

# Estructuras algebraicas

Pedro Valero Mejía

September 21, 2013

## 1 Grupos

Por definición, sea  $X$  un conjunto no vacío, podemos construir el conjunto de pares ordenados  $X \times X = \{(x, y) / x, y \in X\}$ . Vamos a fijar un conjunto  $X \neq \emptyset$  y una función  $\varphi: X \times X \rightarrow X$  que a cada par  $(x, y)$  le asocia un elemento  $\varphi(x, y) \in X$  que expresamos como  $x * y$ , siendo  $*$  cualquier operación.

**Definition** Sea  $S$  un subconjunto no vacío de  $G$ , diremos que  $S$  es cerrado por  $\varphi$  si la combinación por  $\varphi$  de dos elementos de  $S$  da otro elemento del mismo.

Dados  $x, y, z \in X$  puede ser interesante el resultado  $x * y * z$  pero, por definición, esto no tiene sentido. Sin embargo, si tendrían sentido  $(x * y) * z$  ó  $x * (y * z)$ . Estas operaciones podrían tener, o no, el mismo resultado. Queremos un conjunto con una operación donde no tengamos que preocuparnos por la colocación de los paréntesis. Para ello debemos buscar una operación asociativa.

Dado  $G \neq \emptyset$  y  $\varphi: G \times G \rightarrow G$ , diremos que  $G$  es un grupo si:

1.  $(G, *)$  es asociativa
2.  $\exists e \in G$  t.q.  $\forall x \in G: x * e = x$
3.  $\forall x \in G \exists x' \in G$  t.q.  $x * x' = x' * x = e$

**Example**  $(\mathbb{Z}, +)$ ;  $(\mathbb{R}, +)$ ;  $(\mathbb{R} \setminus \{0\}, \cdot)$ ;  $(\mathbb{R}/x > 0, \cdot)$  son grupos, mientras que  $(\mathbb{Z}, \cdot)$ ;  $(\mathbb{R}, \cdot)$  no lo son.

A partir de un conjunto  $A$  definimos  $B(A)$  como el conjunto de todas las biyecciones de  $A$  en sí mismo. Puesto que la composición de dos biyecciones es otra biyección, la composición es una operación definida sobre  $B(A)$ . Si tomamos como elemento  $e$  la biyección identidad y como  $x'$  la función inversa, podemos comprobar que  $B(A)$  es un grupo respecto a la composición.

En todo grupo se cumplen las propiedades de unicidad del elemento neutro y del inverso. La demostración de estas propiedades es bastante trivial.

Sean dos elementos  $e$ , y  $e'$  dos elementos neutros de nuestro grupo  $G$ , se cumple que  $e * e' = e'$ , pero también se cumple que  $e' * e = e$ . Esto implica que  $e' = e$ .

Por otro lado, si suponemos la existencia de dos elementos inversos  $a', a'' \in G$ , entonces  $e = a * a' = a * a''$ . Si multiplicamos por  $a$  en ambos lados de la ecuación tenemos:  $a * (a * a') = (a * a') * a''$ , pudiendo reordenar los paréntesis por la propiedad asociativa. Así pues, obtenemos  $a' = a''$ . En esta última demostración nos hemos apoyado en la propiedad cancelativa, que sólo se presenta cuando trabajamos en un grupo.

**Definition** Transformaciones lineales rígidas son aquellas que conservan las distancias. (En  $\mathbb{R}^2$  sólo están las simetrías y giros).

**Example** Vamos a trabajar con un triángulo equilátero,  $\Delta$  en  $\mathbb{R}^2$  y vamos a encontrar el conjunto de todas las aplicaciones lineales rígidas que llevan el triángulo en sí mismo.  $D_3 = \{f \in G / f(\Delta) \rightarrow \Delta\}$ . Para empezar, dentro de este grupo encontramos todos los giros de ángulo  $120^\circ$ . Si defino  $a = g_{2\pi/3}$ , tenemos las aplicaciones:  $e$ ,  $a$  y  $a * a$ , ya que la aplicación  $a * a * a = e$ ,  $a * a * a * a = a$  y así sucesivamente,

por completar vueltas al círculo unidad. Por otro lado, también tenemos las simetrías que tienen como eje las alturas del triángulo. Denotaremos estas simetrías como:  $S_1$ ,  $S_2$  y  $S_3$ . Sabemos que la combinación de un giro y una simetría tiene como resultado otra simetría. Si combinamos  $a * S_1$  obtenemos otra simetría, que también deja el triángulo en sí mismo. Así pues, esta simetría, debe tratarse de  $S_2$  ó  $S_3$ . Lo mismo ocurre con  $a * a * S_1$ .

Así, tenemos:  $D_3 = \{e, a, a * a, S_1, a * S_1, a^2 * S_1\}$

La representación geométrica de un grupo consiste en la descripción de los elementos geométricos que lo constituyen. En el caso del ejemplo, consistiría en indicar qué giros y simetrías constituyen el grupo. La representación abstracta o algebraica de un grupo suele realizarse por medio de una tabla, o una serie de restricciones sobre las operaciones de combinación de los elementos del grupo, sin necesidad de indicar qué es realmente cada elemento.

**Example** La representación abstracta de  $D_3$  viene dada por tres condiciones:

- $\text{ord}(g)=3$
- $\text{ord}(s)=2$
- $g * s = s * g^2$

Ya que con estas condiciones podríamos construir una tabla con todas las combinaciones 2 a 2 de elementos del grupo sin necesidad de saber nada acerca de esos elementos.

**Definition** Se dice que un elemento  $a \in G$ , siendo  $G$  un grupo, tiene orden finito si  $\exists k \in \mathbb{N}$  t.q  $a^k = e$

**Definition** Dado un elemento de orden finito, decimos que su orden es el menor entero positivo con el que se cumple  $a^k = e$

Sea  $G$  un conjunto y  $\varphi$  la operación con la que forma un grupo, vamos a ver cuando un subconjunto de  $G$  es un grupo de forma natural, esto es lo que denominaremos subgrupo.

**Definition** Diremos que un subconjunto no vacío  $S$  es un subgrupo si:

1.  $S$  es cerrado por la operación
2.  $e \in S$
3.  $s \in S \Rightarrow s^{-1} \in S$ .

**Theorem 1.1** Dados  $S_1, S_2$  subgrupos de  $G \Rightarrow S_1 \cap S_2$  es un subgrupo de  $G$ .

Este teorema también puede aplicarse con una intersección numerable de grupos.

**Definition** Fijado un elemento  $g \in G$ , definimos el grupo generado por  $g$  como:  $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ . Este grupo es un subgrupo de  $G$

**Theorem 1.2** Si  $H$  es un grupo de  $G$  y  $g \in H \Rightarrow \langle g \rangle \subset H$ .

A partir de un conjunto  $C = \{g_1, g_2, g_3 \dots g_s\}$ , contenido en  $G$ , vamos a buscar el menor subgrupo que los contiene.  $\langle g_1, g_2, g_3 \dots g_s \rangle = \bigcup_{k \in \mathbb{N}} \{a_1 * a_2 * a_3 \dots a_k / (a_i \in C) \wedge (a_i \in C^{-1})\}$ . Es un subgrupo que contiene a todos los elementos de  $C$ .

Si  $H$  es un subgrupo que contiene a los elementos de  $C$ , el grupo generado por esos elementos se contiene en  $H$ .

**Notacion:**  $H < G$  denota  $H$  subgrupo de  $G$

**Definition** Dado  $H < G$  se dice que  $H$  es cíclico si existe  $g \in G$  t.q.  $H = \langle g \rangle$

**Theorem 1.3** Si  $G$  es un grupo finito y  $S \cap G$  es un subconjunto no vacío  $\Rightarrow S$  es un grupo  $\Leftrightarrow S$  es cerrado por la operación.

**Proof** La implicación hacia la derecha es obvia por la propia definición de subgrupo. Para la implicación hacia la izquierda partimos de que  $S$  es cerrado y finito. Por tanto  $\exists d \in S$  t.q.  $\text{ord}(d)=n$  y  $\langle d \rangle \subset S \Rightarrow d^n = e \in S$  y  $d^{n-1} = d^{-1} \in S \Rightarrow S$  es un grupo

Dentro de los grupos podríamos realizar una clasificación según fueran finitos o infinitos, por ejemplo. No obstante, nos resultará más interesante la clasificación de grupos según sean abelianos o no.

**Definition** Un grupo es abeliano si cumple la propiedad conmutativa.

**Example**  $(\mathbb{Z}, +)$ ;  $(\mathbb{Z}/n\mathbb{Z}, +)$  y  $\langle s, g^2 \rangle = \{1, g^2, s, sg^2\}$  son abelianos

**Lemma 1.4** *Todo subgrupo cíclico de un grupo  $G$  es abeliano. Por tanto un grupo no abeliano no puede ser cíclico.*

**Example** Dado  $D_4 = \{id, g, g^2, g^3, s, sg, sg^2, sg^3\}$ , (Recordemos que era el conjunto de aplicaciones que mantenían un cuadrado invariable), vamos a ver los grupos cíclicos contenidos en él.  $\langle 1 \rangle = 1$ ,  $\langle g \rangle = \{1, g, g^2, g^3\}$ ,  $\langle g^2 \rangle = \{1, g^2\}$ ,  $\langle g^3 \rangle = \{1, g, g^3\}$ ,  $\langle s \rangle = \{1, s\}$ ,  $\langle sg \rangle = \{1, sg\}$ ,  $\langle sg^2 \rangle = \{1, sg^2\}$ ,  $\langle sg^3 \rangle = \{1, sg^3\}$ .

Además podemos destacar el caso de  $(\mathbb{Z}, +)$ , un grupo cíclico para el cual, todo subgrupo es también cíclico. Esto se demuestra de forma general considerando que un grupo no cíclico estaría generado por varios elementos. En este caso, el máximo común divisor de estos números sería generador del grupo. Por tanto, el grupo sería cíclico.

De forma más estricta podemos decir que dado un subgrupo  $H \subset \mathbb{Z}$  podrá ser  $H = \{0\}$  ó  $H \neq \{0\}$ . En el primer caso,  $H$  ya sería cíclico. En el segundo caso, tenemos que  $\exists d \in H$  t.q.  $d \neq 0$ . Lo que implica que  $\langle d \rangle \subset H$ .

La duda sería si es cierto o no  $H \subset \langle d \rangle$ . Sea  $h \in H \Rightarrow h = qd + r$ . Puesto que tanto  $h$  como  $d$  pertenecen a  $H$ , tenemos que  $r$  pertenece a  $H$  también. Esto implica que  $r$  puede expresarse  $r = pd$ . Lo que conlleva  $h = qd + pd = (q+p)d$ . Por tanto  $h \in \langle d \rangle$

**Theorem 1.5** *En un grupo finito  $G$  todo elemento tiene orden finito. Además si  $g \in G$  tiene  $\text{ord}(g)=k \Rightarrow \langle g \rangle$  tiene  $k$  elementos.*

**Theorem 1.6**  $\forall g \in G \text{ ord}(g)=k \Rightarrow \text{card}(\langle g \rangle)=k$

**Definition** Un retículo de subgrupos es aquel retículo (estructura algebraica parcialmente ordenada) formado por subgrupos de un determinado grupo con una relación de contención. En este retículo, la unión de dos subgrupos es el subconjunto generado por su conexión.

**Example** Tomamos una vez más el grupo  $D_4 = \{1, g, g^2, g^3, s, sg, sg^2, sg^3\}$ . Aquí obtenemos el retículo: