

Estructuras Algebraicas

NyKi

Curso de 2025-2026

Índice general

1. Introducción	5
1.1. Definiciones básicas	5
1.2. Subestructuras	9
1.3. Generadores	11
1.4. Los números enteros	12
2. Grupos	13
3. Anillos	15

Introducción

El estudio de las estructuras algebraicas comienza con una exposición básica sobre las operaciones binarias.

1.1. Definiciones básicas

Definición 1.1.1: Operación binaria

Sea S un conjunto no vacío. Se dice que una aplicación $*$: $S \times S \rightarrow S$ es una **operación binaria** (interna) sobre S .

Generalmente, se usa la notación interna: $a * b = *(a, b)$ ya que es mucho más cómoda que la típica de aplicaciones, y en el contexto que esté claro a que operación nos referimos excluirémos el símbolo: $ab = a * b$.

Una simple operación no tiene nada de interesante que no sepamos de teoría de conjuntos. La riqueza de la teoría algebraica viene de ciertos axiomas que una operación puede satisfacer:

Definición 1.1.2: Asociatividad

Sea $S \neq \emptyset$. Una operación binaria $*$ sobre S se dice **asociativa** si se cumple $(a * b) * c = a * (b * c)$ para todo $a, b, c \in S$.

Este primer axioma es lo más básico que podemos imponer a una operación binaria. Intuitivamente, la asociatividad permite definir sin ambigüedad los productos de una cantidad finita de elementos bajo la operación $*$. Por ejemplo, al escribir $a * b * c * d$ podemos referirnos a cualquiera de las siguientes formas de poner paréntesis a la operación: $((a * b) * c) * d$, $(a * b) * (c * d)$, $((a * (b * c)) * d)$, $(a * (b * (c * d)))$, ... pero bajo la hipótesis de asociatividad todas estas son iguales y por tanto podemos referirnos a cada una de ellas simplemente con $a * b * c * d$. Antes de dar ejemplos vamos a nombrar nuestra primera estructura algebraica.

Definición 1.1.3: Semigrupo

Sea S un conjunto no vacío y $*$ una operación binaria interna sobre S . La tupla $(S, *)$ se dice **semigrupo** si la operación $*$ es asociativa.

Generalmente, una estructura algebraica consiste de uno o varios conjuntos con una o varias operaciones binarias que pueden ser internas o no. El semigrupo es la más simple que vamos a nombrar.

Ejemplo 1.1.1. La operación interna de suma $+$ sobre los números naturales, enteros, racionales, reales o complejos es una operación asociativa. El producto $*$ también es asociativo sobre

cualquiera de estos.

Ejemplo 1.1.2. Para cada dos vectores del espacio \mathbb{R}^3 podemos definir su **producto vectorial**. Esto es un ejemplo de operación no asociativa.

Ejemplo 1.1.3. Sea S un conjunto no vacío. Tomamos el conjunto de todas las aplicaciones $f : S \rightarrow S$ de S en S , y lo denotamos por $\text{Apl}(S)$. Sobre este conjunto, la operación de composición de aplicaciones \circ es una operación interna asociativa. Es decir, $(\text{Apl}(S), \circ)$ es un semigrupo.

Las estructuras no asociativas son interesantes pero no son nuestro objetivo. Mayoritariamente todas las estructuras que vamos a estudiar son asociativas.

Definición 1.1.4: Conmutatividad

Sea $S \neq \emptyset$. Una aplicación binaria $*$ sobre S se dice **conmutativa** si se cumple $a*b = b*a$ para todo $a, b \in S$.

Este es una convención que usaremos mucho: cuando la operación de una estructura algebraica sea conmutativa añadiremos el adjetivo **abeliano** a la estructura algebraica.

Ejemplo 1.1.4. Los semigrupos $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son semigrupos abelianos.

Ejemplo 1.1.5. La estructura $(\mathcal{M}_n(\mathbb{R}), *)$, donde $\mathcal{M}_n(\mathbb{R})$ es el conjunto de matrices cuadradas con entradas reales de orden n y $*$ es la multiplicación de matrices es un semigrupo no abeliano.

Definición 1.1.5: Elemento neutro

Sea $S \neq \emptyset$ y $*$ una aplicación binaria sobre S .

- A un elemento $e_L \in S$ tal que $e_L * a = a$ para todo $a \in S$ se le conoce como **elemento neutro por la izquierda** de $*$.
- A un elemento $e_R \in S$ tal que $a * e_R = a$ para todo $a \in S$ se le conoce como **elemento neutro por la derecha** de $*$.
- A un elemento $e \in S$ tal que $e * a = a * e = a$ para todo $a \in S$ se le conoce como **elemento neutro o identidad** de $*$.

Teorema 1.1.1. Sea $(S, *)$ un semigrupo. Si S posee un elemento neutro, entonces este es único.

DEMOSTRACIÓN. Sean $e_1, e_2 \in S$ dos elementos neutros. Entonces:

$$e_1 = e_1 * e_2 = e_2.$$

Nota 1.1.1. Existen muchas notaciones distintas para operaciones binarias. Generalmente, se suele usar $*$, \cdot o se excluye el símbolo cuando la operación no es conmutativa, y en tal caso el elemento neutro único de un semigrupo $(S, *)$ se denota por 1_S o por 1 . Esta notación recibe el nombre de **notación multiplicativa** (por la multiplicación de matrices, ya que no es conmutativa). Otros símbolos para esta notación pueden ser \otimes , \odot , \star , etc... Si la operación es conmutativa, se usa la **notación aditiva**, con símbolos como $+$, \oplus , etc... , y representando el elemento neutro con 0 . Esto solo se hace por comodidad y tradición. En un contexto más general, e_S representará el elemento neutro de $(S, *)$ si se tiene clara la operación que se está usando.

Teorema 1.1.2. Sea $(S, *)$ un semigrupo. Si S posee al menos un elemento neutro por la izquierda e_L y un elemento neutro por la derecha e_R entonces $e_L = e_R$ y por tanto S

contiene un elemento neutro.

DEMOSTRACIÓN. Sea e_L elemento neutro por la izquierda y e_R elemento neutro por la derecha. Entonces:

$$e_L = e_L * e_R = e_R.$$

Definición 1.1.6: Monoide

Un semigrupo $(S, *)$ que contiene elemento neutro se conoce como **monoide**.

Ejemplo 1.1.6. $(\mathcal{M}_n(\mathbb{R}), *)$ es un monoide, con elemento neutro la matriz identidad de orden n .

Definición 1.1.7: Inversos

Sea $(M, *)$ un monoide, sea $e \in M$ su elemento neutro y sea $a \in M$.

- Si existe un b tal que $a * b = e$ entonces se dice que a es **invertible por la derecha** y que b es su **inverso por la derecha**.
- Si existe un b tal que $b * a = e$ entonces se dice que a es **invertible por la izquierda** y que b es su **inverso por la izquierda**.
- Si existe un b tal que $a * b = b * a = e$ entonces se dice que a es **invertible** y que b es su **inverso** que denotaremos por $b = a^{-1}$.

Teorema 1.1.3. Sea $(M, *)$ un monoide. Si $a \in M$ es invertible entonces su inversa es única.

DEMOSTRACIÓN. Sea $a \in M$, y sean $b, c \in M$ dos elementos que sean inversa de a . Entonces:

$$ab = e \Rightarrow cab = ce = c \Rightarrow eb = c \Rightarrow b = c.$$

Esto justifica la notación $b = a^{-1}$.

Teorema 1.1.4. Sea $(M, *)$ un monoide. Se cumple, para todo $a, b \in M$ invertibles:

1. a^{-1} es invertible y $(a^{-1})^{-1} = a$.
2. ab es invertible y $(ab)^{-1} = b^{-1}a^{-1}$.

Teorema 1.1.5. Sea $(M, *)$ un monoide, y sea $a \in M$.

- Si a es invertible por la derecha entonces $xa = b$ tiene una única solución para cada $b \in M$.
- Si a es invertible por la izquierda entonces $ax = b$ tiene una única solución para cada $b \in M$.

Teorema 1.1.6. Sea $(M, *)$ un monoide abeliano. Si $a \in M$ es invertible por la izquierda (derecha) con inversa por la izquierda (derecha) $b \in M$ entonces es también invertible por la derecha (izquierda) y b es también su inverso por la derecha (izquierda).

Definición 1.1.8: Unidades

Sea $(M, *)$ un monoide. Definimos su **conjunto de unidades** $U(M)$ como el conjunto de todos los elementos invertibles de M .

Definición 1.1.9: Grupo

Sea $(G, *)$ un monoide. Decimos que $(G, *)$ es un **grupo** si y solo si $G = U(G)$ (es decir, $(G, *)$ es un monoide en el que todo elemento es invertible).

Ejemplo 1.1.7. Un ejemplo de grupo muy importante es el grupo simétrico sobre n elementos. Dado un conjunto no vacío S , consideramos el conjunto de aplicaciones biyectivas $f : S \rightarrow S$, que denotamos por $\text{Bij}(S)$. Esto es un grupo bajo la composición de aplicaciones (la composición es asociativa, la aplicación identidad $i : S \rightarrow S$ dada por $i(k) = k$ para todo $k \in S$ actúa como elemento neutro y cada aplicación tiene inversa biyectiva por ser biyectiva) para todo conjunto S . En concreto, para $S = \{1, 2, \dots, n\}$ con $n \in \mathbb{N}$ mayor que 0, llamaremos a este conjunto **grupo simétrico** sobre n elementos, que denotaremos por \mathcal{S}_n , y a cada elemento de este grupo lo llamaremos **permutación**.

Definición 1.1.10: Anillo y cuerpo

Sea $S \neq \emptyset$ y $+, *$ dos operaciones binarias sobre S . Decimos que $(S, +, *)$ es un **anillo** si se cumplen las siguientes condiciones:

1. $(S, +)$ es un grupo.
2. $(S, *)$ es un monoide.
3. Se cumplen las propiedades distributivas: para todo $a, b, c \in S$:
 - $a * (b + c) = a * b + a * c$.
 - $(b + c) * a = b * a + c * a$.

Si además se cumple que $(S, *)$ es abeliano $(S, +, *)$ se denomina **anillo conmutativo**, y si además de esto $(S \setminus \{0\}, *)$ es un grupo, $(S, +, *)$ es un **cuerpo**.

Definición 1.1.11: Espacio vectorial y módulo

Sea $(K, +, *)$ un cuerpo, E un conjunto no vacío, \oplus una operación interna sobre E y $\cdot : K \times E \rightarrow E$ una aplicación, llamada **multiplicación por un escalar**. Decimos que (E, \oplus) es un **espacio vectorial** sobre K (al que llamamos **cuerpo de escalares**) si se cumplen:

1. (E, \oplus) es un grupo abeliano.
2. $(\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x)$ para todo $\alpha, \beta \in K$ y $x \in E$.
3. $(\alpha + \beta) \cdot x = \alpha \cdot x \oplus \beta \cdot x$ para todo $\alpha, \beta \in K$ y $x \in E$.
4. $\alpha \cdot (x \oplus y) = \alpha \cdot x \oplus \alpha \cdot y$ para todo $\alpha \in K$ y $x, y \in E$.
5. $1 \cdot x = x$ para 1 la identidad multiplicativa de K y cualquier $x \in E$.

Si en vez de ser $(K, +, *)$ un cuerpo es un anillo, (E, \oplus) se conoce como un **módulo** sobre K .

Generalmente la multiplicación por un escalar y la multiplicación del cuerpo se representan de la misma manera por omisión del símbolo multiplicativo, y la suma de ambos usa el mismo símbolo.

Definición 1.1.12: Álgebra

Sea $(K, +, *)$ un cuerpo. E un conjunto no vacío, \oplus y \otimes dos operaciones internas sobre E y $\cdot : K \times E \rightarrow E$ una aplicación, llamada **multiplicación por un escalar**. Decimos que (E, \oplus, \otimes) es un **álgebra** sobre K si se cumplen:

1. (E, \oplus) es un espacio vectorial con la multiplicación \cdot .
2. (E, \oplus, \otimes) es un anillo.
3. $\alpha(xy) = (\alpha x)y = x(\alpha y)$ para todo $\alpha \in K$ y $x, y \in E$.

Definición 1.1.13: Conjunto cerrado

Sea S no vacío y $*$ una operación binaria interna sobre S . Decimos que un subconjunto $T \subseteq S$ es **cerrado** bajo $*$ si y solo si

$$ab \in T \quad \forall a, b \in T.$$

Teorema 1.1.7. Sea S no vacío, $*$ una operación binaria interna sobre S y T un conjunto no vacío cerrado bajo $*$. Entonces la imagen de la restricción de $*$ a $T \times T$ está contenida en T . Es decir, se puede restringir el codominio de $*|_{T \times T}$ a T .

DEMOSTRACIÓN. Sea $a \in S$ un elemento de la imagen de $*|_{T \times T}$. Esto significa que $\exists x, y \in T$ tales que $xy = a$. Pero como T es cerrado bajo $*$ se tiene $a = xy \in T$.

1.2. Subestructuras

Definición 1.2.1: Subsemigrupo

Sea $(S, *)$ un semigrupo y $T \subseteq S$ no vacío. Decimos que $(T, *|_{T \times T})$ es un **subsemigrupo** de S si $(T, *|_{T \times T})$ es un semigrupo.

Generalmente, representaremos la operación de la subestructura mediante el mismo símbolo de la operación de la estructura mayor. En la definición es necesario que la operación esté restringida a $T \times T$ solo para ser coherente con la definición de semigrupo (la operación tiene que ser interna). Solo vamos a hacer eso en las definiciones siguientes, y después de eso haremos abuso de notación entendiendo $*$ como $*|_{T \times T}$.

Junto a las definiciones, tendremos unos teoremas más o menos directos que ayudan a la hora de demostrar que algo es una subestructura.

Teorema 1.2.1. Sea $(S, *)$ un semigrupo y $T \subseteq S$ no vacío. Entonces $(T, *)$ es un subsemigrupo si y solo si T es cerrado bajo $*$.

DEMOSTRACIÓN. La implicación directa se cumple por la definición de operación binaria interna. Veamos la implicación contraria. Como T es cerrado bajo $*$, podemos definir $*|_{T \times T} : T \times T \rightarrow T$ por el teorema (1.1.7) y por tanto $*|_{T \times T}$ es operación interna sobre T . Para ver que es asociativa, simplemente vemos que para todo $a, b, c \in T$ tenemos:

$$(a * |_{T \times T} b) * |_{T \times T} c = (a * b) * c = a * (b * c) = a * |_{T \times T} (b * |_{T \times T} c).$$

Ejemplo 1.2.1. Dado un conjunto S no vacío, el grupo $(\text{Biy}(S), \circ)$ del ejemplo (1.1.7) es un subsemigrupo de $(\text{Apl}(S), \circ)$, ya que la composición de dos aplicaciones biyectivas es biyectiva, y el dominio y codominio de cada una es S .

Definición 1.2.2: Submonoide

Sea $(M, *)$ un monoide y $N \subseteq M$ no vacío. Decimos que $(N, *|_{N \times N})$ es un **submonoide** de M si $(N, *|_{N \times N})$ es un monoide y la identidad de $(M, *)$ pertenece a N .

Es importante que la identidad de $(M, *)$ pertenezca al submonoide, ya que $(N, *|_{N \times N})$ puede ser monoide con otro elemento neutro, como en el siguiente ejemplo.

Ejemplo 1.2.2. Consideramos el siguiente subconjunto de $\mathcal{M}_n(\mathbb{R})$

$$A = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\}$$

bajo la multiplicación de matrices. Se puede comprobar que esto es un monoide, con identidad

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

pero esta identidad es diferente a la del monoide $(\mathcal{M}_n(\mathbb{R}), *)$ y por tanto $(A, *)$ no es un submonoide de $\mathcal{M}_n(\mathbb{R})$. Aun así, sí que es un subsemigrupo.

Al igual que para los semigrupos, tenemos el siguiente teorema:

Teorema 1.2.2. Sea $(M, *)$ un monoide y $N \subseteq M$ no vacío. Entonces $(N, *)$ es un submonoide si y solo si se cumplen:

1. N es cerrado bajo $*$.
2. N contiene el elemento neutro de M .

Definición 1.2.3: Subgrupo

Sea $(G, *)$ un grupo y $H \subseteq G$ no vacío. Decimos que $(H, *|_{H \times H})$ es un **subgrupo** de G si $(H, *|_{H \times H})$ es un grupo.

Teorema 1.2.3. Sea $(G, *)$ un grupo y $H \subseteq G$ no vacío. Son equivalentes:

1. $(H, *)$ es un subgrupo.
2. H es cerrado bajo $*$ y para todo $x \in H$ se tiene $x^{-1} \in H$.
3. Para todo $x, y \in H$ se tiene $xy^{-1} \in H$.

Definición 1.2.4: Subanillo

Sea $(R, +, *)$ un anillo y $S \subseteq R$ no vacío. Decimos que $(S, +|_{S \times S}, *|_{S \times S})$ es un **subanillo** de R si $(S, +|_{S \times S}, *|_{S \times S})$ es un anillo y la identidad multiplicativa de R está en S .

Teorema 1.2.4. Sea $(R, +, *)$ un anillo y $S \subseteq R$ no vacío. Entonces $(R, +, *)$ es un subanillo si y solo si se cumplen:

1. Para todo $x, y \in S$ se tiene $x - y \in S$.
2. S es cerrado bajo $*$.
3. S contiene el elemento neutro (multiplicativo) de R .

Definición 1.2.5: Subcuerpo

Sea $(R, +, *)$ un cuerpo y $S \subseteq R$ no vacío. Decimos que $(S, +|_{S \times S}, *|_{S \times S})$ es un **subcuerpo** de R si $(S, +|_{S \times S}, *|_{S \times S})$ es un cuerpo. Además, diremos que R es una **extensión** de S .

Teorema 1.2.5. Sea $(K, +, *)$ un cuerpo y $L \subseteq K$ no vacío. Entonces $(L, +, *)$ es un subcuerpo si y solo si se cumplen:

1. Para todo $x, y \in L$ se tiene $x - y \in L$ (es decir, $(L, +)$ es un subgrupo de $(K, +)$).
2. Para todo $x, y \in L \setminus \{0\}$ se tiene $xy^{-1} \in L$ (es decir, $(L \setminus \{0\}, *)$ es un subgrupo de $(K \setminus \{0\}, *)$).

Definición 1.2.6: Subespacio vectorial

Sea K un cuerpo, $(E, +)$ un espacio vectorial sobre K y $V \subseteq E$ no vacío. Decimos que $(V, +|_{V \times V})$ es un **subespacio vectorial** de E si $(V, +|_{V \times V})$ es un espacio vectorial sobre K .

Definición 1.2.7: Subálgebra

Sea K un cuerpo, $(A, +, *)$ un álgebra sobre K y $B \subseteq A$ no vacío. Decimos que $(B, +|_{B \times B}, *|_{B \times B})$ es un **subálgebra** de A si $(B, +|_{B \times B}, *|_{B \times B})$ es un álgebra sobre K y la identidad multiplicativa del anillo $(A, +, *)$ está en B .

1.3. Generadores

TODO: this is draconian no way i'm putting this here

Teorema 1.3.1. Sea $(S, *)$ un semigrupo y $X \subseteq S$ no vacío. Definimos el conjunto

$$\langle X \rangle = \bigcap \{T : T \text{ es subsemigrupo de } S\}.$$

Se cumple:

1. $\langle X \rangle$ es un subsemigrupo de S .

1.4. Los números enteros

Definición 1.4.1: Divisibilidad

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$. Decimos que a **divide** a b (o que b es múltiplo de a) si existe $m \in \mathbb{Z}$ tal que $b = am$, y lo denotamos por $a|b$.

Teorema 1.4.1 (Algoritmo de división). Sean $a, b \in \mathbb{Z}$ con $b > 0$. Entonces existe una única pareja $q, r \in \mathbb{Z}$ tales que

$$a = bq + r$$

con $0 \leq r < b$.

Teorema 1.4.2. Los subgrupos de $(\mathbb{Z}, +)$ son exactamente los conjuntos de la forma $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\} = \langle m \rangle$ con $m \in \mathbb{Z}$.

Teorema 1.4.3. Sean $a, b \in \mathbb{Z}$ con $a \neq 0$. Entonces $a|b$ si y solo si $b\mathbb{Z} \subseteq a\mathbb{Z}$.

Definición 1.4.2: Máximo común divisor

Sean $a, b \in \mathbb{Z}$ no todos nulos. Decimos que $d \in \mathbb{Z}$ es un **máximo común divisor** de a y b si se cumplen:

1. $d|a$ y $d|b$.
2. Si $d'|a$ y $d'|b$ entonces $d'|d$.
3. $d \geq 1$.

Teorema 1.4.4. Si $a, b \in \mathbb{Z}$ no todos nulos entonces existe un único máximo común divisor, que denotamos por $d = \text{mcd}(a, b)$.

Teorema 1.4.5. Si $a, b \in \mathbb{Z}$ no todos nulos entonces existen $n, m \in \mathbb{Z}$ tales que $\text{mcd}(a, b) = na + mb$. Además, si existen $u, v \in \mathbb{Z}$ tales que $1 = ua + vb$ entonces $\text{mcd}(a, b) = 1$.

Definición 1.4.3: Coprimos

Dos números $a, b \in \mathbb{Z}$ no todos nulos se dicen **coprimos** si $\text{mcd}(a, b) = 1$.

Grupos

Anillos
