

**MATE6201-0U1**  
**Prof. Luis A. Medina**  
**10.00 - 11.20**  
**CNL-A-207**

**Algebra Moderna**

Alec Zabel-Mena

Universidad de Puerto Rico, Recinto de Rio Piedras

01.09.2022

**Lectura 1: Grupos y Subgrupos**

**Definición.** Sea  $G$  un conjunto no vacío junto a una operación binaria  $\cdot$ . Decimos que el par  $(G, \cdot)$  es un **grupo** si:

- (1)  $a \cdot b \in G$  para  $a, b \in G$ .
- (2)  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ , para  $a, b, c \in G$
- (3) Existe un  $e \in G$  tal que  $a \cdot e = e \cdot a = a$  para toda  $a \in G$ .
- (4) Para toda  $a \in G$ , existe una  $a^{-1} \in G$  tal que  $a \cdot a^{-1} = a^{-1} \cdot a = e$ .

Si  $a \cdot b = b \cdot a$  para toda  $a, b \in G$ , entonces decimos que  $G$  es un grupo **Abeliano**.

**Ejemplo 1.** (1) Los naturales  $\mathbb{N}$  junto a la multiplicación se satisface los primeros tres axiomas, pero no es un grupo. De hecho,  $\mathbb{N}$  forma un estructura llamado un “monoide”.

- (2) El grupo mas pequeño es el conjunto  $\{e\}$ , que denotamos como  $\langle e \rangle$ .  $\langle e \rangle$  es, trivialmente, un grupo Abeliano.
- (3) Los enteros  $\mathbb{Z}$  junto con adición  $+$  forma un grupo Abeliano por la commutatividad de adición de los enteros.
- (4) El conjunto  $GL(n, \mathbb{R})$  de matrices  $n \times n$  con entradas reales, nosingular forman un grupo con respecto a multiplicación de matrices.  $GL(n, \mathbb{R})$  no es un grupo Abeliano.
- (5) Sea  $S$  cualquier conjunto y  $A(S)$  el conjunto de todas las funciones 1–1 y sobre llevando elementos de  $S$  a elementos de  $S$ . Entonces  $A(S)$  es un grupo no Abeliano con respecto a composición de funciones,  $\circ$ . Si  $S$  tiene  $n$  elementos, entonces exscribimos  $A(S) = S_n$ .  $A(S)$  también no se Abeliano ya que para funciones cualesquiera  $f, g$ ,  $f \circ g \neq g \circ f$ .

**Definición.** Sea  $G$  un grupo. El **orden** de un grupo es su cardinalidad, y escribimos  $\text{ord } G = |G|$ . Decimos que  $G$  es **finito** si  $\text{ord } G$  es finito; de lo contrario,  $G$  es **infinito**.

**Definición.** Sea  $G$  un grupo, y  $a \in G$ . El **orden** de  $a$ , denotado  $\text{ord } a$ , es el menor entero positivo  $n$  tal que  $a^n = e$  y escribimos  $\text{ord } a = n$ . Si tal  $n$  no existe, entonces decimos que  $a$  es de orden **infinita**, y decimos que  $a$  es un elemento **torsión**.

**Ejemplo 2.** (1) Considera  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ , entonces  $\mathbb{C}^*$  tiene orden infinita, note que si  $\alpha = \exp(\frac{2i\pi}{5}) \in \mathbb{C}^*$ , entonces  $\alpha \neq 1$ , para  $j \neq 1, 2, 3, 4$ , pero  $\alpha^5 = 1$ . Entonces  $\text{ord } \alpha = 5$ .

(2) Considere  $A \in GL(6, \mathbb{R})$  con la forma

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

Entonces

$$A^3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

entonces,  $A^3 = I$ .

(3) En  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ,  $\mathbb{R}^*$  es infinito, y  $\text{ord } 2$  es infinito.

**Definición.** Sea  $G$  un grupo y  $H \subseteq G$  no vacío. Entonces decimos que  $H$  es un **subgrupo** de  $G$  si  $H$  es un grupo bajo la misma operación de  $G$ . Escribimos  $H \leq G$ .

**Ejemplo 3.** (1) Considere  $GL(n, \mathbb{R})$  y sea  $SL(n, \mathbb{R})$  los elementos  $A \in GL(n, \mathbb{R})$  tales que  $\det A = 1$ . Entonces  $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$ .

(2) Sea  $C(\mathbb{R})$  el conjunto de todas las funciones continuas sobre  $\mathbb{R}$ . Entonces  $C(\mathbb{R})$  es un grupo bajo la suma de funciones  $+$ . Sea  $C^1(\mathbb{R})$  el conjunto de funciones primer diferenciables continuas sobre  $\mathbb{R}$ . Es decir, que  $f'$  existe y es continua. Observe lo siguiente:

- (a)  $(f + g)' = f' + g'$
- (b)  $f' + (g + h)' = (f + g)' + h'$ .
- (c)  $c' = 0$ , entonces  $0 \in C^1(\mathbb{R})$
- (d)  $f' - f' = -f' + f' = 0$ .

Suponiendo que  $f', g', h' \in C^1(\mathbb{R})$ , son continuas, entonces vemos que las funciones de arriba también son continuas. Entonces  $C'(\mathbb{R}) \leq C(\mathbb{R})$ .

**Lema 1.** Sea  $G$  un grupo y  $H \subseteq G$  no vacío. Si tenemos que  $ab \in H$ , implicat que  $ab^{-1} \in H$ , entonces  $H \leq G$ .

*Proof.* Como  $H \neq \emptyset$ , sea  $a \in H$ . Entonces  $aa^{-1} = e \in H$ . Luego, también tenemos que  $ea^{-1} = a^{-1} \in H$ . Finalmente, tenemos que si  $b \in H$ , entonces  $ab^{-1} \in H$ , por lo tanto  $b^{-1} \in H$ , entonces  $a(b^{-1})^{-1} = ab \in H$ . ■

**Ejemplo 4.** (1) Considere a los enteros pares  $2\mathbb{Z}$ . Sean  $2n, 2m \in 2\mathbb{Z}$ . Noten que  $2n - 2m = 2(n - m) \in 2\mathbb{Z}$ . Entonces  $2\mathbb{Z} \leq \mathbb{Z}$ .

- (2) Si  $G$  es un grupo, entonces  $\langle e \rangle$  y  $G$  son subgrupos de  $G$ . Llamamos a  $\langle e \rangle$  el grupo **trivial**.
- (3) Si  $G$  es un grupo, y  $a \in G$ , entonces el conjunto  $\langle a \rangle = \{a^j : j \in \mathbb{Z}\}$  es un subgrupo de  $G$ , llamado el **subgrupo generado por  $a$** .
- (4) Si  $G$  es un grupo, y  $a \in G$ , entonces  $C(a) = \{g \in G : ag = ga\}$  y  $Z(G) = \{g \in G : ag = ga \text{ para toda } a \in G\}$  son subgrupos. Nota que  $Z(G) = \bigcap C(a)$ . Llamamos a  $C(a)$  el **centralizador** de  $a$  y  $Z(G)$  el **centro** de  $G$ .
- (5) Sea  $G$  un grupo y  $H \leq G$ , y sea  $a \in G$ , entonces  $a^{-1}Ha \leq G$ . Llamamos a  $a^{-1}Ha$  el **conjugado** de  $H$  **con respecto** a  $a$ .

**Definición.** Suponga que  $G$  y  $H$  son grupos. Un mapa  $\phi : G \rightarrow H$  se llama un **homomorfismo** si para toda  $a, b \in G$ ,  $\phi(ab) = \phi(a)\phi(b)$ . Si  $\phi$  es 1-1 y sobre, entonces lo llamamos un **isomorfismo**. Si  $\phi$  es un isomorfismo, y  $G = H$ , entonces llamamos a  $\phi$  un **automorfismo**.

## Lectura 2: Grupos y Subgrupos

**Ejemplo 5.** (1) Considera  $\mathbb{R}$  bajo la suma  $+$  y  $\mathbb{R}^+$  bajo la multiplicación,  $\cdot$ . Sea  $\phi : \mathbb{R} \rightarrow \mathbb{R}^+$  definido por  $\phi : x \rightarrow \exp x$ . Entonces  $\phi$  es un homomorfismo, ya que

$\exp(x + y) = \exp x + \exp y$ . De igual forma, nota que  $\phi$  es  $1 - 1$  y sobre, por lo tanto, existe inverso; de hecho,  $\phi^{-1} = \log$ , que tambien es un homomorfismo. Pues, tenemos  $\phi$  es un isomorphismo y que  $\mathbb{R} \simeq \mathbb{R}^+$ .

- (2) Sea  $\phi : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$  dado por  $\phi : A \rightarrow \det A$ . Entonces  $\phi$  es un homomorphismo ya que  $\det AB = \det A \det B$ . Nota que  $GL(n, \mathbb{R})$  no es Abeliano, pero  $\mathbb{R}^*$  si, por lo tanto  $GL(n, \mathbb{R}) \not\simeq \mathbb{R}^*$ . Esto también dice que no existe inverso  $\det^{-1}$ . Esto nos dice que los homomorfismos solo preservan el estructura de grupos, pero nada mas de eso.
- (3) Considere  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  dado por  $\phi(m) = m \bmod n$ . Entonces  $\phi(m + k) = (m + k) \bmod n \equiv m \bmod n + k \bmod n = \phi(m) + \phi(k)$ . Así que  $\phi$  es un homomorfismo.
- (4) Sea  $G$  y  $H$  grupos, y sea  $\phi : G \rightarrow H$  un homomorfismo de  $G$  sobre  $H$ . Entonces si  $G$  es Abeliano, también lo es  $H$ . Nota que para  $h, h' \in H$ , exists  $g, g' \in G$  con  $\phi(g) = h$  y  $\phi(g') = h'$ . Entonces  $hh' = \phi(g)\phi(g') = \phi(gg') = \phi(g'g) = \phi(g')\phi(g) = h'h$ .
- (5) Sea  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  dado por  $x \rightarrow 5x$ . Entonces  $\phi(x + y) = 5(x + y) = 5x + 5y = \phi(x) + \phi(y)$ .
- (6) Suponga que  $G$  es Abeliano y defina  $\phi : G \rightarrow G$  por la regla  $\phi(a) = a^{-1}$ . Entonces tenemos que  $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$ . Así que  $\phi$  es un homomorfismo. Nota también que por la ley de inversos de elementos, que  $\phi$  es sobre. También tenemos que  $\phi$  es  $1 - 1$  ya que  $a^{-1} = b^{-1}$  implica que  $a = b$ , por unicidad de inversos. Por lo tanto  $\phi$  es un automorfismo.
- (7) Sea  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  dado por  $x \rightarrow x^2$ .  $\phi$  no es un homomorfismo ya que en general,  $(x + y)^2 \neq x^2 + y^2$ . Pero, si tomamos la mapa  $\psi : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  dado por la misma regla, entonces  $\psi$  es un homomorfismo.

**Definición.** Sea  $G$  y  $H$  grupos, y  $\phi : G \rightarrow H$  un homomorfismo de  $G$  hacia  $H$ . Definimos el **kernel** de  $\phi$  como el conjunto  $\ker \phi = \{a \in G : \phi(a) = e'\}$  donde  $e'$  es la identidad de  $H$ . Definimos también la **imagen** del homomorfismo como el conjunto  $\Im \phi = \phi(G) = \{\phi(a) : a \in G\}$ .

**Lema 2.** Sea  $G$  y  $H$  grupos y  $\phi : G \rightarrow H$  un homomorfismo de  $G$  hacia  $H$ . Entonces  $\ker \phi \leq G$  y  $\phi(G) \leq H$ .

*Proof.* Nota por definicion que  $\ker \phi \subseteq G$ . Tambien tenemos que  $e \in \ker \phi$  por el ley de homomorfismo. Entonces  $\ker \phi$  no es vacio. Ahora, sea  $a, b \in \ker \phi$ . Entonces, tenemos  $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e'e' = e'$ , pues  $ab^{-1} \in \ker \phi$ . ■

**Ejemplo 6.** (1) Considere  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}$  dado por  $m \rightarrow m \bmod 12$ . Entonces  $\ker \phi = \langle 12m \rangle = 12\mathbb{Z}$ . Tambien  $\phi(\mathbb{Z}) = \mathbb{Z}/12\mathbb{Z}$ ; pues  $\phi$  es sobre.

- (2) Considere  $\phi : \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}$  dado por  $m \rightarrow 3m$ .  $\phi$  es un homomorfismo, y  $\ker \phi = \{x \in \mathbb{Z}/12\mathbb{Z} : 3x \equiv_{12} 0\} = \{0, 4, 8\} = \langle 4 \rangle$ . De igual manera,  $\phi(\mathbb{Z}/12\mathbb{Z}) = \{0, 3, 6, 9\} = \langle 3 \rangle$ .
- (3) Sea  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  dado por  $m \rightarrow 5m$ . Entonces  $\ker \phi = \langle 5m \rangle = \langle 0 \rangle = 5\mathbb{Z}$ . Nota que como  $\phi$  es 1-1, si  $a \in 5\mathbb{Z}$ , entonces  $a = 5m \equiv_5 0$ . Note tambien que  $\phi(\mathbb{Z}) = 5\mathbb{Z}$ , por lo tanto  $\phi$  es sobre, asi que tenemos  $\mathbb{Z} \simeq 5\mathbb{Z}$ .
- (4) Sea  $D_n$  el grupo dihedral sobre un poligono regular de  $n$ -vertices. Recuerda que  $r^n = t^2 = e$  y que  $tr^j = r^{n-j}t$ . Considere la homomorfismo  $\phi : D_8 \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , donde  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  es un grupo bajo la suma de productos directos. Entonces si  $\phi(r) = (1, 0)$  y  $\phi(t) = (0, 1)$  entonces tenemos que  $\ker \phi = \langle r^2 \rangle$  y  $\phi(D_8) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

### Lectura 3: Grupos Cíclicos, Clases Laterales, y La Teorema de Lagrange.

**Definición.** Sea  $G$  un grupo. Definimos un **grupo cíclico** de  $G$  **generado** por un elemento  $a \in G$  de ser el subgrupo de  $G$   $\langle a \rangle = \{a^j : j \in \mathbb{Z}\}$ . Llamamos a  $a$  el **generador** del grupo. Si  $G = \langle a \rangle$  para algun  $a \in G$ , entonces decimos que  $G$  es **cíclico**.

**Ejemplo 7.** (1) Considere el grupo  $\langle A \rangle$ , donde

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

Nota que  $A^4 = I$ , entonces  $\langle A \rangle = \{I, A, A^2, A^3\}$  es un subgrupo de orden  $\text{ord } A = 4$  del grupo  $GL(4, \mathbb{R})$ .

- (2) Considere el grupo dihedral  $D_3 = \{e, r, r^2, t, rt, r^2t\}$  Los sobgrupos de  $D_3$  son los sigu-

ientes en la reticulo de subgrupos sigueinte con los ordenes anotados:



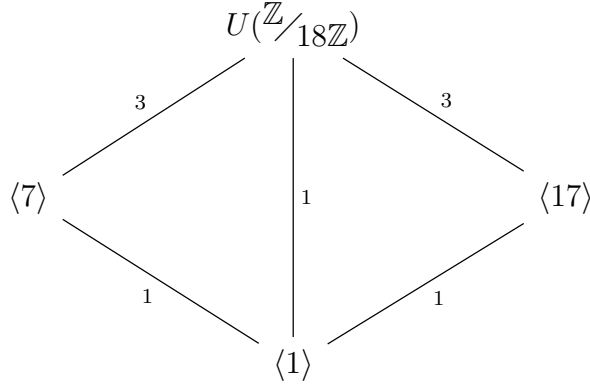
**Teorema 3** (Teorema Fundamental de Grupos Cíclicos). *Todo subgrupo de un grupo cíclico es cíclico. mas aún si  $G = \langle a \rangle$  es un grupo cíclico de orden  $G = n$ , entonces  $G$  tiene un subgrupo de orden  $d$  por cada divisor  $d$  de  $n$ .*

*Proof.* Sea  $G = \langle a \rangle$  y  $H \leq G$ . Observe qu si  $H = \langle e \rangle$ , entonces terminamos. Pues suponga que  $H \neq \langle e \rangle$ . Entonces existe un  $h \in H$  con  $h \neq e$ . Es decir, que  $h = a^j$  para alguna  $j \in \mathbb{Z}$ . Nota que si  $j > 0$  entonces  $h$  es una potencia positiva de  $j$ ; de igual manera, si  $j < 0$  entonces  $h^{-j} = (h^{-1})^j$  es una potencia psotiva de  $j$ . Es decir,  $H$  tiene potencias positivas. Por lo tanto, por el principio de buen orden, existe una potencia positiva mas pequeño, sea  $a^m$ . Sea  $h \in H$ , entonces  $h = a^k$  para algún  $k \in \mathbb{Z}$ . Entonces por la teorema de división, existe  $q, r \in \mathbb{Z}$  tales que  $k = qm + r$  y  $0 \leq r < m$ . Entonces  $a^k = a^{qm+r} = a^{qm}a^r = (a^m)^qa^r$ . Como  $a^k \in H$ , y  $a^m \in H$ , es necesario tener  $(a^m)^qa^r \in H$  para preservar que  $H \leq G$ . Entonces, si  $a^r \neq e$ , tenemos una potencia de  $a$  mas pequeño que  $a^m$ , lo cual no puede pasar. Es decir  $a^r = e$ , y  $a^k = (a^m)^q$ . Es decir todo elemento de  $h$  es una potencia del elemento  $a^m$ , por lo tanto  $H = \langle a^m \rangle$  es cíclico.

Ahora sea  $\text{ord } G = n$  y sea  $d$  un divisor positivo de  $n$ . Como  $d|n$ , entonces existe un  $k \in \mathbb{Z}^+$  con  $n = kd$ . Ahora considere el subgrupo  $\langle a^k \rangle$  Entonces sea  $j \in \mathbb{Z}$  y considere  $(a^k)^j$ . Nota que  $(a^k)^d = a^{kd} = a^n = e$ , y si  $0 < d < j$  entonces  $(a^k)^j = a^{kj} \neq e$  por lo tanto  $\text{ord } a^k = d$ , lo cual dice que  $\text{ord } \langle a^k \rangle = d$ . ■

**Ejemplo 8.** (1) Sea  $U(\mathbb{Z}/18\mathbb{Z}) = \{1, 5, 7, 11, 13, 17\}$  el grupo de unidades dde  $\mathbb{Z}/18\mathbb{Z}$ . Observe que  $U(\mathbb{Z}/18\mathbb{Z}) = \langle 5 \rangle$ , y que  $\text{ord } U(\mathbb{Z}/18\mathbb{Z}) = \text{ord } \langle 5 \rangle = 6$ . Entonces  $U(\mathbb{Z}/18\mathbb{Z})$

tiene los siguientes subgrupos mostrado en la siguiente retículo con ordenes anotados:



- (2) El grupo de unidades de  $\mathbb{Z}/50\mathbb{Z}$ ,  $U(\mathbb{Z}/50\mathbb{Z}) = \langle 3 \rangle$  tiene el siguiente retículo de subgrupos:



**Teorema 4** (Criterio de Igualdad de Potencias). *Suponga que  $G$  es un grupo. Sea  $a \in G$ , y sea  $i, j \in \mathbb{Z}$  tales que  $a^i = a^j$ . Si  $a$  es de orden infinito, entonces  $i = j$ ; de igual manera, si  $\text{ord } a = n$ , entonces  $i \equiv j \pmod{n}$ .*

**Corolario.** *Sí  $j \in \mathbb{Z}^+$ , entonces  $\langle a^j \rangle = \langle a^{(j,n)} \rangle$ , y  $\text{ord } a^j = \frac{n}{(j,n)}$ , donde  $(j, n)$  es el máximo común divisor de  $j$  y  $n$ .*

**Corolario.** *Sí  $G = \langle a \rangle$ , y  $\text{ord } G = \text{ord } \langle a \rangle = n$ , entonces  $a^j$  es generador de  $G$  sí y solo sí  $(j, n) = 1$ . La cantidad de generadores de  $G$  está dado por  $\phi(n)$  donde  $\phi$  es la función Euler- $\phi$ .*

**Ejemplo 9.** Considere de nuevo  $U(\mathbb{Z}/50\mathbb{Z}) = \langle 3 \rangle$ . Tenemos que  $\phi(50) = 20$ , así que los

generadores de  $U(\mathbb{Z}/50\mathbb{Z})$  son potencias  $3^j$  donde  $(j, 50) = 1$ . Es decir, los generadores son:

$$3^1 \quad 3^3 \quad 3^7 \quad 3^9 \quad 3^{11} \quad 3^{13} \quad 3^{17} \quad 3^{19}$$

**Teorema 5.** Sea  $G$  un grupo cíclico. Entonces  $G \simeq \mathbb{Z}$  ó  $G \simeq \mathbb{Z}/n\mathbb{Z}$  para algún  $n \in \mathbb{Z}^+$ .

*Proof.* Sea  $G$  un grupo cíclico. Suponga que  $G$  es infinito. Como los elementos de  $G$  son de la forma  $a^j$  para  $j \in \mathbb{Z}$ , considere el mapa  $\phi : G \rightarrow \mathbb{Z}$  dado por  $a^j \rightarrow j$ . Entonces  $\phi$  es un homomorfismo de  $G$  sobre  $\mathbb{Z}$ , ya que  $j$  corresponde a la potencia de uno de los infinito elementos de  $G$ . Mas aún,  $\phi$  es 1-1, ya que  $a^i = a^k$  implica que  $i = k$ . Es decir  $\phi$  define un isomorfismo entre  $G$  y  $\mathbb{Z}$ .

De igual forma, suponga que  $\text{ord } G = n$ . Nota entonces que  $G$  tiene la forma  $G = \{a^j : j \in \mathbb{Z}/n\mathbb{Z}\}$ . Define entonces  $\phi : G \rightarrow \mathbb{Z}/n\mathbb{Z}$  dado por  $a^j \rightarrow j \pmod n$ .  $\phi$  es un homomorfismo de  $G$  sobre  $\mathbb{Z}/n\mathbb{Z}$ , por definición.  $\phi$  también es 1-1 ya que  $a^i = a^j$  implica  $i \equiv j \pmod n$ . Esto define un isomorfismo de  $G$  sobre  $\mathbb{Z}/n\mathbb{Z}$ . ■

**Ejemplo 10.** Considere  $\mathbb{C}$  y sea  $i \in \mathbb{C}$ . Entonces  $\langle i \rangle = \{1, i, -1, -i\}$  por multiplicación, así que  $\text{ord } \langle i \rangle = \text{ord } i = 4$ . Por la teorema anterior, esto hace  $\langle i \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ .

**Definición.** Sea  $G$  un grupo y  $H \leq G$ . Si  $a \in G$  definimos la **clase lateral por la derecha** de  $H$  **generado** por  $a$  de ser el conjunto  $Ha = \{ha : h \in H\}$ . De igual forma, definimos la **clase lateral por la izquierda** de  $H$  **generado** por  $a$  de ser el conjunto  $aH = \{ah : h \in H\}$ .

**Definición.** Sea  $G$  un grupo y  $H \leq G$ . Defina la relación  $\equiv$  sobre  $G$  de la siguiente forma:  $a \equiv b$  si y solo si  $ab^{-1} \in H$ . Llamamos a  $\equiv$  **congruencia modulo  $H$** . Escribimos  $a \equiv b \pmod H$ , ó simplemente  $a \equiv_H b$ .

**Lema 6.** Sea  $G$  un grupo y  $H \leq G$ . Entonces la relación de congruencia modulo  $H$  sobre  $G$  es una relación de equivalencia.

*Proof.* Como  $H \leq G$ , tenemos que  $e = aa^{-1} \in H$ , así que  $a \equiv a \pmod H$ . Ahora, suponga que  $a \equiv b \pmod H$ , entonces  $ab^{-1} \in H$ . Entonces  $(ab^{-1})^{-1} = ba^{-1} \in H$ , por lo tanto  $b \equiv a \pmod H$ . Finalmente, sea  $a \equiv b \pmod H$ , y  $b \equiv c \pmod H$ . Entonces  $ab^{-1}, bc^{-1} \in H$ , así que  $(ab^{-1})(bc^{-1}) = a(bb^{-1})c^{-1} = ac^{-1} \in H$ , así que  $a \equiv c \pmod H$ . ■

**Corolario.** Las clases de equivalencia de  $\equiv_H$  sobre  $G$  son precisamente las clases laterales por la izquierda  $aH$ .

*Proof.* Exercise. ■



**Corolario.** Tenemos que  $\text{ord } H = |aH|$ .

*Proof.* Considere la mapa  $f : H \rightarrow aH$  dado por la regla  $h \rightarrow ah$ . A todo  $ah \in aH$  podemos asignarlo a  $h$ , así que  $f$  lleva  $H$  sobre  $aH$ . De igual forma, si  $ah = ah'$  para  $h, h' \in H$ , entonces por cancelación  $h = h'$ . Es decir  $f$  es 1-1. ■

**Corolario.** La cantidad de clases laterales por la izquierda de  $H$  en  $G$  es la misma que la de las clases laterales por la derecha de  $H$  en  $G$ .

*Proof.* Considere la mapa  $f : aH \rightarrow Ha$ . ■

**Definición.** Sea  $G$  un grupo y  $H \leq G$ . Definimos el **índice** de  $H$  en  $G$ , denotado por  $[G : H]$ , de ser la cantidad de clases laterales de  $H$  en  $G$ .

**Teorema 7** (La Teorema de Lagrange). Sea  $G$  un grupo y  $H \leq G$ . Entonces tenemos

$$\text{ord } G = [G : H] \text{ord } H$$

*Proof.* Sabemos que  $G = \bigcup_{a \in H} aH$  es una unión disjunta. Como  $aH \cap bH = \emptyset$  si y solo si  $a \neq b$ , entonces tenemos repeticiones. Ahora suponga que el conjunto de clases laterales de  $H$  en  $G$  está indexado por  $J$ . Entonces tenemos que

$$\text{ord } G = \sum_{j \in J} |a_j H| = \sum_{j \in J} \text{ord } H = |J| \text{ord } H$$

Nota que  $|J| = [G : H]$ . ■

**Corolario.** Si  $G$  y  $H$  son finito, entonces el orden de  $H$  divide el orden de  $G$ . Mas aún, tenemos que  $\frac{\text{ord } G}{\text{ord } H} = [G : H]$

#### Lectura 4: Grupos Cocientes y Teoremas de Isomorfismo.

**Definición.** Dado un grupo  $G$  y un subgrupo  $H$  de  $G$ , definimos el **producto de clases laterales** de ser el producto  $aHbH = abH$ .

**Definición.** Sea  $G$  un grupo. Decimos que un subgrupo  $H$  de  $G$  es **normal** si para cualquier  $a \in G$ ,  $aH = Ha$ . Escribimos  $H \trianglelefteq G$ .

**Lema 8.** Sea  $H$  un subgrupo normal de un grupo  $G$ . Entonces los siguientes son equivalentes para todo  $a \in H$ :

(1)  $aHa^{-1} \subseteq H$ .

(2)  $aHa^{-1} = H$ .

(3) Para todo  $a \in G$ , existe un  $b \in G$  tal que  $aH = Hb$ .

*Proof.* Sí  $aHa^{-1} = H$ , entonces  $aHa^{-1} \subseteq H$ . Por el otro lado, si  $aHa^{-1} \subseteq H$ , entonces para  $h, h' \in H$ ,  $aha^{-1} = h'$ , así que  $h' \in aHa^{-1}$ , así que  $H \subseteq aHa^{-1}$ .

Ahora, si  $aHa^{-1} = H$ , entonces tenemos que  $aH = Ha$  para todo  $a \in H$ , por el otro lado, suponga que  $a, b \in H$  tal que  $aH = Hb$ . Entonces nota que  $a \in Hb$  y  $a \in Ha$ , así que  $Ha \cap Hb \neq \emptyset$ . Como  $Ha$  y  $Hb$  son clases de equivalencias, esto forza a  $a = b$ . ■

**Ejemplo 11.**  $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$ , nota que para cualquier  $A \in SL(n, \mathbb{R})$  y  $B \in GL(n, \mathbb{R})$  que  $\det(BAB^{-1}) = (\det B)(1)(\det B^{-1}) = 1$ .

**Teorema 9.** Sí  $G$  es un grupo y  $H \trianglelefteq G$  es subgrupo normal de  $G$ , entonces las clases laterales de  $H$  en  $G$  forman un grupo bajo el producto de clases.

*Proof.* Define la operación  $(aH, bH) \rightarrow aHbH = \{ahbh' : h, h' \in H\} = abH$ . Ya que  $aH$  y  $bH$  son clases de equivalencia, el producto es bien definida.

Ahora sea  $aH$  y  $bH$ , como  $H \trianglelefteq G$ , tenemos que  $aHbH = abHH = abH$ , así que  $abH$  es clase lateral de  $H$  en  $G$ ; nota también que  $aH(bHcH) = aH(bcH) = a(bc)H = abcH = (ab)cH = abHcH = (aHbH)cH$ , así que el producto es asociativa.

Ahora toma la identidad de  $H$ ,  $e \in H \trianglelefteq G$  y para cada  $a \in G$ , toma  $a^{-1}$ . Entonces tenemos que  $aHeH = aeH = eaH = eHaH = H$  y que  $eH = H$ . De igual forma  $aHa^{-1}H = aa^{-1}H = a^{-1}aH = a^{-1}HaH = H$ . Así que  $H$  es la identidad, y  $a^{-1}H$  la inversa de  $aH$ . ■

**Definición.** Sea  $G$  un grupo. Denotamos el conjunto de todas las clases laterales de un subgrupo  $H$  en  $G$  como  $G/H$ . Sí  $H$  es un subgrupo normal, entonces  $G/H$  forma un grupo llamado el **grupo cociente** de  $G$  sobre  $H$ .

**Lema 10.** Sea  $G$  un grupo. Todo subgrupo de  $G$  es normal sí y solo sí  $H$  es el kernel de algún homomorfismo  $\phi$  en  $G$ .

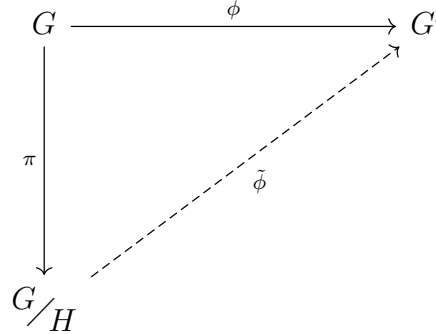
*Proof.* Sea  $H \trianglelefteq G$ . Considere la mapa  $\phi : G \rightarrow G/H$  tal que  $\phi : a \rightarrow aH$ . Entonces  $\ker \phi = \{a \in G : aH = H\}$ . Así que si  $a \in \ker \phi$ , tenemos  $aH = H$ , que nos dice que  $a \in H$ . Por otro lado,  $a \in H$  implica  $aH = H$ , así que  $a \in \ker \phi$ . Es decir  $H = \ker \phi$ .

Por otro lado considere  $\ker \phi$  para algún mapa en  $G$ . Considere cualquier  $a \in G$  y  $h \in \ker \phi$ . Entonces  $\phi(a)\phi(h)\phi^{-1}(a) = \phi(a)e'\phi^{-1}(a) = \phi(a)\phi^{-1}(a) = e'$ , donde  $e'$  es la identidad de  $G'$ . Entonces como  $a$  y  $h$  eran arbitrarios, vemos que  $\phi(a)\ker \phi\phi^{-1}(a) \subseteq \ker \phi$ . Así que  $\ker \phi \trianglelefteq G$ . ■

**Lema 11.** Sea  $G$  un grupo y  $\phi : G \rightarrow G'$  un homomorfismo. Entonces tenemos que Si  $H \trianglelefteq G$  y  $\phi$  es sobre, entonces  $\phi(H) \trianglelefteq G'$ . Mas aún si  $H' \trianglelefteq G'$ , entonces  $\phi^{-1}(H') \trianglelefteq G$ .

*Proof.* Sea  $\phi : G \rightarrow G'$  una mapa de  $G$  sobre  $G'$ . Suponga también que  $H \trianglelefteq G$ . Entonces tome  $y \in G'$ . Pues entonces existe un  $x \in G$  tal que  $y = \phi(x)$ . También existe un  $h \in H$  con  $\alpha = \phi(h)$ . Entonces considere  $y\alpha y^{-1} = \phi(x)\phi(h)\phi^{-1}(y) = \phi(xhx^{-1}) = \phi(h')$ . Por lo tanto  $y\alpha y^{-1} \in \phi(H)$  lo que hace  $y\phi(H)y^{-1} \subseteq \phi(H)$ . Así que  $\phi(H)$  es normal en  $G'$ . Ahora considere  $H' \trianglelefteq G'$ , entonces para todo  $a' \in G$  y  $h' \in H'$ ,  $a'h'a'^{-1} \in H$ . Como  $\phi$  es sobre, tenemos que existen  $x \in G$  y  $h \in H$  con  $x = \phi(a')$  y  $h = \phi(h')$ , osea  $x \in \phi^{-1}(G')$  y  $h \in \phi^{-1}(H')$ . Entonces  $xhx^{-1} = \phi(a')\phi(h)\phi^{-1}(a') = \phi(a'h'a'^{-1}) \in \phi^{-1}(H')$ . Entonces  $x\phi^{-1}(H')x^{-1} \subseteq \phi^{-1}(H')$ , así que  $\phi^{-1}(H') \trianglelefteq G$ . ■

**Teorema 12** (Teorema de Factorización). Suponga que  $G$  y  $G'$  son grupos y  $H \trianglelefteq G$ . Sea  $\phi : G \rightarrow G'$  y  $\pi : G \rightarrow G/H$  dado por  $\pi : a \rightarrow aH$ . Entonces existe un único  $\tilde{\phi} : G/H \rightarrow G'$  tal que  $\phi = \tilde{\phi} \circ \pi$ .



*Proof.* Suponga primero que existe tal  $\tilde{\phi}$ . Sea  $\bar{\phi} : G/H \rightarrow G'$  otro homomorfismo tal que  $\phi = \bar{\phi} \circ \pi$ . Entonces tenemos que  $\tilde{\phi} \circ \pi(a) = \bar{\phi} \circ \pi(a)$ . Es decir que  $\tilde{\phi}(aH) = \bar{\phi}(aH) = \phi(a)$ . Esto hace que  $\tilde{\phi}(G/H) = \bar{\phi}(G/H) = \phi(G)$ , así que tienen la misma imagen y misma relación. Así que  $\tilde{\phi} = \bar{\phi}$ .

Ahora define la mapa  $\tilde{\phi} : G/H \rightarrow G'$  dado por  $aH \rightarrow \phi(a)$ . Sea entonces  $sb \in aH$ , así que  $aH = bH$ , entonces tenemos  $a^{-1}b \in H = \ker \phi$ . Entonces  $\phi(a^{-1}b) = e'$ , la identidad de  $G'$ , entonces  $\phi(a) = \phi(b)$ . Pues  $\tilde{\phi}$  está bien definida. Por último, note que  $\tilde{\phi}(aH) = \tilde{\phi}(\pi(a)) = \tilde{\phi} \circ \pi(a)$ . ■

**Corolario.**  $\phi$  es sobre si y solo si  $\tilde{\phi}$  es sobre, y  $\phi$  es 1-1 si y solo si  $\ker \phi = H$ .

*Proof.* Nota que como  $\tilde{\phi}(G/H) = \phi(G)$ , entonces si  $\tilde{\phi}$  es sobre, entonces  $\phi$  tiene que ser sobre. Por el otro lado, el mismo es cierto.

Ahora si  $\ker \phi = H$ , como  $H$  es identidad del  $G/H$ , entonces  $\phi$  es 1-1. Por el otro lado, si  $\phi$  es 1-1, entonces  $\ker \phi = \langle e_{G/H} \rangle$ , donde  $e_{G/H}$  es la identidad de  $G/H$ ; pero  $e_{G/H} = H$ . ■