Estructuras algebraicas

Natalia Boal
María Luisa Sein-Echaluce
Universidad de Zaragoza

1 Relaciones binarias

1.1 Recordatorio

Definición. Dados dos conjuntos A y B se llama *producto cartesiano de A por B* al conjunto

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

En particular, puede definirse el producto cartesiano de un conjunto por sí mismo. Así, dado un conjunto A se puede definir

$$A \times A = \{ (a_1,a_2) \,|\, a_1 \in A \,, a_2 \in A \}.$$

Observaciones.

- $(a_1,a_2) \neq (a_2,a_1)$.
- En general, dados n conjuntos $A_1, \ldots, A_n$ se define *producto cartesiano*

  $$A_1 \times \cdots \times A_n = \{ (a_1, \ldots, a_n) \,|\, a_i \in A_i, \ \forall i \}.$$

  Los elementos $(a_1, \ldots, a_n)$ se dicen *$n-$tuplas.*

1.2 Relaciones de orden

Definición. Dado un conjunto A se llama *relación de orden* a toda relación binaria $\mathcal{R}$, definida sobre A que satisface las propiedades:

1. *Reflexiva* : $a \mathcal{R} a \ \ \forall a \in A$
2. *Antisimétrica* : $a \mathcal{R} b \ \wedge \ b \mathcal{R} a \Rightarrow a = b$
3. *Transitiva* : $a \mathcal{R} b \ \wedge \ b \mathcal{R} c \Rightarrow a \mathcal{R} c$

Definición. Dado un conjunto A, una relación $\mathcal{R}$ de orden definida sobre A es un *orden total* si

$$\forall (a_1,a_2) \in A \times A, \qquad a_1 \mathcal{R} a_2 \ \vee \ a_2 R a_1.$$

En caso contrario se trata de un *orden parcial.*

1.3 Relaciones de equivalencia

Definición. Dado un conjunto A, se llama *relación de equivalencia sobre* A a toda relación binaria $\mathcal{R}$ verificando las propiedades:

1. *Reflexiva* : $a \mathcal{R} a, \ \forall a \in A$.
2. *Simétrica* : $a \mathcal{R} b \ \Rightarrow \ b \mathcal{R} a$.
3. *Transitiva* : $a \mathcal{R} b \ \wedge \ b \mathcal{R} c \Rightarrow a \mathcal{R} c$.

Definición. Sea un conjunto A y $\mathcal{R}$ una relación de equivalencia definida sobre él. Para todo elemento $a \in A$ se define la *clase de equivalencia de* a como el conjunto

$$[\, a \,] = \{\, b \in A \,/\, a \mathcal{R} b \,\}.$$

Propiedades.

- La clase de equivalencia de un elemento está formada por todos los elementos del conjunto que están relacionados con él y, por tanto, es independiente del elemento escogido para representarla. Así, $a \mathcal{R} b \ \Leftrightarrow \ [\, a \,] = [\, b \,]$.
- Las clases de equivalencia son subconjuntos no vacíos de modo que cada elemento del conjunto A pertenece a una sola clase de equivalencia.
- Se dice que la relación $\mathcal{R}$ establece una *partición* del conjunto A en clases de equivalencia.

Definición. El conjunto formado por las clases de equivalencia definidas en A por $\mathcal{R}$ se llama *conjunto cociente* y se representa por $A/\mathcal{R}$.

2 Grupos

2.1 Definiciones y propiedades

Definición. Sea G un conjunto no vacío y $*$ una operación binaria interna definida en G que verifica las propiedades:

1. Asociativa: $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3, \quad \forall g_1, g_2, g_3 \in G$.
2. Elemento neutro: existe $e \in G$ tal que $g * e = e * g, \quad \forall g \in G$.
3. Elemento simétrico: para cada $g \in G$ existe $g' \in G$ tal que $g * g' = g' * g = e$.

Al par $(G, *)$ se llama *grupo.* Si además se verifica la *propiedad conmutativa*

$$g_1 * g_2 = g_2 * g_1, \quad \forall g_1, g_2 \in G$$

se dice que $(G, *)$ es un *grupo conmutativo o abeliano.*

Propiedades. Sea $(G, *)$ un grupo, entonces

- $(g_1 * g_2)' = g_2' * g_1', \quad \forall g_1, g_2 \in G.$
- $(g')' = g, \quad \forall g \in G.$
- Dados $g, f \in G$, las ecuaciones

  $$g * x = f, \qquad y * g = f$$

  siempre tienen solución única $x = g' * f,\ y = f * g'$. Además, si $(G, *)$ es abeliano $x = y$.

Notación. Tratando de simplificar utilizaremos la notación multiplicativa y nos referiremos al grupo $(G, *)$ simplemente por G.

1. $g * f$ se transforma en gf,
2. e se transforma es 1,
3. g' se transforma en g^{-1}, (elemento simétrico o inverso de g),
4. $g^m = gg^{m-1},\ m \geq 2$,
5. $g^{-m} = g^{-1}g^{-(m-1)},\ m \geq 2$,
6. convenio $g^0 = 1$,
7. $g^m g^n = g^{m+n},\ m, n \in \mathbb{Z}$,
8. $(g^m)^n = g^{mn},\ m, n \in \mathbb{Z}$

Definición. Se dice que un grupo es *finito* si tiene un número finito de elementos. En caso contrario se dice *infinito.*

Definición. Sea G un grupo finito llamaremos *orden de* G y lo denotaremos por $|G|$ al número de elementos del G.

Sean $\{g_1, \ldots, g_n\}$ los distintos elementos de un grupo finito G. El resultado de multiplicar g_i con g_j para $1 \leq i, j \leq n$ se puede disponer convenientemente en forma de tabla

$\cdot$	g_1	g_2	$\cdots$	g_n
g_1	g_1g_1	g_1g_2	$\cdots$	g_1g_n
g_2	g_2g_1	g_2g_2	$\cdots$	g_2g_n
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g_n	g_ng_1	g_ng_2	$\cdots$	g_ng_n

Si G es abeliano la tabla del grupo es simétrica.

Definición. Si g es un elemento de un grupo finito G, llamaremos *orden de* g al menor entero positivo n tal que $g^n = 1$. Si G tiene orden infinito se define el orden de g de la misma manera, siempre que exista; en caso contrario se dice que g tiene orden infinito.

Proposición. Sea G un grupo finito y $g \in G$ de orden n. Entonces $g^s = 1$ si y sólo si s es un múltiplo de n.

2.2 Homomorfismos de grupos

Definición. Sean G y G' dos grupos. Una aplicación $f : G \longrightarrow G'$ es un *homomorfismo de grupos* si para todo $g_1, g_2 \in G$ se cumple

$$f(g_1 g_2) = f(g_1)\, f(g_2).$$

Observación. Cuando escribimos $g_1 g_2$ tenemos que tener claro que estamos "multiplicando" con la operación definida en G que le confiere el carácter de grupo. Análogamente, al hacer $f(g_1)\, f(g_2)$ "multiplicamos" con la operación definida en G'.

Propiedades. Sea $f : G \longrightarrow G'$ un homomorfismo de grupos.

- Sean 1_G y $1_{G'}$ los elementos neutros de G y G' respectivamente. Entonces, $f(1_G) = 1_{G'}$.
- Para todo $g \in G$ se tiene
$$(f(g))^{-1} = f(g^{-1}).$$
- Sean G'' un grupo y $f : G' \longrightarrow G''$ un homomorfismo de grupos. Entonces
$$(h \circ f) : G \to G''$$
un homomorfismo de grupos.

Definición. Sea $f : G \longrightarrow G'$ un homomorfismo de grupos. Se define el *núcleo de un homomorfismo* como el conjunto

$$\text{Ker } f = \{\, g \in G \,/\, f(g) = 1_{G'} \,\}$$

y el *conjunto imagen*

$$\text{Im } f = \{\, g' \in G' \,/\, \text{existe } g \in G \text{ tal que } f(g) = g' \,\}.$$

Proposición. Sea $f : G \longrightarrow G'$ un homomorfismo de grupos. Entonces

1. f es inyectiva $\iff$ Ker $f = \{1_G\}$.
2. f es suprayectiva $\iff$ Im $f = G'$.

Definición. Un *isomorfismo* es un homomorfismo de grupos $f : G \longrightarrow G'$ biyectivo. Escribiremos $G \cong G'$.

2.3 Subgrupos. Clases laterales

Definición. Sea $(G, \cdot)$ un grupo, se llama *subgrupo de* G a todo subconjunto de G no vacío, S, tal que

a) para todo $g_1, g_2 \in S$, $g_1 g_2 \in S$,

b) $(S, \cdot)$ es un grupo.

Observación. Si S es un subgrupo de G se tiene que $1_G \in S$ y además si $g \in S$ entonces $g^{-1} \in S$.

Caracterización de subgrupo. $(S, \cdot)$ es un subgrupo de $(G, \cdot)$ si y sólo si

a) $\emptyset \neq S \subseteq G$,

b) para todo $g_1, g_2 \in S$, $g_1 g_2^{-1} \in S$.

Si S es un subgrupo de G se puede definir la relación en G

$$g_1 \,\mathcal{R}_d\, g_2 \iff g_1 g_2^{-1} \in S, \qquad g_1, g_2 \in G.$$

La relación $\mathcal{R}_d$ es de equivalencia y permite establecer una partición en el conjunto G.

Definición. Dado $g \in G$ el conjunto

$$Sg = \{\, g_1 \in G \,/\, g_1 = sg,\ s \in S\}$$

se dice *clase (lateral) por la derecha de* S *respecto de* g.

Observación. Se tiene que

$$Sg = \{\, g_1 \in G \,/\, g_1 \mathcal{R}_d\, g\}$$

luego Sg es la clase de equivalencia del elemento g considerando la relación $\mathcal{R}_d$.

Sea S un subgrupo finito de y $\{s_1, \ldots, s_m\}$ los distintos elementos de S. Los distintos elementos de la clase lateral Sg son

$$s_1 g,\ s_2 g,\ \ldots,\ s_m g$$

luego, el número de elementos de Sg es m, esto es, $|S|$ (el orden de S).

Proposición. Sean S un subgrupo de G y g_1, $g_2 \in G$. Las clases laterales por la derecha Sg_1 y Sg_2 o bien son idénticas o bien no tienen ningún elemento en común.

De forma análoga, podemos definir en G la relación de equivalencia

$$g_1 \,\mathcal{R}_i\, g_2 \iff g_2^{-1} g_1 \in S, \qquad g_1, g_2 \in G.$$

Definición. Dado $g \in G$ el conjunto

$$gS = \{\, g_1 \in G \,/\, g_1 = gs,\ s \in S\}$$

se dice *clase (lateral) por la izquierda de S respecto de g*. Este conjunto gS es la clase equivalencia del elemento g considerando la relación $\mathcal{R}_i$.

Observación. En general, dado $g \in G$, $gS \neq Sg$. Sin embargo, si S es finito todas las clases laterales (por la derecha o por la izquierda) tienen es el mismo número de elementos y es exactamente $|S|$.

Teorema de Lagrange. Sea G un grupo finito. El orden de un subgrupo divide al orden del grupo.

Corolario. Sea G un grupo finito. El orden de cualquier elemento divide al orden del grupo.

Definición. Sean G un grupo finito y S un subgrupo de G. Se llama *índice de S en G* y se escribe $|G : S|$ al cociente$|G|/|S|$.

Definición. Un subgrupo S de G se dice *normal* si para todo $s \in S$ y para todo $g \in G$ se verifica $g^{-1}sg \in S$.

Caracterización de subgrupo normal. Sea S un subgrupo de G. Entonces S es normal si y sólo si $gS = Sg$ para todo $g \in G$.

Observaciones.

- Los subgrupos $\{1\}$ y G son trivialmente normales.
- En el caso particular de G grupo conmutativo, se tiene que todo subgrupo es normal.
- Si S es un subgrupo normal las clases laterales por la derecha y por la izquierda coinciden. Por tanto, las relaciones de equivalencia $\mathcal{R}_d$ y $\mathcal{R}_d$ generan la misma partición de G y el mismo conjunto cociente que denotaremos por G/S.

Definición. El conjunto cociente G/S con la operación binaria

$$[g_1]\,[g_2] = [g_1 g_2]$$

(producto de clases de equivalencia) es un grupo y se dice *grupo cociente.*

2.4 Grupos cíclicos

Definición. Un grupo G se llama *cíclico* si está generado por un solo elemento g (que se dice *generador de G*). Escribiremos $G = \langle g \rangle$.

Observaciones

- $\langle g \rangle$ sólo contiene a $1, g, g^{-1}$ y las potencias de éstos. Por tanto, si G es cíclico

  $$G = \{\, g^n \,/\, n \in \mathbb{Z}\}$$

  donde por convenio se tiene que $g^0 = 1,\ g^{-n} = (g^{-1})^n$.

- Todo grupo cíclico es abeliano.
- Todo subgrupo de un grupo cíclico es también cíclico.
- Si G tiene orden infinito, $g^n = 1$ sólo si $n = 0$.

2.5 Grupos simétrico

Definición. Sea $A = \{a_1, \ldots, a_n\}$ un conjunto con n elementos. Una *permutación* de A es una aplicación biyectiva $\sigma : A \to A$.

Denotamos por S_A el conjunto de todas las permutaciones de A. Como la composición de permutaciones es también una permutación y además se cumplen las propiedades:

- asociativa: $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$ para toda permutación $\sigma_1, \sigma_2, \sigma_3$
- elemento neutro: existe I_d (la permutación identidad) tal que $\sigma \circ I_d = I_g \circ \sigma = \sigma$
- elemento inverso: como σ es biyectiva existe σ^{-1} y $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = I_d$

se verifica que $(S_A, \circ)$ es un grupo y se dice *grupo simétrico de A.*

Para simplificar, consideraremos $A = \{1, 2, \ldots, n\}$. Denotaremos por S_n al conjunto de permutaciones de $\{1, 2, \ldots, n\}$ y $\sigma \circ \tau$ lo escribiremos como $\sigma\tau$. Se tiene que $S_A \cong S_n$.

Definición. $(S_n, \circ)$ se dice *grupo simétrico de grado n.*

Una permutación concreta $\sigma \in S_n$ queda determinada especificando las imágenes de los elementos: $1, 2, \ldots, n$

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Observaciones

- Orden de S_n : $|S_n| = n!$
- El grupo simétrico de grado 2, $S_2 = \{I_d, \sigma\}$ con

  $$\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

  es conmutativo.
- S_n con $n \geq 3$ no es conmutativo. Para comprobarlo, consideramos las permutaciones

  $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 3 & 2 & 4 & \ldots & n \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 3 & 2 & 1 & 4 & \ldots & n \end{pmatrix}.$$

  Se tiene que

  $$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 3 & 1 & 4 & \ldots & n \end{pmatrix} \neq \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 3 & 1 & 2 & 4 & \ldots & n \end{pmatrix}.$$

Definición. Un elemento j se denomina *fijo* por una permutación $\sigma \in S_n$ si $\sigma(j) = j$.

Definición. Se dice que una permutación $\sigma \in S_n$ es un *ciclo de orden* k o $k-$*ciclo* dado por $i_1, i_2, \ldots, i_k$, con i_j distintos, si

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \ldots,\ \sigma(i_{k-1}) = i_k,\ \sigma(i_k) = i_1,$$

y deja fijos el resto de elementos. Escribiremos $\sigma = (i_1\ i_2\ \ldots\ i_k)$.

Definición. Se dice que dos ciclos de S_n $(i_1\ i_2\ \ldots\ i_k)$ y $(j_1\ j_2\ \ldots\ j_\ell)$ son *disjuntos* si actúan sobre elementos distintos.

Proposición. Toda permutación $\sigma \in S_n$ con $\sigma \neq I_d$ se puede escribir como producto de ciclos disjuntos.

Observación. Los ciclos disjuntos conmutan y, salvo reordenación, la descomposición de toda permutación como producto de ciclos disjuntos es única.

Proposición. Sea $\sigma \in S_n$ dada por $\sigma = \tau_1\tau_2 \ldots \tau_m$ con τ_i ciclos disjuntos de órdenes k_i, entonces

$$\text{orden } \sigma = \text{m.c.m } (k_1,\ k_2,\ \ldots,\ k_m).$$

Definición. Una *trasposición* es un ciclo de orden 2.

Proposición. Todo ciclo se puede expresar como producto de trasposiciones (no necesariamente disjuntas).

Observación. La descomposición de un ciclo $\tau = (i_1\ i_2\ \ldots\ i_k)$ como producto de trasposiciones no es única. Por ejemplo, τ admite, al menos, las descomposiciones

$$\begin{aligned} \tau &= (i_1\ i_2)\,(i_2\ i_3)\ldots(i_{k-1}\ i_k), \\ \tau &= (i_1\ i_k)\,(i_1\ i_{k-1})\ldots(i_1\ i_2). \end{aligned}$$

Proposición. Si la permutación σ admite las descomposiciones como producto de trasposiciones $\sigma = \alpha_p \ldots \alpha_2\alpha_1 = \beta_q \ldots \beta_2\beta_1$, entonces p y q tienen la misma paridad.

Definición. Una permutación $\sigma \in S_n$ se dice *par* si se descompone en un número par de trasposiciones. Si el número de trasposiciones en el que se descompone es impar se dice *impar.*

Observación. La identidad es una permutación par.

Definición. Se define la *aplicación signo* $\text{sgn} : S_n \to \{+1, -1\}$ tal que

$$\begin{aligned} \text{sgn}\,(\sigma) &= +1, \quad \text{si } \sigma \text{ es par} \\ \text{sgn}\,(\sigma) &= -1, \quad \text{si } \sigma \text{ es impar.} \end{aligned}$$

Se cumple que:

- $\text{sgn}\,(I_d) = 1$.
- $\text{sgn}\,(\sigma\tau) = \text{sgn}\,(\tau\sigma) = \text{sgn}\,(\sigma)\,\text{sgn}\,(\tau)$.

- Sea $\sigma = (i_1\ i_2\ \ldots\ i_k)$ un ciclo de orden k, entonces $\operatorname{sgn}(\sigma) = (-1)^{k-1}$. En particular, si σ es una trasposición, entonces $\operatorname{sgn}(\sigma) = -1$.

Proposición. Sea $\sigma \in S_n$ dada por $\sigma = \tau_1\tau_2 \ldots \tau_m$ con τ_i ciclos disjuntos de órdenes k_i, entonces

$$\operatorname{sgn}(\sigma) = (-1)^n \quad \text{con} \quad n = \sum_{i=1}^{m}(k_i - 1).$$

Definición. El conjunto de las permutaciones pares de S_n

$$A_n = \{\, \sigma \in S_n \,/\, \sigma \text{ es par } \}$$

es un subgrupo de S_n y se dice *subgrupo alternado.*

Observación. A_n es un subgrupo normal de S_n y $|A_n| = n!/2$.

3 Anillos y cuerpos

Definición. Un *anillo* es un conjunto no vacío, A, en el que hay definidas dos operaciones binarias internas "+" (suma) y "$\cdot$" (producto) que cumplen las siguientes propiedades:

- $(A, +)$ es un grupo conmutativo,
- "$\cdot$" es asociativa: $a\cdot(b\cdot c) = (a\cdot b)\cdot c$, para todo $a, b, c \in A$,
- existe elemento neutro para el producto que denotamos por 1 : $1\cdot a = a\cdot 1 = a$ para todo $a \in A$,
- propiedad distributiva: para todo $a, b, c \in A$

$$\begin{aligned} a \cdot (b + c) &= (a\cdot b) + (a\cdot c) \\ (a + b) \cdot c &= (a\cdot c) + (b\cdot c). \end{aligned}$$

Si además el producto verifica la propiedad conmutativa, esto es, $a\cdot b = b\cdot a$ para todo $a, b \in A$, se dice que $(A, +, \cdot)$ es un *anillo conmutativo o abeliano.*

Observaciones.

- El elemento neutro para la suma lo denotaremos por 0, así, $a + 0 = 0 + a = a$ para todo $a \in A$.
- Dado $a \in A$, nos referiremos al elemento simétrico de a (respecto de la suma) como *opuesto de* a y lo denotaremos por $-a$.

Definición. Sea un anillo $(A, +, \cdot)$, un elemento $a \in A$ se dice *inversible o regular* si existe $a' \in A$ tal que $a\cdot a' = a'\cdot a$. En tal caso, el elemento a' se dice *inverso de* a y lo denotaremos por $a' = a^{-1}$.

Proposición. Denotamos por $U(A)$ al conjunto de elementos regulares de A. Entonces $(U(A), \cdot)$ es un grupo y se dice *grupo multiplicativo.*

Definición. Un elemento $a \in A$ se dice *divisor de cero* si existe $b \in A$ (no nulo) tal que $ab = 0$ ó $ba = 0$.

Definición. Se llama *cuerpo* a toda terna $(\mathbb{K}, +, \cdot)$ donde $\mathbb{K}$ es un conjunto no vacío, $+$ y $\cdot$ dos operaciones binarias internas tales que:

- $(\mathbb{K}, +)$ es un grupo conmutativo,
- $(\mathbb{K} \setminus \{0\}, \cdot)$ es un grupo conmutativo,
- Propiedad distributiva: para todo $a, b, c \in \mathbb{K}$

$$\begin{aligned} a(b+c) &= ab + ac \\ (a+b)c &= ac + bc \end{aligned}$$

Observación. Todo cuerpo tiene al menos dos elementos (0 y 1) y se puede definir como un anillo conmutativo en el que todo elemento no nulo es regular.