# Semigrupos y grupos

Matemáticas Discretas
Matemáticas Aplicadas y Computación 2016-I

# 1. Grupos

## 1.1. Primeros pasos

**Definición 1.1.** Sea $G$ un conjunto y $\cdot$ una operación binaria en $G$. La estructura $(G, \cdot)$ se dice un *grupo* si,

1. Para cada $x$, $y$ y $z$ en $G$,
$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$
2. Existe un elemento $e \in G$ tal que para todo $x$ en $G$,
$$x \cdot e = e \cdot x = x.$$
3. Para cada $x$ en $G$ existe un elemento $y$ en $G$ tal que
$$x \cdot y = y \cdot e.$$

**Lema 1.1.** *Si $f$ es un elemento tal que $x \cdot f = f \cdot x = x$, entonces $f = e$. En ese caso*

*Demostración.* Por las definiciones, tenemos
$$e = e \cdot f = f.$$
□

**Lema 1.2.** *Dados $a$ y $b$ en un grupo $G$, entonces las ecuaciones $a \cdot x = b$ y $y \cdot a = b$ tienen soluciones únicas en $G$*

*Demostración.* Al ser $G$ un grupo basta tomar $x = a^{-1} \cdot b$ y $y = b \cdot a^{-1}$. Supongagmos que $x'$ es otro elemento de $G$ tal que $a \cdot x' = b$, entonces
$$\begin{aligned} x &= a^{-1} \cdot b \\ &= a^{-1} \cdot (a \cdot x') \\ &= (a^{-1} \cdot a) \cdot x' \\ &= e \cdot x' \\ &= x'. \end{aligned}$$

De manera análoga podemos probar lo mismo para $y$. Esto concluye la prueba. $\square$

**Corolario 1.3.** *En un grupo $G$, son válidas las leyes de cancelación:*

$$a \cdot x = a \cdot y \text{ implica } x = y.$$

*y*

$$x \cdot a = y \cdot b \text{ implica } x = y.$$

**Corolario 1.4.** *Sean $a$, $b$ y $b'$ elementos de $G$ tales que, $a \cdot b = e$ y $a \cdot b' = e$, entonces $b = b'$.*

**Corolario 1.5.** *Sean $a$, $b$ y $b'$ elementos de $G$ tales que, $b \cdot a = e$ y $b' \cdot a = e$, entonces $b = b'$.*

De estos resultados anteriores podemos concluir que la identidad el elemento descrito en los axiomas de grupo es único y lo llamaremos la identidad del grupo, mientras que los elementos de la propiedad también son únicos y para cada $a$, denotaremos por $a^{-1}$, el inverso de $a$, al único elemento $a \cdot a^{-1} = a^{-1} \cdot a = e$.

**Definición 1.2.** Para un elemento $a$ de un grupo $G$ definimos

1. $a^0 = e$ y $a^{n+1} = a^n \cdot a$.
2. $a^{-n} = (a^n)^{-1}$

**Lema 1.6.** *Para cualquier $a$ en un grupo $G$,*

$$(a^{-1})^{-1} = a.$$

*Demostración.* Tenemos

$$a^{-1} \cdot (a^{-1})^{-1} = e = a^{-1} \cdot a,$$

usando las leyes de cancelación podemos concluir que $a = (a^{-1})^{-1}$. $\square$

**Lema 1.7.** *Para cualesquiera $a$ y $b$ en un grupo $G$, tenemos*

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

*Demostración.* Basta notar,

$$\begin{aligned}
(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= ((a \cdot b) \cdot b^{-1}) \cdot a^{-1} \\
&= (a \cdot (b \cdot b^{-1})) \cdot a^{-1} \\
&= (a \cdot e) \cdot a^{-1} \\
&= a \cdot a^{-1} \\
&= e.
\end{aligned}$$

Como $(a \cdot b) \cdot (a \cdot b)^{-1} = e$, entonces el resultado que buscamos sigue. $\square$

## 1.2. Subgrupos

**Definición 1.3.** Un subconjunto $H$ no vacío de un grupo $G$ se dice *subgrupo de* $G$ si

1. Para todo $x$ y $y$ en $H$, $x \cdot y$ está también en $H$.

2. Para todo $x$ en $H$, $x^{-1}$ está en $H$.

**Teorema 1.8.** *Cualquier subgrupo $H$ de un grupo $G$, es un grupo.*

*Demostración.* Lo único que se debe probar es que $H$ contiene a la identidad, pues por definición es cerrado y contiene a todos los inversos. Como un subgrupo $H$ es no vacío, sea $x \in H$. Entonces $x^{-1} \in H$ y en consecuencia $x \cdot x^{-1} \in H$, pero $x \cdot x^{-1} = e$. De esto sigue el resultado. $\square$

**Lema 1.9.** *Sea $H$ un subconjunto finito y no vacío de un grupo $G$. Si $H$ es cerrado bajo la operación de $G$, entonces $H$ es un subgrupo de $G$.*

*Demostración.* Como $H$ es no vacío, sea $a \in H$. Como es cerrado bajo la operación de $G$, todos los elementos

$$a, a^2, \dots a^n \dots$$

están en $H$. Ahora, $H$ por lo que la anterior secuencia no puede continuar indefinidamente, esto quiere decir que deben existir naturales $r > s > 0$ tales que $a^r = a^s$. Esto quiere decir que $e \cdot a^s = a^r$, por lo que $a^{r-s} = e$ como $r - s > 0$ entonces $e \in H$. Además,

$$a \cdot a^{r-s-1} = a^{r-s} = e,$$

por lo que $a^{-1} = a^{r-s-1}$ y como $r - s - 1 \geq 0$, entonces $a^{-1} \in H$. Por la definición sigue la afirmación. $\square$

**Definición 1.4.** Sea $H$ un subgrupo de $G$. Si $x \cdot y^{-1} \in H$, decimos que $x$ es congruente con $y$ módulo $H$, en símbolos

$$x \equiv y \mod H.$$

**Lema 1.10.** *La relación* $\mod H$ *es una relación de equivalencia en $G$.*

*Demostración.* Se deben mostrar tres cosas:

1. Para todo $a \in G$, $a \equiv a \mod H$.

2. Si $a \equiv b \mod H$, entonces $b \equiv a \mod H$.

3. Si $a \equiv b \mod H$ y $b \equiv c \mod H$, entonces $a \equiv c \mod H$.

Para probar 1., basta notar que para cualquier $a \in G$, entonces $aa^{-1} = e \in H$ al ser $H$ un subgrupo por lo que $a \equiv a \mod H$.

Para probar 2., tomaremos $a \equiv b \mod H$, esto quiere decir que $ab^{-1} \in H$, en ese caso $ba^{-1} = (ab^{-1})^{-1} \in H$ al ser $H$ un subgrupo, por lo que $b \equiv a \mod H$.

Para probar 3., tomaremos $a \equiv b \mod H$ y $b \equiv c \mod H$; en ese caso $ab^{-1} \in H$ y también $bc^{-1} \in H$, entonces $ac^{-1} = a(b^{-1}b)c^{-1} = (ab^{-1})(bc^{-1}) \in H$ al ser $H$ un subgrupo. Esto implica que $a \equiv c \mod H$. □

**Definición 1.5.** Sea $G$ un grupo y sea $H$ un subgrupo de $G$. Para un elemento $a \in G$ definimos *una clase lateral derecha de $H$ en $G$* , como $Ha = \{ha \mid h \in H\}$.

**Teorema 1.11.** *Para cualquier $a \in G$, tenemos que*

$$Ha = \{x \mid x \equiv a \mod H\}.$$

*Demostración.* Sea $[a] = \{x \mid x \equiv a \mod H\}$. Queremos probar que $Ha = [a]$, para conseguirlo probaremos dos contenciones. Primero, $Ha \subset [a]$; en efecto, si $ha \in Ha$, como $h \in H$, entonces $h^{-1} \in H$, pero

$$a(ha)^{-1} = aa^{-1}h^{-1} = h^{-1}$$

por lo que $a(ha)^{-1} \in H$. Esto quiere decir que $a \equiv ha \mod H$ por lo que $ha \in [a]$.

Afirmamos ahora $[a] \subset Ha$. Si $x \in [a]$, entonces $x \equiv a \mod H$ por lo que $xa^{-1} \in H$. Sea $xa^{-1} = h$ con $h \in H$, en ese caso $x = ha \in Ha$, en ese caso $[a] \subset Ha$, como afirmamos. Con las dos contenciones mostradas esto termina la prueba. □

**Lema 1.12.** *Sean $a$ y $b$ elementos del grupos $G$. Entonces existe una biyección entre $Ha$ y $Hb$.*

*Demostración.* Definimos $f\colon Ha \to Hb$ como $f(x) = xa^{-1}b$; lo primero que debemos notar es que está bien definida, pues

$$f(ha) = (ha)a^{-1}b = hb \in Hb.$$

Probaremos primero que es inyectiva; en efecto, si $f(x) = f(y)$, entonces $x(a^{-1}b) = y(a^{-1}b)$ y por las leyes de cancelación $x = y$.

Supongamos ahora que$y \in Hb$, podemos proponer elemento $x = yb^{-1}a$. Entonces,

$$f(x) = (yb^{-1}a)(a^{-1}b) = y.$$

Con esto hemos probado que $f$ es sobreyectiva, y junto con el argumento en el párrafo anterior $f$ es biyectiva. Esto concluye la prueba. □

Este lema es de especial interés cuando $G$ es un grupo finito. Al resultado presentado a continuación se le conoce como el teorema de Lagrange, un importante teorema en álgebra moderna.

**Teorema 1.13.** *Si $G$ es un grupo finito y $H$ es un subgrupo de $G$, entonces $|H|$ divide a $|G|$.*

*Demostración.* Sean
$$H_1, \ldots, H_k$$
las distintas clases laterales derechas de $H$ en $G$, como estás coinciden con las clases de equivalencia, entonces si $i \neq j$ $H_i \cup H_j = \varnothing$, además

$$G = H_1 \cup \cdots \cup H_k.$$

No sólo eso, como $H = He$ $H$ es una clase lateral derecha de $H$ en $G$ y como todas las clases laterales son biyectivas y $H$ debe ser un conjunto finito, entonces

$$|H| = |H_1| = \cdots = |H_k|.$$

En ese caso
$$|G| = \sum_{i=1}^{k} |H_k| = k|H|.$$
Esto es precisamente lo que afirma el teorema que $|H|$ divide a $|G|$. □

**Definición 1.6.** Si $G$ es un grupo y $a \in G$, entonces $o(a)$ es el mínimo entero positivo $m$ tal que $a^m = e$, en ese caso decimos que $a$ tiene orden $m$. Si dicho número no existe, entonces decimos que el orden de $a$ es infinito.

**Corolario 1.14.** *Si $G$ es un grupo finito y $a \in G$, entonces $o(a)$ divide a $|G|$.*

*Demostración.* Aplicaremos el teorema de Lagrange a un subgrupo que tenga orden $|a|$. Consideremos el conjunto

$$H = \{a^n \mid n \in \mathbb{N}\};$$

como $H$ es finito, basta comprobar que es cerrado bajo el producto, lo cual es cierto por la definición de exponentes en un grupo. Como $a^{o(a)} = e$ por definición entonces $|H| \leq o(a)$. Si $|H| < o(a)$ entonces podríamos encontrar $0 \leq i < j < o(a)$ tal que $a^i = a^j$ por lo que $a^{j-i} = e$ de forma $0 < j - i < o(a)$ lo que es imposible al ser $o(a)$ el mínimo entero positivo con dicha propiedad. En ese caso debemos tener que $|H| = o(a)$ y en consecuencia $o(a)$ divide a $|G|$ como buscábamos. □

**Corolario 1.15.** *Si $G$ es un grupo finito, entonces $a^{|G|} = e$.*

*Demostración.* Es un resultado del lema anterior, sea $|G| = k \cdot o(a)$

$$\begin{aligned} a^{|G|} &= a^{k \cdot o(a)} \\ &= (a^{o(a)})^k \\ &= e^k \\ &= e. \end{aligned}$$

Esto es lo que se quería probar. □

**Definición 1.7.** Sea $G$ un grupo y sea $a \in G$. Definimos *el grupo cíclico generado por $a$* como el subgrupo

$$(a) = \{a^k \mid k \in \mathbb{N}\}.$$

Decimos que $G$ es cíclico, si $G = (a)$ para algún $a \in G$.

**Corolario 1.16.** *Si $G$ es un grupo finito cuyo orden es un número primo $p$, entonces $G$ es un grupo cíclico.*

*Demostración.* Supongamos que $H$ es un subgrupo de $G$, de acuerdo con el teorema de Lagrange, $|H|$ divide a $p$, pero $p$ sólo admite como divisores a 1 y $p$ por lo que $|H| = 1$ o $|H| = p$. En el primer caso $H = (e)$ en el segundo $H = G$.

Ahora, como el orden $G$ es primo, $|G| \leq 2$ por lo que existe $a \in G$ de forma que $a \neq e$. En ese caso $|(a)| \neq 1$ por lo que $|(a)| = p$ y en ese caso $G = (a)$. De aquí, $G$ es un grupo cíclico. □

## 1.3. Un poco de teoría de números

Vamos a explorar una aplicación del teorema de Lagrange a la teoría de números donde derivaremos un par de famosos teoremas como corolarios del teorema de Lagrange. Para esto, vamos a introducir algunos conceptos.

**Definición 1.8.** Sean $x$, $y$ y $m$ enteros cualesquiera. Definimos $x \equiv y \mod n$ si $x - y$ es múltiplo de $n$.

**Proposición 1.17.** *La relación* $\mod n$ *es una relación de equivalencia.*

En ese caso podemos definir

$$\mathbb{Z}/n\mathbb{Z} = \{[x]_n \mid x \in \mathbb{Z}\}$$

y además podemos definir una suma y producto en este conjunto.

$$[x]_n + [y]_n = [x + y]_n$$

y

$$[x]_n \cdot [y]_n = [x \cdot y]_n.$$

# 2. Semigrupos

**Definición 2.1.**

¡++¿

## Referencias

[BM70] Birkohff, Garrett y Mac Lane, Saunders: *Álgebra Moderna.* Vicens-vives, 4ª edición, 1970.

[Fra87] Fraleigh, John B.: *Álgebra abstracta: primer curso.* Addison Wesley, 1987.

*Comentario.* Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentalo. El único objectivo al que sirven, es preparar el curso de Matemáticas Discretas impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.