = M_n(\mathbb{R})$ el conjunto de todas las matrices cuadradas de orden n con coeficientes reales. En M hay definidas dos operaciones internas, la suma y el producto, y una operación externa, el producto de un escalar por una matriz.

Ejemplo 1.7. Dada una ley de composición $a * b$, se define la *ley de composición opuesta* como $a *^o b = b * a$ para todo a, b . Si la ley de partida es interna $A \times A \rightarrow A$, también lo es la opuesta. Si la ley es una acción por la izquierda, la opuesta es una acción por la derecha y viceversa.

Una *estructura algebraica* se define por datos de tres tipos:

- Un conjunto A , que se llama *conjunto subyacente*.
- Una o varias leyes de composición (internas o externas) definidas sobre A .

- Unos axiomas que deben verificar dichas leyes.

En rigor la estructura algebraica está formada por el conjunto A junto con las operaciones. Pero por abuso de lenguaje, se suele designar con la misma letra a la estructura y al conjunto subyacente.

Existen muchas estructuras algebraicas, pero las más importantes son las tres siguientes.

Definición 1.8. Un grupo $(G, *)$ es un conjunto G junto con una ley de composición interna $G \times G \rightarrow G$ denotada por $(a, b) \mapsto a * b$ que verifica:

- *Asociatividad:* $\forall a, b, c \in G \ a * (b * c) = (a * b) * c,$
- *Existencia de neutro:* $\exists e \in G \ \forall a \in G \ e * a = a = a * e,$
- *Existencia de opuesto:* $\forall a \in G \ \exists a' \in G \ a * a' = e = a' * a.$

El elemento e se llama *elemento neutro* para la operación y el elemento a' se llama *opuesto de a* .

En el caso particular en que la operación se denote por $a + b$, el elemento neutro se llama *elemento nulo o cero* y se denota por 0 .

El opuesto de a se denota por $-a$.

Si la operación se denota por ab , $a \cdot b$ o $a \times b$, el elemento neutro se llama *unidad o uno* y se denota por 1 . Y el opuesto de a se llama *inverso* y se denota por a^{-1} .

Un grupo se llama *conmutativo o abeliano* si verifica el axioma adicional

- *Conmutatividad:* $\forall a, b \in G \ a * b = b * a.$

Definición 1.9. Un anillo $(A, +, \cdot)$ es un conjunto A junto con dos operaciones binarias $A \times A \rightarrow A$ denotadas por suma $a + b$ y producto ab que verifican los axiomas:

- *Asociatividad de la suma:* $\forall a, b, c \in A \ a + (b + c) = (a + b) + c,$
- *Existencia de cero:* $\exists 0 \in A \ \forall a \in A \ 0 + a = a = a + 0,$
- *Existencia de opuesto:* $\forall a \in A \ \exists -a \in A \ a + (-a) = 0 = (-a) + a,$

- *Conmutatividad de la suma:* $\forall a, b \in A \ a + b = b + a$.
Estos cuatro primeros axiomas se resumen en uno: $(A, +)$ es un grupo abeliano.
- *Asociatividad del producto:* $\forall a, b, c \in A \ a(bc) = (ab)c$,
- *Distributividad:* $\forall a, b, c \in A \ a(b + c) = ab + ac$, $(b + c)a = ba + ca$,
- *Existencia de uno:* $\exists 1 \in A \ \forall a \in A \ 1a = a = a1$.

Un anillo se llama *conmutativo* o *abeliano* si verifica el axioma

- *Conmutatividad del producto:* $\forall a, b \in A \ ab = ba$.

Un *anillo de división* es un anillo que verifica el axioma adicional

- *Existencia de inverso:* $\forall a \in A, \ a \neq 0, \ \exists a^{-1} \in A \ aa^{-1} = 1 = a^{-1}a$.

Un *cuerpo* es un anillo de división conmutativo.

Definición 1.10. Sea A un anillo. Un *módulo por la izquierda sobre A* o *A -módulo* $(M, +, \cdot)$ es un conjunto M junto con una ley de composición interna $M \times M \rightarrow M$ dada por $(x, y) \mapsto x + y$ y una ley de composición externa $A \times M \rightarrow M$ denotada $(a, x) \mapsto ax$ que verifican los axiomas:

- *Asociatividad:* $\forall x, y, z \in M \ x + (y + z) = (x + y) + z$,
- *Existencia de cero:* $\exists 0 \in M \ \forall x \in M \ 0 + x = x = x + 0$,
- *Existencia de opuesto:* $\forall x \in M \ \exists -x \in M \ x + (-x) = 0 = (-x) + x$,
- *Conmutatividad:* $\forall x, y \in M \ x + y = y + x$.

Estos cuatro primeros axiomas pueden resumirse en uno: $(M, +)$ es un grupo abeliano.

- *Distributividad respecto a escalares:* $\forall a, b \in A \ \forall x \in M \ (a + b)x = ax + bx$,
- *Distributividad respecto a vectores:* $\forall a \in A \ \forall x, y \in M \ a(x + y) = ax + ay$,
- *Pseudoasociatividad:* $\forall a, b \in A \ \forall x \in M \ a(bx) = (ab)x$,

- *Acción trivial del uno:* $\forall x \in M \ 1x = x$.

Los elementos de M se llaman *vectores* y los elementos de A se llaman *escalares*.

En el caso particular en que A es un cuerpo, M se llama *espacio vectorial sobre A* .

De manera análoga se define el concepto de *módulo por la derecha sobre A* .

Definición 1.11. Sea K un anillo conmutativo. Un *álgebra (lineal, asociativa y unitaria) sobre K* es un conjunto A junto con dos leyes de composición internas $A \times A \rightarrow A$ denotadas por $a + b$ y ab y una ley de composición externa $K \times A \rightarrow A$ denotada por $\lambda * a$ que verifican:

- $(A, +, *)$ es un K -módulo,
- $(A, +, \cdot)$ es un anillo.
- *pseudoasociatividad:* $\forall \lambda \in K \ \forall a, b \in A \ (\lambda * a)b = \lambda * (ab) = a(\lambda * b)$.

2. Ejemplos

El que una estructura algebraica resulte interesante depende del número e importancia de los ejemplos que posea. Veamos ejemplos de las estructuras que hemos definido.

2.1. Ejemplos de grupos

Ejemplo 2.1. Sea $G = \{e\}$ un conjunto con un único elemento. Sólo hay una operación binaria posible, $e * e = e$. Este grupo $(G, *)$ es el más pequeño posible y se llama *grupo trivial*. Cualquier grupo con más de un elemento es un *grupo no trivial*.

Ejemplo 2.2. Para cualquier grupo $(G, *)$, el *grupo opuesto* G^o es el grupo $(G, *^o)$ donde $*^o$ es la operación opuesta de $*$. En particular, G es abeliano si y sólo si $G = G^o$.

Ejemplo 2.3. Los ejemplos más sencillos de grupos son los numéricos. Los casos más evidentes son:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y \mathbb{C} son grupos para $+$, siendo 0 el elemento neutro y $-a$ el opuesto de cada a .
2. $\mathbb{Q}^\times = \{a \in \mathbb{Q} \mid a \neq 0\}$, $\mathbb{R}^\times = \{a \in \mathbb{R} \mid a \neq 0\}$, $\mathbb{C}^\times = \{a \in \mathbb{C} \mid a \neq 0\}$, $\mathbb{Q}^+ = \{a \in \mathbb{Q} \mid a > 0\}$ y $\mathbb{R}^+ = \{a \in \mathbb{R} \mid a > 0\}$ son grupos para \times con 1 como elemento neutro y siendo el opuesto de a su inverso $a^{-1} = 1/a$. (Nótese que $\{a \in \mathbb{Z} \mid a \neq 0\}$ no es un grupo para \times , ya que no todo elemento tiene inverso).

3. Generalizamos el ejemplo anterior: Sea A un anillo arbitrario y sea $A^\times = U(A)$ el conjunto de elementos $a \in A$ que tienen un inverso $a^{-1} \in A$. Entonces $(A, +)$ es un grupo (el *grupo aditivo de A*), y (A^\times, \times) también es un grupo (el *grupo multiplicativo de A*).
4. Los axiomas para un espacio vectorial V sobre un cuerpo K incluyen en particular el hecho de que $(V, +)$ es un grupo abeliano. En particular, \mathbb{R}^n es un grupo aditivo.
5. Para todo número $n \in \mathbb{Z}$, $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ es un anillo, así que $(\mathbb{Z}/n\mathbb{Z}, +)$ y $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ son grupos, donde $(\mathbb{Z}/n\mathbb{Z})^\times = U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (\text{m. c. d.}(a, n) = 1)\}$.

No deben confundirse los grupos $\mathbb{Z}/n\mathbb{Z}$ (bajo la suma) y $(\mathbb{Z}/n\mathbb{Z})^\times$ (bajo multiplicación), aunque el último sea un subconjunto del primero, *no es un subgrupo*.

2.2. Ejemplos de anillos

Ejemplo 2.4. Sea $A = \{a\}$ un conjunto con un único elemento. En este caso sólo hay una operación binaria posible, y por tanto la suma y el producto coinciden: $a + a = a = aa$ y $0 = a = 1$. Este anillo $(A, +, \cdot)$ es el más pequeño posible y se llama *anillo trivial*. Cualquier anillo con más de un elemento es un *anillo no trivial*.

Ejemplo 2.5. Para cualquier anillo $(A, +, \cdot)$, definimos el *anillo opuesto* A° como el anillo $(A, +, \cdot^\circ)$ donde \cdot° es la operación opuesta de \cdot ; en particular, A es abeliano si y sólo si $A = A^\circ$.

Ejemplo 2.6. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y \mathbb{C} son anillos conmutativos respecto a la suma y producto usuales. En todos los casos el neutro para la suma es el número 0 y el neutro para el producto es el número 1. Además \mathbb{Q}, \mathbb{R} y \mathbb{C} son cuerpos.

Ejemplo 2.7. Para todo natural positivo n las clases de restos módulo n , \mathbb{Z}_n con la suma y producto de clases es también un anillo conmutativo. Este anillo es un cuerpo si y sólo si n es primo.

Ejemplo 2.8. Sea $\mathbb{J} = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\} \subset \mathbb{C}$. Para cualesquiera $a + bi, c + di \in \mathbb{J}$ se verifica

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i \in \mathbb{J}, \\(a + bi)(c + di) &= (ac - bd) + (ad + bc)i \in \mathbb{J}, \\0, 1 &\in \mathbb{J}, \\-(a + bi) &= (-a) + (-b)i \in \mathbb{J}.\end{aligned}$$

Como la suma y el producto de números complejos son asociativas y conmutativas y verifican la distributividad, tenemos un anillo conmutativo $(\mathbb{J}, +, \cdot)$ que se llama *anillo de los enteros de Gauss*.



Ejemplo 2.9. Sea $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Es obvio que este conjunto es cerrado para la suma y el producto, y como estas operaciones son asociativas y conmutativas en \mathbb{R} , también lo son en $\mathbb{Q}(\sqrt{2})$. De la misma manera se comprueba que el producto es distributivo respecto a la suma. Además $0 = 0 + 0\sqrt{2}$ y $1 = 1 + 0\sqrt{2}$ pertenecen a $\mathbb{Q}(\sqrt{2})$, y para todo $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ se verifica que $-x = (-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. En resumen, $\mathbb{Q}(\sqrt{2})$ es un anillo.

Para ver que es un cuerpo, observamos que para todo $a + b\sqrt{2} \in \mathbb{Q}$ distinto de cero se verifica que $a^2 - 2b^2 \neq 0$ (porque en otro caso, $\sqrt{2}$ sería racional). Así que

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2} \sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

luego es un cuerpo.

Ejemplo 2.10. Un subconjunto interesante del ejemplo anterior es

$$\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$$

que obviamente es cerrado para la suma, el producto, el cero y el uno. Para un elemento $u = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ el inverso u^{-1} pertenece a $\mathbb{Z}[\sqrt{2}]$ si y sólo si $m^2 - 2n^2 = \pm 1$.

Ejemplo 2.11. Un tipo de anillos importantes son los anillos de funciones. Sea X cualquier conjunto no vacío y sea A un anillo arbitrario. Sea $B = \{f : X \rightarrow A\}$. Definimos en B una suma y un producto punto a punto: $(f + g)(x) = f(x) + g(x)$ y $(fg)(x) = f(x)g(x)$. De cada axioma de anillo de A se deduce el axioma correspondiente en B . El anillo B es conmutativo si y sólo si lo es A .

Si X y A tienen más estructura podemos formar otros anillos de funciones que respetan esta estructura. Por ejemplo si $A = \mathbb{R}$ y X es el intervalo cerrado $X = [0, 1] \subset \mathbb{R}$ podemos formar el anillo conmutativo B de las funciones continuas $[0, 1] \rightarrow \mathbb{R}$. Los teoremas básicos sobre límites nos garantizan que la suma y el producto de funciones continuas son también funciones continuas.

Ejemplo 2.12. Sea A un anillo arbitrario y sea $n > 0$ un entero. Sea $M_n(A)$ el conjunto de todas las matrices $n \times n$ con coeficientes en A . Este conjunto es un anillo para las operaciones usuales de suma y producto de matrices. Si $n > 1$, el anillo $M_n(A)$ no es conmutativo.

Ejemplo 2.13. Sea A un anillo conmutativo. El conjunto $A[X]$ de todos los polinomios en una indeterminada con coeficientes en A junto con la suma y el producto es un anillo conmutativo.

2.3. Ejemplos de módulos

Ejemplo 2.14. El grupo abeliano \mathbb{Z}_n es un \mathbb{Z} -módulo con la acción

$$\mathbb{Z} \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

definida por $a[b]_n = [ab]_n$.

Ejemplo 2.15. Todo grupo abeliano M es un \mathbb{Z} -módulo de manera única, definiendo la acción $\mathbb{Z} \times M \rightarrow M$ por inducción:

$$ax = \begin{cases} 0 & \text{si } a = 0 \\ (a-1)x + x & \text{si } a > 0 \\ -(-ax) & \text{si } a < 0 \end{cases}$$

Ejemplo 2.16. El conjunto de vectores libres (del plano o del espacio) con la suma por la “regla del paralelogramo” y el producto escalar usual forman un espacio vectorial sobre \mathbb{R} (De hecho la nomenclatura y las propiedades intuitivas provienen de este ejemplo).

Ejemplo 2.17. Sean K un cuerpo, M un espacio vectorial sobre K y $t : M \rightarrow M$ una aplicación lineal. Definimos una ley externa $K[X] \times M \rightarrow M$ como

$$(a_m X^m + a_{m-1} X^{m-1} + \cdots + a_2 X^2 + a_1 X + a_0) \cdot u = a_m t^m(u) + a_{m-1} t^{m-1}(u) + \cdots + a_2 t^2(u) + a_1 t(u) + a_0 u.$$

Con esta operación, M pasa a ser un $K[X]$ -módulo (de hecho, todos los $K[X]$ -módulos se obtienen de esta manera).

2.4. Ejemplos de álgebras

Ejemplo 2.18. Sea M un A -módulo arbitrario. Para cualesquiera $x, y \in M$ definimos $xy = 0$. Con este producto obtenemos un álgebra asociativa, aunque no unitaria.

Ejemplo 2.19. Cualquier anillo A es una \mathbb{Z} -álgebra (asociativa y unitaria) de manera única.

Ejemplo 2.20. Todo anillo conmutativo A es un A -álgebra definiendo el producto externo igual al producto interno del anillo.

Ejemplo 2.21. Los números complejos con las operaciones usuales son un álgebra sobre los reales.

Ejemplo 2.22. Sea A un anillo conmutativo. Las matrices cuadradas $M_n(A)$ con la suma, producto y producto escalar usuales forman un A -álgebra (asociativa y unitaria).

Ejemplo 2.23. Sea A un anillo conmutativo. El conjunto $A[X]$ de todos los polinomios en una indeterminada con coeficientes en A junto con la suma, producto y producto escalar usuales es un álgebra sobre A (asociativa, conmutativa y unitaria).

Ejemplo 2.24. Sea K un cuerpo y sea $n > 1$. En el conjunto de matrices cuadradas $M_n(K)$ definimos un nuevo producto: $[A, B] = AB - BA$, donde el producto del segundo miembro es el producto usual de matrices (este nuevo producto se llama *corchete de Lie*). El conjunto $M_n(K)$ con la suma, el corchete de Lie y el producto escalar forma un álgebra no asociativa.

3. Reglas de cálculo

De los axiomas de cada estructura algebraica se deducen unas cuantas consecuencias sencillas pero importantes para manipular expresiones y realizar cálculos en la estructura, y por ello se llaman *reglas de cálculo*. Vamos a estudiar las correspondientes a grupos y anillos.

3.1. Reglas de cálculo para grupos

Proposición 3.1. Sea G un grupo con unidad e .

1. La unidad de un grupo es única
2. El inverso de cualquier elemento es único
3. (Propiedad cancelativa): Para $x, y, z \in G$,

$$xy = xz \text{ implica } y = z \quad yx = zx \text{ implica } y = z.$$

4. $e^{-1} = e$
5. Para todo elemento $x \in G$ se verifica $(x^{-1})^{-1} = x$
6. Para cualesquiera $x, y \in G$ se verifica $(xy)^{-1} = y^{-1}x^{-1}$
7. Para cualesquiera $x, y \in G$ existen únicos $u, v \in G$ tales que $xu = y$ y $vx = y$.

Demostración. 1. Sean $e, f \in G$ dos unidades. Entonces $e = ef = f$

2. Sean x', x^{-1} dos inversos para $x \in G$. Entonces $x' = x'e = x'(xx^{-1}) = (x'x)x^{-1} = ex^{-1} = x^{-1}$
3. Sea $xy = xz$. Multiplicamos ambos miembros por x^{-1} por la izquierda: $y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$. Igual por el otro lado.
4. De la misma definición: $ee = e$, luego $e = e^{-1}$
5. Por definición, $xx^{-1} = e = x^{-1}x$, luego de la misma definición de inverso obtenemos que $(x^{-1})^{-1} = x$
6. Un simple cálculo: $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = e$, luego $(xy)^{-1} = y^{-1}x^{-1}$

7. Otro simple cálculo muestra que $u = x^{-1}y$ y $v = yx^{-1}$ verifican las condiciones pedidas y son los únicos que las verifican. \square

Las propiedad asociativa garantiza que en un cálculo podemos introducir paréntesis arbitrariamente. Sean $x_1, \dots, x_n \in G$. Definimos por recurrencia: $\prod_{i=1}^n x_i = (\prod_{i=1}^{n-1} x_i)x_n$.

Proposición 3.2 (Ley asociativa general). Sea G un conjunto con una operación interna asociativa. Para cualesquiera enteros $m > n > 0$ sean x_1, \dots, x_m elementos de G . Se verifica

$$\left(\prod_{i=1}^n x_i\right)\left(\prod_{i=n+1}^m x_i\right) = \prod_{i=1}^m x_i.$$

Demostración. Por inducción sobre $m - n$ (el número de factores del segundo producto). Si $m - n = 1$, la expresión dada es

$$\left(\prod_{i=1}^n x_i\right)x_{n+1} = \prod_{i=1}^{n+1} x_i.$$

Sea ahora $m - n = k > 1$ y suponemos cierto el resultado cierto siempre que el segundo producto del primer miembro tenga menos de k factores. Calculamos usando la propiedad asociativa:

$$\left(\prod_{i=1}^n x_i\right)\left(\prod_{i=n+1}^m x_i\right) = \left(\prod_{i=1}^n x_i\right)\left(\left(\prod_{i=n+1}^{m-1} x_i\right)x_m\right) = \left(\left(\prod_{i=1}^n x_i\right)\left(\prod_{i=n+1}^{m-1} x_i\right)\right)x_m = \left(\prod_{i=1}^{m-1} x_i\right)x_m = \prod_{i=1}^m x_i. \quad \square$$

De la misma forma, cuando se verifica la propiedad conmutativa podemos multiplicar los elementos en cualquier orden:

Proposición 3.3 (Ley conmutativa general). Sea G un conjunto con una operación interna que es asociativa y conmutativa. Sean $x_1, \dots, x_n \in G$ y sea σ una permutación del conjunto $\{1, \dots, n\}$. Se verifica:

$$\prod_{i=1}^n x_i = \prod_{i=1}^n x_{\sigma(i)}.$$

Demostración. Por inducción sobre n . Para $n = 2$ sólo hay dos permutaciones: La identidad σ_0 y la trasposición $\sigma_1 = (1\ 2)$. Para σ_0 la igualdad es trivial: $x_1x_2 = x_1x_2$. Y para σ_1 es el enunciado de la propiedad conmutativa: $x_1x_2 = x_2x_1$.

Sea ahora $n > 2$ y suponemos el resultado cierto para todo producto con menos factores. Sea $k = \sigma(n)$. Entonces para todo $i \neq k$ existe un $j < n$ tal que $i = \sigma(j)$.

Calculamos:

$$\prod_{i=1}^n x_i = \prod_{i=1}^{k-1} x_i \left(x_k \prod_{i=k+1}^n x_i\right) = \prod_{i=1}^{k-1} x_i \left(\left(\prod_{i=k+1}^n x_i\right)x_k\right) = \left(\prod_{i=1}^{k-1} x_i \left(\prod_{i=k+1}^n x_i\right)\right)x_k = \left(\prod_{j=1}^{n-1} x_{\sigma(j)}\right)x_{\sigma(n)} = \prod_{i=1}^n x_{\sigma(i)}. \quad \square$$

Sea (G, \cdot) un grupo con elemento neutro 1 y sea $a \in G$ arbitrario. Para todo entero positivo n definimos por inducción: $a^0 = 1$ y $a^n = (a^{n-1})a$. Para $n < 0$ definimos también $a^n = (a^{-1})^{-n}$.

Si la operación se denota aditivamente, la notación que se usa es na .

Proposición 3.4. Para todo $a \in G$ y cualesquiera $m, n \in \mathbb{Z}$ se verifica:

$$a^{m+n} = a^m a^n \quad a^{mn} = (a^m)^n.$$

Si $a, b \in G$ y $ab = ba$, entonces para todo $n \in \mathbb{Z}$ se verifica

$$(ab)^n = a^n b^n.$$

Demostración. Todos los casos se demuestran por inducción sobre n . □

Si el grupo se denota aditivamente, las expresiones de la proposición anterior son

$$(m+n)a = ma + na, \quad (nm)a = n(ma), \quad n(a+b) = na + nb.$$

Corolario 3.5. Todo grupo abeliano es un \mathbb{Z} -módulo de manera única.

Este corolario nos dice que los conceptos “ \mathbb{Z} -módulo” y “grupo abeliano” son idénticos.

Si $m > n$ y $a^m = a^n$, necesariamente $a^{m-n} = 1$. Luego si en algún momento la sucesión a^0, a^1, a^2, \dots se repite, necesariamente el primer término que se repite es $a^0 = 1$.

Definición 3.6. Sea G un grupo y sea $a \in G$. Si para todo $n > 0$ se verifica $a^n \neq 1$, decimos que el orden de a es infinito y lo representamos por $o(a) = \infty$.

En otro caso, el menor $k > 0$ que verifica $a^k = 1$ se llama orden de a y se representa por $o(a) = k$. En este caso decimos que a es un elemento de orden finito o que es un elemento de torsión.

3.2. Reglas de cálculo para anillos

Proposición 3.7. Sea A un anillo.

1. Para todo $a \in A$ se verifica $a0 = 0 = 0a$
2. Si A no es el anillo trivial, $0 \neq 1$.
3. Para todo $a, b \in A$, $(-a)b = -(ab) = a(-b)$. En particular $-a = (-1)a$.

4. Para todo $a, b \in A$, $(-a)(-b) = ab$. En particular $(-1)(-1) = 1$.

Demostración. 1. $a + 0 = a$. Multiplicamos por a y usamos la propiedad distributiva: $aa + a0 = a(a + 0) = aa$. Restamos aa y obtenemos $a0 = 0$. Igual por el otro lado.

2. Si $0 = 1$, para todo $a \in A$ se verifica $a = a1 = a0 = 0$ y A es el anillo trivial.

3. Por la primera regla y la distributividad,

$$0 = 0b = (a + (-a))b = ab + (-a)b$$

Restando ab de ambos miembros obtenemos $-(ab) = (-a)b$. Igual por el otro lado.

4. Corolario inmediato de la regla anterior.

□

Proposición 3.8 (Ley distributiva general). Sea A un anillo. Para cualesquiera $a_1, \dots, a_n, b_1, \dots, b_m \in A$ se verifica

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$$

Demostración. Por doble inducción sobre m y n . Para $m = 1$ y $n = 2$ es la propiedad distributiva. Sea $m = 1$ y $n > 2$. Por inducción sobre n :

$$\left(\sum_{i=1}^n a_i \right) b_1 = \left(\left(\sum_{i=1}^{n-1} a_i \right) + a_n \right) b_1 = \left(\sum_{i=1}^{n-1} a_i \right) b_1 + a_n b_1 = \left(\sum_{i=1}^{n-1} a_i b_1 \right) + a_n b_1 = \left(\sum_{i=1}^n a_i b_1 \right).$$

Sea ahora $m > 1$. Por inducción

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^m b_j \right) = \left(\sum_{i=1}^n a_i \right) \left(\left(\sum_{j=1}^{m-1} b_j \right) + b_m \right) = \left(\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^{m-1} b_j \right) \right) + \left(\sum_{i=1}^n a_i \right) b_m = \sum_{i=1}^n \sum_{j=1}^{m-1} a_i b_j + \sum_{i=1}^n a_i b_m = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

□

Corolario 3.9. Para todo $n \in \mathbb{Z}$ y todo $a, b \in A$ se verifica

$$(na)b = n(ab) = a(nb).$$

Proposición 3.10 (Teorema del binomio). Sea A un anillo conmutativo y sea n un entero positivo. Para todo $a, b \in A$ se verifica

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

Definición 3.11. La *característica* de un anillo A es el orden de 1 en el grupo aditivo $(A, +)$ si este orden es finito. En otro caso la característica de A es cero. Se representa por $\text{car}(A)$.

Es decir, $\text{car}(A) = m > 0$ si m es el menor entero positivo tal que $m \cdot 1 = 0$. Si para todo $n > 0$ se verifica $n \cdot 1 \neq 0$, entonces $\text{car}(A) = 0$.

Proposición 3.12. Sea $\text{car}(A) = m$. Entonces para todo $a \in A$ se verifica $ma = 0$.

Demostración. Si $\text{car}(A) = 0$ el resultado es trivial. Supongamos $\text{car}(A) = m > 0$. Para cualquier $a \in A$ tenemos $ma = m(1a) = (m1)a = 0a = 0$. \square

4. Homomorfismos

4.1. Homomorfismos de grupos

Definición 4.1. Dados dos grupos G y H llamamos *homomorfismo* de G a H a toda aplicación $f : G \rightarrow H$ tal que para todo $x, y \in G$ verifique $f(xy) = f(x)f(y)$.

Ejemplo 4.2. La aplicación signo $\text{sgn} : S_n \rightarrow \{1, -1\}$ es un homomorfismo de grupos.

Ejemplo 4.3. La aplicación logaritmo $\log : \mathbb{R}^+ \rightarrow \mathbb{R}$ es un homomorfismo del grupo multiplicativo (\mathbb{R}^+, \times) en el grupo aditivo $(\mathbb{R}, +)$.

Ejemplo 4.4. Sea K un cuerpo. Llamamos *grupo lineal general* sobre K y representamos por $GL_n(K)$ al grupo $U(M_n(K))$, es decir al conjunto de todas las matrices $n \times n$ invertibles con la operación producto de matrices. La aplicación determinante $\det : GL_n(K) \rightarrow K^\times = U(K)$ que asigna a cada matriz su determinante es un homomorfismo de grupos.

Para un homomorfismo f arbitrario el grupo G se llama *dominio* de f y el grupo H se llama *codominio* o *rango* de f .

El conjunto $\text{Im}(f) = f(G) = \{f(x) \mid x \in G\} \subset H$ se llama *imagen* de f y el conjunto $\ker(f) = \{x \in G \mid f(x) = 1\} \subset G$ se llama *núcleo* de f .

Un homomorfismo de grupos f se llama *monomorfismo* si es una aplicación inyectiva, se llama *epimorfismo* si es una aplicación suprayectiva. Se llama *isomorfismo* si es una biyección y se representa por $f : G \cong H$.

Si el dominio y el codominio coinciden, $G = H$, diremos que f es un *endomorfismo*. Un endomorfismo biyectivo se llama *automorfismo*.

Proposición 4.5. 1. Para todo grupo G la aplicación identidad $1_G : G \rightarrow G$ es un automorfismo.


2. Sean $f_1 : G \rightarrow H$, $f_2 : H \rightarrow K$ dos homomorfismos de grupos. Entonces la aplicación compuesta $f_2 f_1 : G \rightarrow K$ es un homomorfismo.

3. Sea $f : G \rightarrow H$ un isomorfismo de grupos. Entonces la aplicación inversa $f^{-1} : H \rightarrow G$ también es un isomorfismo.

Corolario 4.6. Para un grupo arbitrario G , el conjunto de todos los automorfismos de G forman un grupo (con la composición de aplicaciones como operación), que se llama grupo de los automorfismos de G y se representa por $\text{Aut}(G)$.

Proposición 4.7. Todo homomorfismo de grupos $f : G \rightarrow H$ verifica:

1. $f(1) = 1$
2. $\forall x \in G \ f(x^{-1}) = f(x)^{-1}$.

Demostración. 1. $f(1) \cdot 1 = f(1) = f(1 \cdot 1) = f(1)f(1)$. Simplificando nos queda $1 = f(1)$. 

2. $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$, luego $f(x^{-1}) = f(x)^{-1}$.

□

4.2. Homomorfismos de anillos

Sean A y B dos anillos.

Definición 4.8. Un homomorfismo de A a B es una aplicación $f : A \rightarrow B$ que verifica:

$$\begin{aligned}\forall x, y \in A, \quad f(x + y) &= f(x) + f(y), \\ \forall x, y \in A, \quad f(xy) &= f(x)f(y), \\ f(1) &= 1.\end{aligned}$$

Obsérvese que la última condición no se deduce de las dos primeras.

Ejemplo 4.9. Sea B un anillo no trivial y sea f la aplicación cero. Entonces $f(1) = 0 \neq 1$, aunque $f(x + y) = 0 = f(x) + f(y)$ y $f(xy) = 0 = f(x)f(y)$.

Ejemplo 4.10. Sea $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ la aplicación definida por $f(x) = [x]_n$. Esta f es un homomorfismo de anillos.

Ejemplo 4.11. En general, para cualquier anillo A existe un único homomorfismo de anillos $u : \mathbb{Z} \rightarrow A$, que viene dado por $u(n) = n \cdot 1$ y que se llama homomorfismo unital de A .

Ejemplo 4.12. Sea A un anillo conmutativo y sea $a \in A$ arbitrario. La evaluación en a $E_a : A[X] \rightarrow A$ definida por $E_a(f(X)) = f(a)$ es un homomorfismo de anillos.

Para cualquier homomorfismo f el anillo A se llama *dominio* de f y el anillo B se llama *codominio* o *rango* de f .

El conjunto $\text{Im}(f) = f(A) = \{f(x) \mid x \in A\} \subset B$ se llama *imagen* de f y el conjunto $\ker(f) = \{x \in A \mid f(x) = 0\} \subset A$ se llama *núcleo* de f .

El homomorfismo de anillos f se llama *monomorfismo* si es una aplicación inyectiva, se llama *epimorfismo* si es una aplicación suprayectiva. Se llama *isomorfismo* si es una biyección y se representa por $f : A \cong B$.

Si el dominio y el codominio coinciden, $A = B$, diremos que f es un *endomorfismo*. Un endomorfismo biyectivo se llama *automorfismo*.

Proposición 4.13. 1. Para todo anillo A la aplicación identidad $1_A : A \rightarrow A$ es un automorfismo.



2. Sean $f_1 : A \rightarrow B$, $f_2 : B \rightarrow C$ dos homomorfismos de anillos. Entonces la aplicación compuesta $f_2 f_1 : A \rightarrow C$ es un homomorfismo.

3. Sea $f : A \rightarrow B$ un isomorfismo de anillos. Entonces la aplicación inversa $f^{-1} : B \rightarrow A$ también es un isomorfismo.

Corolario 4.14. Para un anillo arbitrario A , el conjunto de todos los automorfismos de A forman un grupo (con la composición de aplicaciones como operación), que se llama grupo de los automorfismos de A y se representa por $\text{Aut}(A)$.

4.3. Homomorfismos de módulos

Sea A un anillo y sean M y N dos A -módulos por la izquierda.

Definición 4.15. Un homomorfismo de A -módulos es una aplicación $f : M \rightarrow N$ que verifica:

$$\begin{aligned} \forall x, y \in M, \quad f(x + y) &= f(x) + f(y), \\ \forall a \in A, \forall x \in M \quad f(ax) &= af(x). \end{aligned}$$

El módulo M se llama *dominio* de f y el módulo N se llama *codominio* o *rango* de f .

El conjunto $\text{Im}(f) = f(M) = \{f(x) \mid x \in M\} \subset N$ se llama *imagen* de f y el conjunto $\ker(f) = \{x \in M \mid f(x) = 0\} \subset M$ se llama *núcleo* de f .

El homomorfismo de módulos f se llama *monomorfismo* si es una aplicación inyectiva, se llama *epimorfismo* si es una aplicación suprayectiva. Se llama *isomorfismo* si es una biyección y se representa por $f : M \cong N$.

Si el dominio y el codominio coinciden, $M = N$, diremos que f es un *endomorfismo*. Un endomorfismo biyectivo se llama *automorfismo*.

Proposición 4.16. 1. Para todo módulo M la aplicación identidad $1_M : M \rightarrow M$ es un automorfismo.

2. Sean $f_1 : M \rightarrow N$, $f_2 : N \rightarrow L$ dos homomorfismos de módulos. Entonces la aplicación compuesta $f_2 f_1 : M \rightarrow L$ es un homomorfismo.

3. Sea $f : M \rightarrow N$ un isomorfismo de módulos. Entonces la aplicación inversa $f^{-1} : N \rightarrow M$ también es un isomorfismo.
4. Sean $f_1, f_2 : M \rightarrow N$ y sea $a \in A$ arbitrario dos homomorfismos de módulos. Entonces las aplicaciones $f_1 + f_2, af_1 : M \rightarrow N$ son homomorfismos.

Corolario 4.17. Para dos módulos arbitrarios M, N el conjunto de todos los homomorfismos $f : M \rightarrow N$ forman un A -módulo (con la suma y el producto por escalares como operaciones) que se representa por $\text{Hom}_A(M, N)$.

Para un módulo arbitrario M , el conjunto de todos los endomorfismos de M forman un anillo (con la suma y la composición de aplicaciones como operaciones), que se llama anillo de los endomorfismos de M y se representa por $\text{End}_A(M)$.

Para un módulo arbitrario M , el conjunto de todos los automorfismos de M forman un grupo (con la composición de aplicaciones como operación), que se llama grupo de los automorfismos de M y se representa por $\text{Aut}_A(M)$.

5. Subestructuras

5.1. Subgrupos

Definición 5.1. Dados dos grupos (G, \cdot) y (H, \circ) , decimos que H es un subgrupo de G , y lo representamos por $H < G$, cuando H es un subconjunto de G y la aplicación de inserción $H \rightarrow G$ es un homomorfismo de grupos.

Ejemplo 5.2. Todo grupo G tiene dos subgrupos: El grupo formado sólo por el elemento unidad, que es el subgrupo trivial, y el mismo G , que es el subgrupo total. Ambos son los subgrupos impropios. Cualquier otro subgrupo es un subgrupo propio.

Por abuso de lenguaje se suele identificar al subgrupo (H, \circ) con el subconjunto H , ya que la ley de composición está determinada por el grupo G .

Proposición 5.3 (Caracterizaciones de subgrupo). 1. Sea G un grupo y sea $\emptyset \neq H \subset G$. Entonces H es un subgrupo de G si y sólo si se verifica:

- a) Para todo par de elementos $x, y \in H$ también $xy \in H$.
- b) $1 \in H$
- c) Para todo $x \in H$ también $x^{-1} \in H$.

2. Sea G un grupo y sea $\emptyset \neq H \subset G$. Entonces H es un subgrupo de G si y sólo si para todo par de elementos $x, y \in H$ se verifica que $xy^{-1} \in H$.
3. Sea G un grupo finito y sea $\emptyset \neq H \subset G$. Entonces H es un subgrupo de G si y sólo si para todo par de elementos $x, y \in H$ se verifica que $xy \in H$.

Demostración. 1. Trivial

2. Sea H un subgrupo de G y sean $x, y \in H$. Por ser H un subgrupo es cerrado para el inverso, luego $y^{-1} \in H$, y para la composición, luego $xy^{-1} \in H$.

Sea ahora H un subconjunto de G no vacío verificando la propiedad del enunciado. Por ser no vacío existe un $x \in H$, luego $1 = xx^{-1} \in H$ y $x^{-1} = 1x^{-1} \in H$. Y para cualesquiera $x, y \in H$, $xy = x(y^{-1})^{-1} \in H$. Así que H es cerrado para la unidad, el inverso y la composición. Luego es un subgrupo de G .

3. Por ser G un grupo finito, $\forall x \in G \exists n > 0 \ x^n = 1$ y por tanto $x^{-1} = x^{n-1}$. Por inducción sobre n , de la propiedad del enunciado y de $x \in H$ deducimos que $x^{n-1} \in H$. El resto es igual al apartado anterior. \square

Ejemplo 5.4. Para cualquier homomorfismo de grupos $f : G \rightarrow H$, el conjunto $\ker(f)$ es un subgrupo de G y el conjunto $\text{Im}(f)$ es un subgrupo de H .

Proposición 5.5. Sea K subgrupo de H y sea H subgrupo de G . Entonces K es un subgrupo de G .

Como ilustración del criterio vamos a demostrar el siguiente resultado.

Proposición 5.6. Sea $\{H_\lambda \mid \lambda \in \Lambda\}$ una familia de subgrupos de un grupo G . Entonces $H = \cap_\lambda H_\lambda$ es un subgrupo de G .

Demostración. Sea 1 el elemento unidad de G . Para todo λ , $1 \in H_\lambda$ así que $1 \in \cap_\lambda H_\lambda$ y por tanto H es no vacío.

Sean ahora $x, y \in H$ arbitrarios. Para todo λ se verifica que $x, y \in H_\lambda$ y por ser H_λ un subgrupo tenemos que $\forall \lambda \ xy^{-1} \in H_\lambda$. Luego $xy^{-1} \in \cap_\lambda H_\lambda = H$. \square

Esta proposición nos permite definir dos conceptos importantes.

Definición 5.7. Sea S un subconjunto de G . Llamamos *subgrupo generado por S* a la intersección H de todos los subgrupos de G que contienen a S . Lo representamos por $H = \langle S \rangle$.

Definición 5.8. Sea $\{H_\lambda \mid \lambda \in \Lambda\}$ una familia arbitraria de subgrupos de G . Llamamos *compuesto de los H_λ* al subgrupo generado por $S = \cup_\lambda H_\lambda$. Lo representamos por $\vee_\lambda H_\lambda$.

En el caso particular en que la familia es finita, sea H_1, \dots, H_n , su compuesto se representa por $H_1 \vee \dots \vee H_n$.

Proposición 5.9. 1. Sea $S = \emptyset$. Entonces $\langle S \rangle$ es el subgrupo trivial.

2. Para cualquier $S \subset G$ no vacío, $\langle S \rangle$ es el conjunto de todos los elementos de G que se expresan como producto finito de elementos de S y de sus inversos.

3. Sea G un grupo finito. Para cualquier $S \subset G$ no vacío, $\langle S \rangle$ es el conjunto de todos los elementos de G que se expresan como producto finito de elementos de S .

5.2. Subanillos e ideales

Definición 5.10. Dados dos anillos $(A, +, \cdot)$ y $(B, +, \circ)$, decimos que B es un subanillo de A , y lo representamos por $B < A$, cuando B es un subconjunto de A y la aplicación de inserción $B \rightarrow A$ es un homomorfismo de anillos.

Todo anillo A tiene dos subanillos: El anillo formado por los múltiplos de 1, que es el *subanillo primo*, y el mismo A , que es el *subanillo total*. Este último es el *subanillo impropio*. Cualquier otro subanillo es un *subanillo propio*.

Por abuso de lenguaje se suele identificar al subanillo $(B, +, \circ)$ con el subconjunto B , ya que la ley de composición está determinada por el anillo A .

Proposición 5.11 (Caracterizaciones de subanillo). 1. Sea A un anillo y sea $\emptyset \neq B \subset A$. Entonces B es un subanillo de A si y sólo si se verifica:

- a) Para todo par de elementos $x, y \in B$ también $x + y, xy \in B$.
- b) $0, 1 \in B$
- c) Para todo $x \in B$ también $-x \in B$.

2. Sea A un anillo y sea $\emptyset \neq B \subset A$. Entonces B es un subanillo de A si y sólo si para todo par de elementos $x, y \in B$ se verifica que $x - y, xy \in B$ y además $1 \in B$.

Obsérvese que para que B sea subanillo de A hay que comprobar explícitamente que la identidad es la misma en A que en B .

Ejemplo 5.12. El anillo \mathbb{Z} es un subanillo de $\mathbb{Z}[i]$ y de $\mathbb{Z}[\sqrt{2}]$. Ninguno de estos dos es un subanillo del otro, aunque ambos son subanillo de \mathbb{C} .

Además el anillo $\mathbb{Z}[\sqrt{2}]$ es un subanillo de $\mathbb{Q}(\sqrt{2})$.




Ejemplo 5.13. El subconjunto $\{[0], [2], [4]\} \subset \mathbb{Z}_6$ es un anillo con unidad $[4]$, pero no es un subanillo de \mathbb{Z}_6 porque el elemento neutro no es el mismo.

Ejemplo 5.14. Sea $A = M_n(\mathbb{R})$ el anillo de todas las matrices $n \times n$ con coeficientes en \mathbb{R} y sea B el subconjunto de todas las matrices de la forma

$$\begin{pmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots & a \end{pmatrix}$$

Es fácil comprobar que con la suma y producto usuales de matrices, B es un anillo cuya unidad es la matriz



$$\begin{pmatrix} 1/n & 1/n & \dots & 1/n \\ 1/n & 1/n & \dots & 1/n \\ \dots & \dots & \dots & \dots \\ 1/n & 1/n & \dots & 1/n \end{pmatrix}$$

Pero B no es un subanillo de A porque no tienen la misma unidad, aunque la suma y el producto sean los mismos.

Ejemplo 5.15. Para cualquier homomorfismo de anillos $f : A \rightarrow B$ el conjunto $\text{Im}(f)$ es un subanillo de B .

Proposición 5.16. Sea C subanillo de B y sea B subanillo de A . Entonces C es un subanillo de A .

Como ilustración del criterio vamos a demostrar lo siguiente.

Proposición 5.17. Sea $\{B_\lambda \mid \lambda \in \Lambda\}$ una familia de subanillos de un anillo A . Entonces $B = \bigcap_\lambda B_\lambda$ es un subanillo de A .

Esta proposición nos permite definir dos conceptos importantes.

Definición 5.18. Sea S un subconjunto de A . Llamamos *subanillo generado por S* a la intersección B de todos los subanillos de A que contienen a S . Lo representamos por $B = \mathbb{Z}[S]$.

Ejemplo 5.19. El anillo \mathbb{J} de los enteros de Gauss es el subanillo generado por i

Definición 5.20. Sea $\{B_\lambda \mid \lambda \in \Lambda\}$ una familia arbitraria de subanillos de A . Llamamos *compuesto de los B_λ* al subanillo generado por $S = \bigcup_\lambda B_\lambda$.

Proposición 5.21. 1. Sea $S = \emptyset$. Entonces $\mathbb{Z}[S]$ es el subanillo primo.

2. Sea A conmutativo. Para cualquier $S \subset A$ no vacío, $\mathbb{Z}[S]$ es el conjunto de todos los elementos de A que se expresan como polinomios en los elementos de S con coeficientes enteros.

Proposición 5.22. Sea B un subanillo cualquiera de A . Entonces B contiene al subanillo primo de A .

En anillos existe otra subestructura importante, que pasamos presentar ahora.

Definición 5.23. Sea A un anillo y sea I un subconjunto no vacío. Decimos que I es un *ideal* de A si se verifica:

- I es un subgrupo de $(A, +)$,
- $\forall a \in A \forall x \in I \ ax, xa \in I$,

Ejemplo 5.24. Todo anillo tiene dos ideales: el ideal trivial o nulo formado sólo por el elemento 0, y el ideal total que es todo el anillo. Estos son los *ideales impropios*. Cualquier otro ideal es un *ideal propio*.

Proposición 5.25. Un ideal I de A contiene al 1 si y sólo si $I = A$.

Corolario 5.26. Un ideal I de A es propio si y sólo si no es trivial y $1 \notin I$.

Ejemplo 5.27. Para cualquier homomorfismo de anillos $f : A \rightarrow B$ el núcleo $\ker(f)$ es un ideal de A .

Ejemplo 5.28. Sea A un anillo conmutativo y sea a un elemento de A . El conjunto $Aa = \{xa \mid x \in A\}$ es un ideal de A que se llama *ideal principal generado por a* .

Proposición 5.29. Sea $\{I_\lambda \mid \lambda \in \Lambda\}$ una familia de ideales de un anillo A . Entonces $I = \bigcap_\lambda I_\lambda$ es un ideal de A .

Proposición 5.30. Sean I, J ideales de un anillo A . Entonces $I + J$ es un ideal de A .

Definición 5.31. Sea S un subconjunto del anillo A . Llamamos *ideal generado por S* a la intersección de todos los ideales que contienen a S . Se representa por (S) .

Si $S = \{a_1, \dots, a_n\}$ es un conjunto finito, el ideal generado por S se representa por (a_1, \dots, a_n) .

Ejemplo 5.32. Si $S = \emptyset$, $(S) = 0$ es el ideal nulo.

Ejemplo 5.33. Si A es conmutativo y $a \in A$, $(a) = Aa$ el ideal principal generado por a .

Proposición 5.34. Sea A un anillo conmutativo y S un subconjunto no vacío suyo. Entonces

$$(S) = \left\{ \sum_{s \in S} x_s s \mid x_s \in A, \text{ de los cuales todos son cero salvo un número finito} \right\}.$$

Corolario 5.35. Sea $S = \{a_1, \dots, a_n\}$. Entonces

$$(a_1, \dots, a_n) = \{x_1 a_1 + \dots + x_n a_n \mid x_i \in A\} = Aa_1 + \dots + Aa_n.$$

5.3. Submódulos

Sea A un anillo fijo. Todos los módulos que vamos a considerar son módulos por la izquierda sobre A .

Definición 5.36. Dados dos módulos $(M, +)$ y $(N, +)$, decimos que N es un *submódulo de M* , y lo representamos por $N < M$, cuando N es un subconjunto de M y la aplicación de inserción $N \rightarrow M$ es un homomorfismo de módulos.

Ejemplo 5.37. Todo módulo M tiene dos submódulos: el módulo formado sólo por el elemento cero, que es el *submódulo trivial*, y el mismo M , que es el *submódulo total*. Ambos son los *submódulos impropios*. Cualquier otro submódulo es un *submódulo propio*.

Por abuso de lenguaje se suele identificar al submódulo $(N, +)$ con el subconjunto N , ya que la ley de composición está determinada por el módulo N .

Proposición 5.38 (Caracterizaciones de submódulo). 1. Sea M un módulo y sea $\emptyset \neq N \subset M$. Entonces N es un submódulo de M si y sólo si se verifica:

- a) Para todo par de elementos $x, y \in N$ también $x + y \in N$.
- b) Para todo $a \in A$ y todo $x \in N$ también $ax \in N$.
2. Sea M un módulo y sea $\emptyset \neq N \subset M$. Entonces N es un submódulo de M si y sólo si se verifica: Para todo par de escalares $a, b \in A$ y todo par de elementos $x, y \in N$ también $ax + by \in N$.

Ejemplo 5.39. Para cualquier homomorfismo de módulos $f : M \rightarrow N$, el conjunto $\ker(f)$ es un submódulo de M y el conjunto $\text{Im}(f)$ es un submódulo de N .

Proposición 5.40. Sea L submódulo de N y sea N submódulo de M . Entonces L es un submódulo de M .

El siguiente resultado sirve como ilustración de este criterio.

Proposición 5.41. Sea $\{N_\lambda \mid \lambda \in \Lambda\}$ una familia de submódulos de un módulo M . Entonces $N = \bigcap_\lambda N_\lambda$ es un submódulo de M .

Esta proposición nos permite definir dos conceptos importantes.

Definición 5.42. Sea S un subconjunto de M . Llamamos *submódulo generado por S* a la intersección N de todos los submódulos de M que contienen a S . Lo representamos por $N = A\langle S \rangle$.

Proposición 5.43. Sean N_1, N_2 submódulos de M . Entonces $N_1 + N_2$ es un submódulo de M .

Proposición 5.44. 1. Sea $S = \emptyset$. Entonces $\langle S \rangle$ es el submódulo trivial.

2. Para cualquier $S \subset M$ no vacío,

$$A\langle S \rangle = \left\{ \sum a_x x \mid a_x \in A \text{ casi todos cero, } x \in S \right\}$$

es el conjunto de todos los elementos de G que se expresan como combinaciones lineales finitas de elementos de S con coeficientes en A .

6. Anillos cocientes

Sean A un anillo e I un ideal suyo. Definimos una relación binaria en A por la regla

$$a \sim b \text{ si } a - b \in I. \quad (6.1)$$

Lema 6.1. La relación 6.1 es una relación de equivalencia.

Representamos por $\bar{a} = a + I$ a la clase de equivalencia del elemento $a \in A$. Cualquier elemento de \bar{a} se llama *representante de la clase \bar{a}* . Representamos por A/I al conjunto de todas las clases de equivalencia para la relación 6.1. En A/I definimos dos operaciones internas:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad (6.2)$$


$$\bar{a}\bar{b} = \overline{ab}. \quad (6.3)$$

Lema 6.2. Sean $\bar{a} = \overline{a_1}$ y $\bar{b} = \overline{b_1}$. Entonces $\overline{a + b} = \overline{a_1 + b_1}$ y $\overline{ab} = \overline{a_1 b_1}$.

Este lema nos dice que las operaciones 6.2 están bien definidas, es decir que son independientes de los representantes elegidos.

Proposición 6.3. El conjunto A/I junto con las operaciones 6.2 forman un anillo que se llama anillo cociente de A sobre I .

Llamamos *proyección de A sobre A/I* a la aplicación $p : A \rightarrow A/I$ dada por $p(a) = \bar{a}$.

Proposición 6.4. La proyección $p : A \rightarrow A/I$ es un epimorfismo de anillos con núcleo $\ker(p) = I$. 

Corolario 6.5. Un subconjunto $I \subset A$ es un ideal si y sólo si existe un homomorfismo de anillos $f : A \rightarrow B$ tal que $I = \ker f$.

Teorema 6.6 (Propiedad universal del anillo cociente). Sean A un anillo e I un ideal suyo. Para todo homomorfismo de anillos $f : A \rightarrow B$ tal que $\ker f \supset I$ existe un único homomorfismo de anillos $\bar{f} : A/I \rightarrow B$ tal que $\bar{f}p = f$.

Además $\text{Im } \bar{f} = \text{Im}(f)$ y $\bar{a} \in \ker(\bar{f})$ si y sólo si $a \in \ker(f)$.

Corolario 6.7. \bar{f} es un epimorfismo si y sólo si f es un epimorfismo.

\bar{f} es un monomorfismo si y sólo si $I = \ker(f)$.

Proposición 6.8 (Descomposición canónica de un homomorfismo). Todo homomorfismo de anillos $f : A \rightarrow B$ se descompone como un producto

$$A \xrightarrow{f_1} \frac{A}{\ker(f)} \xrightarrow{f_2} \text{Im}(f) \xrightarrow{f_3} B,$$

donde f_1 es un epimorfismo, f_2 es un isomorfismo y f_3 es un monomorfismo.

Corolario 6.9 (Primer teorema de isomorfismo). Para todo homomorfismo de anillos $f : A \rightarrow B$ existe un isomorfismo $A/\ker(f) \cong \text{Im}(f)$ dado por $\bar{a} \leftrightarrow f(a)$.

Teorema 6.10 (Teorema de correspondencia). Sean A un anillo e I un ideal suyo y sea $p : A \rightarrow A/I$ la proyección. Sean

$$S = \{U \mid U \text{ es un subgrupo aditivo de } A \text{ y } U \supset I\},$$

$$S_I = \{V \mid V \text{ es un subgrupo aditivo de } A/I\}.$$

1. La aplicación $U \rightarrow p(U) = U/I$ establece una biyección $S \cong S_I$.
2. En esta biyección $S \subset T$ si y sólo si $p(S) \subset p(T)$.
3. S es un subanillo de A si y sólo si $p(S)$ es un subanillo de A/I .
4. S es un ideal de A si y sólo si $p(S)$ es un ideal de A/I .

Teorema 6.11 (Segundo teorema de isomorfismo). Sea A un anillo y sean B un subanillo e I un ideal de A . Entonces:

1. $B + I = \{b + x \mid b \in B, x \in I\}$ es un subanillo de A e I es un ideal de $B + I$.
2. $B \cap I$ es un ideal de B
3. Existe un isomorfismo

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

dado por $b + B \cap I \leftrightarrow b + I$.

Teorema 6.12 (Tercer teorema de isomorfismo). Sea A un anillo y sean $I \supset J$ ideales suyos. Entonces I/J es un ideal de A/J y existe un isomorfismo

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

7. Dominios de integridad y cuerpos

Sea A un anillo conmutativo.

Definición 7.1. Un elemento $a \in A$ se llama *divisor de cero* si existe un $b \in A$, $b \neq 0$ tal que $ab = 0$.

Un *dominio de integridad* es un anillo conmutativo A no trivial sin divisores de cero no nulos.

En otras palabras, un anillo conmutativo A es un dominio de integridad si $1 \neq 0$ y si $ab = 0$ implica $a = 0$ o $b = 0$.

Proposición 7.2. Un anillo conmutativo no trivial A es un dominio de integridad si y sólo si satisface la ley cancelativa:

$$ab = ac \text{ y } a \neq 0 \text{ implica } b = c.$$

Corolario 7.3. Sea A un dominio de integridad y sea B un subanillo de A . Entonces B es un dominio de integridad.

Definición 7.4. Un cuerpo es un anillo conmutativo no trivial en el que todo elemento no nulo tiene un inverso multiplicativo. Un subcuerpo de un cuerpo F es un subanillo que es un cuerpo.

En otras palabras, el cuerpo K es un subcuerpo de F si y sólo si es un subconjunto y la aplicación de inclusión $i : K \rightarrow F$ es un homomorfismo.

Lema 7.5. Un subconjunto de un cuerpo F es un subcuerpo si y sólo si es cerrado para la suma, la multiplicación, el cero, el uno, el opuesto aditivo y el inverso multiplicativo.

Proposición 7.6. Todo cuerpo es un dominio de integridad.

Proposición 7.7. Todo dominio de integridad finito es un cuerpo.

Proposición 7.8. Un anillo conmutativo no trivial es un cuerpo si y solo si no tiene ideales propios.

Corolario 7.9. Todo homomorfismo de cuerpos $K \rightarrow F$ es inyectivo.

Definición 7.10. Sea A un anillo conmutativo. Un ideal I de A se llama *maximal* si $I \neq A$ y si para J ideal de A , $I \subset J$ implica $J = I$ o $J = A$.

Un ideal I de A se llama *primo* si $I \neq A$ y si para $a, b \in A$ $ab \in I$ implica $a \in I$ o $b \in I$.

Proposición 7.11. Sea A un anillo conmutativo y sea I un ideal suyo. El ideal I es *maximal* si y sólo si el anillo cociente A/I es un cuerpo. El ideal I es *primo* si y sólo si el anillo cociente A/I es un dominio de integridad.

Corolario 7.12. Todo ideal maximal es primo.

Definición 7.13. Un anillo de integridad o anillo íntegro es un anillo (no necesariamente conmutativo) sin divisores de cero.

Un anillo de división es un anillo (no necesariamente conmutativo) en el que todo elemento distinto de cero tiene un inverso.

Así que un dominio de integridad es lo mismo que un anillo de integridad conmutativo y un cuerpo es lo mismo que un anillo de división conmutativo. Naturalmente todo anillo de división es un anillo de integridad.

Proposición 7.14. La característica de un dominio de integridad es o cero o un número primo.

Proposición 7.15. Sea K un cuerpo. La intersección de una familia arbitrarias de subcuerpos de K es un subcuerpo de K .

Definición 7.16. Sea K un cuerpo. Se llama *subcuerpo primo* de K a la intersección de todos los subcuerpos de K .

Es decir, que el subcuerpo primo es el mínimo subcuerpo de K .

8. El cuerpo de fracciones

Sea A un dominio de integridad. Llamamos S al conjunto de elementos no nulos de A . En el conjunto producto cartesiano $S \times A$ definimos la siguiente relación binaria:

$$(s_1, a_1) \sim (s_2, a_2) \text{ si } s_1 a_2 = s_2 a_1. \quad (8.1)$$

Proposición 8.1. *La relación 8.1 es una relación de equivalencia.*

Al conjunto cociente $S \times A / \sim$ lo representamos por $Q(A)$ o por $S^{-1}A$. En este conjunto la clase De (s, a) se representa por a/s y se llama *fracción*; el elemento a es el *numerador* y s es el *denominador* de la fracción.

Definimos dos operaciones binarias $Q(A) \times Q(A) \rightarrow Q(A)$ por las reglas:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2 a_1 + s_1 a_2}{s_1 s_2}, \quad (8.2)$$

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}. \quad (8.3)$$

Proposición 8.2. *Las operaciones 8.2 y 8.3 están bien definidas (es decir, son independientes de los representantes elegidos para las fracciones).*

Proposición 8.3. *El conjunto $Q(A)$ con las operaciones 8.2 y 8.3 es un cuerpo que se llama cuerpo de fracciones del anillo A .*

Ejemplo 8.4. Cuando $A = \mathbb{Z}$, el cuerpo de fracciones es el cuerpo de los números racionales $Q(A) = \mathbb{Q}$.

Ejemplo 8.5. $Q(\sqrt{2})$ es el cuerpo de fracciones de $\mathbb{Z}[\sqrt{2}]$.

Ejemplo 8.6. $Q(\sqrt{-1}) = \{a + bi \mid a, b \in \mathbb{Q}\}$ es el cuerpo de fracciones del anillo de los enteros de Gauss $\mathbb{J} = \mathbb{Z}[i]$.

El anillo A determina unívocamente al cuerpo $Q(A)$ (salvo isomorfismos). Pero para un cuerpo K puede ocurrir que $K = Q(A) = Q(B)$ aunque A y B no sean isomorfos:

Ejemplo 8.7. Sea $B = \{a/b \in \mathbb{Q} \mid b \equiv 1 \pmod{2}\}$. Es fácil ver que $Q(B) = \mathbb{Q}$, aunque $B \neq \mathbb{Z}$.

Proposición 8.8. *La aplicación $\lambda : A \rightarrow Q(A)$ definida por $\lambda(a) = a/1$ es un monomorfismo de anillos.*

Usualmente se identifica el anillo A con la imagen del anterior monomorfismo, es decir que tomamos $a = a/1$. Con esta identificación A es un subanillo de $Q(A)$.

Lema 8.9. *Todo dominio de integridad es un subanillo de algún cuerpo.*

Este resultado es falso para anillos de integridad. Malcev ha dado ejemplos de anillos de integridad que no se pueden sumergir en un anillo de división.

Teorema 8.10. *Para todo monomorfismo $f : A \rightarrow K$ donde K es un cuerpo existe un único homomorfismo $\bar{f} : Q(A) \rightarrow K$ tal que $\bar{f}\lambda = f$. Además $\text{Im}(\bar{f}) \cong Q(A)$.*

Corolario 8.11. *Sea A un subanillo de un cuerpo K tal que todo elemento $u \in K$ se puede expresar como $u = ab^{-1}$ con $a, b \in A$. Entonces $Q(A) \cong K$.*

Proposición 8.12. *Sea K un cuerpo. Si $\text{car}(K) = 0$, el cuerpo primo de K es isomorfo a \mathbb{Q} . Si $\text{car}(K) = p$, el cuerpo primo es isomorfo a \mathbb{Z}_p .*

Índice alfabético

- álgebra, 8
 - asociativa y unitaria, 5
 - no asociativa, 8
- acción
 - por la derecha, 2
 - por la izquierda, 2
- anillo, 3
 - íntegro, 24
 - abeliano, 4
 - cociente, 22
 - conmutativo, 4, 8
 - de división, 4, 24
 - de endomorfismos, 16
 - de integridad, 24
 - enteros de Gauss, 6
 - no trivial, 6
 - opuesto, 6
 - trivial, 6
- asociatividad, 3, 4
 - de la suma, 3
 - del producto, 4
- automorfismo, 13, 15
- característica
 - de un anillo, 13
- cero, 3, 4
- codominio
 - de un homomorfismo, 13, 15
- conjunto
 - subyacente, 2
- conmutatividad, 3, 4
 - de la suma, 4
 - del producto, 4
- corchete de Lie, 8
- cuerpo, 4, 24
 - de fracciones, 25
 - de los números racionales, 25
- denominador, 25
- distributividad, 4
 - respecto a escalares, 4
 - respecto a vectores, 4
- divisor de cero, 23
- dominio
 - de integridad, 23
 - de un homomorfismo, 13, 15
- elemento
 - cero, 3
 - de orden finito, 11
 - de torsión, 11
 - neutro, 3
 - nulo, 3
- endomorfismo, 13, 15
- epimorfismo, 13, 15
- escalar, 5
- espacio
 - vectorial, 5
- estructura algebraica, 2
- evaluación, 14
- fracción, 25
- grupo, 3
 - abeliano, 3, 4
 - aditivo, 6

- conmutativo, 3
- de automorfismos, 14–16
- lineal general, 13
- multiplicativo, 6
- no trivial, 5
- opuesto, 5
- trivial, 5
- homomorfismo
 - de anillos, 14
 - de grupos, 13
 - de módulos, 15
 - unital, 14
- ideal, 19
 - generado, 20
 - impropio, 19
 - maximal, 24
 - primo, 24
 - principal, 20
 - propio, 19
- imagen
 - de un homomorfismo, 13, 15
- inverso, 3, 4
- isomorfismo, 13, 15
- ley
 - cancelativa, 24
 - de composición interna, 2
 - de composición opuesta, 2
- módulo, 4
 - derecha, 5
 - izquierda, 4
- monomorfismo, 13, 15
- núcleo
 - de un homomorfismo, 13, 15
- numerador, 25
- operación
 - binaria, 2
- opuesto, 3, 4
- orden
 - de un elemento, 11
- propiedad
 - cancelativa, 9
- proyección, 22
- pseudoasociatividad, 4, 5
- rango
 - de un homomorfismo, 13, 15
- reglas de cálculo, 9
- subanillo, 18
 - compuesto, 19
 - generado, 19
 - impropio, 18
 - primo, 18
 - propio, 18
 - total, 18
- subcuerpo, 24
 - primo, 24
- subgrupo, 16
 - compuesto, 17
 - generado, 17
 - impropio, 16
 - propio, 16
 - total, 16
 - trivial, 16
- submódulo, 20

generado, 21
impropio, 20
propio, 20
total, 20
trivial, 20

unidad, 3

uno, 3, 4

vector, 5