

**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

05.10.2022

**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 isomorfismo 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 homomorfismo ya que  $\det AB = \det A \det B$ . Nota que  $GL(n, \mathbb{R})$  no es Abelian, 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 Abelian, 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 Abelian 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:



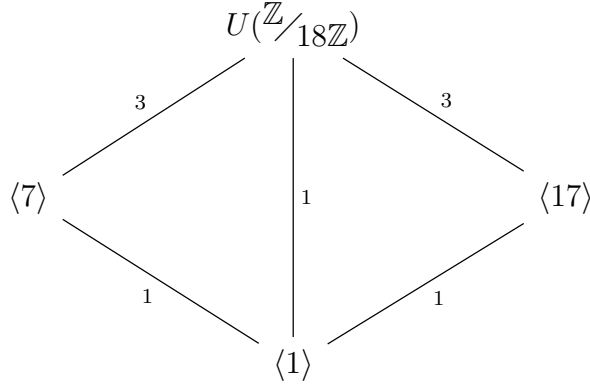
**Teorema 3** (Teorema Fundamental de Grupos Cíclicos). *Todo subgrupo de un grupo cíclico es cíclico. mas aún si  $G = \langle a \rangle$  es un grupo cíclico de orden  $G = n$ , entonces  $G$  tiene un subgrupo de orden  $d$  por cada divisor  $d$  de  $n$ .*

*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

**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 fuerza 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  $G$ .

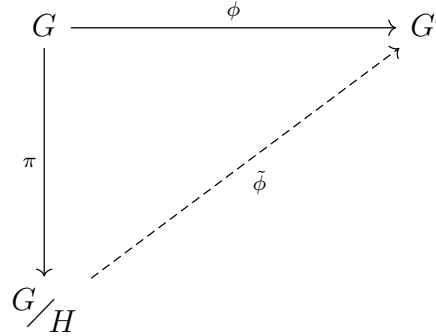
*Proof.* Sea  $H \trianglelefteq G$ . Considere la mapa  $\phi : G \rightarrow G/H$  tal que  $\phi : a \rightarrow aH$ . Entonces  $\ker \phi = \{a \in G : aH = H\}$ . Así que si  $a \in \ker \phi$ , tenemos  $aH = H$ , que nos dice que  $a \in H$ . Por otro lado,  $a \in H$  implica  $aH = H$ , así 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 tambien que  $H \trianglelefteq G$ . Entonces tome  $y \in G'$ . Pues entonces existe un  $x \in G$  tal que  $y = \phi(x)$ . Tambien 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 del Factor). Suponga que  $G$  y  $G'$  son grupos y  $H \trianglelefteq G$ . Sea  $\phi : G \rightarrow G'$  y  $\pi : G \rightarrow G/H$  dado por  $\pi : a \rightarrow aH$ . Enotnces 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 el 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  $\tilde{\phi}$  esta bien definida. Por ultimo, note que  $\tilde{\phi}(aH) = \tilde{\phi}(\pi(a)) = \tilde{\phi} \circ \pi(a)$ . ■

**Corolario.**  $\phi$  es sobre sí 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  $e_{G/H} = H$ . ■

## Lectura 5: Teoremas de Isomorfismo.

**Teorema 13** (Primer Teorema del Isomorfismo). *Sí  $\phi : G \rightarrow H$  es un homomorfismo con kernel  $K$ , entonces*

$$\phi(G) \simeq H/K$$

*Proof.* Por el teorema del factor, sea  $\tilde{\phi} : H/K \rightarrow H$ . Entonces  $\tilde{\phi}$  es un isomorfismo sí y solo sí  $\phi$  es sobre. Nota que  $\phi : G \rightarrow \phi(G)$  hace  $\phi$  sobre. ■

**Ejemplo 12.**  $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$ . Considere entonces  $\det : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$ , entonces  $\ker \det = SL(n, \mathbb{R})$ , así que por el primer teorema del isomorfismo,  $\det(GL(n, \mathbb{R})) = \mathbb{R}^* \simeq GL(n, \mathbb{R})/SL(n, \mathbb{R})$ .

**Definición.** Sea  $\{G_n\}$  una colección de grupos, y  $\{\phi_n\}$  una colección de homomorfismos de  $G_i \rightarrow G_{i+1}$ . Llamamos la secuencia  $\rightarrow G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} \dots \xrightarrow{\phi_{n-1}} G_n \xrightarrow{\phi_n} \dots$  una **secuencia exacta en un punto**  $G_i$  sí  $\phi_i(G_i) = \ker \pi_{i+1}$ . Llamamos la secuencia **exacta** sí es exacta en todo  $G_i$  para  $i \in \mathbb{Z}^+$ .

**Definición.** Una **secuencia exacta corta** es una secuencia exacta de la forma:

$$\langle e \rangle \xrightarrow{i} G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \xrightarrow{j} \langle e \rangle$$

Donde  $i : \langle e \rangle \rightarrow G_1$  es la inclusión y  $j : G_3 \rightarrow \langle e \rangle$  es la constante dado por  $j : g \rightarrow e$  para todo  $g \in G_3$ .

**Lema 14.** *Dada una secuencia exacta corta, tenemos que  $\phi_1$  es 1-1 y que  $\phi_2$  es sobre.*

*Proof.* De seguro, tenemos que  $i(\langle e \rangle) = \langle e \rangle = \ker \phi_1$  por definición, así que  $\phi_1$  es 1-1. Igualmente, tenemos que  $\phi_2(G_2) = \ker j = G_3$ , como  $j$  es la constante, así que  $\phi_2$  es sobre. ■

**Lema 15.** *Dada una secuencia exacta corta,  $\phi_1(G_1) \trianglelefteq G_2$  y  $G_2/\phi_1(G_1) \simeq G_3$ .*

*Proof.* Como  $\langle e \rangle \xrightarrow{i} G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \xrightarrow{j} \langle e \rangle$  es exacta corta, tenemos que  $\phi_1(G_1)$  es un kernel, así que  $\phi_1(G_1)$  es normal en  $G_2$ . Mas aún, por el primer teorema del isomorfismo, como  $\phi_2 : G_2 \rightarrow G_3$ , lo cual tiene kernel  $\phi_1(G_1)$ , y como  $\phi_2(G_2) = G_3$  tenemos que

$$G_2/\phi_1(G_1) \simeq G_3$$

■

**Teorema 16** (Segundo Teorema del Isomorfismo). *Sí  $G$  es un grupo con  $H \leq G$  un subgrupo, y  $N \trianglelefteq G$  un subgrupo normal en  $G$ , entonces:*

$$HN/N \simeq H/H \cap N$$

**Teorema 17** (Tercer Teorema del Isomorfismo). *Sí  $G$  es un grupo, y  $H, N \trianglelefteq G$  subgrupos normales en  $G$ , con  $N \leq H$ , entonces*

$$(G/N)/(H/N) \simeq G/H$$

**Ejemplo 13.** Nota que  $8\mathbb{Z} \leq 4\mathbb{Z}$ , así que  $4\mathbb{Z}/8\mathbb{Z} = \{8\mathbb{Z}, 4 + 8\mathbb{Z}\}$ . De igual forma,  $\mathbb{Z}/8\mathbb{Z} = \{8\mathbb{Z}, 1 + 8\mathbb{Z}, 2 + 8\mathbb{Z}, 3 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 5 + 8\mathbb{Z}, 6 + 8\mathbb{Z}, 7 + 8\mathbb{Z}\}$ . Entonces vemos que

$$(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z}) = \{4\mathbb{Z}/8\mathbb{Z}, (1 + 8\mathbb{Z}) + 4\mathbb{Z}/8\mathbb{Z}, (2 + 8\mathbb{Z}) + 4\mathbb{Z}/8\mathbb{Z}, (3 + 8\mathbb{Z}) + 4\mathbb{Z}/8\mathbb{Z}\}$$

Nota que  $(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z})$  es cíclico de 4 elementos, así que  $(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z}) \simeq \mathbb{Z}/4\mathbb{Z}$ , con acuerdo a la tercer teorema del isomorfismo.

**Teorema 18** (Teorema de la Correspondencia). *Sea  $\phi : G \rightarrow G'$  u homomorfismo de  $G$  sobre  $G'$  con kernel  $K$ . Sí  $H' \leq G'$ , y  $\phi^{-1}(H') = H$ , entonces  $H \leq G$ ,  $K \trianglelefteq H$ , y  $H/K \simeq H'$ .*

*Proof.* Tenemos que  $e \in H$ , como  $\phi(e) = e' \in H'$ . Ahora sí  $a, b \in H$ , entonces  $\phi(a), \phi(b) \in H'$ , así que  $\phi(ab^{-1}) \in H'$ , lo que hace  $ab^{-1} \in H$ . Por lo tanto  $H \leq G$ . Tambin tenemos que  $\phi(K) = \langle e' \rangle$ , lo que hace  $K \trianglelefteq H$ .

Ahora considere la mapa  $\phi' : H \rightarrow H'$  dado por  $\phi' : h \rightarrow \phi(h)$ . Entonces  $\phi'$  es sobre, por definición de  $H$ , y  $\ker \phi' = K$ . Por lo tanto el primer teorema del isomorfismo garantiza que  $H/K \simeq H'$ . ■

**Corolario.** *Sí  $H' \trianglelefteq G'$ , entonces  $H \trianglelefteq G$ .*

*Proof.* Sí  $H' \trianglelefteq G'$ , entonces como  $H = \phi^{-1}(H')$ , sí  $a \in G$  y  $h \in H$ , entonces por normalidad,  $\phi(a)\phi(h)\phi^{-1}(a) = \phi(aha^{-1}) \in H'$ , tenemos que  $aha^{-1} \in H$ . Esto hace  $H \trianglelefteq G$ . ■

**Ejemplo 14.** Sea  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/24\mathbb{Z}$ . Los subgrupos de  $\mathbb{Z}/24\mathbb{Z}$  y  $\mathbb{Z}$  estan desplegados en los siguientes reticulos del figura 1. Nota, que en el reticulo de  $\mathbb{Z}$ , se reproduce el reticulo de  $\mathbb{Z}/24\mathbb{Z}$ . Así que  $\mathbb{Z}/24\mathbb{Z}$  tiene subreticulo en el reticulo de  $\mathbb{Z}$ , desplegado por el figura 2.

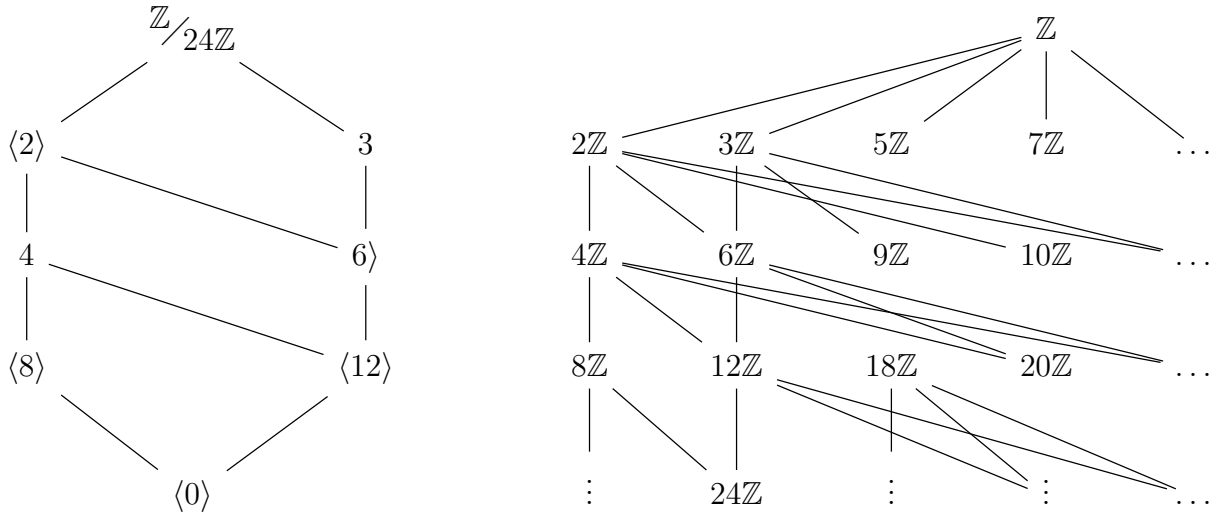


Figure 1: El reticulo de subgrupos de  $\mathbb{Z}/24\mathbb{Z}$  al lado del reticulo de subgrupos de  $\mathbb{Z}$ .

## Lectura 6: Sumas Directas y Productos Semidirectas.

**Definición.** Dado grupos  $G$  y  $H$ , definimos el **producto directo** de  $G$  y  $H$  de ser el grupo  $G \times H$  bajo la operacion  $((a, b), (g, h)) \rightarrow (ah, bg)$ .

**Lema 19.** Sean  $G$  y  $H$  grupos, entonces el producto directo de  $G$  y  $H$  es un grupo bajo su operación.

**Ejemplo 15.** (1) El grupo Klein-4 es un producto directo,  $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

$$(2) \quad \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

$$(3) \quad \mathbb{Z}/70\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

**Lema 20.** Si  $G \times H$  es un producto directo, entonces  $G \times H$  contine subgrupos  $G'$  y  $H'$  con  $G' \simeq G$  y  $H' \simeq H$ .

*Proof.* Sea  $G' = \{(g, e_H) : g \in G\}$  y  $H' = \{(e_G, h) : h \in H\}$ . Considere entonces las proyecciones del primer y segundo partes,  $\pi_1 : G \times H \rightarrow G$  y  $\pi_2 : G \times H \rightarrow H$  dados por  $\pi_1 : (g, e_H) \rightarrow g$  y  $\pi_2 : (e_G, h) \rightarrow h$ . Entonces  $\pi_1$  y  $\pi_2$  son isomorfismos. ■

**Corolario.**  $G'$  y  $H'$  son normales en  $G \times H$ .

**Corolario.**  $G'H' = G \times H$  y  $G' \cap H' = \langle e \rangle$ , donde  $e = (e_G, e_H)$  es la identidad de  $G \times H$ .

**Definición.** Decimos que  $G$  es un **producto directo interior** si existen subgrupos  $G'$  y  $H'$  tales que:

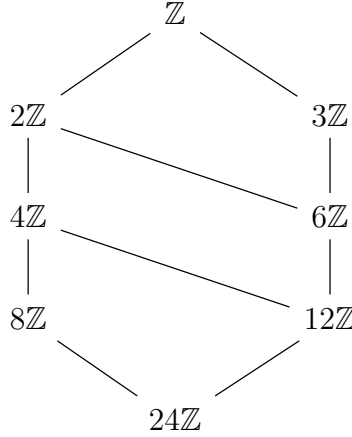


Figure 2:  $\mathbb{Z}/24\mathbb{Z}$  como subreticulo del reticulo de  $\mathbb{Z}$ .

- (1)  $G'$  y  $H'$  son normales en  $G$ .
- (2)  $G' \cap H' = \langle e \rangle$ .
- (3)  $G'H' = G$ .

**Teorema 21.** *Sí  $G = HK$  es un grupo donde  $H, K \leq G$ , entonces  $G \simeq H \times K$ .*

*Proof.* Defina  $\phi : H \times K \rightarrow HK$  pro  $(h, k) \rightarrow hk$ . Nota que  $h \in H$  y  $k \in K$  implica que  $hk = kh$ . Sí  $(h^{-1}k^{-1}h)K \in K$  y  $h^{-1}(k^{-1}hk) \in H$ , entonces  $h^{-1}k^{-1}hk \in H \cap K = \langle e \rangle$ . Nota que sí  $(h_1, k_1)$  y  $(h_2, k_2) \in H \times K$ , entonces  $\phi((h_1, k_1), (h_2, k_2)) = (h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$ . Entonces  $\phi$  es un homomorfismo

Ahora suponga que  $\phi(h, k) = e$ . Entonces  $hk = e$ , así loq que dice que  $h \in K$  y  $k \in H$ , entonces  $h = k = e$ . Por lo tanto  $\ker \phi = \langle e \rangle$ . Mas aún,  $\phi$  es sobre por definición, así que  $HK \simeq H \times K$ . ■

**Definición.** Sí  $G$  es un grupo que contiene subgrupos normales  $\{H_i\}_{i=1}^n$ , y  $g \in G$  se puede escribir unicamente como  $g = h_1 \dots h_n$ , donde  $h_i$ , entonces se llama  $G$  el **producto directo interno** de  $\{H_i\}$ .

**Lema 22.** *Suponga que  $H = H_1 \dots H_n$  donde  $H_i \trianglelefteq G$  para toda  $1 \leq i \leq n$ . Los siguientes enunicados son equivalente:*

- (1)  $G$  es producto directo interno de  $\{H_i\}$ .
- (2)  $(H_1 \dots H_{i-1}) \cap H_i = \langle e \rangle$  para todo  $1 \leq i \leq n$ .

*Proof.* Supong que  $G$  es producto directo interno de  $\{H_i\}$ . Entonces, para todo  $g \in G$ ,  $g = h_1 \dots h_n$ . Sea que  $g \in (H_1 \dots H_{i-1}) \cap$

$H_i$ . Entonces  $g \in H_1 \dots H_{i-1}$ , entonces  $g = h_1 \dots h_{i-1} e_{i-1} e_{i-2} \dots e_1$ . Ahora tambien tenemos que  $g \in H_i$ , así que  $g = e_1 \dots e_{i-1} g e_{i-1} \dots e_1$ . Como  $g$  es de representacion unica,  $h_1 \dots h_{i-1} e_{i-1} \dots e_1 = e_1 e_2 \dots g e_{i+1} \dots e_n$ . Por correspondencia, tenemos que  $g = e$ . Por lo tanto  $(H_1 \dots H_{i-1}) \cap H_i = \langle e \rangle$ .

Suponga ahora que  $(H_1 \dots H_{i-1}) \cap H_i = \langle e \rangle$ . Suponga que  $g = h_1 \dots h_{i-1} \in (H_1 \dots H_{i-1})$  y  $g = k_1 \dots k_n \in H_i$ . Como  $H_i \trianglelefteq G$ , tenemos que  $h_i k_i = k_i h_i$ . Por lo tanto, como  $h_1 \dots h_n = k_1 \dots k_n$ . Entonces tenemos  $h_2 \dots h_n = (h_1^{-1} k_1) k_2 \dots k_n$ , y que  $h_3 \dots h_n = (h_1^{-1} k_1) (h_2^{-1} k_2) k_3 \dots k_n$ . Procediendo recursivamente, tenemos que  $(h_1^{-1} k_1) \dots (h_{n-1}^{-1} k_{n-1}) = h_n k_n^{-1}$ , y como  $h_n k_n^{-1} \in H_n \cap (H_1 \dots H_{n-1})$ , tenemos que  $h_i^{-1} k_i = e$  para todo  $i$ . Por lo tanto  $h_i = k_i$  y  $g$  tiene representación unica. Como  $G = H_1 \dots H_n$ , esto hace  $G$  el producto directo interno de  $\{H_i\}$ . ■

**Ejemplo 16.**  $D_3 = \langle r \rangle \langle t \rangle$  y es una representacion unica, pero  $\text{ord} \langle r \rangle = 3$  y  $\text{ord} \langle t \rangle = 2$ , pero  $D_3$  no es abeliano, así que  $D_3$  no puede ser el producto directo interno de  $\langle r \rangle$  y  $\langle t \rangle$ .

**Definición.** Sea  $G$  un grupo, definimos a  $\text{Aut } G$  el **grupo de automorfismos** de  $G$  sobre si mismo.

**Lema 23.** Sean  $H, K$  grupos, y sea  $r : K \rightarrow \text{Aut } H$  dado por  $k \xrightarrow{r} r_k$  y  $r_k : H \rightarrow H$  es un autmorfismo de  $H$ . Considere la operacion bianria  $(H \times K) \times (H \times K) \rightarrow H \times K$  dado por  $(h_1, k_1), (h_2, k_2) \rightarrow (h_1 r_k(h_2), k_1 k_2)$ . Esta operación induce un grupo sobre  $H \times K$ .

*Proof.* Como  $r_k$  es un automorfismo de  $H$ , es un homomorfismo, así que tenemos que  $r(kn) = r_k n = r_k r_n = r(k) r(n)$ , así que  $r$  es un homorfismo, y se cierra la operación en  $H \times K$ .

Ahora nota que  $(h, k)(e_H, e_K) = (h r_k(e_H), k e_K) = (h e_H, k e_K) = (h, k)$  y  $(e_H, e_K)(h, k) = (e_H r_{e_K}(h), e_K k) = (e_H h, e_K k) = (h, k)$ , como  $r_{e_H}$  es la identidad. Así que  $e = (e_H, e_K)$  es la identidad.

De igual manera, tenemos  $(h, k)(r_k^{-1}(h^{-1}), k^{-1}) = (h r_k(r_k^{-1}(h^{-1})), k k^{-1}) = (h h^{-1}, k k^{-1}) = e$ , y  $(r_k^{-1}(h^{-1}), k^{-1})(h, k) = (r_k^{-1}(h^{-1}) r_h(h), k^{-1} k) = (r_{e_H}(h^{-1}), k^{-1} k) = (h^{-1} h, k^{-1} k) = e$ , com  $r_k^{-1} r_k = r_{e_H}$ , la identidad. Así que  $H \times K$  tiene inversos.

Finalmente, nota que

$$\begin{aligned} ((h_1, k_1)(h_2, k_2))(h_3, k_3) &= (h_1 r_{k_1}(h_2), k_1 k_2)(h_3, k_3) \\ &= ((h_1 r_{k_1}(h_2)) r_{k_3}(h_3), k_1 k_2 k_3) \\ &= (h_1 h_2 r_{k_1 k_3}(h_3), k_1 k_2 k_3) \end{aligned}$$



$$\begin{aligned}
(h_1, k_1)((h_2, k_2)(h_3, k_3)) &= (h_1, k_1)(h_2 r_{k_3}(h_3), k_2 k_3) \\
&= (h_1 h_2 r_{k_1 k_3}(h_3), k_1 k_2 k_3)
\end{aligned}$$

y asociatividad se preserva. ■

**Definición.** Sea  $H, K$  grupos, y  $r : K \rightarrow \text{Aut } H$  un homomorfismo. Definimos el **producto semidirecto externo** de ser el grupo  $H \times_r K$  bajo la operación  $(h_1, k_1)(h_2, k_2) = (h_1 r_{k_1}(h_2), k_1 k_2)$ .

**Ejemplo 17.** (1)  $D_3 \simeq \langle r \rangle \times_r \langle t \rangle \simeq \mathbb{Z}/3\mathbb{Z} \times_r \mathbb{Z}/2\mathbb{Z}$ , donde  $r : x \rightarrow -x$ . En ambos grupos.

(2) Sea  $G = H \times_r K$ . Sea  $H' = \{(h, e_K), h \in H\}$  y  $K' = \{(e_H, k) : k \in K\}$ . Nota que  $H' \simeq H$ , que  $K' \simeq K$ , y que  $H' \trianglelefteq H \times_r K$ , pero no necesariamente  $K' \trianglelefteq H \times_r K$ . Tambien tenemos que  $H' \cap K' = \langle e \rangle$ . Ahora,  $(h, e_K)(e_H, k) = (hr_{e_H}(e_H), e_K k) = (he_H, e_K k) = (h, k)$ , así que  $H \times_r K = H'K'$ .

**Definición.** Sea  $G$  un grupo, y  $H \trianglelefteq G$  y  $K \leq G$ . Decimos que  $G$  es el **producto semidirecto interno** sí  $G = HK$  y  $H \cap K = \langle e \rangle$ . Lo denotamos como  $G = H \rtimes K$ .

**Ejemplo 18.**  $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \langle r \rangle \rtimes \langle t \rangle$ . Nota que  $\langle r \rangle \trianglelefteq D_n$  y que  $[D_n, \langle r \rangle] = 2$ .

**Lema 24.** Suponga que  $G$  es un grupo semidirecto interno de  $H \trianglelefteq G$ , y  $K \leq G$ . Entonces  $G \simeq H \times_r K$ , donde  $r : K \rightarrow \text{Aut } H$  esta dado por  $r_k : h \rightarrow khk^{-1}$ .

*Proof.* Note que  $r_k$  es un automorfismo de  $H$ , como  $H \trianglelefteq G$  así que  $r$  esta bien definida. Por la lemma 22, todo  $g \in G$  se escribe unicamenet como  $hk$ . Por lo tanto, sea  $\phi : H \times_r K \rightarrow G$  dado por  $(h, k) \rightarrow hk$ . Vemos que  $\phi$  es 1-1, y que es sobre.

Ahora dado  $(h, k)$  y  $(h', k')$ , tenemos que  $\phi((h, k)(h', k')) = \phi(hr_k(h'), kk') = \phi(hkhk^{-1}, kk') = (hkh'k^{-1})(kk') = (hk)(h'k') = \phi(h, k)\phi(h', k')$ . Por lo tanto  $\phi$  es un isomorfismo y terminamos. ■

**Lema 25.** Sea  $G$  un grupo y  $H, K \leq G$ . Suponga que  $G = HK$ , y que  $H \cap K = \langle e \rangle$ . Entonces para todo  $g \in G$ , se puede escribir de manera unica de la forma  $g = hk$  donde  $h \in H$  y  $k \in K$ .

## Lectura 7: Acciones de Grupos.

**Teorema 26** (EL Teorema de Cayley). *Todo grupo es isomorfo a un subgrupo del grupo de simetrico.*

*Proof.* Sea  $G$  un grupo y  $A(G)$  el grupo simetrico de  $G$ . Definia  $\lambda : G \rightarrow A(G)$  dado por  $g \rightarrow \lambda_g$ , donde  $\lambda_g : G \rightarrow G$  esta dado por  $x \rightarrow gx$ . Note que  $\lambda_g$  es un permutacion de los elementos de  $G$ , es sobre, y es 1-1 por cancelacion, así que  $\lambda_g \in A(G)$ . Así que  $\lambda$  es bien definido.

Ahora suponga que que  $\lambda(g) = \lambda(h)$ , entonces para algún  $x \in G$ ,  $\lambda_g(x) = \lambda_h(x)$ , pues  $gx = hx$ . Por cancelación, tenemos que  $g = h$ . sí que  $\lambda$  es 1-1. Ahora dado  $x \in G$ , que  $(gh)(x) = \lambda_{gh}(x) = (gh)x = g(hx) = g(\lambda_h(x)) = \lambda_g(\lambda_h(x)) = \lambda_g \lambda_h(x)$ . Así que  $\lambda$  definia una isomorfismo de  $G$  hacia  $\lambda(G)$  lo cual es subgrupo de  $A(G)$ . ■

**Ejemplo 19.** Por la teorema de Cayley, tenemos que  $D_3 \simeq S_6$ .

**Definición.** Un grupo  $G$  **actua** sobre un conjunto  $X$  sí para todo  $g \in G$ , existe una mapa  $G \times X \rightarrow X$  dado por  $(g, x) \rightarrow g \cdot x$  tal que:

- (1)  $h \cdot (g \cdot x) = (hg) \cdot x$ .
- (2)  $e \cdot x = x$  para todo  $x \in X$ .

**Ejemplo 20.** (1) Todo grupo actua sobre si mismo bajo multiplicacion pr la izquierda. Llamamos esto el **accion regular**.

- (2) Todo grupo actua sobre si mismo via la accion de **conjugacion** definido pro  $(g, x) \rightarrow gxg^{-1}$ . Nota que  $h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1} = (hg) \cdot x$ . Tambein  $e \cdot x = exe^{-1} = x$ .

**Definición.** Definimos el **kernel** de una accion  $G \times X \rightarrow X$  de ser el conjunto  $= \{g \in G : g \cdot x = x\}$ .

**Ejemplo 21.** (1) Sí  $G$  actua sobre si mismo via conjugacion, entonces si  $gxg^{-1} = x$ , tenemos que  $gx = xg$  para todo  $x \in G$ . Por lo tanto  $\ker = \{g \in G : gx = xg \text{ para todo } x \in G\}$ . Llamamos este kernel el **centro** de  $G$ , y lo denotamos como  $Z(G)$ .

- (2) Conisdere  $\mathcal{B}_n$  el conjunto de todos funciones booleanas  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  en  $n$  variables. Defina una operacion de  $S_n$  sobre  $\mathcal{B}_n$  definida por  $s \cdot f(x_1, \dots, x_n) = f(x_{s(1)}, \dots, x_{s(n)})$ . Este operación definia una acción de grupos de  $S_n$  sobre  $\mathcal{B}_n$ . Nota que el kernel de este accion es trivial.

**Definición.** Sea  $G$  un grupo que actúa sobre un conjunto  $X$ . La **órbita** de un  $x \in X$  es el conjunto  $\mathcal{O}(x) = \{g \cdot x : g \in G\}$ .

**Ejemplo 22.** (1) Sea  $G$  un grupo actuando sobre si mismo por su multiplicación (por izquierda). Suponga que  $x \in G$  y sea  $g \in G$  un elemento cualquiera. Entonces existe un  $g_0 \in G$  tal que  $g = g_0x$ . Esto hace  $G \subseteq \mathcal{O}(x)$ . Por lo tanto  $\mathcal{O}(x) = G$ .

(2) Considere un grupo  $G$  actuando sobre si mismo mediante conjugación. Sea  $x \in G$ . Entonces  $\mathcal{O}(x) = \{gxg^{-1} : g \in G\} = \text{cl } x$ . Llamamos a  $\text{cl } x$  la **clase de conjugación** de  $x$ .

(3) Considere  $\mathcal{B}_3$  y defina  $f(x_1, x_2, x_3) = x_1 + x_2x_3 + x_1x_2x_3$ . Sea  $S_3 = \{(1), (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)\}$ . Entonces:

$$\begin{aligned} (1) \cdot f &= x_1 + x_2x_3 + x_1x_2x_3 = f \\ (2\ 3) \cdot f &= x_1 + x_3x_2 + x_1x_3x_2 = f \\ (1\ 2) \cdot f &= x_2 + x_1x_3 + x_2x_1x_3 = f_1 \\ (1\ 2\ 3) \cdot f &= x_2 + x_3x_1 + x_3x_2x_1 = f_1 \\ (1\ 3\ 2) \cdot f &= x_3 + x_1x_2 + x_3x_1x_2 = f_2 \\ (1\ 3) \cdot f &= x_3 + x_2x_1 + x_3x_2x_1 = f_2 \end{aligned}$$

Así que  $\mathcal{O}(f) = \{f, f_1, f_2\}$ . Nota que  $|\mathcal{O}(x)|$  divide a  $\text{ord } S_3$ .

**Lema 27.** Sea  $G$  un grupo que actúa sobre un conjunto  $X$ . Entonces las órbitas de  $X$  particionan a  $X$ .

*Proof.* Sea  $x \in \mathcal{O}(y)$  y  $x \in \mathcal{O}(z)$  para  $x, y, z \in X$ . Entonces vemos que  $x = gy$  y  $x = hz$ , por lo tanto  $gy = hz$ . Es decir  $y = (g^{-1}h)z$ , por lo tanto  $y \in \mathcal{O}(z)$ . De igual forma,  $z \in \mathcal{O}(y)$ . Esto hace que  $\mathcal{O}(y) = \mathcal{O}(z)$ . ■

**Definición.** Sea  $G$  un grupo actuando sobre un conjunto  $X$ . El **estabilizador** de  $x \in X$  es el conjunto  $\text{stab } x = \{g \in G : g \cdot x = x\}$ .

**Lema 28.** Sea  $G$  un grupo que actúa sobre un conjunto  $X$ . Entonces el estabilizador de todo  $x_1X$  es subgrupo de  $G$ .

*Proof.* Sea  $x \in X$  y sea  $g, h \in \text{stab } x$ . Entonces  $x = gx$  y  $x = h^{-1}x$ . Por lo tanto  $(gh^{-1}) \cdot x = x$ . ■

**Ejemplo 23.** Para cualquier grupo actuando sobre si mismo bajo conjugacion,  $\text{stab } x = \{g : gx = xg\} = C(x)$  que se llama el **centralizador** de  $x$ .

**Teorema 29** (Teorema del Órbita-Estabilizador.). *Suponga que  $G$  es un grupo que actua sobre un conjunto  $X$ . Sean  $\mathcal{O}(x)$  y  $\text{stab } x$  la órbita y estabilizador de un  $x \in X$ . Entonces:*

$$|\mathcal{O}(x)| = [G : \text{stab } x]$$

*Proof.* Suponga que  $y \in \mathcal{O}(x)$ . Entonces  $y = g \cdot x$  para algún  $g \in G$ . Defina ahora la mapa  $f : \mathcal{O}(x) \rightarrow G/\text{stab } x$  dado por  $y = g \cdot x \rightarrow g \text{stab } x$ . Sea ahora  $y = g \cdot x = h \cdot x$ . Entonces vemos que  $x = (g^{-1}h) \cdot x$ , así que  $g^{-1}h \in \text{stab } x$ . Esto hace que  $g \text{stab } x = h \text{stab } x$ . Por lo tanto  $f$  es bien definida.

Ahora, vemos que  $f$  es sobre; sí  $y \in \mathcal{O}(x)$ , entonces  $y = g \cdot x$  para algún  $g \in G$ , así que a cada  $y \in \mathcal{O}(x)$  está asignada a un  $g \text{stab } x$ . Más aun,  $f$  es 1-1. Sean  $y = gx$  y  $y' = hx$ . Sí  $g \text{stab } x = h \text{stab } x$ , entonces  $g^{-1}h \in \text{stab } x$ , así que  $gx = hx$ , es decir  $y = y'$ . Por lo tanto, tenemos una mapa 1-1 de  $\mathcal{O}(x)$  sobre el conjunto  $G/\text{stab } x$ , que tiene cardinalidad  $[G : \text{stab } x]$ . ■

**Corolario.** *Sí  $G$  es un grupo finito, entonces  $|\mathcal{O}(x)|$  divide a  $\text{ord } G$ . En particular*

$$|\mathcal{O}(x)| = \frac{\text{ord } G}{\text{ord } (\text{stab } x)}$$

**Ejemplo 24.** Sea  $G$  un grupo finito y sea la accion de  $G$  sobre si mismo la conjugacion. Entonces  $\mathcal{O}(x) = \text{cl } x$ . Nota que  $x \in \text{cl } x$ . Suponga que  $|\text{cl } x| = 1$ , entonces  $gxg^{-1} = x$  asi que  $gx = xg$  lo que hace  $x \in Z(G)$ . Nota igualmente que  $G = \bigcup \text{cl } x$ . Entonces

$$\text{ord } G = \sum \text{cl } x = \text{ord } Z(G) + \sum [G : C(x)] = \text{ord } Z(G) + \sum \text{cl } x$$

Llamamos a esta equacion la **ecuacion de clase**.

**Teorema 30** (Conteo de Órbitas). *Sea  $G$  un grupo finito que actua sobre un conjunto finitio  $X$ . Denota  $X^g = \{x \in X : g \cdot x = x\}$ . Sea  $\mathcal{O}$  la colleccion de todas las orbitas de  $x \in X$ . Entonces:*

$$|\mathcal{O}| = \frac{1}{\text{ord } G} \sum |X^g|$$

*Proof.* Sabemos que  $X^g = \{(g, x) \in G \times X : g \cdot x = x\}$ . Sea:

$$\begin{array}{ccccccc} (g_1, x_1) & & (g_1, x_3) & & (g_1, x_4) & & \\ & (g_2, x_2) & & (g_2, x_3) & & & (g_2, x_5) \\ (g_3, x_1) & & (g_3, x_3) & & (g_3, x_4) & & \dots \\ \vdots & & & & & & \end{array}$$

Nota que las columnas de este arreglo forman los estabilizadores de los  $x_i$ , ahora vemos que

$$\sum |X^g| = \sum \text{stab } x = \sum \frac{\text{ord } G}{|\mathcal{O}(x)|}$$

Por el teorema del órbiata estabilizador, tenemos que

$$\text{ord } G \sum \frac{1}{|\mathcal{O}(x)|} = \text{ord } G \sum_{\mathcal{O}(x) \in \mathcal{O}} \sum_x |\mathcal{O}(x)| = \text{ord } G |\mathcal{O}|$$

Rearreglando los terminos, tenemos el resultado. ■

## Lectura 8: Las Teoremas de Sylow

**Definición.** Sea  $p \in \mathbb{Z}^+$  un primo. Llamamos a un grupo  $G$  un  **$p$ -grupo** sí cada  $g \in G$  es una potencia de  $p$ .

**Ejemplo 25.** (1) El grupo Klein  $V_4 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  es un 2-grupo.

(2) Los grupos  $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  y  $D_{16}$  son 2-grupos.

(3) El grupo  $\bigoplus_{n=1}^{\infty} \mathbb{Z}/5^n\mathbb{Z}$  es un 5-grupo, pero  $\prod_{n=1}^{\infty} \mathbb{Z}/5^n\mathbb{Z}$  solo es un 5-grupo cuando  $n = 1$ .

**Definición.** Sí  $G$  es un grupo con orden  $p^r m$  donde  $p$  es primo y  $p \nmid m$ , entonces llamamos un subgrupo  $P \leq G$  un  **$p$ -subgrupo de Sylow**, o un  **$p$ -Sylow** sí  $\text{ord } P = p^r$ .

**Lema 31.** Sí  $G$  es un grupo de orden  $p^r m$  con  $p$  primo, y  $p \nmid m$  y  $P \leq G$  es un  $p$ -Sylow de  $G$ , entonces  $P$  es de orden lo máximo posible.

*Proof.* Por el teorema de Lagrange. ■

**Ejemplo 26.**  $|D_6| = 2^2 \cdot 3$ . Nota que  $P_1 = \{e, r^3, tr^3t\}$ ,  $P_2 = \{e, r^3, rt, r^4t\}$ , y  $P_3 = \{e, r^3, r^2t, r^5t\}$  son 2-Sylows de  $D_6$  y  $P = \{e, r, r^4\}$  es 3-Sylow.

**Lema 32.** *Sí  $n = p^r m$  con  $p$  primo y  $p \nmid m$ , entonces*

$$\binom{n}{p^r} \equiv m \pmod{p}$$

*Proof.* Nota que  $(x+1)^{p^r} = \sum_{k=1}^{p^r} \binom{p^r}{k} x^{p^r-k} \equiv x^{p^r m} + 1 \pmod{p}$ . Entonces  $(x+1)^{p^r m} \equiv (x^{p^r} + 1)^m \pmod{p}$ , así que

$$\sum \binom{p^r m}{k} x^{p^r m - k} \equiv \sum \binom{m}{k} (x^{p^r})^{m-k} \pmod{p}$$

Mirando el coeficiente de  $x^{p^r}$ , en la izquierda, tenemos que este término ocurre cuando  $k = p^r(m-1)$ , y obtenemos  $\binom{p^r m}{p^r} = \binom{n}{p^r}$ . Por el lado derecho, el término  $x^{p^r}$  ocurre cuando  $k = m-1$  y por simetría obtenemos  $\binom{m}{1} = m$ . ■

**Teorema 33** (El Primer Teorema de Sylow). *Sea  $G$  un grupo finito de orden  $p^r m$  donde  $p$  es primo, y  $p \nmid m$ . Entonces existe al menos un  $p$ -subgrupo de Sylow, de  $G$ .*

*Proof.* Sea  $X = \binom{G}{p^r}$ . Note que  $G$  actúa sobre  $X$  vía la multiplicación por la izquierda. Ahora, esta acción induce en  $X$  una partición de  $X$  en órbitas. Es decir

$$\binom{G}{p^r} = \bigcup \mathcal{O}(S)$$

entonces  $p \nmid \sum |\mathcal{O}(S)|$ . Por lo tanto, existe un  $S \in X$  con  $p \nmid |\mathcal{O}(S)|$ . Sea  $P = \text{stab } S$ . Entonces por el teorema del órbita-estabilizador, tenemos

$$|\mathcal{O}(S)| = \frac{\text{ord } G}{\text{ord } P} = \frac{p^r m}{\text{ord } P}$$

Como  $p \nmid |\mathcal{O}(S)|$ ,  $\text{ord } P$  tiene que ser un múltiplo de  $p^r$ , es decir que  $p^r \mid \text{ord } P$ , por lo tanto  $p^r \leq \text{ord } P$ .

Por otro lado, defina la mapa  $\lambda_x : P \rightarrow S$ , para  $x \in S$  dado por  $\lambda_x : g \rightarrow \lambda_x(g) = g \cdot x$ . Vemos que esta mapa es bien definida, y que es 1-1. Por lo tanto  $\text{ord } P \leq |S| = p^r$ . Por lo tanto  $P$  es un  $p$ -subgrupo de Sylow. ■