



INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICA

ÁLGEBRA MODERNA I

Apuntes Álgebra Moderna I

Profesor:

Escobar Gracia Cé-
sar Alberto

Alumnos:

Ramírez León Christian Yael
Silva Sierra Joshua Joaquín

5FM1

27 de diciembre de 2025

Índice general

1. Conceptos Previos	1
1.1. Divisibilidad	1
1.2. Cardinalidad de conjuntos	2
1.3. Enteros Módulo n	4
1.4. Función φ de Euler	4
2. Grupos	7
2.1. Grupos	7
2.2. Subgrupos	10
2.3. Grupo de permutaciones	14
2.4. Grupo Cociente	16
2.4.1. Producto de subgrupos	16
2.4.2. Clases laterales	16
2.4.3. Grupo cociente	23
3. Isomorfismos de Grupos	25
4. Productos Directos	27
4.1. Productos Directos	27
4.2. El grupo Simétrico S_n	32
5. Acciones de Grupos	47
5.1. Acciones de Grupo	47
5.2. Grupos Sylow	58
6. Automorfismos de Grupos	65
6.1. Automorfismos de Grupos	65

CAPÍTULO 1

Conceptos Previos

1.1. Divisibilidad

Definición 1.1.1 (Divisibilidad). *Sean $a, b \in \mathbb{Z}$, con $a \neq 0$, se dice que $a|b$ si $\exists k \in \mathbb{Z}$ tal que $b = ak$.*

Definición 1.1.2 (Máximo Común Divisor). *Sea $a, b \in \mathbb{Z}$, al menos uno distinto de cero, definimos a $d \in \mathbb{Z}$ un máximo común divisor de a y b , denotado por (a, b) , si cumple:*

- I) $d > 0$.
- II) $d|a$ y $d|b$.
- III) Si $c|a$ y $c|b$, entonces $c|d$.

Proposición 1.1.1 (Propiedades de la Divisibilidad). *Sean $a, b, c \in \mathbb{Z}$, con $a, b \neq 0$, entonces:*

- I) Si $a|b$ y $b|c$, entonces $a|c$.
- II) Si $a|b$ y $a|c$, entonces $a|(b + c)$.
- III) Si $a|b$, entonces $a|bk$ para todo $k \in \mathbb{Z}$.
- IV) Si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$.
- V) Si $a|b$ y $b|a$, entonces $a = \pm b$.
- VI) Si $a|b$, entonces $(a, b) = |a|$.
- VII) Si $c|a$ y $c|b$, entonces $c = ax + by$ para algunos $x, y \in \mathbb{Z}$.

Proposición 1.1.2. *Sea $a, b \in \mathbb{Z}$, al menos uno distinto de cero, entonces existe un único máximo común divisor de a y b .*

Teorema 1.1.1 (Algoritmo de la división). *Sean $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen únicos $q, r \in \mathbb{Z}$ tales que:*

$$a = bq + r, \quad 0 \leq r < |b|.$$

1.2. Cardinalidad de conjuntos

Dado un conjunto A , se denotará su cardinalidad (número de elementos) como $|A|$. Si A es un conjunto finito, entonces $|A|$ es un número natural. Si A es infinito, entonces $|A| = \infty$.

Observación 1.1. *Sean A, B , conjuntos finitos, con $B \subseteq A$. Entonces:*

$$|A \setminus B| = |A| - |B|$$

En efecto, basta notar que $B \cup (A \setminus B) = A$ y que $B \cap (A \setminus B) = \emptyset$, luego $|A| = |B \cup (A \setminus B)| = |B| + |A \setminus B|$, así $|A \setminus B| = |A| - |B|$. \square

Observación 1.2. *Sean A y B dos conjuntos finitos, entonces:*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

En efecto, Sean A y B conjuntos finitos, note que:

$$A \cup B = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) \cup (A \cap B)$$

Además: $(A \setminus (A \cap B))$, $(B \setminus (A \cap B))$, $(A \cap B)$, son disjuntos, más aún:

$$\begin{aligned} |A \setminus (A \cap B)| &= |A| - |A \cap B| \\ |B \setminus (A \cap B)| &= |B| - |A \cap B| \end{aligned}$$

Así:

$$\begin{aligned} |A \cup B| &= |A \setminus (A \cap B)| + |B \setminus (A \cap B)| + |A \cap B| \\ &= |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| \\ &= |A| + |B| - |A \cap B| \end{aligned}$$

\square

Proposición 1.2.1 (Principio de inclusión exclusión). *Sean A_1, \dots, A_n conjuntos finitos, se tiene:*

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

Observación 1.3. Suponga que C_1 es la condición que cumplen los elementos A y C_2 los de B , i.e.:

$$\begin{aligned} A &= \{x \in \Omega : x \text{ cumple } C_1\} \\ B &= \{x \in \Omega : x \text{ cumple } C_2\} \end{aligned}$$

Denotemos $N(C_i)$ a la cantidad de elementos que cumplen C_i , $N(C_1, C_2)$ a los que cumplen ambas, $N(\bar{C}_i)$ a los que no cumplen y $N(\bar{C}_1, \bar{C}_2)$ los que no cumplen C_1 ni C_2 , entonces:

$$N(\bar{C}_1, \bar{C}_2) = |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2))$$

En efecto, Note que:

$$\begin{aligned} N(\bar{C}_1, \bar{C}_2) &= |A^c \cap B^c| = |(A \cup B)^c| = |\Omega \setminus (A \cup B)| = |\Omega| - |A \cup B| \\ &= |\Omega| - (|A| + |B| - |A \cap B|) \\ &= |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2)) \end{aligned}$$

□

Ejemplo 1.1. Sea $\Omega = \{x \in \mathbb{Z} : 1 \leq x \leq 1000\}$ ¿Cuántos enteros de estos no son divisibles por 3 o 5?

Sol. Consideremos:

$$\begin{aligned} C_1 &: x \text{ sea divisible por 3} \\ C_2 &: x \text{ sea divisible por 5} \end{aligned}$$

Así $N(C_1) = 333$, $N(C_2) = 200$, $N(C_1, C_2) = 66$.

Luego:

$$\begin{aligned} N(\bar{C}_1, \bar{C}_2) &= |\Omega| - (N(C_1) + N(C_2) - N(C_1, C_2)) \\ &= 1000 - (333 + 200 - 66) \\ &= 533 \end{aligned}$$

Sea A_1, \dots, A_n una colección finita de conjuntos finitos, definidos:

$$A_i = \{x \in \Omega : x \text{ cumplía } C_i\}, \quad C_i \text{ condición.}$$

Definamos de este modo:

$$\begin{aligned} S_1 &= N(C_1) + \dots + N(C_n) \\ S_2 &= N(C_1, C_2) + \dots + N(C_1, C_n) + N(C_2, C_3) + \dots + N(C_{n-1}, C_n) \\ &\vdots \\ S_i &= \sum_{1 \leq j_1 < \dots < j_i \leq n} N(C_{j_1}, \dots, C_{j_i}) \\ &\vdots \\ S_n &= N(C_1, \dots, C_n) \end{aligned}$$

Por el principio de inclusión exclusión generalizado:

$$N(\bar{C}_1, \dots, \bar{C}_n) = |\Omega| - (S_1 - S_2 + \dots + (-1)^{n-1} S_n)$$

1.3. Enteros Módulo n

Definición 1.3.1. Sea $n \in \mathbb{Z}$, $n > 1$, se define la relación de $a \sim b$ si y sólo si $n \mid (a - b)$, es decir, a es congruente con b módulo n .

Es fácil ver que esta es una relación de equivalencia en \mathbb{Z} . Ahora, definamos en el conjunto cociente (\mathbb{Z}/\sim) las siguientes operaciones:

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a + b} \\ \bar{a} \cdot \bar{b} &= \overline{a \cdot b}\end{aligned}$$

Con $a, b \in \mathbb{Z}$. Entonces las operaciones están bien definidas, i.e., no dependen del representante de clase.

En efecto, sea $\bar{a} = \bar{a}_1$, $\bar{b} = \bar{b}_1 \iff a \sim a_1$ y $b \sim b_1 \iff n \mid (a - a_1) \wedge n \mid (b - b_1)$.

Esto implica:

$$n \mid (a - a_1) + (b - b_1) = (a + b) - (a_1 + b_1) \iff (a + b) \sim (a_1 + b_1) \iff \overline{a + b} = \overline{a_1 + b_1}$$

Análogamente para el producto.

□

Al conjunto de clases de equivalencia módulo n junto con las operaciones definidas se les denotará por $\mathbb{Z}/n\mathbb{Z}$ o \mathbb{Z}_n .

1.4. Función φ de Euler

Definición 1.4.1 (Función φ de Euler). Definimos la función $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ como:

$$n \mapsto |\{a \in \mathbb{N} : (a, n) = 1 \wedge a \leq n\}|$$

Proposición 1.4.1. Sean $p, q \in \mathbb{Z}^+$ primos distintos:

- I) $\varphi(p) = p - 1$
- II) $\varphi(p^k) = p^{k-1}(p - 1)$, $k \in \mathbb{N}$
- III) $\varphi(p^k q^t) = \varphi(p^k) \cdot \varphi(q^t)$, $k, t \in \mathbb{N}$

Demostración.

I) Es evidente.

II) Sea $\Omega = \{x \in \mathbb{N} : x \leq p^k\}$, sea $a \in \Omega$ tal que $(a, p^k) \neq 1$.

Así $(a, p) \neq 1$, más aún $a = pl$ para algún $l \in \mathbb{N}$. Luego, como $a \in \Omega$, $a = pl \leq p^k$, por lo cual $l \leq p^{k-1}$. De este modo:

$$|\{a \in \Omega : p \mid a\}| = |\{a \in \Omega : a = pl, l \in \mathbb{N}\}| = |\{l \in \mathbb{N} : l \leq p^{k-1}\}| = p^{k-1}$$

Ahora:

$$\begin{aligned} \varphi(p^k) &= |\{a \in \Omega : (a, p^k) = 1\}| \\ &= |\Omega| - |\{a \in \Omega : p \mid a\}| \\ &= p^k - p^{k-1} = p^{k-1}(p - 1) \end{aligned}$$

III) Consideremos $\Omega = \{x \in \mathbb{N} : x \leq p^k q^t, k, t \in \mathbb{N}\}$, $A = \{a \in \Omega : p \mid a\}$ y $B = \{b \in \Omega : q \mid b\}$.

Ahora $A \cap B = \{a \in \Omega : p \mid a \wedge q \mid a\}$. Note que de manera análoga a ii), tenemos:

$$|A| = p^{k-1} q^t, \quad |B| = p^k q^{t-1}$$

Por otro lado si $a \in A \cap B$, tenemos $p \mid a \wedge q \mid a \implies \exists l \in \mathbb{N}$ tal que $a = pql$. Además como $pql = a \leq p^k q^t$, se sigue que $l \leq p^{k-1} q^{t-1}$, por lo cual:

$$|A \cap B| = p^{k-1} q^{t-1}$$

Por último, sabemos que $\varphi(p^k q^t) = |\{a \in \Omega : (a, p^k q^t) = 1\}|$. Por la proposición 1.2.1 tenemos:

$$\begin{aligned} \varphi(p^k q^t) &= |\Omega| - (|A| + |B| - |A \cap B|) \\ &= p^k q^t - p^{k-1} q^t - p^k q^{t-1} + p^{k-1} q^{t-1} \\ &= q^t (p^k - p^{k-1}) - q^{t-1} (p^k - p^{k-1}) \\ &= (p^k - p^{k-1})(q^t - q^{t-1}) \\ &= [p^{k-1}(p-1)][q^{t-1}(q-1)] \\ &= \varphi(p^k) \cdot \varphi(q^t) \end{aligned}$$

□

Proposición 1.4.2. Sean $p_1, \dots, p_n \in \mathbb{N}$ primos distintos, sean $k_1, \dots, k_n \in \mathbb{N} \cup \{0\}$:

$$\begin{aligned}\varphi(p_1^{k_1} \dots p_n^{k_n}) &= p_1^{k_1} \dots p_n^{k_n} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_n}\right) \\ &= \varphi(p_1^{k_1}) \dots \varphi(p_n^{k_n})\end{aligned}$$

Demostración.

Falta demostrar. □

Observación 1.4. Observe que dados $n, m \in \mathbb{N}$, tales que $(m, n) = 1$, entonces:

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

En efecto, Por el teorema fundamental de la aritmética, podemos expresar $n = p_1^{k_1} \dots p_l^{k_l}$, $m = q_1^{t_1} \dots q_r^{t_r}$, con $p_1, \dots, p_l, q_1, \dots, q_r \in \mathbb{N}$ primos distintos y $k_1, \dots, k_l, t_1, \dots, t_r \in \mathbb{N} \cup \{0\}$, así:

$$\begin{aligned}\varphi(n \cdot m) &= \varphi(p_1^{k_1} \dots p_l^{k_l} q_1^{t_1} \dots q_r^{t_r}) \\ &= \varphi(p_1^{k_1} \dots p_l^{k_l}) \cdot \varphi(q_1^{t_1} \dots q_r^{t_r}) \\ &= \varphi(n) \cdot \varphi(m)\end{aligned}$$

□

CAPÍTULO 2

Grupos

2.1. Grupos

Definición 2.1.1 (Grupo). *Un grupo es un conjunto no vacío G junto con una operación $\circ : G \times G \rightarrow G$, que satisface:*

- I) *font Asociatividad:* $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G$
- II) *font Elemento neutro:* $\exists e \in G : a \circ e = a \quad \forall a \in G$
- III) *font Inverso:* $\forall a \in G \quad \exists b \in G : a \circ b = e$

Se denota a esta estructura: (G, \circ, e) , en caso de no conocer la identidad (G, \circ) . Además, para facilitar la notación el inverso de a elemento de un grupo se denota como a^{-1} .

Ejemplo 2.1. *Sea \mathbb{Z} , y la suma usual en los números enteros, es claro que es un grupo.*

Ejemplo 2.2. $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +)$ son grupos.

Ejemplo 2.3. $(\mathbb{Z}/n\mathbb{Z}, +)$ es un grupo.

En efecto, Anteriormente se había probado que $+$ es cerrado y está bien definida $\bar{a} + \bar{b} = \overline{a + b}$.

I) $+$ es asociativa, pues:

$$\bar{a} + \overline{(b + c)} = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{(a + b)} + \bar{c}$$

II) Note que la identidad es $\bar{0}$, ya que:

$$\bar{a} + \bar{0} = \overline{a + 0} = \bar{a} \quad \forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}$$

III) Ahora dado $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, note que $a + (-a) = 0$, luego:

$$\begin{aligned}\overline{a + (-a)} &= \bar{0} \\ \bar{a} + \overline{(-a)} &= \bar{0}\end{aligned}$$

Así $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z} \quad \exists \overline{(-a)} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} + \overline{(-a)} = \bar{0}$.

□

Ejemplo 2.4. Sean A un conjunto no vacío, sea V un espacio vectorial, sea \mathcal{H} el conjunto de funciones $f : A \rightarrow V$, definamos la operación suma sobre \mathcal{H} como:

$$\begin{aligned}+ : \mathcal{H} \times \mathcal{H} &\rightarrow \mathcal{H} \\ (f + g)(a) &\mapsto f(a) + g(a) \quad \forall a \in A\end{aligned}$$

En efecto, note:

I) Sean $f, g, h \in \mathcal{H}$, sea $a \in A$:

$$\begin{aligned}[(f + g) + h](a) &= (f + g)(a) + h(a) \\ &= (f(a) + g(a)) + h(a) \\ &= f(a) + (g(a) + h(a)) \\ &= f(a) + (g + h)(a) \\ &= [f + (g + h)](a)\end{aligned}$$

$$\therefore (f + g) + h = f + (g + h)$$

II) Tenemos $\underline{0} \in \mathcal{H}$, definida por: $\underline{0}(a) = 0 \quad \forall a \in A$, sea $f \in \mathcal{H}$, sea $a \in A$,

$$(f + \underline{0})(a) = f(a) + \underline{0}(a) = f(a) + 0 = f(a)$$

Así $f + \underline{0} = f$, i.e. $\underline{0}$ es el elemento neutro.

III) Sea $f \in \mathcal{H}$, sea $a \in A$, note que existe $-f(a)$, tal que:

$$f(a) + (-f(a)) = 0 \quad \forall a \in A,$$

entonces $-f$ es inverso de f .

□

Ejemplo 2.5. Sea V un espacio vectorial real, entonces $(V, +)$ es un grupo.

Ejemplo 2.6. $(\mathcal{M}_{m \times n}(\mathbb{R}), +)$ es un grupo.

Ejemplo 2.7. Sea $GL_{(n)}(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : \det(A) \neq 0\}$, con el producto de matrices forma un grupo.

Ejemplo 2.8. Considera $\mathbb{Z}/n\mathbb{Z}$, sea $G \subseteq \mathbb{Z}/n\mathbb{Z}$, el conjunto

$$G = \{\bar{a} : (a, n) = 1\}$$

entonces (G, \cdot) con la op. definida por el producto de clases es un grupo.

En efecto, Note:

I) $\forall \bar{a}, \bar{b}, \bar{c} \in G, \quad \bar{a}(\bar{b} \cdot \bar{c}) = \bar{a}(\overline{\bar{b} \cdot \bar{c}}) = \overline{\bar{a}(\bar{b} \cdot \bar{c})} = \overline{(\bar{a}\bar{b})\bar{c}} = (\bar{a}\bar{b})\bar{c} = (\bar{a}\bar{b})\bar{c}$.

II) $\bar{1} \in G$, pues $(1, n) = 1$, además $\forall \bar{a} \in G \quad \bar{a} \cdot \bar{1} = \bar{a}$.

III) Sea $\bar{a} \in G$, entonces $(a, n) = 1$, por tanto $\exists x, y \in \mathbb{Z}$, tal que:

$$ax + ny = 1$$

Tomando la clase:

$$\bar{1} = \overline{ax + ny} = \overline{ax} + \overline{ny} = \bar{a}\bar{x} + \bar{n}\bar{y} = \bar{a}\bar{x} + \bar{0}\bar{y} = \bar{a}\bar{x} + \bar{0} = \bar{a}\bar{x}$$

i.e. existe $\bar{x} \in G$, tal que $\bar{a} \cdot \bar{x} = 1$.

□

Definición 2.1.2 (Grupo abeliano). Sea (G, \circ, e) un grupo, si cumple que $a \circ b = b \circ a \quad \forall a, b \in G$, diremos que es un grupo abeliano.

Ejemplo 2.9. $(\mathbb{Z}, +, 0)$ es abeliano.

Ejemplo 2.10. $(\mathbb{Z}/n\mathbb{Z}, +, \bar{0})$ es abeliano.

Ejemplo 2.11. $((\mathbb{Z}/n\mathbb{Z})^*, \cdot, \bar{1})$ es abeliano.

Proposición 2.1.1. Sea (G, \circ) un grupo, sea $g \in G$ tal que $g \circ g = g$ entonces $g = e$.

Demostración.

Como $g \in G \implies \exists g' \in G$ tal que $g \circ g' = e$, luego:

$$g = g \circ e = g \circ (g \circ g') = (g \circ g) \circ g' = g \circ g' = e$$

□

Proposición 2.1.2. Sea (G, \circ) grupo, $g \in G$, entonces:

$$g^{-1} \circ g = g \circ g^{-1} = e$$

Demostración.

$$(g^{-1} \circ g) \circ (g^{-1} \circ g) = (g^{-1} \circ (g \circ g^{-1})) \circ g = (g^{-1} \circ e) \circ g = g^{-1} \circ g$$

Luego por la prop. anterior:

$$g^{-1} \circ g = e, \quad \text{i.e. } g \circ g^{-1} = g^{-1} \circ g = e$$

□

Proposición 2.1.3. Si (G, \circ) es un grupo y $g \in G$, entonces:

$$e \circ g = g \circ e = g$$

Demostración.

$$e \circ g = (g \circ g^{-1}) \circ g = g \circ (g^{-1} \circ g) = g \circ e = g = g \circ e$$

□

Proposición 2.1.4. Sea (G, \circ) un grupo, el elemento neutro e , es único.

Demostración.

Supongamos que existe $e' \in G$ tal que $g \circ e' = g$, $\forall g \in G$, en particular:

$$e = e \circ e' = e' \circ e = e', \quad \text{i.e. } e \text{ es único.}$$

□

Ejemplo 2.12. Sea $G_1 = \mathbb{Z}/n\mathbb{Z}$, sea $G_2 = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$, entonces se tienen los grupos: $(G_1, +, \bar{0})$, $(G_2, \cdot, \bar{1})$, es claro que no son iguales ya que: $|G_1| = n$, $|G_2| = \varphi(n)$.

Proposición 2.1.5. Si (G, \circ) es un grupo y $g \in G$, entonces g^{-1} es único.

Demostración.

Suponga $g' \in G$ tal que $g \circ g' = e$, entonces:

$$g^{-1} = g^{-1} \circ e = g^{-1} \circ (g \circ g') = (g^{-1} \circ g) \circ g' = e \circ g' = g'$$

□

2.2. Subgrupos

Definición 2.2.1 (Subgrupo). Sea (G, \circ, e) un grupo, sea $H \subseteq G$ un subconjunto de G , diremos que H es un subgrupo de G , si con la misma operación \circ , definida en G , forma un grupo. Se denominará $H \leq G$.

Ejemplo 2.13. Sea $(G = \mathbb{Z}, +, 0)$, para algún $a \in \mathbb{Z}$, definimos:

$$H_a = \{t \in \mathbb{Z} : t = na, n \in \mathbb{Z}\}$$

entonces $(H_a, +, 0)$ es un subgrupo de G .

Demostración.

Claramente $H_a \subseteq G$, además $+$ es cerrada en H_a , pues si $n_1a, n_2a \in H_a \implies n_1a + n_2a = (n_1 + n_2)a \in H_a$.

I) $+$ es asociativa, porque hereda la asociatividad de G .

II) $0 \in H_a$, ya que $0 = 0 \cdot a \in H_a$, además $na + 0 = na \quad \forall na \in H_a$.

III) Si $na \in H_a$, como $n \in \mathbb{Z} \implies -n \in \mathbb{Z}$, así $\exists -na \in H_a \implies na + (-na) = 0$.

□

Ejemplo 2.14. Sea $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$, entonces $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$, este es llamado el grupo especial lineal.

Observación 2.1. Sea (G, \circ, e) grupo, sea $H \leq G$, entonces $e \in H$.

En efecto, como $H \neq \emptyset$, $\exists g \in H$, además $\exists g^{-1} \in H$ al ser un subgrupo, así:

$$g \circ g^{-1} = e, \quad \text{i.e. } e \in H.$$

□

Proposición 2.2.1. Si (G, \circ, e) es un grupo y $\{H_\lambda\}_{\lambda \in I}$ es una colección arbitraria de subgrupos, entonces:

$$\bigcap_{\lambda \in I} H_\lambda, \text{ es un subgrupo de } G.$$

Demostración.

Como $H_\lambda \leq G \quad \forall \lambda \in I$, $\bigcap_{\lambda \in I} H_\lambda \neq \emptyset$ pues $e \in H_\lambda \quad \forall \lambda \in I$. Sean $a, b \in \bigcap_{\lambda \in I} H_\lambda$, entonces $a, b \in H_\lambda \quad \forall \lambda \in I$, además \circ es cerrada en $\bigcap_{\lambda \in I} H_\lambda$, ya que $a \circ b \in H_\lambda \quad \forall \lambda \in I$, así $a \circ b \in \bigcap_{\lambda \in I} H_\lambda$. Luego:

I) \circ es asociativa en $\bigcap_{\lambda \in I} H_\lambda$, ya que es asociativa en $H_\lambda, \forall \lambda \in I$.

II) $e \in \bigcap_{\lambda \in I} H_\lambda$.

III) Dado que $a \in \bigcap_{\lambda \in I} H_\lambda$, entonces $a \in H_\lambda \forall \lambda \in I$, así $\exists a^{-1} \in H_\lambda \forall \lambda \in I$ tal que $a \circ a^{-1} = e$, luego $a^{-1} \in \bigcap_{\lambda \in I} H_\lambda$.

□

Proposición 2.2.2. Sea (G, \circ, e) un grupo, sean $H, K \leq G$, entonces $H \cup K$ es un subgrupo de G si y sólo si $H \subseteq K \vee K \subseteq H$.

Demostración.

Será demostrada primero la reciprocidad.

(\Leftarrow) Basta notar que si $H \subseteq K$, $H \cup K = K$ y $K \leq G$, así $H \cup K \leq G$. Análogo si $K \subseteq H$.

(\Rightarrow) Sea $H \cup K \leq G$. Supongamos que $H \not\subseteq K \wedge K \not\subseteq H$, sean $a \in H \setminus K$ y $b \in K \setminus H$. Sea $c = a \circ b$. Como $H \cup K \leq G$, entonces $c \in H \cup K$, así $c \in H \vee c \in K$.

Si $c \in H \implies a^{-1} \circ c = b \in H$, lo cual no puede ser (pues $b \in K \setminus H$). Si $c \in K \implies c \circ b^{-1} = a \in K$, lo cual no puede ser (pues $a \in H \setminus K$).

Por lo cual $H \subseteq K \vee K \subseteq H$.

□

Definición 2.2.2 (Orden de un grupo). *Sea (G, \circ, e) un grupo, el orden del grupo será la cardinalidad de G y se denota $|G|$.*

Definición 2.2.3. *Sea (G, \circ, e) un grupo, diremos que es un grupo finito si G es un conjunto finito. En caso contrario se le dice infinito.*

Definición 2.2.4. *Sea (G, \circ, e) un grupo, sea $S \subseteq G$, con $S \neq \emptyset$, el grupo generado por S en G denotado por $\langle S \rangle$ es el menor de los subgrupos que lo contiene, i.e.:*

$$\langle S \rangle = \bigcap_{\substack{S \subseteq H \\ H \leq G}} H$$

Si S es finito, y sea $H = \langle S \rangle$, diremos que H es finitamente generado.

Ejemplo 2.15. *Todo subgrupo finito de G es finitamente generado, más aún, si $H \leq G$ y es finito $\langle H \rangle = H$.*

Demostración.

Dado que:

$$\langle H \rangle = \bigcap_{\substack{H' \leq G \\ H \subseteq H'}} H' \subseteq H' \quad \forall H' \leq G \text{ tales que } H \subseteq H',$$

además como $H \leq G$ y $H \subseteq H$, entonces H es uno de los términos de la intersección, así:

$$\langle H \rangle \subseteq H \wedge H \subseteq \bigcap_{\substack{H' \leq G \\ H \subseteq H'}} H' = \langle H \rangle$$

Por lo tanto $\langle H \rangle = H$. □

Ejemplo 2.16. $(\mathbb{Z}, +, 1)$ es finitamente generado, basta notar que:

$$\mathbb{Z} = \langle \{1\} \rangle$$

Ejemplo 2.17. $(\mathbb{Q}, +, 1)$, \mathbb{Q} no es finito ni es finitamente generado.

Proposición 2.2.3. *Sea (G, \circ, e) un grupo, $H \subseteq G$ no vacío, entonces las cond. son equivalentes:*

- I) $H \leq G$
- II) $\forall x, y \in H$ se tiene que $x \circ y \in H \wedge x^{-1} \in H$.
- III) $\forall x, y \in H$ se tiene que $x \circ y^{-1} \in H$.

Demostración.

Se probarán las implicaciones en ciclo.

- I \Rightarrow II) Se sigue de la definición ya que la operación en G debe ser una operación en H , además de que si H es un subgrupo $\forall x \in H \implies \exists x^{-1} \in H$.
- II \Rightarrow III) Si $x, y \in H$ por ii) $y^{-1} \in H$, luego $x \circ y^{-1} \in H$ (por ii).
- III \Rightarrow I) Sea $x \in H$, entonces $x \circ x^{-1} = e$, luego, note que si $x \in H$ entonces $x^{-1} = e \circ x^{-1} \in H$.

Ahora probemos que la operación es cerrada: sea $x, y \in H$, entonces $y^{-1} \in H$, más aún $(y^{-1})^{-1} = y$, ya que $y^{-1} \circ y = y^{-1} \circ (y^{-1})^{-1} = e$ y por la unicidad del inverso $(y^{-1})^{-1} = y$. Por lo cual $x \circ y = x \circ (y^{-1})^{-1} \in H$, por lo tanto la operación es cerrada en H .

□

Observación 2.2. *Sea (G, \circ, e) un grupo, sean $a, b \in G$ entonces:*

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

En efecto,

$$(a \circ b)(b^{-1} \circ a^{-1}) = a(b \circ b^{-1}) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$$

Por la unicidad del inverso se sigue $b^{-1} \circ a^{-1} = (a \circ b)^{-1}$. □

Cuando no haya perdida de generalidad para facilitar la escritura de la operación \circ en un grupo G , se denotará expresará como el producto, es decir: $a \circ b := ab$. Además, se podrá expresar la potencia de un elemento $a \in G$ como:

$$a^n = \underbrace{a \cdots a}_{n-\text{veces}}$$

para $n \in \mathbb{Z}^+$. Si $n = 0$, $a^0 = e$ y podemos observar que $a^{-n} = (a^n)^{-1}$ para $n \in \mathbb{N}$.

Observación 2.3. *Si $S \neq \emptyset$, es un subconjunto de un grupo G , entonces:*

$$\langle S \rangle = \{s_1^{i_1} \dots s_n^{i_n} : s_j \in S, i_j = \pm 1, j = 1, \dots, n, n \in \mathbb{N}\}$$

Demostración.

Sea $H = \{s_1^{i_1} \dots s_n^{i_n} : s_i \in S, i_j = \pm 1, j = 1, \dots, n, n \in \mathbb{N}\}$. Sean $s, t \in H$, tales que $s = s_1^{i_1} \dots s_n^{i_n}$, $t = t_1^{j_1} \dots t_m^{j_m}$, con $s_1, \dots, s_n, t_1, \dots, t_m \in S$, $i_1, \dots, i_n, j_1, \dots, j_m \in \{1, -1\}$. Notemos que:

$$st^{-1} = s_1^{i_1} \dots s_n^{i_n} (t_1^{j_1} \dots t_m^{j_m})^{-1} = s_1^{i_1} \dots s_n^{i_n} t_m^{-j_m} \dots t_1^{-j_1} \in H$$

Así por la proposición 2.2.3 $H \leq G$, así $\langle S \rangle \subseteq H$. Ahora sea $N \leq G$, tal que $S \subseteq N$, es claro que $s \in N$ (cualquier elemento de esa forma está en N), así $H \subseteq N$, así $H = \langle S \rangle$. □

Definición 2.2.5 (Grupo cíclico). *Sea G un grupo, si $\exists g \in G$, tal que $\langle g \rangle = G$ diremos que G es cíclico.*

Ejemplo 2.18. $(\mathbb{Z}, +, 0)$ es cíclico, pues:

$$\langle 1 \rangle = \mathbb{Z}$$

Ejemplo 2.19. S_3 no es cíclico.

Ejemplo 2.20. $(\mathbb{Q}, +, 0)$ no es cíclico.

Observación 2.4 (Nota). Note que si G es cíclico:

$$\langle g \rangle = \{g^t : t \in \mathbb{Z}\}$$

Proposición 2.2.4. Si (G, \circ, e) es cíclico, entonces G es abeliano.

*Demuestra*ción.

Sea (G, \circ, e) cíclico, entonces $\exists g \in G$, tal que $\langle g \rangle = G$. Sean $a, b \in G$, tal que $a = g^n, b = g^m$, con $n, m \in \mathbb{Z}$. Es fácil probar que $g^p g^q = g^{p+q} \quad \forall p, q \in \mathbb{Z}$, así:

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba$$

□

Observación 2.5 (Observación). *El recíproco del teorema anterior es falso. En efecto, tome los contraejemplos:*

1. Sea $n \in \mathbb{Z}^+$, no primo (por ejemplo $n = 8$), $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ es abeliano, pero no cíclico.
2. (\mathbb{R}^+, \cdot) es abeliano pero no cíclico.

2.3. Grupo de permutaciones

Definición 2.3.1 (Grupo de Permutaciones). *Sea X un conjunto no vacío, sea $\mathcal{H} = \{f : X \rightarrow X : f \text{ es biyectiva}\}$, consideremos la composición de funciones, entonces \mathcal{H} forma un grupo llamado el grupo de permutaciones del conjunto X denotado por S_X .*

En caso de que X sea finito, podemos enlistar los elementos de X por a_1, \dots, a_n , podemos representar con un arreglo bidimensional de renglones colocando:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{\sigma(1)} & a_{\sigma(2)} & \dots & a_{\sigma(n)} \end{pmatrix}$$

Donde $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$, tal que $\sigma(i) = j$, si $f(a_i) = a_j$, de este modo podemos prescindir de los elementos de X y fijarnos solo en los subíndices e identificar a f con:

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

En este caso se escribirá como S_n con $n = |X|$.

Ejemplo 2.21. S_3 es el grupo formado por los elementos:

$$\{e, \sigma, \theta, \sigma \cdot \theta, \theta \cdot \sigma, \theta^2\}$$

Donde:

$$\begin{array}{lll} e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \theta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \theta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \sigma \cdot \theta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \theta \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{array}$$

\circ	e	θ	σ	θ^2	$\sigma \cdot \theta$	$\theta \cdot \sigma$
e	e	θ	σ	θ^2	$\sigma \cdot \theta$	$\theta \cdot \sigma$
θ	θ	θ^2	$\theta \cdot \sigma$	e	σ	$\sigma \cdot \theta$
σ	σ	$\sigma \cdot \theta$	e	$\theta \cdot \sigma$	θ	θ^2
θ^2	θ^2	e	$\sigma \cdot \theta$	θ	$\theta \cdot \sigma$	σ
$\sigma \cdot \theta$	$\sigma \cdot \theta$	$\theta \cdot \sigma$	θ^2	σ	e	θ
$\theta \cdot \sigma$	$\theta \cdot \sigma$	σ	θ	$\sigma \cdot \theta$	θ^2	e

Es evidente que S_3 no es abeliano, basta notar $\theta \circ \sigma \neq \sigma \circ \theta$. Además observe que si el orden de X es n , $|S_n| = n!$.

Observación 2.6. Si $n \geq 3$, entonces S_n no es abeliano.

En efecto, Basta tomar:

$$\sigma = \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ 1 & \dots & i+1 & i & \dots & n \end{pmatrix}, \quad \theta = \begin{pmatrix} 1 & \dots & j & j+1 & \dots & n \\ 1 & \dots & j & j+1 & \dots & n \end{pmatrix} \quad \text{con } i \neq j$$

y notar que $\sigma \circ \theta \neq \theta \circ \sigma$.

Además podemos notar que trivialmente S_1 y S_2 son un grupo abeliano. \square

2.4. Grupo Cociente

2.4.1. Producto de subgrupos

Definición 2.4.1 (Producto de subgrupos). *Sea (G, \circ, e) un grupo, sean $S, T \leq G$, definimos el producto de S y T como:*

$$ST = \{st : s \in S, t \in T\}$$

Observación 2.7. *Sea (G, \circ, e) un grupo, $S, T \subseteq G$, ST , no es necesariamente un subgrupo.*

Proposición 2.4.1. *Sea (G, \circ, e) un grupo, sean $H, K \leq G$ entonces HK es un subgrupo si y sólo si $HK = KH$.*

Demuestração.

\Rightarrow) Suponga que $HK \leq G$, sean $hk \in HK$, entonces $h \in H$ y $k \in K$, entonces: $k^{-1}h^{-1} = (hk)^{-1} \in HK$, por otro lado, como $k^{-1}h^{-1} \in KH$, así: $HK = (k^{-1}h^{-1})^{-1} \in KH$, luego $HK \subseteq KH$, análogamente $KH \subseteq HK$, por lo tanto $HK = KH$.

\Leftarrow) Supongamos que $HK = KH$, notemos que $HK \neq \emptyset$, ya que $e \circ e \in HK$. Sean $x, y \in HK$, entonces existe $h_1, h_2 \in H, k_1, k_2 \in K$, tal que $x = h_1k_1, y = h_2k_2$, es claro que $y^{-1} \in HK$, pues $y^{-1} = k_2^{-1}h_2^{-1} \in KH = HK$, así que probemos que $xy^{-1} \in HK$. En efecto, $xy^{-1} = h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Note que $k_1k_2^{-1}h_2^{-1} \in KH = HK$, entonces digamos $h_3k_3 = k_1k_2^{-1}h_2^{-1}$ con $h_3 \in H, k_3 \in K$. Luego: $h_1(k_1k_2^{-1}h_2^{-1}) = h_1(h_3k_3) \in HK$, por lo tanto $xy^{-1} \in HK$, y por una proposición anterior HK es un subgrupo de G . \square

Definición 2.4.2. *Sea (G, \circ, e) un grupo, sean $H, K \leq G$, HK se llama el producto de H con K .*

Corolario 2.4.1. *Si (G, \circ, e) es un grupo abeliano el producto finito de subgrupos es un subgrupo.*

En efecto, es inmediato usando inducción y el hecho que el producto de subgrupos es asociativo. \square

2.4.2. Clases laterales

Observación 2.8. *Sea (G, \circ, e) un grupo, sea $H \leq G$, entonces $Hg = H$ si y sólo si $g \in H$.*

Demuestração.

\Rightarrow) Supongamos que $Hg = H$, entonces $\forall hg \in Hg, hg \in H$, en particular tome $h = e$, así $eg = g \in H$.

\Leftrightarrow) Suponga que $g \in H$, entonces $Hg = \{hg : h \in H\} \subseteq H$, ahora dado $h \in H$, note que $hg^{-1} \in H$, luego $h = (hg^{-1})g \in Hg$, por lo cual $H \subseteq Hg$. $\therefore Hg = H$. \square

Proposición 2.4.2. *Sea (G, \circ, e) un grupo, $H \leq G$, entonces $Hg = Hg_1$ si y sólo si $gg_1^{-1} \in H$.*

En efecto, $gg_1^{-1} \in H \iff H = Hgg_1^{-1} \iff Hg_1 = (Hgg_1^{-1})g_1 = Hg$. \square

Definición 2.4.3. *Sea (G, \circ, e) un grupo, sea $H \leq G$, sea $g \in G$, a Hg se le llama clase derecha, análogamente gH se le llama clase izquierda.*

Definición 2.4.4. *Sea (G, \circ, e) un grupo, sea $H \leq G$, sea $\mathcal{L} = \{gH : g \in G\}$ se le llama conjunto de clases izquierdas y $\mathcal{R} = \{Hg : g \in G\}$ se le llama conjunto de clases derechas.*

Proposición 2.4.3. *Sea (G, \circ, e) un grupo, sea $H \leq G$, entonces \mathcal{L} y \mathcal{R} forman una partición de G .*

Demostración.

Basta probar que \mathcal{R} induce una relación de equivalencia, i.e. la relación \sim definida por $a \sim b \iff a, b \in Hg$ es de equivalencia.

I) REFLEXIVIDAD: $a \sim a \iff a, a \in Hg$. (Esto se cumple pues $a \in Ha$).

II) SIMÉTRICA: $a \sim b \implies a, b \in Hg \implies b, a \in Hg \implies b \sim a$.

III) TRANSITIVIDAD: Si $a \sim b \wedge b \sim c \implies a, b \in Hg_1 \wedge b, c \in Hg_2$. Sea $a = h_1g_1$, $b = h_2g_1$, $b = h_3g_2$, $c = h_4g_2$, así note que $g_1 = (h_2^{-1}h_3)g_2$. Luego podemos expresar $a = h_1(h_2^{-1}h_3)g_2$, como $(h_1h_2^{-1}h_3) \in H$, $a \in Hg_2$, así $a, c \in Hg_2 \implies a \sim c$.

\therefore Las clases derechas forman una partición de G .

Análogamente las clases izquierdas forman una partición de G . \square

Observación 2.9. *Si (G, \circ, e) es abeliano cada clase izquierda es la misma clase derecha.*

En efecto, Sea $H \leq G$, sea $\mathcal{L} = \{gH : g \in G\}$, sea $\mathcal{R} = \{Hg : g \in G\}$, sea $Hg \in \mathcal{R}$, sea $hg \in Hg$, $hg = gh \in gH \in \mathcal{L}$, así $\mathcal{R} \subseteq \mathcal{L}$, análogamente $\mathcal{L} \subseteq \mathcal{R}$, por lo cual $\mathcal{L} = \mathcal{R}$. \square

Observación 2.10. *El recíproco es no necesariamente cierto.*

Ejemplo 2.22. En S_3 , sea $H = \left\{ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, e \right\} = \langle \sigma \rangle \leq G$.

Veamos cuáles son las clases derechas de H :

$$\mathcal{R} = \{H, H\theta = \{\theta, \sigma \circ \theta\}, H\theta^2 = \{\theta^2, \sigma \circ \theta^2 = \theta \circ \sigma\}\}$$

Ahora las clases izquierdas:

$$\mathcal{L} = \{H, \theta H = \{\theta, \theta \circ \sigma\}, \theta^2 H = \{\theta^2, \theta^2 \circ \sigma\}\}$$

Proposición 2.4.4. *Sea (G, \circ, e) un grupo, entonces la cardinalidad de cada clase izquierda o derecha es la misma e igual a $|H|$.*

Demuestra.

Sea $Hg \in \mathcal{R}$, definamos $\varphi : H \rightarrow Hg$, $h \mapsto hg$, probemos que es una función biyectiva.

En efecto, sean $h_1, h_2 \in H$, tal que $\varphi(h_1) = \varphi(h_2)$, entonces $h_1g = h_2g \iff h_1 = h_2$, por lo tanto es inyectiva.

Sea $hg \in Hg \implies \exists h \in H$ tal que $\varphi(h) = hg$, por lo tanto es suprayectiva.

$\therefore \varphi$ es biyectiva, así $|H| = |Hg|$. Análogamente se prueba que $|H| = |gH|$. \square

Teorema 2.4.1 (Índice de Lagrange). *Sea (G, \circ, e) un grupo sea $H \leq G$, entonces $|H| \mid |G|$ y además:*

$$|G| = |H| \cdot [G : H]$$

Donde $[G : H] := |\mathcal{L}| = |\mathcal{R}|$ se llama índice de Lagrange de H en G .

Demuestra.

Primero veamos que $|\mathcal{L}| = |\mathcal{R}|$. Sea $\varphi : \mathcal{R} \rightarrow \mathcal{L}$, $Ha \mapsto a^{-1}H$, probemos que es un isomorfismo (biyección entre conjuntos).

Sean $g_1H, g_2H \in \mathcal{R}$, tal que $\varphi(Hg_1) = \varphi(Hg_2)$, entonces:

$$g_1^{-1}H = g_2^{-1}H \iff g_1(g_2^{-1})^{-1} \in H \iff g_1g_2^{-1} \in H \iff Hg_1 = Hg_2$$

Por lo tanto es inyectiva. (Nota: en la imagen la cadena de equivalencias usa propiedades de clases laterales).

Ahora sea $g^{-1}H \in \mathcal{L}$, como existe $g = (g^{-1})^{-1} \in G$, se sigue que $\exists Hg \in \mathcal{R}$, tal que $\varphi(Hg) = g^{-1}H$, por lo cual es biyectiva.

$\therefore \varphi$ es biyectiva y así es un isomorfismo (de conjuntos). $\therefore |\mathcal{R}| = |\mathcal{L}|$.

Ahora como las clases son una partición de G , entonces:

$$\begin{aligned} |G| &= \left| \bigcup_{a \in G} Ha \right| \\ &= \sum_{a \in G} |Ha| = \sum_{a \in G} |H| \\ &= |\mathcal{R}| |H| = |H| [G : H] \end{aligned}$$

Así: $|H| \mid |G|$ y $[G : H] \mid |G|$. \square

En particular si G es finito, se cumple que:

$$\frac{|G|}{|H|} = [G : H]$$

Definición 2.4.5. *Sea (G, \circ, e) un grupo, sea $g \in G$, se denota por $o(g)$ como el menor entero no negativo tal que $g^{o(g)} = e$, si existe ese entero, en caso contrario, diremos $o(g) = +\infty$.*

Ejemplo 2.23. En $(\mathbb{Z}, +, 0)$, $\forall a \in \mathbb{Z}$, $o(a) = 0$ (o infinito según la convención).

Ejemplo 2.24. En (S_3, \circ, e) $o(\sigma) = 2$, $o(\theta) = 3$.

Ejemplo 2.25. En $(\mathbb{Z}/8\mathbb{Z}, +, 0)$, $o(2) = 4$, $o(3) = 8$, $o(4) = 2$.

Observación 2.11. Sea (G, \circ, e) un grupo finito $\forall g \in G, \exists m \in \mathbb{Z}^+$, tal que $o(g) \leq m$.

Demostración.

Sea $|G| = n$, tome el conjunto $\{g^{i_1}, \dots, g^{i_{n+1}}\}$, con $i_1, \dots, i_{n+1} \in \mathbb{Z}^+$ con $i_1 < i_2 < \dots < i_{n+1}$. Entonces al menos 2 son iguales, i.e. $g^{i_j} = g^{i_k}$, para $1 \leq j < k \leq n + 1$. Luego:

$$g^{i_k - i_j} = g^{i_k} \cdot g^{-i_j} = g^{i_j} g^{-i_j} = e, \quad \text{tomemos } m = i_k - i_j > 0.$$

$\therefore \exists m \in \mathbb{Z}^+$ tal que $g^m = e$, luego como $o(g)$ es el mínimo entero positivo tal que $g^{o(g)} = e$, entonces $o(g) \leq m$. \square

Observación 2.12. Sea (G, \circ, e) un grupo finito, sea $g \in G$, $o(g) = |\langle g \rangle|$, más aún $o(g) \mid |G|$.

Demostración.

Sea $H = \{e, g, g^2, \dots, g^{o(g)-1}\}$, claramente $H \subseteq \langle g \rangle$, además notemos que es un subgrupo.

En efecto: sean $g^i, g^j \in H$, $0 \leq i < j \leq o(g) - 1$, entonces $g^i g^j = g^{i+j}$, se tiene que $0 \leq i+j \leq o(g)-1 \vee o(g) \leq i+j$. Si se cumple la primera condición es evidente que $g^{i+j} \in H$. Por lo cual tomemos el caso $o(g) \leq i+j$, por el algoritmo de Euclides $\exists k, r \in \mathbb{Z}^+$ tal que: $i+j = k \cdot o(g) + r$, con $0 \leq r < o(g)$, así:

$$g^{i+j} = g^{k \cdot o(g) + r} = (g^{o(g)})^k g^r = (e)^k g^r = g^r \in H,$$

por lo tanto es cerrada, además se hereda de G las propiedades del grupo.

Ahora sea $a \in \langle g \rangle$, podemos expresar $a = g^i, i \in \mathbb{Z}$, así por Euclides $\exists k, r \in \mathbb{Z}$, con $0 \leq r < o(g)$ tal que $g^i = o(g)k + r$, de este modo podemos expresar $a = g^i = g^r \in H$.

$\therefore \langle g \rangle \subseteq H$, así $|\langle g \rangle| = |H| = o(g)$, más aún como H es subgrupo de G , $|H| \mid |G|$, así $o(g) \mid |G|$. \square

Corolario 2.4.2. Sea (G, \circ, e) un grupo finito entonces $g^{|G|} = e \quad \forall g \in G$.

Demostración.

Dado que $o(g) = |\langle g \rangle| \mid |G|$, entonces $\exists s$ tal que $o(g)s = |G|$ y

$$g^{|G|} = g^{o(g)s} = (g^{o(g)})^s = (e)^s = e$$

\square

Corolario 2.4.3 (Teorema de Euler). *Sea $a \in (\mathbb{Z}/n\mathbb{Z})^*$ entonces $a^{\varphi(n)} = 1$ (mód n).*

Demuestra.

$|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ y por el corolario anterior

$$a^{\varphi(n)} = 1 \quad (\text{mód } n)$$

□

Corolario 2.4.4 (Teorema Pequeño de Fermat). *Si $a \in (\mathbb{Z}/p\mathbb{Z})^*$ con p primo, entonces: $a^p \equiv a$ (mód p) y $a^{p-1} = 1$.*

En efecto, Por el corolario anterior dado $a \in (\mathbb{Z}/p\mathbb{Z})^*$, $a^{\varphi(p)} = 1$ (mód p), como $\varphi(p) = p-1$, se sigue $a^{p-1} = 1$ (mód p), luego $a^p = a$. □

Definición 2.4.6. *Sea (G, \circ, e) un grupo sea $N \leq G$, diremos que N es un subgrupo normal en G denotado por $N \trianglelefteq G$, si $gNg^{-1} = N, \forall g \in G$.*

Observación 2.13. *Si (G, \circ, e) es un grupo, sea $N \subseteq G$, arbitrario entonces $gNg^{-1} \subseteq G$. En este caso diremos que gNg^{-1} es subgrupo conjugado de N .*

En efecto, Es claro que $gNg^{-1} \neq \emptyset$ pues $N \neq \emptyset$. Además para $h_1, h_2 \in gNg^{-1}$, $\exists n_1, n_2 \in N$ tal que $h_1 = gn_1g^{-1}$, $h_2 = gn_2g^{-1}$, luego:

$$h_1h_2^{-1} = gn_1g^{-1}(gn_2g^{-1})^{-1} = gn_1g^{-1}(g^{-1})^{-1}n_2^{-1}g^{-1} = gn_1n_2^{-1}g^{-1} \in gNg^{-1}$$

∴ es un subgrupo de G . □

Teorema 2.4.2. *Sea (G, \circ, e) un grupo, $N \leq G$, entonces las siguientes condiciones son equivalentes:*

- I) $N \trianglelefteq G$.
- II) $gNg^{-1} \subseteq N \quad \forall g \in G$.
- III) $gNg^{-1} = N \quad \forall g \in G$. (Nota: en la imagen dice $gN \subseteq Ng$, pero el punto iii suele referirse a la igualdad de conjugación o commutación de clases. Transcribo lo que dice la imagen literalmente en la demostración: $gNg^{-1} \subseteq N \implies gN \subseteq Ng$).
- IV) $gN = Ng \quad \forall g \in G$.
- V) El único subgrupo conjugado de N es N .

Demostración.

- I \Rightarrow II) De la definición $gNg^{-1} = N \quad \forall g \in G$, en particular $gNg^{-1} \subseteq N \quad \forall g \in G$.
- II \Rightarrow III) $gNg^{-1} \subseteq N \implies (gNg^{-1})g \subseteq Ng$ y $g(gNg^{-1}) = gN$, así $gN \subseteq Ng \quad \forall g \in G$. (Nota: Aquí la transcripción se ajusta a la lógica del manuscrito que parece deducir la igualdad de clases o contención).
- III \Rightarrow IV) Resta ver que $Ng \subseteq gN$. Tenemos que $gN \subseteq Ng \quad \forall g \in G$, se sigue: $g^{-1}N \subseteq Ng^{-1} \quad \forall g \in G \implies g(g^{-1}N) \subseteq gNg^{-1} \implies N \subseteq gNg^{-1} \quad \forall g \in G$, así: $Ng \subseteq (gNg^{-1})g = gN \quad \forall g \in G$.
- IV \Rightarrow V) Sea H el conjugado de N entonces $H = gNg^{-1}$ para algún $g \in G$, entonces:

$$Hg = (gNg^{-1})g = gN = Ng$$

de donde

$$H = (Hg)g^{-1} = (Ng)g^{-1} = N$$

- V \Rightarrow I) Se sigue de la definición.

□

Observación 2.14. Si $N \trianglelefteq G$ y $H \leq G$ entonces $HN = NH$ y por tanto $NH \leq G$.

En efecto, $HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$. □

Ejemplo 2.26. Dado el grupo S_3 , calcule los subgrupos: $S_3 = \{e, \sigma, \theta, \theta^2, \sigma\theta, \theta\sigma\}$

Sol.

$$\begin{aligned} H_0 &= \langle e \rangle = \{e\} \\ H_1 &= \langle \sigma \rangle = \{e, \sigma\} \\ H_2 &= \langle \theta \rangle = \{e, \theta, \theta^2\} = \{e, \theta^2, \theta\} \\ H_3 &= \langle \sigma \circ \theta \rangle = \{e, \sigma \circ \theta\} \\ H_4 &= \langle \theta \circ \sigma \rangle = \{e, \theta \circ \sigma\} \\ H_5 &= \langle \{\sigma, \theta\} \rangle = S_3 \end{aligned}$$

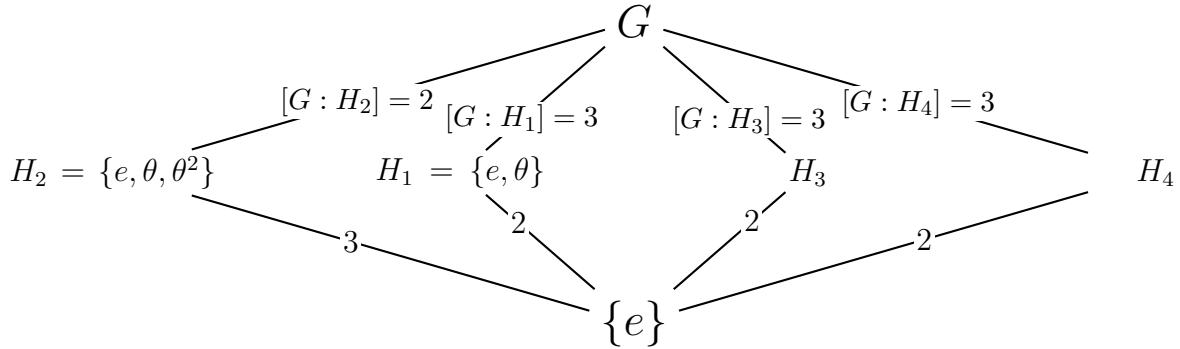
Además podemos notar:

- $H_0 \trianglelefteq G$, de manera trivial.
- $H_1 \not\trianglelefteq G$, ya que $H_1\theta \neq \theta H_1$.
- $H_2 \trianglelefteq G$, $H_2\sigma = \{\sigma, \theta \circ \sigma, \theta^2 \circ \sigma\} = \{\sigma, \theta \circ \sigma, \sigma \circ \theta\} = \sigma H_2$.

- $H_3 \not\leq G, H_3\theta \neq \theta H_3$.
- $H_4 \not\leq G, H_4\theta \neq \theta H_4$.
- $H_5 \trianglelefteq G$, ya que $H_5 = S_3$.

Por otro lado note:

$$\begin{aligned}\theta H_1\theta^{-1} &= \theta H_1\theta^2 = \{e, \theta \circ \sigma \circ \theta^2\} = \{e, \theta \circ \theta \circ \sigma\} = \{e, \theta^2 \circ \sigma\} = \{e, \sigma \circ \theta\} = H_3. \\ \theta H_3\theta^{-1} &= \theta H_3\theta^2 = \{e, \theta \circ (\sigma \circ \theta) \circ \theta^2\} = \{e, \theta \circ \sigma\} = H_4\end{aligned}$$



Observación 2.15 (Observación). *Sea (G, \circ, e) un grupo, ser conjugado es una relación de equivalencia.*

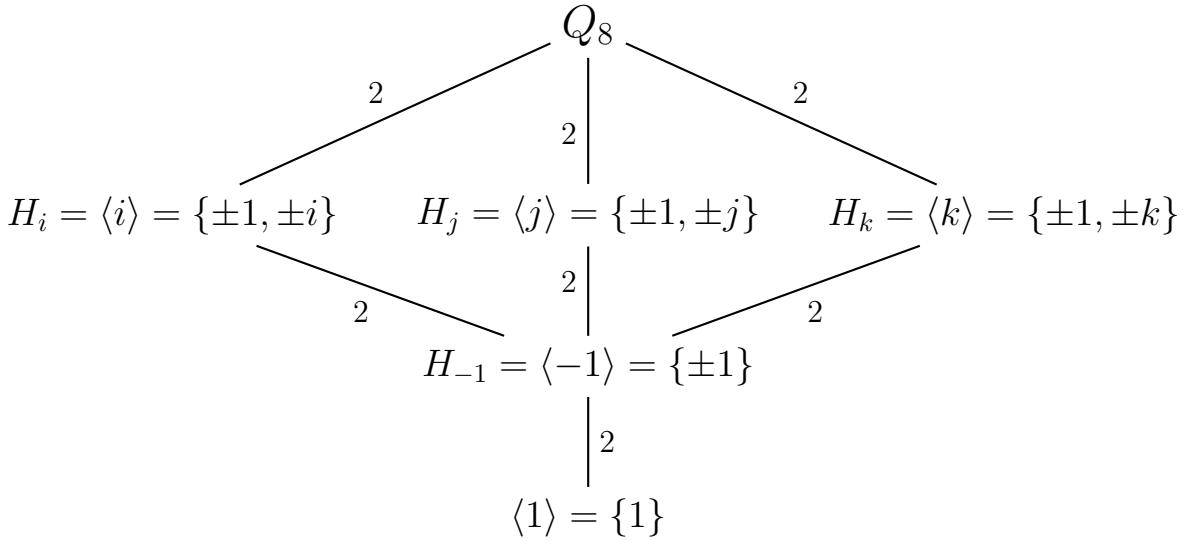
Demostración.

- REFLEXIVIDAD: $H \sim H$ pues $eHe^{-1} = H \quad \forall H \leq G$.
- SIMETRÍA: Sean H_1, H_2 , tal que $H_1 \sim H_2$, entonces $H_1 = gH_2g^{-1}$, luego: $g^{-1}H_1g = H_2$, así $H_2 \sim H_1$.
- TRANSITIVA: Sean $H_1, H_2, H_3 \leq G$ tal que $H_1 \sim H_2, H_2 \sim H_3$, entonces existen $g_1, g_2 \in G$ tal que $H_2 = g_1H_1g_1^{-1}, H_3 = g_2H_2g_2^{-1} = g_2(g_1H_1g_1^{-1})g_2^{-1} = (g_2g_1)H_1(g_2g_1)^{-1}$. Dado que $g_2g_1 \in G, H_1 \sim H_3$.

Además note que son conjugados $|H_1| = |H_3|$. Si son conjugados $\exists g \in G$ tal que $H_3 = gH_1g^{-1}$, sea $\varphi : H_1 \rightarrow H_3$, dada por $\varphi(h_1) = gh_1g^{-1}$, podemos probar que es biyectiva.

□

Ejemplo 2.27. Sea $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, con $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, -k = ji, -i = kj, -j = ki$. Calcule los subgrupos normales y calcule los conjugados.



2.4.3. Grupo cociente

Es fácil observar que dado un grupo (G, \circ, e) y $N \leq G$, tal que sea normal, cada clase derecha es una clase izquierda, de este modo se tiene la siguiente proposición.

Proposición 2.4.5. *Sea (G, \circ, e) un grupo, sea $N \trianglelefteq G$, sea $G/N = \mathcal{L} = \mathcal{R}$, * definida por $(aN) * (bN) = ab$ en G/N está bien definida, i.e. no depende del representante de clase, más aún G/N es un grupo.*

Demostración.

Veamos que * está bien definida:

En efecto, sean $aN, a_1N, bN, b_1N \in G/N$, tales que $aN = a_1N, bN = b_1N$, entonces $Nb = Nb_1$, así $a^{-1}a_1 \in N, b^{-1}b_1 \in N$. Como $N \trianglelefteq G \implies g(a^{-1}a_1)g^{-1} \in N, \forall g \in G$. En particular, tome $g = b^{-1}$:

$$b^{-1}(a^{-1}a_1)b_1 = b^{-1}a^{-1}a_1b_1$$

Luego:

$$(ab)^{-1}a_1b_1 = b^{-1}a^{-1}a_1b_1 \in N$$

Es decir $(ab)N = (a_1b_1)N$. Por lo tanto la función está bien definida.

Ahora probemos que G/N es un grupo:

En efecto, es asociativa, sean $aN, bN, cN \in G/N$:

$$(aN * bN) * cN = abN * cN = (ab)cN = a(bc)N = aN * (bc)N = aN * (bN * cN)$$

Note que existe la identidad, tome $N = eN = Ne \in G/N$,

$$aN * N = aN * eN = (ae)N = aN$$

Además existe el inverso, dado $aN \in G/N$, existe $a^{-1}N \in G/N$:

$$aN * a^{-1}N = (aa^{-1})N = eN = N, \text{ entonces } a^{-1}N \text{ es inverso de } aN.$$

$\therefore G/N$ es un grupo. \square

Definición 2.4.7 (Grupo Cociente). *Sea (G, \circ, e) , sea $N \trianglelefteq G$ normal, definimos al grupo cociente: $G/N := \mathcal{R} = \mathcal{L}$, con la siguiente operación:*

$$(aN) * (bN) = abN, \quad \text{para } aN, bN \in G/N.$$

CAPÍTULO 3

Isomorfismos de Grupos

CAPÍTULO 4

Productos Directos

4.1. Productos Directos

Definición 4.1.1. Sea $(H, \circ), (K, *)$ dos grupos, definamos en $G = H \times K$, la función $\odot : G \times G \rightarrow G$, dada por:

$$(h_1, k_1) \odot (h_2, k_2) = (h_1 \circ h_2, k_1 * k_2)$$

Claramente \odot es una operación en G y se verifica que con esta operación, G forma un grupo con identidad (e_H, e_K) .

También se tiene que $\bar{H} = H \times \{e_K\}$ y $\{e_H\} \times K = \bar{K}$ son subgrupos normales de G tales que $\bar{H} \cap \bar{K} = e_G = (e_H, e_K)$ y $G = \bar{H}\bar{K}$ en este caso a G se le llama el producto directo externo de H con K .

Definición 4.1.2. Si G es un grupo tal que existen $H, K \leq G$ con $H \triangleleft G, K \triangleleft G, G = HK, H \cap K = \{e\}$, diremos que G es el producto directo interno de H y K .

Observación 4.1. El producto directo de una cantidad finita de grupos es asociativo (la igualdad se da salvo isomorfismo); es decir,

$$(H_1 \times H_2) \times H_3 \cong H_1 \times (H_2 \times H_3) \quad (\text{Se escribe } H_1 \times H_2 \times H_3)$$

Verificarlo.

Teorema 4.1.1 (Teorema chino del residuo). Sea $n \in \mathbb{N} \setminus \{1\}$. Entonces $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ en donde $n = p_1^{e_1} \cdots p_k^{e_k}$ es la factorización en primos de n .

Demostración.

Sea $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ la función definida por:

$$[a]_n \mapsto ([a]_{p_1^{e_1}}, \dots, [a]_{p_k^{e_k}})$$

La función φ está bien definida. Supongamos que $[a]_n = [b]_n$, entonces $n \mid a - b$. Dado que $p_i^{e_i} \mid n$, por transitividad se tiene que $p_i^{e_i} \mid a - b$, es decir $[a]_{p_i^{e_i}} = [b]_{p_i^{e_i}}$, de donde se concluye que $\varphi([a]_n) = \varphi([b]_n)$.

- φ es inyectiva: $\varphi([a]_n) = \varphi([b]_n)$ si y solo si $[a]_{p_i^{e_i}} = [b]_{p_i^{e_i}}$ para todo $1 \leq i \leq k$. Esto implica que $p_i^{e_i} \mid a - b$ para todo $1 \leq i \leq k$. Como los p_i son primos distintos, tenemos que $(p_i^{e_i}, p_j^{e_j}) = 1$ para todo $i \neq j$. En consecuencia, el producto $n = p_1^{e_1} \dots p_k^{e_k}$ divide a $a - b$, de donde $[a]_n = [b]_n$.

Nótese además que las cardinalidades coinciden: $n = |\mathbb{Z}_n| = |\mathbb{Z}_{p_1^{e_1}} \times \dots \times \mathbb{Z}_{p_k^{e_k}}| = p_1^{e_1} \dots p_k^{e_k}$. Al ser una función inyectiva entre conjuntos finitos del mismo tamaño, φ es biyectiva.

- φ es un homomorfismo:

$$\begin{aligned}\varphi([a]_n + [b]_n) &= \varphi([a + b]_n) = ([a + b]_{p_1^{e_1}}, \dots, [a + b]_{p_k^{e_k}}) \\ &= ([a]_{p_1^{e_1}} + [b]_{p_1^{e_1}}, \dots, [a]_{p_k^{e_k}} + [b]_{p_k^{e_k}}) \\ &= ([a]_{p_1^{e_1}}, \dots, [a]_{p_k^{e_k}}) + ([b]_{p_1^{e_1}}, \dots, [b]_{p_k^{e_k}}) \\ &= \varphi([a]_n) + \varphi([b]_n)\end{aligned}$$

Finalmente, φ es un isomorfismo y por lo tanto $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \dots \times \mathbb{Z}_{p_k^{e_k}}$. \square

Ejemplo 4.1. Sea G un grupo de orden pq con p, q primos distintos. Si H, K son subgrupos normales de G con $|H| = p$ y $|K| = q$, entonces $G \cong H \times K$.

*Demuestra*ción.

Como $H, K \trianglelefteq G$, si tomamos $g \in H \cap K$ entonces $o(g) \mid |H| = p$ y $o(g) \mid |K| = q$. Dado que p y q son distintos, $o(g) = 1$, lo que implica que $H \cap K = \{e\}$.

Más aún, el orden del producto es $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{pq}{1} = |G|$, luego $G = HK$. Además, si $g \in HK$ tuviera dos representaciones $g = h_1k_1 = h_2k_2$ con $h_1, h_2 \in H$ y $k_1, k_2 \in K$, entonces $h_1^{-1}h_2 = k_1k_2^{-1}$. Este elemento pertenecería a la intersección $H \cap K = \{e\}$, lo que implica $h_1 = h_2$ y $k_1 = k_2$. Es decir, la representación de $g \in G$ como producto de un elemento de H y uno de K es única.

Definimos la función $\varphi : G \rightarrow H \times K$ mediante:

$$g = hk \mapsto (h, k)$$

Note que si $h \in H$ y $k \in K$, tenemos que $hkh^{-1}k^{-1}$ pertenece a $H \cap K$ (pues H y K son normales), y como la intersección es trivial, $hkh^{-1}k^{-1} = e$, luego $hk = kh$.

- φ es un homomorfismo: Sean $g = hk$ y $g_1 = h_1k_1$ en G con $h, h_1 \in H$ y $k, k_1 \in K$. Usando que los elementos de H y K comutan:

$$\begin{aligned}\varphi(gg_1) &= \varphi(hkh_1k_1) = \varphi(hh_1kk_1) = (hh_1, kk_1) \\ &= (h, k)(h_1, k_1) = \varphi(g)\varphi(g_1)\end{aligned}$$

- φ es inyectiva: Si $g = hk$, $g_1 = h_1k_1$ y $\varphi(g) = \varphi(g_1)$, entonces $(h, k) = (h_1, k_1)$, luego $h = h_1$ y $k = k_1$, de donde $g = g_1$.
- φ es sobreyectiva: Dado un par $(h, k) \in H \times K$, existe el elemento $g = hk \in G$ tal que $\varphi(g) = (h, k)$.

Por lo tanto $G \cong H \times K$; de hecho, G es el producto directo interno de H y K . \square

Corolario 4.1.1. *Sea G un grupo abeliano de orden pq con p, q primos distintos, entonces:*

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q$$

Demostración.

Basta ver que existe un elemento de orden p y un elemento de orden q , lo cual nos lo dará el teorema de Cauchy (Ver más adelante). \square

Teorema 4.1.2 (Teorema de Cayley). *Todo grupo G es isomorfo a un subgrupo de permutaciones.*

Demostración.

Sea S_G el grupo de todas las permutaciones del conjunto G (biyecciones de G en sí mismo). Definimos la función $\varphi : G \rightarrow S_G$ dada por $\varphi(g) = f_g$, donde $f_g : G \rightarrow G$ es la función de multiplicación por la izquierda:

$$f_g(h) = gh \quad \forall h \in G$$

Veamos que φ es un isomorfismo sobre su imagen, en efecto:

- φ está bien definida (es decir, $f_g \in S_G$): Para cualquier $g \in G$, la función f_g es biyectiva. En efecto, tiene inversa, la cual es $f_{g^{-1}}$, ya que para todo $h \in G$:

$$(f_g \circ f_{g^{-1}})(h) = f_g(g^{-1}h) = g(g^{-1}h) = h = \text{id}(h)$$

De manera análoga, $f_{g^{-1}} \circ f_g = \text{id}$. Al ser biyectiva, f_g es una permutación de G , por lo que $f_g \in S_G$.

- φ es un homomorfismo: Sean $g, k \in G$. Queremos ver que $\varphi(gk) = \varphi(g) \circ \varphi(k)$. Evaluamos ambas funciones en un elemento arbitrario $h \in G$:

$$\begin{aligned} \varphi(gk)(h) &= f_{gk}(h) = (gk)h \\ (\varphi(g) \circ \varphi(k))(h) &= f_g(f_k(h)) = f_g(kh) = g(kh) \end{aligned}$$

Por asociatividad, $(gk)h = g(kh)$, por lo tanto $f_{gk} = f_g \circ f_k$, lo que implica que φ preserva la operación.

- φ es inyectiva: Supongamos que $\varphi(g) = \varphi(k)$. Esto significa que las funciones son idénticas, es decir, $f_g = f_k$.

$$f_g(h) = f_k(h) \quad \forall h \in G \implies gh = kh \quad \forall h \in G$$

En particular, tomando $h = e$ (neutro de G), obtenemos $ge = ke$, lo que implica $g = k$.

Concluimos que φ es un isomorfismo entre G e $\text{Im}(\varphi)$. Dado que $\text{Im}(\varphi)$ es un subgrupo de S_G , hemos demostrado que G es isomorfo a un subgrupo de permutaciones. \square

Ejemplo 4.2. Para ilustrar el teorema anterior, consideremos el grupo $S_3 = \{\text{id}, \theta, \sigma, \theta\sigma, \sigma\theta, \theta^2\}$. La función $\varphi : S_3 \rightarrow S_{S_3}$ asocia a cada $g \in S_3$ una permutación de los elementos de S_3 .

Por ejemplo, si tomamos $g = \theta$, la función asociada $f_\theta : S_3 \rightarrow S_3$ definida por $h \mapsto \theta h$ permuta los elementos de S_3 de la siguiente forma:

$$\begin{aligned} \text{id} &\mapsto \theta \\ \theta &\mapsto \theta^2 \\ \sigma &\mapsto \theta\sigma \\ \theta\sigma &\mapsto \theta^2\sigma \\ \sigma\theta &\mapsto \sigma \\ \theta^2 &\mapsto \text{id} \end{aligned}$$

Corolario 4.1.2. Sea G un grupo de orden finito n , entonces $G \hookrightarrow S_n$.

Demostración.

Sabemos que $G \hookrightarrow S_X$ y $S_X \cong S_n$. En efecto, si $G = \{a_1, \dots, a_n\}$, definimos $\psi : S_X \rightarrow S_n$ dada por $f \mapsto \bar{f}$, en donde si $f(a_i) = a_j$, entonces $\bar{f}(i) = j$, con $X = \{a_1, \dots, a_n\}$ y $\{1, \dots, n\}$.

- ψ está bien definida: Pues si $f : X \rightarrow X$ es biyectiva, en efecto:
 - \bar{f} inyectiva: $\bar{f}(i) = \bar{f}(j) \implies f(a_i) = f(a_j) \implies a_i = a_j \implies i = j$ (pues f es inyectiva).
 - \bar{f} es sobre: Dado $j \in \{1, \dots, n\}$, tenemos $a_j \in G$. Como f es biyectiva, $\exists a_i \in \{1, \dots, n\}$ tal que $f(a_i) = a_j$, luego $\bar{f}(i) = j$.
- ψ es homomorfismo: $\psi(g \circ f) = \psi(g) \circ \psi(f)$. En efecto, $\overline{g \circ f}(i) = j$ si $(g \circ f)(a_i) = a_j$. Suponga que $f(a_i) = a_k$ y $g(a_k) = a_j$, entonces $\bar{f}(i) = k$ y $\bar{g}(k) = j$. Más aún, $(g \circ f)(a_i) = g(f(a_i)) = g(a_k) = a_j$, así que $\overline{g \circ f}(i) = j$. Luego $(\bar{g} \circ \bar{f})(i) = \bar{g}(\bar{f}(i)) = \bar{g}(k) = j$. Así que $\overline{g \circ f} = \bar{g} \circ \bar{f}$, de donde $\psi(g \circ f) = \overline{g \circ f} = \bar{g} \circ \bar{f} = \psi(g) \circ \psi(f)$.
- ψ es inyectiva: $\psi(f) = \psi(g) \implies \bar{f} = \bar{g} \implies \bar{f}(i) = \bar{g}(i) \quad \forall 1 \leq i \leq n \implies f(a_i) = g(a_i) \quad \forall 1 \leq i \leq n \implies f = g$.

- ψ es sobre: Sea $h \in S_n$, entonces $\exists f : S_X \rightarrow S_X$ dada por $f(a_i) = a_{h(i)}$ tal que $(\psi(f))(i) = f(i) = h(i) \forall 1 \leq i \leq n$. Por lo tanto $h = f = \psi(f)$.

Luego $S_X \cong S_n$ y $G \hookrightarrow S_n$. □

Teorema 4.1.3. *Sea G un grupo finito, $H \leq G$. $X = \{Hg \mid g \in G\} = (G/H)$ entonces existe $\varphi : G \rightarrow S_X$ un homomorfismo tal que $N = \text{Ker } \varphi$ es el mayor subgrupo normal en G contenido en H .*

Demostración.

Sea $\varphi : G \rightarrow S_X$ definida por $\varphi(g) = f_g$ con $f_g : X \rightarrow X$ dada por:

$$f_g(Hk) = Hkg^{-1}$$

Veamos que f_g no depende del representante de clase (f_g es función). En efecto, Si $Hk = Hk_1$, entonces $kk_1^{-1} \in H$, luego $kgg^{-1}k_1^{-1} \in H$ o $Hkg^{-1} = Hk_1g^{-1}$, así que $f(Hk) = Hkg^{-1} = f(Hk_1)$, por lo cual, f_g es función.

Note que $f_g \in S_X$ pues,

- f_g es inyectiva: $f_g(Hk) = f_g(Hk_1)$ si y solo si $Hkg^{-1} = Hk_1g^{-1}$ si y solo si $Hk = Hk_1$.
- f_g es sobreyectiva: Dado $Hk \in X$ se tiene $f_g(Hkg) = Hkg^{-1} = Hk$.

Veamos que φ es homomorfismo:

$$\varphi(gg_1) = f_{gg_1} \stackrel{?}{=} f_g \circ f_{g_1} = \varphi(g)\varphi(g_1)$$

pues

$$f_{gg_1}(Hk) = Hk(gg_1)^{-1} = H(kg_1^{-1})g^{-1} = f_g(Hkg_1^{-1}) = f_g(f_{g_1}(Hk)) = (f_g \circ f_{g_1})(Hk)$$

Sea $N = \text{Ker } \varphi$, claramente $N \trianglelefteq G$, además para $n \in N$ tenemos:

$$\text{Id} = \varphi(n) = f_n \quad \text{con } f_n(Hk) = Hkn^{-1}$$

Así que $Hkn^{-1} = Hk \quad \forall Hk \in X$ o $Hkn^{-1} = Hk \quad \forall k \in G$, en particular para $k \in H$, $H = Hk$ y $Hn^{-1} = Hkn^{-1} = Hk = H$ de donde $n \in H$. Luego $N \subseteq H$.

Sea $N_1 \trianglelefteq G$ con $N_1 \subseteq H$, veamos que $N_1 \subseteq N$. Sea $n_1 \in N_1$, $\varphi(n_1) = f_{n_1}$ con $f_{n_1}(Hk) = Hkn_1^{-1} = Hkn_1^{-1}k^{-1}k \quad \forall k \in G$. Como $N_1 \trianglelefteq G$, $kn_1^{-1}k^{-1} \in N_1 \subseteq H$ así que $H(kn_1^{-1}k^{-1})k = Hk$, es decir $f_{n_1}(Hk) = Hk$ de donde $f_{n_1} = \text{Id}$, es decir $n_1 \in \text{Ker } \varphi$ y $N_1 \subseteq N$. □

Corolario 4.1.3. *Sea G finito $H \leq G$, $H \neq G$ tal que $|G| \nmid [G : H]!$ entonces H contiene un subgrupo normal en G no trivial.*

Demostración.

Si φ fuera inyectiva entonces $G \cong \varphi(G) \leq S_X$ así que $|G| \mid |S_X| = [G : H]!$ lo cual por hipótesis no se cumple. Luego $\{e\} \neq \text{Ker } \varphi \subseteq H$, y como $\text{Ker } \varphi \trianglelefteq G$, concluimos que H contiene un subgrupo normal no trivial (y $\text{Ker } \varphi \neq G$ pues $H \neq G$). \square

Corolario 4.1.4. *Sea p primo, G un grupo finito tal que p es el menor primo que divide a $|G|$ y $H \leq G$, $H \neq G$ con $[G : H] = p$, entonces $H \trianglelefteq G$.*

Demostración.

Sea $|G| = pm$.

Si $m = 1$, como $[G : H] = p$, entonces $|H| = \frac{|G|}{[G:H]} = \frac{pm}{p} = m = 1$, luego $H = \{e\}$, el cual es normal en G .

Si $m \neq 1$, los factores primos de m son mayores o iguales a p . Veamos que esto implica que $|G| \nmid [G : H]!$, es decir, $pm \nmid p!$. Procedemos por reducción al absurdo para justificar esta afirmación: Supongamos que $|G| \mid p!$, entonces $pm \mid p!$, lo que implica que $m \mid (p-1)!$. Si q es un factor primo de m , entonces $q \mid (p-1)!$, lo cual implica que $q \leq p-1$. Sin embargo, q es un factor de $|G|$ (a través de m), y por hipótesis p es el menor primo que divide a $|G|$, por lo que $q \geq p$. Tenemos así que $q \leq p-1$ y $q \geq p$, lo cual es una contradicción.

Por lo tanto, $|G| \nmid p!$. (La demostración concluye aplicando el corolario anterior). \square

4.2. El grupo Simétrico S_n

Recordemos que S_n con la composición de funciones es un grupo. Cada elemento de S_n se llama una permutación (la cual es una función biyectiva de $\{1, \dots, n\}$ en sí mismo). En este caso si $\sigma \in S_n$ se denotará:

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

Definición 4.2.1. *Un ciclo de longitud $1 \leq k \leq n$ en S_n es un elemento de S_n tal que existen $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ con $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ y $\sigma(j) = j \forall j \notin \{i_1, \dots, i_k\}$.*

Note que en este caso:

$$\begin{aligned} \sigma^2(i_1) &= \sigma(\sigma(i_1)) = \sigma(i_2) = i_3 & \text{y} & \quad \sigma^k(i_1) = i_1 \\ \sigma^3(i_1) &= \sigma(\sigma^2(i_1)) = \sigma(i_3) = i_4 \\ &\vdots \\ \sigma^l(i_1) &= i_{1+l} & \text{si } 1 \leq l+1 \leq k, \quad l \leq k-1, & \quad \sigma^k(i_j) = i_{j+k-k} = i_j \end{aligned}$$

Más aún:

$$\sigma^l(i_j) = i_{j+l} \quad 1 \leq j+l \leq k$$

$$\sigma^l(i_j) = i_{j+l-k} \quad j + l > k \quad (1 \leq l \leq k - j)$$

En este caso, en lugar de escribir

$$\sigma = \begin{pmatrix} 1 & \cdots & i_1 & i_2 & \cdots & i_k & \cdots & n \\ 1 & \cdots & i_2 & i_3 & \cdots & i_1 & \cdots & n \end{pmatrix}$$

Escribiremos $\sigma = (i_1 \ i_2 \ i_3 \ \dots \ i_k)$ y se tiene que σ se puede denotar de k diferentes formas, a saber:

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

Si $k = 1$, $\sigma(i) = i \ \forall i$, es decir, $\sigma = id$ y se denota por $\sigma = (1) = (2) = \dots = (k) = (n)$.

Si $k = 2$, $\sigma(i_1, i_2)$ y se llama una transposición. En este caso:

$$\begin{aligned} \sigma^2(i_1) &= \sigma(i_2) = i_1 \\ \sigma^2(i_2) &= \sigma(i_1) = i_2 \end{aligned}$$

Así, $\sigma^2 = id$, es decir, $\sigma = \sigma^{-1}$.

Si σ es un ciclo de longitud k también se le llama un k -ciclo. Observe que si σ es un k -ciclo, $\sigma^k = id$, de hecho $|\sigma| = k$.

$$\sigma^l(i_j) = \begin{cases} i_{j+l} & \text{si } 1 \leq l \leq k - j \\ i_{l-k+j} & \text{si } k - j < l \leq k \end{cases}$$

En particular si $k = l$, $\sigma^k(i_j) = i_{k-k+j} = i_j$. Así $|\sigma| \mid k$. Además $\sigma^l(i_1) \neq i_1, \forall 1 \leq l < k$ así que $|\sigma| \geq k$, de donde $|\sigma| = k$.

Definición 4.2.2. Diremos que dos ciclos $\sigma, \tau \in S_n$ son disjuntos si:

- i) Cuando $\sigma(i_1) = i_2$ con $i_1 \neq i_2$ se tiene que $\tau(i_1) = i_1$.
- ii) Cuando $\tau(i_1) = i_2$ con $i_1 \neq i_2$ se tiene que $\sigma(i_1) = i_1$.

(Parafraseando, los elementos que mueve σ, τ los fija y recíprocamente).

Ejemplo 4.3. Consideremos S_5 , entonces $\sigma = (1 \ 2)$ y $\tau = (3 \ 4 \ 5)$ son disjuntos.

Nota 4.2.1. Si $\sigma = (i_1, \dots, i_k)$ y $\tau = (j_1, \dots, j_l)$, entonces σ y τ son disjuntos si y sólo si

$$\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$$

Observación 4.2. Si σ, τ son ciclos disjuntos, entonces $\sigma \circ \tau = \tau \circ \sigma$, es decir, comutan.

Demostración.

Sea $\sigma = (i_1, \dots, i_k)$ y $\tau = (j_1, \dots, j_l)$. Claramente $\sigma \circ \tau$ y $\tau \circ \sigma$ tienen el mismo dominio. Ahora si $s \notin \{i_1, \dots, i_k, j_1, \dots, j_l\}$:

$$\begin{aligned}(\sigma \circ \tau)(s) &= \sigma(\tau(s)) = \sigma(s) = s \\ (\tau \circ \sigma)(s) &= \tau(\sigma(s)) = \tau(s) = s\end{aligned}$$

Si $s \in \{i_1, \dots, i_k\}$ entonces $s \notin \{j_1, \dots, j_l\}$, así que:

$$(\sigma \circ \tau)(s) = \sigma(\tau(s)) = \sigma(s)$$

Más aún $\sigma(s) \in \{i_1, \dots, i_k\}$, luego $\sigma(s) \notin \{j_1, \dots, j_l\}$ y $\tau(\sigma(s)) = \sigma(s)$, por lo tanto $(\tau \circ \sigma)(s) = (\sigma \circ \tau)(s)$.

Por simetría si $s \in \{j_1, \dots, j_l\}$, $(\tau \circ \sigma)(s) = (\sigma \circ \tau)(s)$ en cualquier caso se tiene la igualdad y por lo tanto $\sigma \circ \tau = \tau \circ \sigma$. \square

Teorema 4.2.1. *Sea $\theta \in S_n$, entonces θ se puede representar de manera única como producto de ciclos ajenos (disjuntos) salvo orden.*

Demostración.

Sea $\{i_1, \dots, i_k\}$ los elementos que mueve θ y procedamos por inducción sobre k .

Para $k = 1$, $\theta = id$ no hay nada que ver $id = (1)$.

Para $k = 2$, $\theta = (i_1, i_2)$ y ya se tiene.

Suponga el resultado para todo $1 \leq l \leq k$ y considere que θ mueve a los elementos $\{i_1, \dots, i_k, i_{k+1}\}$. Considere que θ mueve a los elementos $\{i_1, \dots, i_k, i_{k+1}\}$. Observe que $i_1, \theta(i_1), \theta^2(i_1), \dots, \theta^{k+1}(i_1) \in \{i_1, \dots, i_{k+1}\}$, por lo tanto $\{i_1, \theta(i_1), \dots, \theta^{k+1}(i_1)\} \subseteq \{i_1, \dots, i_{k+1}\}$, luego existen $1 \leq l, l' \leq k + 2$ y $\theta^l(i_1) = \theta^{l'}(i_1)$ y podemos suponer $l > l'$, en este caso $\theta^{l-l'}(i_1) = i_1$, y $1 \leq l - l' \leq k + 2 - l' \leq k + 1$, es decir existe p tal que $\theta^p(i_1) = i_1$, $1 \leq p \leq k + 1$.

Sea p el mínimo entero para el cual pasa esto.

Sea $\sigma = (i_1, \theta(i_1), \dots, \theta^{p-1}(i_1))$. $\{i_1, \theta(i_1), \dots, \theta^{p-1}(i_1)\} \subseteq \{i_1, \dots, i_{k+1}\}$ y definamos

$$\tau(i_j) = \begin{cases} \sigma(i_j) & \text{si } \sigma(i_j) = \theta^l(i_1) \text{ para algún } 1 \leq l \leq p-1 \\ \theta(i_j) & \text{si } i_j \neq \theta^l(i_1) \forall 1 \leq l \leq p-1 \end{cases}$$

Entonces $\sigma \circ \tau = \theta$. Si $j \notin \{i_1, \dots, i_{k+1}\}$ entonces $j \neq \theta^l(i_1) \forall 1 \leq l \leq p-1$ y entonces

$$(\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(\theta(j)) = \sigma(j) = j = \theta(j)$$

Si $j \in \{i_1, \dots, i_{k+1}\} \cap \{i_1, \theta(i_1), \dots, \theta^{p-1}(i_1)\}$, entonces $j = \theta^l(i_1)$ con $0 \leq l \leq p-1$.

$$\theta(j) = \theta^{l+1}(i_1) \quad \text{y} \quad \sigma \circ \tau(j) = \sigma(\tau(j)) = \sigma(\theta^l(i_1)) = \theta^{l+1}(i_1) = \theta(j)$$

(Definición: Como j está en el soporte de σ , $\tau(j) = \theta(j)$, luego $\sigma(\theta(j)) = \theta(j)$. Y como σ es el ciclo $(i_1, \dots, \theta^{p-1}(i_1))$, $\sigma(j) = \theta(j)$). En cualquier caso $\theta(j) = (\sigma \circ \tau)(j)$ por lo tanto $\theta = \sigma \circ \tau$.

Ahora τ mueve a los elementos $\{i_1, \dots, i_{k+1}\} \setminus \{i_1, \sigma(i_1), \dots, \sigma^{p-1}(i_1)\}$ cuya cardinalidad es menor o igual a k . Por hipótesis de inducción τ es producto de ciclos disjuntos y por lo tanto θ lo es.

Unicidad: Suponga ahora que

$$\theta = \sigma_1 \dots \sigma_k = \tau_1 \dots \tau_l$$

Con los σ_i 's ciclos disjuntos a pares y los τ_i 's ciclos disjuntos a pares.

Si $\theta = id$ no hay nada que ver, si no, sea i_1 un elemento que mueve θ , entonces existen $1 \leq i \leq k$ y $1 \leq j \leq l$ tales que σ_i, τ_j mueven a i_1 , de hecho i, j son únicos pues los σ_i 's y los τ_i 's son disjuntos o más aún como son disjuntos comutan, por lo que podemos pensar que $i = 1 = j$, en este caso $\sigma_2, \dots, \sigma_k, \tau_2, \dots, \tau_l$ no mueven a i_1 .

Además $\sigma_1 = (i_1, \sigma_1(i_1), \dots, \sigma_1^{s-1}(i_1))$, $\tau_1 = (i_1, \tau_1(i_1), \dots, \tau_1^{r-1}(i_1))$ con s y r los órdenes de σ_1 y τ_1 respectivamente. Como los σ_i 's son disjuntos σ_j no mueve a ninguno de $\{i_1, \sigma_1(i_1), \dots, \sigma_1^{k-1}(i_1)\} \forall 1 < j \leq k$. Análogamente τ_j no mueve a ninguno de $\{i_1, \tau_1(i_1), \dots, \tau_1^{l-1}(i_1)\} \forall 1 < j \leq l$. Por tanto para $m \in \mathbb{N}$

$$\begin{aligned} \theta^m(i_1) &= (\sigma_1 \dots \sigma_k)^m(i_1) = (\sigma_1 \dots \sigma_k)^{m-1}((\sigma_1 \dots \sigma_k)(i_1)) \\ &= (\sigma_1 \dots \sigma_k)^{m-1}(\sigma_1(i_1)) = \dots = \sigma_1^m(i_1) \end{aligned}$$

Análogamente

$$\begin{aligned} \theta^m(i_1) &= \tau_1^m(i_1) \\ \sigma_1^m(i_1) &= \tau_1^m(i_1) \end{aligned}$$

Ahora podemos suponer que $s \leq r$, entonces

$$i_1 = \sigma_1^s(i_1) = \tau_1^s(i_1)$$

$s > r - 1$ o $s \geq r$, de donde $s = r$.

Más aún, como $\sigma_1^m(i_1) = \tau_1^m(i_1) \forall m \in \mathbb{N}$ se tiene que $\sigma_1 = \tau_1$. Ahora de la igualdad $\theta = \sigma_1 \dots \sigma_k = \tau_1 \dots \tau_l$ se obtiene $\sigma_2 \dots \sigma_k = \tau_2 \dots \tau_l$. Podemos suponer $k \leq l$. En cuyo caso realizando el mismo proceso obtenemos $\sigma_k = \tau_k$ y $Id = \tau_{k+1} \dots \tau_l$. Como los τ_j son disjuntos a pares necesariamente $\tau_{k+1} \dots \tau_l$ tienen longitud uno. Por lo tanto $l = k$. \square

Corolario 4.2.1. *Sea $\theta \in S_n$, entonces el orden de θ es el mínimo común múltiplo de los órdenes de los ciclos que aparecen en su factorización.*

Demostración.

Sea $\theta = \sigma_1 \dots \sigma_k$ con los σ_i 's ciclos disjuntos a pares y $n_i = o(\sigma_i)$, $m = [n_1, \dots, n_k]$ entonces

$$\theta^m = (\sigma_1 \dots \sigma_k)^m = \sigma_1^m \dots \sigma_k^m = id$$

De donde $o(\theta) | m$. Si $o(\theta) < m$, $Id = \theta^{o(\theta)} = \sigma_1^{o(\theta)} \dots \sigma_k^{o(\theta)}$, por lo cual $n_i | o(\theta) \forall i$, de donde $m = [n_1, \dots, n_k] | o(\theta)$ de donde $m = o(\theta)$. \square

Observación 4.3. 1. Sea $(i \ j)$ una transposición de S_n , entonces $(i \ j) = (1 \ i)(1 \ j)(1 \ i)$.

2. Sean x_1, \dots, x_n variables. Definimos

$$P_n = P_n(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \quad \forall n \geq 2$$

y hagamos actuar el grupo de permutaciones sobre P_n de la siguiente forma.

Para $\theta \in S_n$:

$$\theta(P_n) = P_n^\theta = \prod_{1 \leq i < j \leq n} (x_{\theta(i)} - x_{\theta(j)})$$

3. Si $1 < k \leq n$ y $\theta = (1, k)$, entonces $\theta(P_n) = -P_n$.

4. Si $\theta = (i \ j)$ es una transposición, $\theta(P_n) = -P_n$.

5. Sea $\theta \in S_n$ un r-ciclo, entonces θ es producto de transposiciones (se puede representar como un producto de transposiciones, no necesariamente única).

Demostración de 1).

Queremos demostrar que la transposición $(i \ j)$ es igual al producto $(1 \ i)(1 \ j)(1 \ i)$. Llamemos $\sigma = (1 \ i)(1 \ j)(1 \ i)$ y evaluemos su acción sobre los elementos de $\{1, \dots, n\}$ actuando de derecha a izquierda (orden de composición de funciones). Asumimos $1, i, j$ distintos (si alguno es igual, la igualdad es trivial).

- Para el elemento 1:

$$1 \xrightarrow{(1 \ i)} i \xrightarrow{(1 \ j)} i \xrightarrow{(1 \ i)} 1$$

Luego $\sigma(1) = 1$. (El 1 queda fijo, lo cual es correcto pues $(i \ j)$ no mueve al 1).

- Para el elemento i :

$$i \xrightarrow{(1 \ i)} 1 \xrightarrow{(1 \ j)} j \xrightarrow{(1 \ i)} i$$

Luego $\sigma(i) = j$.

- Para el elemento j :

$$j \xrightarrow{(1 \ i)} j \xrightarrow{(1 \ j)} 1 \xrightarrow{(1 \ i)} i$$

Luego $\sigma(j) = i$.

- Para cualquier otro elemento $k \notin \{1, i, j\}$: Todas las transposiciones en el producto fijan a k , por lo tanto $\sigma(k) = k$.

Como σ intercambia i con j y deja fijos a los demás elementos (incluido el 1), concluimos que $\sigma = (i \ j)$. \square

Demostración de 2).

Queremos verificar que la acción definida cumple con la propiedad de grupo $(\tau \circ \theta)(P_n) = \tau(\theta(P_n))$.

Recordemos que la acción de una permutación σ sobre un polinomio en variables x_1, \dots, x_n consiste en reemplazar cada subíndice k por $\sigma(k)$. Es decir, σ actúa sobre las posiciones de las variables.

Sea $P_n = \prod(x_i - x_j)$. Primero aplicamos θ :

$$\theta(P_n) = \prod_{1 \leq i < j \leq n} (x_{\theta(i)} - x_{\theta(j)})$$

Llamemos $Q(x_1, \dots, x_n)$ a este nuevo polinomio. Notemos que el término que ocupaba la posición asociada al índice k ahora tiene el índice $\theta(k)$.

Ahora aplicamos τ al polinomio Q . La regla dice que τ reemplaza cualquier variable con índice m por la variable con índice $\tau(m)$. En Q , tenemos variables de la forma $x_{\theta(i)}$. Aquí el índice es $m = \theta(i)$. Al aplicar τ , reemplazamos $x_{\theta(i)}$ por $x_{\tau(\theta(i))}$.

$$\tau(\theta(P_n)) = \prod_{1 \leq i < j \leq n} (x_{\tau(\theta(i))} - x_{\tau(\theta(j))})$$

Por otro lado, consideremos la permutación compuesta $\rho = \tau \circ \theta$. Si aplicamos ρ directamente a P_n , reemplazamos cada índice k por $\rho(k) = \tau(\theta(k))$.

$$(\tau \circ \theta)(P_n) = \prod_{1 \leq i < j \leq n} (x_{(\tau \circ \theta)(i)} - x_{(\tau \circ \theta)(j)}) = \prod_{1 \leq i < j \leq n} (x_{\tau(\theta(i))} - x_{\tau(\theta(j))})$$

Comparando ambas expresiones, tenemos que $(\tau \circ \theta)(P_n) = \tau(\theta(P_n))$. \square

Demostración de 3).

Procedamos por inducción sobre n .

Para $n = 2$, tenemos $1 < k \leq 2 \implies k = 2$, luego $\theta = (1, 2)$.

$$\theta(P_2) = \theta(x_1 - x_2) = x_{\theta(1)} - x_{\theta(2)} = x_2 - x_1 = -(x_1 - x_2) = -P_2$$

Suponga el resultado cierto para n , es decir, para $1 < k \leq n$. Note que:

$$\begin{aligned} P_{n+1} &= \prod_{1 \leq i < j \leq n+1} (x_i - x_j) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \cdot \prod_{1 \leq i \leq n} (x_i - x_{n+1}) \\ &= P_n \cdot \prod_{1 \leq i \leq n} (x_i - x_{n+1}) \end{aligned}$$

Caso A: Si $1 < k \leq n$, entonces $\theta = (1, k) \in S_n \subseteq S_{n+1}$ (fija a $n+1$).

$$\begin{aligned} \theta(P_{n+1}) &= \theta \left(P_n \cdot \prod_{1 \leq i \leq n} (x_i - x_{n+1}) \right) \\ &= \theta(P_n) \cdot \theta \left(\prod_{1 \leq i \leq n} (x_i - x_{n+1}) \right) \\ &\stackrel{\text{H.I.}}{=} (-P_n) \cdot \prod_{1 \leq i \leq n} (x_{\theta(i)} - x_{n+1}) \end{aligned}$$

Como θ solo permuta los elementos $\{1, \dots, n\}$, el conjunto de factores en la productoria es el mismo (solo cambia el orden), por lo tanto el producto permanece invariante.

$$= -P_n \cdot \prod_{1 \leq i \leq n} (x_i - x_{n+1}) = -P_{n+1}$$

Caso B: Si $k = n + 1$, entonces $\theta = (1, n + 1)$. Descomponemos P_{n+1} cuidadosamente:

$$\begin{aligned} \theta(P_{n+1}) &= \theta \left[\prod_{1 < i < j \leq n} (x_i - x_j) \cdot \prod_{1 < j \leq n} (x_1 - x_j) \cdot \prod_{1 < i < n+1} (x_i - x_{n+1}) \cdot (x_1 - x_{n+1}) \right] \\ &= \prod_{1 < i < j \leq n} (x_i - x_j) \cdot \prod_{1 < j \leq n} (x_{n+1} - x_j) \cdot \prod_{1 < i < n+1} (x_i - x_1) \cdot (x_{n+1} - x_1) \\ &= \prod_{1 < i < j \leq n} (x_i - x_j) \cdot \prod_{1 < j \leq n} [-(x_j - x_{n+1})] \cdot \prod_{1 < i < n+1} [-(x_1 - x_i)] \cdot [-(x_1 - x_{n+1})] \\ &\quad - \left[\prod_{1 < i < j \leq n} (x_i - x_j) \cdot \prod_{1 < j \leq n} (x_j - x_{n+1}) \cdot \prod_{1 < i < n+1} (x_1 - x_i) \cdot (x_1 - x_{n+1}) \right] \\ &= - \left(\prod_{1 \leq i < j \leq n} (x_i - x_j) \cdot \prod_{1 \leq j \leq n} (x_j - x_{n+1}) \right) \\ &= P_n \cdot \prod_{1 \leq i \leq n} (x_i - x_{n+1}) = -P_{n+1} \end{aligned}$$

□

Demostración de 4).

Si $\theta = (i \ j)$ es una transposición, por la observación 1 sabemos que $(i \ j) = (1 \ i)(1 \ j)(1 \ i)$. Usando la propiedad 3 repetidamente:

$$\begin{aligned} \theta(P_n) &= [(1 \ j)(1 \ i)(1 \ j)]P_n \\ &= (1 \ j)((1 \ i)((1 \ j)P_n)) \\ &= (1 \ j)((1 \ i)(-P_n)) \\ &= (1 \ j)(-(-P_n)) \\ &= (1 \ j)(P_n) = -P_n \end{aligned}$$

□

Demostración de 5).

Sea $\theta = (i_1, \dots, i_k)$ un k -ciclo. Podemos descomponerlo verificando la acción sobre los elementos:

$$(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \dots (i_{k-2}, i_{k-1})(i_{k-1}, i_k)$$

□

Ejemplo 4.4. $(1 \ 2 \ 3) = (1 \ 2)(2 \ 3)$. También se puede escribir de forma no única, por ejemplo: $(1 \ 2 \ 3) = (4 \ 5)(1 \ 2)(2 \ 3)(4 \ 5) = (1 \ 2)(1 \ 2)(1 \ 2)(2 \ 3)(3 \ 2)(3 \ 2)$.

Teorema 4.2.2. *Sea $\theta \in S_n$, entonces θ se representa siempre como un producto de una cantidad par de transposiciones ó siempre como un producto de una cantidad impar de transposiciones.*

Demostración.

Por un teorema anterior θ es producto de ciclos disjuntos y cada ciclo es producto de transposiciones, luego θ es producto de transposiciones. Suponga que:

$$\theta = \sigma_1 \dots \sigma_k = \tau_1 \dots \tau_s \quad \text{con}$$

σ_i 's y τ_j 's transposiciones, entonces para P_n el polinomio definido anteriormente

$$\theta(P_n) = (\sigma_1 \dots \sigma_k)(P_n) = (-1)^k P_n = (\tau_1 \dots \tau_s)P_n = (-1)^s P_n$$

De donde $(-1)^k = (-1)^s$ o $(-1)^{k-s} = 1$, es decir, $k - s$ siempre es par, luego ambos son pares o ambos son impares. \square

Definición 4.2.3. *Sea $\theta \in S_n$ diremos que θ es par si al representarla como producto de transposiciones consta de un número par de ellas. Es impar en caso contrario.*

Observación 4.4. *Sea $A_n = \{\theta \in S_n \mid \theta \text{ es par}\} \forall n \geq 2$, entonces $A_n \leq S_n$, con $[S_n : A_n] = 2$ y por lo tanto $A_n \trianglelefteq S_n$.*

Demostración.

Primero probemos que es un subgrupo ($A_n \leq S_n$). Si $\theta \in A_n$, entonces $\theta = \tau_1 \dots \tau_s$ con $s = 2k$ y los τ_i 's son transposiciones. Luego, el inverso es $\theta^{-1} = (\tau_1 \dots \tau_s)^{-1} = \tau_s^{-1} \dots \tau_1^{-1}$. Como la inversa de una transposición es ella misma ($\tau_i^{-1} = \tau_i$), tenemos $\theta^{-1} = \tau_s \dots \tau_1$, que sigue teniendo $s = 2k$ transposiciones. Así, $\theta^{-1} \in A_n$.

Si además $\theta_1 \in A_n$, digamos $\theta_1 = \rho_1 \dots \rho_r$ con $r = 2l$ y ρ_j 's transposiciones. Entonces el producto $\theta \circ \theta_1 = \tau_1 \dots \tau_s \rho_1 \dots \rho_r$ consta de $s + r = 2k + 2l = 2(k + l)$ transposiciones. Como $2(k + l)$ es par, $\theta \circ \theta_1 \in A_n$. Por lo tanto $A_n \leq S_n$.

Ahora analicemos el índice. Si $\theta \in S_n$, entonces: Si θ es par, $\theta \in A_n$. Si θ es impar, entonces $\theta \notin A_n$, es decir, $\theta A_n \neq A_n$.

Más aún, para cualquier otra permutación impar $\theta_1 \in S_n$, veamos que definen la misma clase lateral, es decir $\theta A_n = \theta_1 A_n$. Esto ocurre si y solo si $\theta_1^{-1} \theta \in A_n$. Como θ y θ_1 son impares, podemos escribir las como:

$$\theta = \tau_1 \dots \tau_{2k+1} \quad \text{y} \quad \theta_1 = \rho_1 \dots \rho_{2m+1}$$

con los τ_i y ρ_j transposiciones. Entonces:

$$\theta_1^{-1} \theta = (\rho_1 \dots \rho_{2m+1})^{-1} (\tau_1 \dots \tau_{2k+1}) = \rho_{2m+1} \dots \rho_1 \tau_1 \dots \tau_{2k+1}$$

El número total de transposiciones es $(2m + 1) + (2k + 1) = 2m + 2k + 2 = 2(m + k + 1)$, que es un número par. Por lo tanto $\theta_1^{-1} \theta \in A_n$, lo que implica $\theta A_n = \theta_1 A_n$.

Así que las clases laterales izquierdas son exactamente dos: A_n (las pares) y θA_n (las impares, donde θ es cualquier permutación impar fija). Luego, $[S_n : A_n] = 2$.

En particular, como 2 es el menor primo que divide a $|S_n| = n!$ (para $n \geq 2$), sabemos por un resultado anterior que cualquier subgrupo de índice igual al menor primo divisor del orden del grupo es normal. Así que $A_n \trianglelefteq S_n$. \square

Teorema 4.2.3. $A_n = \langle \{\theta \in S_n \mid \theta \text{ es un 3-ciclo}\} \rangle$, $n \geq 3$.

*Demuestra*ción.

Sea $H = \langle \{\theta \in S_n \mid \theta \text{ es 3-ciclo}\} \rangle$. Sea θ un 3-ciclo, es decir, $\theta = (a_1, a_2, a_3)$, entonces

$$\theta = (a_1, a_2, a_3) = (a_1, a_2)(a_2, a_3) \in A_n$$

luego

$$\langle \{\theta \in S_n \mid \theta \text{ es 3-ciclo}\} \rangle \subseteq A_n$$

Para la contención inversa basta ver que cada producto de 2 transposiciones es un producto de 3-ciclos. Consideremos (a_1, a_2) y (b_1, b_2) 2 transposiciones.

Si $\{a_1, a_2\} = \{b_1, b_2\}$, entonces:

$$(a_1, a_2)(b_1, b_2) = (a_1, a_2)(a_1, a_2) = id = (a_1, a_2, a_3)(a_1, a_3, a_2)$$

Si tiene un solo elemento distinto podemos suponer que son $(a_1, a_2), (a_2, b_2)$ con $a_1 \neq b_2$ y:

$$(a_1, a_2)(a_2, b_2) = (a_1, a_2, b_2)$$

Si no tienen elementos en común, es decir $(a_1, a_2)(b_1, b_2)$:

$$(a_1, a_2)(b_1, b_2) = (a_1, a_2, b_1)(a_2, b_1, b_2)$$

En cualquier caso cada par de transposiciones es el producto de 3-ciclos, luego, cada permutación par es producto de 3-ciclos, así

$$A_n \subseteq \langle \{\theta \in S_n \mid \theta \text{ es 3-ciclo}\} \rangle \quad \text{y} \quad A_n = H$$

\square

Teorema 4.2.4. Sea $n \geq 2$, entonces A_n es el único subgrupo de índice 2 de S_n .

*Demuestra*ción.

Si $n = 2$, $A_2 = \{e\}$ y es claro el resultado. Suponga $n \geq 3$ y sea $H \leq S_n$ tal que $[S_n : H] = 2$.

Probemos que H contiene a todos los 3-ciclos. Sea σ un 3-ciclo. Como $[S_n : H] = 2$, sabemos que H es un subgrupo normal de S_n ($H \trianglelefteq S_n$). Consideremos el grupo cociente S_n/H , el cual tiene orden 2. Por lo tanto, el cuadrado de cualquier elemento en el cociente es la identidad del cociente (H). Es decir:

$$(\sigma H)^2 = \sigma^2 H = H \implies \sigma^2 \in H$$

Ahora, dado que σ es un 3-ciclo, su orden es 3, por lo que $\sigma^3 = id$. Esto implica que $\sigma^4 = \sigma$. Podemos escribir σ como:

$$\sigma = \sigma^4 = (\sigma^2)^2$$

Como ya demostramos que $\sigma^2 \in H$ y H es un subgrupo (cerrado bajo la operación), entonces el cuadrado de σ^2 también debe estar en H . Por lo tanto, $\sigma \in H$.

Esto demuestra que H contiene a todos los 3-ciclos. Como sabemos por un teorema anterior que A_n está generado por los 3-ciclos, concluimos que $A_n \subseteq H$.

Finalmente, utilizamos la multiplicidad del índice:

$$[S_n : A_n] = [S_n : H][H : A_n]$$

Sustituyendo los valores conocidos:

$$2 = 2 \cdot [H : A_n] \implies [H : A_n] = 1$$

Lo cual implica que $H = A_n$. □

Observación 4.5. Consideremos el grupo multiplicativo $\{1, -1\}$ con la operación definida por:

$$1 \cdot 1 = 1, \quad 1(-1) = -1, \quad (-1)(-1) = 1$$

Definamos la función $\varphi : S_n \rightarrow \{1, -1\}$ como:

$$\varphi(\theta) = \begin{cases} 1 & \text{si } \theta \text{ es par} \\ -1 & \text{si } \theta \text{ es impar} \end{cases}$$

Demostración.

φ es homomorfismo. a) Si θ, θ_1 son pares, $\theta \cdot \theta_1$ es par y $\varphi(\theta \cdot \theta_1) = 1 = \varphi(\theta)\varphi(\theta_1)$. Si θ es par y θ_1 impar o viceversa, $\theta \cdot \theta_1$ es impar, luego $\varphi(\theta\theta_1) = -1 = \varphi(\theta)\varphi(\theta_1)$. Si θ y θ_1 son impares $\varphi(\theta) = -1 = \varphi(\theta_1)$ y $\theta\theta_1$ es par y

$$\varphi(\theta\theta_1) = 1 = (-1)(-1) = \varphi(\theta)\varphi(\theta_1)$$

En cualquier caso $\varphi(\theta\theta_1) = \varphi(\theta)\varphi(\theta_1)$. Más aún $\theta \in \text{Ker } \varphi$ si y solo si $\varphi(\theta) = 1$ si y solo si θ es par si y solo si $\theta \in A_n$ si y solo si $\text{Ker } \varphi = A_n$. □

Nota 4.2.2. φ es sobreyectiva.

$$\frac{S_n}{A_n} \cong \{1, -1\} \implies [S_n : A_n] = 2 \quad y \quad A_n \trianglelefteq S_n$$

Definición 4.2.4. Sea $\theta, \theta_1 \in G$, G grupo diremos que θ y θ_1 son conjugados si existe $\sigma \in G$ tal que $\theta = \sigma\theta_1\sigma^{-1}$ (conjugación).

Observación 4.6. Ser conjugado determina una relación de equivalencia, es decir, la relación $\theta \sim \theta_1$ si y solo si θ y θ_1 son conjugados es de equivalencia.

- i) Reflexiva: $\theta \sim \theta$ pues $\theta = e\theta e^{-1}$.
- ii) Simétrica: $\theta \sim \theta_1$ si y solo si existe $\sigma \in G$ tal que $\theta = \sigma\theta_1\sigma^{-1}$ si y solo si existe $\sigma \in G$ tal que $\theta_1 = \sigma^{-1}\theta\sigma$ si y solo si existe $\sigma^{-1} \in G$ tal que $\theta_1 = \sigma^{-1}\theta(\sigma^{-1})^{-1}$ si y solo si $\theta_1 \sim \theta$.
- iii) Transitiva: $\theta \sim \theta_1$ y $\theta_1 \sim \theta_2$ entonces existen $\sigma_1, \sigma_2 \in G$ tales que $\theta = \sigma_1\theta_1\sigma_1^{-1}$, $\theta_1 = \sigma_2\theta_2\sigma_2^{-1}$, entonces

$$\theta = \sigma_1(\sigma_2\theta_2\sigma_2^{-1})\sigma_1^{-1} = (\sigma_1\sigma_2)(\theta_2)(\sigma_2^{-1}\sigma_1^{-1}) = (\sigma_1\sigma_2)(\theta_2)(\sigma_1\sigma_2)^{-1}$$

y $\sigma_1\sigma_2 \in G$, luego $\theta \sim \theta_2$.

A las clases de equivalencia correspondientes las llamaremos clases de conjugación. Denotemos a la clase de conjugación de θ por $[\theta]$. Entonces para $\theta \in G$, $[\theta] = \{\theta\}$ si y solo si $\theta \in Z(G)$, $[\theta] = \{\sigma\theta\sigma^{-1} \mid \sigma \in G\} = \{\theta\}$ si y solo si $\sigma\theta\sigma^{-1} = \theta \forall \sigma \in G$ si y solo si $\sigma\theta = \theta\sigma \forall \sigma \in G$ si y solo si $\theta \in Z(G)$.

Definición 4.2.5. Sean $\theta_1, \theta_2 \in S_n$, diremos que θ_1 y θ_2 tienen la misma estructura en ciclos cuando $\theta_1 = \sigma_1 \dots \sigma_s$, $\theta_2 = \tau_1 \dots \tau_k$ son las respectivas factorizaciones de θ_1 y θ_2 como producto de ciclos disjuntos, entonces $s = k$ y salvo el orden σ_i y τ_i son conjugados (tienen la misma longitud) $\forall 1 \leq i \leq s = k$.

- Ejemplo 4.5.**
1. Considere S_6 . $\theta_1 = (1\ 3)(4\ 5\ 6)$, $\theta_2 = (2\ 4)(1\ 3\ 5)$. θ_1 y θ_2 tienen la misma estructura en ciclos.
 2. Considere S_{10} . $\theta_1 = (1\ 2)(3\ 4)(5\ 6\ 7)$, $\theta_2 = (3\ 4)(5\ 6\ 7)(8\ 9\ 10)$. θ_1 y θ_2 tienen la misma estructura en ciclos.

Observación 4.7. Si $\theta = (a_1, \dots, a_r)$ es un r -ciclo y $\gamma \in S_n$, entonces:

$$\gamma\theta\gamma^{-1} = (\gamma(a_1), \dots, \gamma(a_r))$$

Es decir, conjugar un ciclo θ por γ resulta en un ciclo de la misma longitud obtenido aplicando γ a los elementos de θ .

Demostración.

En efecto. Si $a = \gamma(a_i)$ para algún $1 \leq i \leq r$, entonces $\gamma^{-1}(a) = a_i$.

$$(\gamma\theta\gamma^{-1})(a) = (\gamma \circ \theta)(\gamma^{-1}(a)) = \gamma(\theta(a_i)) = \gamma(a_{i+1})$$

(Con la convención $a_{r+1} = a_1$). Esto coincide con la acción del ciclo $(\gamma(a_1), \dots, \gamma(a_r))$ sobre el elemento $a = \gamma(a_i)$.

Si $a \notin \{\gamma(a_1), \dots, \gamma(a_r)\}$, entonces $\gamma^{-1}(a) \notin \{a_1, \dots, a_r\}$. Como θ fija los elementos fuera de su soporte:

$$\theta(\gamma^{-1}(a)) = \gamma^{-1}(a)$$

Así:

$$(\gamma \circ \theta \circ \gamma^{-1})(a) = \gamma(\theta(\gamma^{-1}(a))) = \gamma(\gamma^{-1}(a)) = a$$

Por lo tanto, $\gamma\theta\gamma^{-1}$ fija a todo elemento fuera de $\{\gamma(a_1), \dots, \gamma(a_r)\}$.

En conclusión:

$$\gamma\theta\gamma^{-1} = (\gamma(a_1) \dots \gamma(a_r))$$

□

Teorema 4.2.5. Sean $\theta_1, \theta_2 \in S_n$, entonces θ_1 y θ_2 tienen la misma estructura en ciclos si y solo si θ_1 y θ_2 son conjugados.

Demostración.

⇒) Supongamos que θ_1 y θ_2 tienen la misma estructura en ciclos. Sean $\theta_1 = \sigma_1 \dots \sigma_k$ y $\theta_2 = \tau_1 \dots \tau_k$ sus respectivas descomposiciones en ciclos disjuntos (incluyendo los ciclos de longitud 1 para cubrir todo el conjunto $\{1, \dots, n\}$). Podemos ordenar los ciclos de tal manera que σ_i y τ_i tengan la misma longitud para todo $1 \leq i \leq k$.

Denotemos los elementos de cada ciclo como:

$$\sigma_i = (a_{i,1}, a_{i,2}, \dots, a_{i,r_i}) \quad \text{y} \quad \tau_i = (b_{i,1}, b_{i,2}, \dots, b_{i,r_i})$$

donde r_i es la longitud del ciclo i .

Definamos la permutación $\gamma \in S_n$ tal que aplique cada elemento de σ_i en el elemento correspondiente de τ_i . Es decir:

$$\gamma(a_{i,j}) = b_{i,j} \quad \forall 1 \leq i \leq k, 1 \leq j \leq r_i$$

Como los ciclos son disjuntos y cubren todo el conjunto, γ es una biyección bien definida.

Ahora verifiquemos la conjugación para cada ciclo. Por la observación anterior:

$$\gamma\sigma_i\gamma^{-1} = (\gamma(a_{i,1}), \dots, \gamma(a_{i,r_i})) = (b_{i,1}, \dots, b_{i,r_i}) = \tau_i$$

Entonces:

$$\gamma\theta_1\gamma^{-1} = \gamma(\sigma_1 \dots \sigma_k)\gamma^{-1} = (\gamma\sigma_1\gamma^{-1}) \dots (\gamma\sigma_k\gamma^{-1}) = \tau_1 \dots \tau_k = \theta_2$$

Por lo tanto, θ_1 y θ_2 son conjugados.

⇐) Supongamos ahora que θ_1 y θ_2 son conjugados. Es decir, existe $\gamma \in S_n$ tal que $\theta_2 = \gamma\theta_1\gamma^{-1}$. Sea $\theta_1 = \sigma_1 \dots \sigma_k$ la descomposición de θ_1 en ciclos disjuntos. Entonces:

$$\theta_2 = \gamma(\sigma_1 \dots \sigma_k)\gamma^{-1} = (\gamma\sigma_1\gamma^{-1}) \dots (\gamma\sigma_k\gamma^{-1})$$

Por la observación anterior, cada término $(\gamma\sigma_i\gamma^{-1})$ es un ciclo de la misma longitud que σ_i . Además, como los σ_i son disjuntos a pares, sus conjugados también lo son (si σ_i y σ_j no mueven elementos en común, sus conjugados tampoco).

Por la unicidad de la descomposición en ciclos disjuntos (salvo el orden), concluimos que la estructura de ciclos de θ_2 es exactamente la misma que la de θ_1 (los mismos ciclos transformados, conservando sus longitudes). \square

Corolario 4.2.2. *Sea $n \geq 3$.*

- a) *Si $N \trianglelefteq A_n$ y N contiene un 3-ciclo, entonces $N = A_n$.*
- b) *Si $N \trianglelefteq S_n$ y N contiene una transposición (2-ciclo), entonces $N = S_n$.*

Demostración.

a) Supongamos que $N \trianglelefteq A_n$ contiene un 3-ciclo $\theta_1 = (a_1 a_2 a_3)$. Queremos ver que N contiene a cualquier otro 3-ciclo $\theta_2 = (b_1 b_2 b_3)$, y dado que los 3-ciclos generan A_n , esto implicará $N = A_n$.

Sabemos que en S_n todos los 3-ciclos son conjugados. Es decir, existe $\gamma \in S_n$ tal que:

$$\theta_2 = \gamma\theta_1\gamma^{-1}$$

Analicemos si podemos garantizar que el conjugador esté en A_n (es decir, que sea par):

Caso $n \geq 5$: Si $\gamma \in A_n$, entonces $\theta_2 \in N$ por la normalidad de N en A_n . Si $\gamma \notin A_n$ (es impar), como $n \geq 5$, existen al menos dos elementos $\{c_1, c_2\}$ en $\{1, \dots, n\}$ que no están en el soporte de θ_1 (que tiene 3 elementos). Definimos $\gamma' = \gamma(c_1 \ c_2)$. Como $(c_1 \ c_2)$ es una transposición disjunta de θ_1 , conmuta con θ_1 . Además, γ' es par (producto de impar por impar). Entonces:

$$\gamma'\theta_1(\gamma')^{-1} = \gamma(c_1 \ c_2)\theta_1(c_1 \ c_2)^{-1}\gamma^{-1} = \gamma\theta_1\gamma^{-1} = \theta_2$$

Como $\gamma' \in A_n$ y $N \trianglelefteq A_n$, concluimos que $\theta_2 \in N$.

Caso $n = 3$: $A_3 = \{(1), (1 \ 2 \ 3), (1 \ 3 \ 2)\}$. Si N contiene un 3-ciclo, por ejemplo $(1 \ 2 \ 3)$, al ser subgrupo debe contener a su inverso $(1 \ 3 \ 2)$ y a la identidad. Por lo tanto, N contiene a todos los elementos de A_3 , así que $N = A_3$.

Caso $n = 4$: En A_4 , los 3-ciclos se dividen en dos clases de conjugación (por ejemplo, la clase de $(1 \ 2 \ 3)$ y la de $(1 \ 3 \ 2)$). Supongamos que N contiene a $\theta = (1 \ 2 \ 3)$. Como $N \trianglelefteq A_4$, N contiene a toda la clase de conjugación de θ en A_4 (que son 4 elementos: $(1 \ 2 \ 3), (1 \ 4 \ 2), (1 \ 3 \ 4), (2 \ 4 \ 3)$). Además, N debe contener a los inversos de estos elementos (por ejemplo, $(1 \ 3 \ 2)$). Al contener elementos de ambas clases de 3-ciclos y ser cerrado bajo productos, N contendrá a todos los 3-ciclos. Como los 3-ciclos generan A_4 , entonces $N = A_4$.

En todos los casos, $N = A_n$.

b) Sea $N \trianglelefteq S_n$ tal que contiene una transposición $\tau = (a \ b)$. Como N es normal en S_n , contiene a todos los conjugados de τ . Sabemos que en S_n cualquier transposición es conjugada de τ (tienen la misma estructura de ciclos). Por lo tanto, N contiene a todas las transposiciones. Como todo elemento de S_n se puede escribir como producto de transposiciones, concluimos que $N = S_n$. \square

Definición 4.2.6. Sea G un grupo. Diremos que G es simple si sus únicos subgrupos normales son $\{e\}$ y el mismo G .

Teorema 4.2.6. Sea $n \geq 5$, entonces el grupo alternante A_n es simple.

Demostración.

Sea $H \trianglelefteq A_n$ con $H \neq \{e\}$. Probaremos que H contiene un 3-ciclo. Por el corolario anterior, esto implicará que $H = A_n$. Sea $\alpha \in H$ con $\alpha \neq e$. Analicemos la descomposición de α en ciclos disjuntos:

Caso 1: α contiene un ciclo de longitud $r \geq 4$. Sea $\alpha = (a_1 \ a_2 \ a_3 \ \dots \ a_r)\tau$, donde τ son los demás ciclos disjuntos. Sea $\beta = (a_1 \ a_2 \ a_3) \in A_n$. Consideremos el conmutador $\rho = \alpha\beta\alpha^{-1}\beta^{-1} \in H$ (pues $H \trianglelefteq A_n$).

$$\begin{aligned}\rho &= \alpha(a_1 \ a_2 \ a_3)\alpha^{-1}(a_1 \ a_3 \ a_2) \\ &= (\alpha(a_1) \ \alpha(a_2) \ \alpha(a_3))(a_1 \ a_3 \ a_2) \\ &= (a_2 \ a_3 \ a_4)(a_1 \ a_3 \ a_2) \\ &= (a_1 \ a_4 \ a_2)\end{aligned}$$

Así, $\rho = (a_1 \ a_4 \ a_2)$ es un 3-ciclo que pertenece a H .

Caso 2: α contiene 3-ciclos en su descomposición. Si α es un 3-ciclo, ya terminamos. Si no, $\alpha = (a_1 \ a_2 \ a_3)(a_4 \ a_5 \ a_6) \dots$. Sea $\beta = (a_1 \ a_2 \ a_4) \in A_n$. Consideremos $\rho = \alpha\beta\alpha^{-1}\beta^{-1} \in H$:

$$\begin{aligned}\rho &= (\alpha(a_1) \ \alpha(a_2) \ \alpha(a_4))(a_1 \ a_4 \ a_2) \\ &= (a_2 \ a_3 \ a_5)(a_1 \ a_4 \ a_2) \\ &= (a_1 \ a_4 \ a_3 \ a_5 \ a_2)\end{aligned}$$

ρ es un 5-ciclo. Aplicando el Caso 1 a ρ , concluimos que H contiene un 3-ciclo.

Caso 3: α es producto de transposiciones disjuntas.

- i) $\alpha = (a_1 \ a_2)(a_3 \ a_4)$. (Solo dos transposiciones). Como $n \geq 5$, existe $a_5 \notin \{a_1, a_2, a_3, a_4\}$. Sea $\beta = (a_1 \ a_2 \ a_5) \in A_n$.

$$\rho = \alpha\beta\alpha^{-1}\beta^{-1} = (a_2 \ a_1 \ a_5)(a_1 \ a_5 \ a_2) = (a_1 \ a_5)(a_2 \ a_5) = (a_1 \ a_2 \ a_5)$$

Obtenemos directamente un 3-ciclo en H .

- ii) $\alpha = (a_1 \ a_2)(a_3 \ a_4)(a_5 \ a_6) \dots$ (Más de dos transposiciones). Sea $\beta = (a_1 \ a_2 \ a_3) \in A_n$.

$$\rho = \alpha\beta\alpha^{-1}\beta^{-1} = (a_2 \ a_1 \ a_4)(a_1 \ a_3 \ a_2) = (a_1 \ a_4)(a_2 \ a_3)$$

Ahora ρ tiene la forma del subcaso (i) anterior. Aplicando el argumento de (i) a ρ , obtenemos un 3-ciclo.

En cualquier caso, H contiene un 3-ciclo. Por lo tanto, $H = A_n$. \square

Teorema 4.2.7. *A_4 no tiene subgrupos de orden 6.*

Demostración.

Sabemos que $|A_4| = \frac{4!}{2} = 12$. Supongamos que existe $H \leq A_4$ tal que $|H| = 6$. Entonces el índice es $[A_4 : H] = \frac{12}{6} = 2$.

Sabemos que todo subgrupo de índice 2 es normal, por lo tanto $H \trianglelefteq A_4$. Además, en el grupo cociente A_4/H (que es de orden 2), el cuadrado de cualquier elemento es la identidad. Esto significa que para todo $\sigma \in A_4$, $\sigma^2 H = H$, es decir, $\sigma^2 \in H$.

Consideremos los 3-ciclos de A_4 . Sea θ un 3-ciclo. Entonces $\theta^3 = e$, de donde $\theta^4 = \theta$. Podemos escribir $\theta = (\theta^2)^2$. Como $\theta^2 \in H$ (por la propiedad del índice 2), y H es subgrupo, entonces $(\theta^2)^2 \in H$, luego $\theta \in H$.

Esto implica que H debe contener a **todos** los 3-ciclos de A_4 . Los 3-ciclos en A_4 son: $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$. Hay 8 3-ciclos en total.

Por lo tanto, $|H| \geq 8$, lo cual contradice la hipótesis de que $|H| = 6$. Concluimos que no existe tal subgrupo. \square

CAPÍTULO 5

Acciones de Grupos

5.1. Acciones de Grupo

Definición 5.1.1. Sea G un grupo y X un conjunto no vacío. Diremos que G actúa en X (o que X es un G -conjunto) si existe un homomorfismo $\varphi : G \rightarrow S_X$, donde S_X es el grupo de permutaciones de X (biyecciones de X en sí mismo).

Ejemplo 5.1. Teorema de Cayley: Todo grupo G actúa en sí mismo. Sea $X = G$ y definamos $\varphi : G \rightarrow S_G$ dada por $\varphi(g) = f_g$, donde $f_g : G \rightarrow G$ se define como $f_g(a) = ga$ para todo $a \in G$ (traslación izquierda).

Veamos que $f_g \in S_G$:

1. f_g es inyectiva: Si $f_g(a) = f_g(b)$, entonces $ga = gb$. Multiplicando por g^{-1} a la izquierda, obtenemos $a = b$.
2. f_g es sobreyectiva: Sea $b \in G$. Queremos encontrar a tal que $f_g(a) = b$. Tomamos $a = g^{-1}b$, entonces $f_g(g^{-1}b) = g(g^{-1}b) = (gg^{-1})b = b$.

Además, φ es un homomorfismo de grupos: Para $g, h \in G$, queremos ver que $\varphi(gh) = \varphi(g) \circ \varphi(h)$. Evaluando en un elemento $a \in G$:

$$\varphi(gh)(a) = f_{gh}(a) = (gh)a = g(ha) = f_g(ha) = f_g(f_h(a)) = (\varphi(g) \circ \varphi(h))(a)$$

Por lo tanto, $\varphi(gh) = \varphi(g) \circ \varphi(h)$.

Teorema 5.1.1. *Sea G un grupo y X un conjunto no vacío. Las siguientes condiciones son equivalentes:*

1. *G actúa en X (existe un homomorfismo $\varphi : G \rightarrow S_X$).*
2. *Existe una función $\cdot : G \times X \rightarrow X$, denominada por $(g, x) \mapsto g \cdot x$, tal que:*
 - a) *$e \cdot x = x$ para todo $x \in X$.*
 - b) *$(gh) \cdot x = g \cdot (h \cdot x)$ para todo $g, h \in G$ y $x \in X$.*

Demostración.

\Rightarrow) Supongamos que existe un homomorfismo $\varphi : G \rightarrow S_X$. Para cada $g \in G$, $\varphi(g)$ es una permutación de X , es decir, una función biyectiva $\varphi(g) : X \rightarrow X$. Definamos la función $\cdot : G \times X \rightarrow X$ mediante:

$$g \cdot x = (\varphi(g))(x)$$

para todo $g \in G$ y $x \in X$.

Verifiquemos las dos condiciones de la definición de acción:

- (i) Como φ es un homomorfismo de grupos, envía el neutro de G al neutro de S_X . Es decir, $\varphi(e) = Id_X$ (la función identidad en X). Entonces, para cualquier $x \in X$:

$$e \cdot x = (\varphi(e))(x) = Id_X(x) = x$$

- (ii) Sean $g, h \in G$ y $x \in X$. Por la definición de la operación y la propiedad de homomorfismo de φ :

$$(gh) \cdot x = (\varphi(gh))(x)$$

Como φ es homomorfismo, $\varphi(gh) = \varphi(g) \circ \varphi(h)$. Así:

$$(\varphi(gh))(x) = (\varphi(g) \circ \varphi(h))(x)$$

Por la definición de composición de funciones:

$$(\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x))$$

Usando nuevamente la definición de la acción ($g \cdot y = \varphi(g)(y)$):

$$\varphi(g)(\varphi(h)(x)) = g \cdot (\varphi(h)(x)) = g \cdot (h \cdot x)$$

Por lo tanto, $(gh) \cdot x = g \cdot (h \cdot x)$.

\Leftarrow) Supongamos que existe una función $\cdot : G \times X \rightarrow X$ que satisface las condiciones (a) y (b). Queremos construir un homomorfismo $\varphi : G \rightarrow S_X$. Para cada $g \in G$, definamos la función $\sigma_g : X \rightarrow X$ dada por:

$$\sigma_g(x) = g \cdot x$$

Primero, debemos demostrar que σ_g es una biyección (es decir, $\sigma_g \in S_X$).

1. σ_g es inyectiva: Supongamos que $\sigma_g(x) = \sigma_g(y)$ para $x, y \in X$.

$$g \cdot x = g \cdot y$$

Operamos con g^{-1} por la izquierda (usando la propiedad (b)):

$$g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y)$$

$$(g^{-1}g) \cdot x = (g^{-1}g) \cdot y$$

$$e \cdot x = e \cdot y$$

Usando la propiedad (a) ($e \cdot x = x$):

$$x = y$$

2. σ_g es sobreyectiva: Sea $y \in X$ arbitrario. Queremos encontrar $x \in X$ tal que $\sigma_g(x) = y$.

Proponemos $x = g^{-1} \cdot y$. Evaluamos $\sigma_g(x)$:

$$\sigma_g(g^{-1} \cdot y) = g \cdot (g^{-1} \cdot y)$$

Por la propiedad (b):

$$g \cdot (g^{-1} \cdot y) = (gg^{-1}) \cdot y = e \cdot y$$

Por la propiedad (a):

$$e \cdot y = y$$

Así, σ_g es sobreyectiva.

Al ser inyectiva y sobreyectiva, $\sigma_g \in S_X$.

Ahora definimos la función $\varphi : G \rightarrow S_X$ como $\varphi(g) = \sigma_g$. Veamos que φ es un homomorfismo de grupos. Sean $g, h \in G$. Queremos ver que $\varphi(gh) = \varphi(g) \circ \varphi(h)$. Dos funciones son iguales si toman el mismo valor para todo elemento del dominio. Sea $x \in X$:

$$(\varphi(gh))(x) = \sigma_{gh}(x) = (gh) \cdot x$$

Por otro lado:

$$(\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x)) = \sigma_g(\sigma_h(x))$$

$$\sigma_g(\sigma_h(x)) = \sigma_g(h \cdot x) = g \cdot (h \cdot x)$$

Como la propiedad (b) nos dice que $(gh) \cdot x = g \cdot (h \cdot x)$, concluimos que:

$$(\varphi(gh))(x) = (\varphi(g) \circ \varphi(h))(x) \quad \forall x \in X$$

Por lo tanto, $\varphi(gh) = \varphi(g) \circ \varphi(h)$, y φ es un homomorfismo. \square

Ejemplo 5.2. 1. G actúa en sí mismo por multiplicación izquierda (o simplemente por la operación del grupo). La acción está dada por $\varphi : G \rightarrow S_G$ o equivalentemente $\tilde{\varphi} : G \times G \rightarrow G$ definida por:

$$(g, h) \mapsto gh$$

2. Sea G un grupo, $H \leq G$ y $X = \{aH \mid a \in G\}$ el conjunto de clases laterales izquierdas. G actúa en X por traslación izquierda. La acción está definida por $\varphi : G \rightarrow S_X$, donde para cada $g \in G$, la función $f_g : X \rightarrow X$ es:

$$f_g(aH) = (ga)H$$

Equivalentemente, $\tilde{\varphi}(g, aH) = gaH$.

3. Sea G un grupo y $X = \{H \mid H \leq G\}$ el conjunto de subgrupos de G . G actúa en X por conjugación. Definimos $\varphi : G \rightarrow S_X$ tal que $g \mapsto f_g$, con $f_g(H) = gHg^{-1}$. Verifiquemos que es una acción:

- $e \cdot H = eHe^{-1} = H$.
- $(gh) \cdot H = (gh)H(gh)^{-1} = g(hHh^{-1})g^{-1} = g(h \cdot H)g^{-1}$.

4. Sea G un grupo y $X = G$. G actúa en sí mismo por conjugación. Definimos la acción $\cdot : G \times G \rightarrow G$ como:

$$g \cdot h = ghg^{-1}$$

5. Sea $G = SL(2, \mathbb{C}) = \{A \in M_{2 \times 2}(\mathbb{C}) \mid \det A = 1\}$ y sea $X = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$ el semiplano superior. Para $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, definimos la acción:

$$A \cdot z = \frac{az + b}{cz + d}$$

Se verifica que $I \cdot z = z$ y $A \cdot (B \cdot z) = (AB) \cdot z$.

6. Sea $X = \mathbb{R}^2$ y G el grupo de rotaciones del plano (isomorfo a $SO(2)$):

$$G = \{T_\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \mid T_\theta(x, y) = (x \cos \theta - y \sin \theta, x \sin \theta + y \cos \theta)\}$$

Entonces, para un punto $(x_0, y_0) \in \mathbb{R}^2$, su órbita es:

$$\mathcal{O}_{(x_0, y_0)} = \{T_\theta(x_0, y_0) \mid T_\theta \in G\} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = x_0^2 + y_0^2\}$$

Es decir, las órbitas son circunferencias centradas en el origen.

Definición 5.1.2. Diremos que una acción de G en X es transitiva si existe $x \in X$ tal que su órbita cubre todo el conjunto, es decir:

$$\mathcal{O}_x = G \cdot x = X$$

(Esto implica que solo existe una única órbita).

Definición 5.1.3. Sea X un G -conjunto. Diremos que $x \in X$ es un punto fijo si $g \cdot x = x$ para todo $g \in G$. Esto es equivalente a cualquiera de las siguientes condiciones:

- La órbita de x es trivial: $\mathcal{O}_x = \{x\}$.
- El estabilizador de x es todo el grupo: $St_G(x) = G$.

Observación 5.1. Si X es un G -conjunto y $x \in X$, entonces el estabilizador $St_G(x)$ es un subgrupo de G .

Demostración.

Sean $g, h \in St_G(x)$. Entonces $g \cdot x = x$ y $h \cdot x = x$. Esto implica que $h^{-1} \cdot x = x$ (multiplicando por h^{-1}). Luego:

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x$$

Por lo tanto $gh^{-1} \in St_G(x)$, lo que prueba que es un subgrupo. \square

Nota 5.1.1. El conjunto de todos los puntos fijos de X bajo la acción de G se denota por X^G .

Observación 5.2. Sea X un G -conjunto, entonces las órbitas forman una partición de X . Para ver esto basta verificar que inducen una relación de equivalencia, es decir, la relación en X definida por $x \sim y$ si y solo si y y x están en la misma órbita (si y solo si $y = g \cdot x$ para algún $g \in G$) es de equivalencia.

1. *Reflexiva:* Existe $e \in G$ tal que $e \cdot x = x$, así $x \sim x$.
2. *Simétrica:* $x \sim y$, entonces existe $g \in G$ tal que $y = g \cdot x$. Entonces $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = e \cdot x = x$. Así, $x = g^{-1} \cdot y$, de donde $y \sim x$.
3. *Transitiva:* $x \sim y$ y $y \sim z$, entonces existen $g_1, g_2 \in G$ tales que $y = g_1 \cdot x$, $z = g_2 \cdot y$. Entonces

$$z = g_2 \cdot (g_1 \cdot x) = (g_2 g_1) \cdot x$$

luego $x \sim z$.

En particular si $\mathcal{O}_x = Orb(x) = G \cdot x$, tenemos:

$$X = \bigcup_{x \in X} \mathcal{O}_x = \left(\bigcup_{x \in X^G} \mathcal{O}_x \right) \cup \left(\bigcup_{x \notin X^G} \mathcal{O}_x \right) = \left(\bigcup_{x \in X^G} \{x\} \right) \cup \left(\bigcup_{x \notin X^G} \mathcal{O}_x \right)$$

En particular, si X es finito:

$$|X| = |X^G| + \left| \bigcup_{x \notin X^G} \mathcal{O}_x \right|$$

Ejemplo 5.3. Consideremos la acción de G en sí mismo por conjugación, es decir, la acción definida por:

$$g \cdot h = ghg^{-1} \quad \forall g, h \in G$$

En este caso, un elemento $h \in G$ es un punto fijo si y solo si su órbita tiene tamaño 1, es decir:

$$g \cdot h = h \quad \forall g \in G$$

Esto equivale a:

$$ghg^{-1} = h \iff gh = hg \quad \forall g \in G$$

Por lo tanto, el conjunto de puntos fijos de esta acción es exactamente el Centro de G :

$$G^G = Z(G) = \{h \in G \mid gh = hg, \forall g \in G\}$$

Aplicando la ecuación de las órbitas (vista anteriormente) a esta acción específica, obtenemos la **Ecuación de Clase**:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)]$$

donde $C_G(x_i)$ es el centralizador de x_i (que corresponde al estabilizador bajo esta acción).

Teorema 5.1.2 (Teorema). Sea X un G -conjunto, $x \in X$, entonces existe una biyección entre las clases laterales de $S_t(x) \leq G$ y \mathcal{O}_x .

Demostración.

Definamos $\varphi : \mathcal{L} \rightarrow \mathcal{O}_x$ (donde \mathcal{L} es el conjunto de clases laterales izquierdas) dada por:

$$gS_t(x) \mapsto g \cdot x$$

Note que esta asignación no depende del representante de clase. Si $gS_t(x) = g_1S_t(x)$, entonces $g^{-1}g_1 \in S_t(x)$, si y solo si $(g^{-1}g_1) \cdot x = x$, si y solo si $g_1 \cdot x = g \cdot x$. Es decir, $\varphi(gS_t(x)) = \varphi(g_1S_t(x))$. Luego, φ está bien definida.

φ es inyectiva:

$$\begin{aligned} \varphi(gS_t(x)) = \varphi(g_1S_t(x)) &\iff g \cdot x = g_1 \cdot x \iff g^{-1}g_1 \cdot x = x \\ &\iff g^{-1}g_1 \in S_t(x) \iff gS_t(x) = g_1S_t(x) \end{aligned}$$

φ es sobreyectiva: Dado $y \in \mathcal{O}_x$, existe $g \in G$ tal que $y = g \cdot x$, luego:

$$\varphi(gS_t(x)) = g \cdot x = y$$

Por lo tanto φ es biyectiva y en particular:

$$|\mathcal{O}_x| = |\mathcal{L}| = |\mathcal{G}| = [G : S_t(x)]$$

□

Observación 5.3. Más aún, de la ecuación de las órbitas tenemos:

$$|X| = |X^G| + \sum_{x \notin X^G} [G : St_G(x)]$$

Todavía más, si G actúa en sí mismo por conjugación. En este caso $X^G = Z(G)$ y al estabilizador $St_G(x)$ se le denomina el Centralizador de x en G y se denota por $C_G(x)$. La ecuación se convierte en:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : C_G(x)]$$

donde la suma corre sobre un sistema de representantes de las clases de conjugación no triviales.

Ejemplo 5.4. Sea G un grupo y $X = \{H \mid H \leq G\}$ el conjunto de subgrupos de G . Hagamos actuar a G en X por conjugación, es decir, la acción dada por:

$$g \cdot H = gHg^{-1}$$

En este caso, al estabilizador de un elemento $H \in X$ se le llama el Normalizador de H en G y se denota por $N_G(H)$.

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

Observación 5.4. Si $H \leq G$, entonces se cumplen las siguientes propiedades del normalizador $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$:

1. $H \trianglelefteq G$ si y solo si $N_G(H) = G$.
2. $H \leq N_G(H)$ (es decir, H es un subgrupo del normalizador).
3. En general, no siempre ocurre que $N_G(H) = G$. (Ver ejemplo en S_3).
4. $H \trianglelefteq N_G(H)$ (es decir, H es un subgrupo normal de su propio normalizador).

Demostración de 1.

Queremos probar que $H \trianglelefteq G \iff N_G(H) = G$.

\Rightarrow) Supongamos que $H \trianglelefteq G$. Por definición de subgrupo normal, para todo $g \in G$ se cumple que $gHg^{-1} = H$. La definición del normalizador es $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. Como la condición se cumple para todo $g \in G$, entonces todo elemento de G pertenece a $N_G(H)$. Por lo tanto, $G \subseteq N_G(H)$. Como $N_G(H) \subseteq G$ es siempre cierto, concluimos que $N_G(H) = G$.

\Leftarrow) Supongamos que $N_G(H) = G$. Esto significa que para todo $g \in G$, $g \in N_G(H)$. Por la definición del conjunto $N_G(H)$, esto implica que para todo $g \in G$, se cumple $gHg^{-1} = H$. Esta es exactamente la definición de que H sea un subgrupo normal de G . Por lo tanto, $H \trianglelefteq G$. \square

Demostración de 2.

Queremos probar que $H \subseteq N_G(H)$. Sea $h \in H$ un elemento arbitrario. Queremos ver que $h \in N_G(H)$, es decir, que $hHh^{-1} = H$.

Como H es un subgrupo (cerrado bajo la operación):

- Para cualquier $x \in H$, el conjugado hxh^{-1} es producto de elementos de H , por lo que $hxh^{-1} \in H$. Esto muestra que $hHh^{-1} \subseteq H$.
- Para la contención inversa, dado $y \in H$, podemos escribir $y = h(h^{-1}yh)h^{-1}$. Como $h^{-1}yh \in H$, entonces y es un conjugado por h de un elemento de H .

(Más simplemente: conjugación por un elemento del mismo subgrupo es un automorfismo interno restringido que envía H en H).

Por lo tanto, $hHh^{-1} = H$ para todo $h \in H$. Así, todo elemento de H cumple la condición de estar en el normalizador. Conclusión: $H \leq N_G(H)$. \square

Demostración de 3 (Ejemplo en S_3).

Consideremos el grupo simétrico S_3 . Sea $N = \langle(1, 2, 3)\rangle = \{e, (1, 2, 3), (1, 3, 2)\}$. Sabemos que $|S_3| = 6$ y $|N| = 3$. El índice es $[S_3 : N] = 2$, por lo que $N \trianglelefteq S_3$. Usando la propiedad 1, como es normal, su normalizador es todo el grupo: $N_{S_3}(N) = S_3$.

Ahora consideremos $H = \langle(1, 2)\rangle = \{e, (1, 2)\}$. Calculemos su normalizador $N_{S_3}(H)$. Buscamos los $g \in S_3$ tales que $gHg^{-1} = H$.

- Claramente $H \subseteq N_{S_3}(H)$ (por la propiedad 2), así que e y $(1, 2)$ están en el normalizador.
- Probemos con otro elemento, por ejemplo $\sigma = (1, 3)$. Conjugamos el generador de H :

$$(1, 3)(1, 2)(1, 3)^{-1} = (1, 3)(1, 2)(1, 3) = (2, 3)$$

Como $(2, 3) \notin H$, entonces $(1, 3)H(1, 3)^{-1} \neq H$. Por lo tanto, $(1, 3) \notin N_{S_3}(H)$.

De hecho, haciendo las cuentas para los demás elementos, vemos que el único subgrupo que normaliza a H es el mismo H . Así que $N_{S_3}(H) = H \neq S_3$. Esto demuestra que $N_G(H)$ no siempre es todo G . \square

Demostración de 4.

Queremos probar que $H \trianglelefteq N_G(H)$. Ya sabemos por la propiedad 2 que H es un subgrupo de $N_G(H)$. Solo falta probar la normalidad dentro de este grupo.

Sea $g \in N_G(H)$ un elemento cualquiera del normalizador. Por la definición misma de $N_G(H)$, este g cumple la condición:

$$gHg^{-1} = H$$

Esta igualdad nos dice directamente que conjugando H por cualquier elemento de $N_G(H)$, obtenemos H nuevamente.

Esta es, textualmente, la definición de ser subgrupo normal. Por lo tanto, H es normal en $N_G(H)$. \square

Teorema 5.1.3 (de Cauchy). *Sea G un grupo finito y p un número primo tal que p divide al orden de G ($p \mid |G|$). Entonces, G contiene al menos un elemento de orden p . Más precisamente, la cantidad de elementos de G de orden p es congruente con -1 módulo p .*

Demostración.

Consideremos el conjunto X formado por las p -tuplas de elementos de G cuyo producto es la identidad:

$$X = \{(x_1, x_2, \dots, x_p) \in G^p \mid x_1 x_2 \dots x_p = e\}$$

Paso 1: Calcular la cardinalidad de X . Para formar una tupla en X , podemos elegir los primeros $p - 1$ elementos (x_1, \dots, x_{p-1}) arbitrariamente en G . Una vez elegidos, el último elemento x_p está forzado, pues debe cumplir:

$$x_1 \dots x_{p-1} x_p = e \implies x_p = (x_1 \dots x_{p-1})^{-1}$$

Dado que x_p es único para cada elección de los primeros $p - 1$ términos, el tamaño de X es:

$$|X| = |G|^{p-1}$$

Como por hipótesis p divide a $|G|$, entonces p divide a $|G|^{p-1}$ (para $p - 1 \geq 1$), por lo que:

$$|X| \equiv 0 \pmod{p}$$

Paso 2: Definir la acción de grupo. Sea $\mathbb{Z}_p = \langle \sigma \rangle$ el grupo cíclico de orden p . Hacemos actuar a \mathbb{Z}_p sobre el conjunto X mediante permutación cíclica de las componentes:

$$\sigma \cdot (x_1, x_2, \dots, x_p) = (x_2, x_3, \dots, x_p, x_1)$$

Verifiquemos que esta acción está bien definida, es decir, que si $(x_1, \dots, x_p) \in X$, entonces su permutación cíclica también está en X . Si $x_1 x_2 \dots x_p = e$, multiplicando por x_1^{-1} a la izquierda y por x_1 a la derecha (conjugando por x_1), obtenemos:

$$x_1^{-1} (x_1 x_2 \dots x_p) x_1 = x_1^{-1} e x_1 = e$$

Simplificando el lado izquierdo:

$$(x_1^{-1} x_1) x_2 \dots x_p x_1 = x_2 \dots x_p x_1 = e$$

Por lo tanto, la tupla rotada (x_2, \dots, x_p, x_1) cumple la condición de producto identidad y pertenece a X .

Paso 3: Analizar las órbitas y los puntos fijos. Por el Teorema Órbita-Estabilizador, el tamaño de cualquier órbita divide al orden del grupo que actúa. Aquí, $|\mathbb{Z}_p| = p$ (primo). Por tanto, el tamaño de cualquier órbita $|\mathcal{O}_x|$ solo puede ser 1 o p .

Las órbitas de tamaño 1 corresponden a los puntos fijos de la acción $(X^{\mathbb{Z}_p})$. Una tupla $x = (x_1, \dots, x_p)$ es un punto fijo si:

$$(x_1, x_2, \dots, x_p) = (x_2, x_3, \dots, x_p, x_1)$$

Esto implica que $x_1 = x_2 = \dots = x_p$. Además, como la tupla está en X , el producto debe ser la identidad:

$$x_1 \cdot x_1 \dots x_1 = x_1^p = e$$

Así, los puntos fijos son precisamente las tuplas de la forma (g, g, \dots, g) donde $g^p = e$.

Paso 4: Conclusión usando la Ecuación de Clase. La ecuación de clase para esta acción es:

$$|X| = |X^{\mathbb{Z}_p}| + \sum |\mathcal{O}_{\text{tamaño } p}|$$

Tomando módulo p :

$$|X| \equiv |X^{\mathbb{Z}_p}| \pmod{p}$$

(Pues las órbitas de tamaño p son congruentes con 0 módulo p).

Sabemos por el Paso 1 que $|X| \equiv 0 \pmod{p}$. Entonces:

$$|X^{\mathbb{Z}_p}| \equiv 0 \pmod{p}$$

Sabemos que existe al menos un punto fijo trivial: la tupla (e, e, \dots, e) , donde $e^p = e$. Por lo tanto, $|X^{\mathbb{Z}_p}| \geq 1$. Como $|X^{\mathbb{Z}_p}|$ es un múltiplo de p y es al menos 1, debe ser al menos p (es decir, $|X^{\mathbb{Z}_p}| \geq p$).

Esto significa que existen al menos $p - 1$ tuplas fijas distintas de la trivial. Sea (a, a, \dots, a) una de estas tuplas con $a \neq e$. Entonces $a \in G$ satisface $a^p = e$ y $a \neq e$. Por lo tanto, a es un elemento de orden p . \square

Definición 5.1.4. *Sea G un grupo y p un número primo. Diremos que G es un p -grupo si todo elemento de G tiene orden igual a una potencia de p . Es decir, para todo $g \in G$, existe $k \geq 0$ tal que $o(g) = p^k$.*

Observación 5.5. *Si G es un p -grupo, no necesariamente es finito. (Existen p -grupos infinitos, como por ejemplo el grupo de Prüfer \mathbb{Z}_{p^∞}).*

Corolario 5.1.1. *Si G es un p -grupo finito, entonces $|G| = p^n$ para algún $n \in \mathbb{N}$.*

Demostración.

Supongamos que $|G|$ no es una potencia de p . Entonces, por el Teorema Fundamental de la Aritmética, existe un primo q tal que $q \mid |G|$ y $q \neq p$. Por el Teorema de Cauchy, como q divide al orden del grupo, existe un elemento $g \in G$ tal que $o(g) = q$. Pero q no es una potencia de p (pues $q \neq p$ son primos). Esto contradice la hipótesis de que G es un p -grupo (todos sus elementos deben tener orden potencia de p). Por lo tanto, el único divisor primo de $|G|$ es p , lo que implica que $|G| = p^n$. \square

Corolario 5.1.2. *Sea G un grupo finito. Entonces G es un p -grupo si y solo si $|G| = p^n$ para algún $n \in \mathbb{N}$.*

Demostración.

$\Rightarrow)$ Ya fue probado en el corolario anterior.

$\Leftarrow)$ Supongamos que $|G| = p^n$. Sea $g \in G$ un elemento cualquiera. Por el Teorema de Lagrange, el orden del elemento divide al orden del grupo, es decir, $o(g) \mid |G|$. Como $|G| = p^n$, los únicos divisores son de la forma p^k con $0 \leq k \leq n$. Por lo tanto, $o(g) = p^k$. Como esto vale para todo $g \in G$, concluimos que G es un p -grupo. \square

Ejemplo 5.5. *Sea G un grupo de orden pq , con p, q primos distintos. Sin pérdida de generalidad, supongamos $p < q$. Por el Teorema de Cauchy, existen elementos $a, b \in G$ tales que $o(a) = p$ y $o(b) = q$. Sean $H = \langle a \rangle$ y $K = \langle b \rangle$ los subgrupos generados.*

Observamos que:

- $[G : K] = p$. Como p es el menor primo que divide al orden de G (pues $p < q$), sabemos por un resultado anterior que $K \trianglelefteq G$.
- $H \cap K = \{e\}$, pues los órdenes de sus elementos son coprimos (salvo la identidad).
- $|HK| = \frac{|H||K|}{|H \cap K|} = pq = |G|$, por lo tanto $G = HK$.

Ahora analizamos la normalidad de H :

- i) *Si $H \trianglelefteq G$, como ya tenemos $K \trianglelefteq G$ y intersección trivial, entonces G es el producto directo interno:*

$$G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

En este caso, G es cíclico y abeliano.

- ii) *Si H no es normal en G , entonces G no es abeliano (pues en un grupo abeliano todo subgrupo es normal). Sabemos que siempre existe el grupo cíclico \mathbb{Z}_{pq} . Si G no es abeliano, su estructura es un producto semidirecto no trivial.*

Corolario 5.1.3. *Sea G un grupo de orden p^2 , con p primo. Entonces G es abeliano.*

Demostración.

Por el Teorema de Cauchy, existe $a \in G$ tal que $o(a) = p$. Sea $H = \langle a \rangle$. Como $|H| = p$ y $|G| = p^2$, el índice es $[G : H] = p$. Como p es el menor primo que divide a $|G|$, entonces $H \trianglelefteq G$.

Consideremos un elemento $b \in G \setminus H$.

- **Caso 1:** Si $o(b) = p^2$, entonces $G = \langle b \rangle \cong \mathbb{Z}_{p^2}$, el cual es abeliano.

- **Caso 2:** Si todo elemento en $G \setminus H$ tiene orden p . Sea $K = \langle b \rangle$. Como $b \notin H$ y $|H| = p$ (primo), $H \cap K = \{e\}$. Al ser H normal y $H \cap K = \{e\}$, el subgrupo HK es isomorfo al producto directo. Como $|HK| = p^2 = |G|$, entonces $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$. El producto directo de grupos abelianos es abeliano.

En cualquier caso, G es abeliano. □

Teorema 5.1.4. *Sea G un p -grupo finito no trivial (es decir, $|G| = p^n$ con $n \geq 1$).*

Entonces su centro es no trivial:

$$Z(G) \neq \{e\}$$

Demostración.

Hagamos actuar a G en sí mismo por conjugación:

$$g \cdot x = gxg^{-1}$$

La Ecuación de Clase para esta acción es:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)]$$

donde la suma recorre un sistema de representantes de las clases de conjugación no triviales (aquellas con más de un elemento).

Analicemos la divisibilidad por p :

1. $|G| = p^n$, por lo que $|G|$ es divisible por p (pues $n \geq 1$).
2. Para cada $x_i \notin Z(G)$, su centralizador $C_G(x_i)$ es un subgrupo propio de G (si fuera todo G , x_i estaría en el centro). Por el Teorema de Lagrange, $[G : C_G(x_i)] = \frac{|G|}{|C_G(x_i)|}$. Como $|G|$ es potencia de p , este índice también debe ser una potencia de p . Como $x_i \notin Z(G)$, el índice es mayor que 1. Por lo tanto, p divide a $[G : C_G(x_i)]$.

Entonces, en la ecuación de clase:

$$\underbrace{|G|}_{\text{divisible por } p} = |Z(G)| + \underbrace{\sum [G : C_G(x_i)]}_{\text{divisible por } p}$$

Esto implica que p debe dividir a $|Z(G)|$.

Como el neutro e siempre está en el centro, $|Z(G)| \geq 1$. Al ser múltiplo de p , concluimos que $|Z(G)| \geq p$, por lo que $Z(G) \neq \{e\}$. □

5.2. Grupos Sylow

Definición 5.2.1. *Sea G un grupo, diremos que H es un subgrupo maximal de G si cuando N es un subgrupo de G con $H \subseteq N \subseteq G$, entonces $N = G$ o $N = H$*

Definición 5.2.2. Sea G un grupo, p un primo que divide a $|G|$. Diremos que P es un p -subgrupo de Sylow de G si P es un p -grupo maximal (con respecto a la propiedad de ser p -grupo) es decir, si H es un p -grupo tal que $P \subseteq H \subseteq G$ entonces $H = G$ o $H = P$

Observación 5.6. Si G es un grupo finito, y p es primo que divide a $|G|$ entonces existe un p -subgrupo Sylow de G

Demostración.

Sea $\mathcal{A} = \{H \leq G \mid H \text{ es } p\text{-grupo}\}$. Por el teorema de Cauchy G tiene elementos de orden p , si $o(a) = p$, entonces $H = \langle a \rangle \in \mathcal{A}$. Luego, $\mathcal{A} \neq \emptyset$.

Sea $\{H_\lambda\}_{\lambda \in \Lambda}$ una cadena en \mathcal{A} . Sea $H = \bigcup_{\lambda \in \Lambda} H_\lambda$, entonces $H \in \mathcal{A}$ y en efecto si $a, b \in H$, existe $\lambda_1, \lambda_2 \in \Lambda$ tal que $a \in H_{\lambda_1}$ y $b \in H_{\lambda_2}$, como los $\{H_\lambda\}_{\lambda \in \Lambda}$ forman una cadena. Podemos suponer $H_{\lambda_1} \subseteq H_{\lambda_2}$ en cuyo caso $a, b \in H_{\lambda_2}$ y como $H_{\lambda_2} \leq G$, $ab^{-1} \in H_{\lambda_2} \subseteq H$, así $H \leq G$.

Más aún si $a \in H$, $a \in H_\lambda$ para algún $\lambda \in \Lambda$ así que $o(a) = p^n$ para algún $n \in \mathbb{N}$, luego H es p -grupo. Por lo tanto $H \in \mathcal{A}$, luego, \mathcal{A} tiene elementos maximales y por el lema de Zorn G los tiene. \square

Teorema 5.2.1 (Segundo y Tercer Teorema de Sylow). *Sea G grupo finito, p primo que divide a $|G|$, ℓ_p la cantidad de p -grupos Sylow, entonces:*

- i) $\ell_p \mid |G|$ y $\ell_p \equiv 1 \pmod{p}$.
- ii) Los p -grupos Sylow son conjugados.

Demostración.

Sea P un p -grupo Sylow de G y $X = \{gPg^{-1} \mid g \in G\}$ los subgrupos conjugados de P . (Note que $|X| < +\infty$). Hagamos actuar G en X por conjugación como sigue:

$$\tilde{\varphi} : G \times X \rightarrow X$$

$$(g, aPa^{-1}) \mapsto g(aPa^{-1})g^{-1}$$

$\tilde{\varphi}$ es acción pues:

$$\text{i)} \quad e(aPa^{-1})e = eaPa^{-1}e = aPa^{-1}.$$

$$\text{ii)} \quad (gh)(aPa^{-1}) = (gh)(aPa^{-1})(gh)^{-1}$$

$$= g(haPa^{-1}h^{-1})g^{-1}$$

$$= g \cdot (haPa^{-1})$$

$$= g \cdot (h \cdot aPa^{-1})$$

Además cada elemento de X es un p -grupo Sylow. Si Q es un p -subgrupo de G con $aPa^{-1} \subseteq Q \subsetneq G$ entonces $P = a^{-1}(aPa^{-1})a \subseteq a^{-1}Qa \subsetneq G$ y $a^{-1}Qa$ es un p -grupo (si $q \in a^{-1}Qa$, $g = a^{-1}qa$ con $q \in Q \implies g^{p^s} = (a^{-1}qa)^{p^s} = a^{-1}q^{p^s}a = a^{-1}ea = e$ si p^s es el orden de q , luego g tiene orden potencia de p). Por la maximalidad de P , $P = a^{-1}Qa$, luego $aPa^{-1} = Q$, así aPa^{-1} es maximal.

Restringiendo $\tilde{\varphi}$ a P , se tiene que P actúa en X . Sea $Q \in X$, entonces $[P : St_P(Q)] = p^s$ para algún s . Más aún si $s = 0$, entonces $P = St_P(Q) = \{p \in P \mid pQp^{-1} = Q\} = P \cap St_G(Q)$, de donde $P \subseteq St_G(Q)$. Además $Q \trianglelefteq St_G(Q) = N_G(Q)$, luego PQ es subgrupo de $St_G(Q)$, más aún es p -subgrupo de G y $P, Q \leq PQ$. Como P es Sylow, luego $PQ = G$ o $P = PQ = Q$. Si $G = PQ$ entonces $G = St_G(Q)$, luego $Q \trianglelefteq G$. Pero $Q = aPa^{-1}$ para algún $a \in G$, $Q = a^{-1}Qa = P$.

En cualquier caso entonces $P = Q$. Es decir, el único elemento de X que bajo la acción se queda fijo es P , por lo tanto

$$|X| = 1 + \sum_{Q \notin X^P} [P : St_P(Q)]$$

En particular $|X| \equiv 1 \pmod{p}$.

Sea ahora un Q p -subgrupo Sylow y suponga que $Q \notin X$, entonces restringiendo $\tilde{\varphi}$ a Q . Un argumento análogo muestra que

$$|X| \equiv 0 \pmod{p}$$

En efecto, si $Q_1 \in X$, entonces $[Q : St_Q(Q_1)] = p^s$ y $s = 0$ si y sólo si $Q = St_Q(Q_1) = St_G(Q_1) \cap Q$, luego $Q \subseteq St_G(Q_1)$ y como $Q_1 \trianglelefteq St_G(Q_1)$ entonces $QQ_1 \leq St_G(Q_1)$. Más aún QQ_1 es p -subgrupo. Así $Q \subseteq QQ_1 \subseteq G$ de donde $QQ_1 = G$ o $Q = QQ_1 = Q_1$. Si $QQ_1 = G$, $G = St_G(Q_1)$, luego $Q_1 \trianglelefteq G$, de donde $Q_1 = P \trianglelefteq G$. Luego $P \subsetneq QQ_1$ y QQ_1 es p -grupo lo cual no puede ser por la maximalidad de P . Por lo tanto $Q = Q_1 \# C$ (Contradicción) pues $Q_1 \in X$ y $Q \notin X$, es decir, con la acción $\tilde{\varphi}|_Q$, no hay puntos fijos y así

$$|X| = \sum_{Q_1 \notin X^G} [Q : St_Q(Q_1)] \equiv 0 \pmod{p}$$

Lo cuál no puede ser pues contradice (i), luego $Q \in X$, es decir, es un conjugado de P y por tanto $\ell_p = |X|$ y se tiene $\ell_p \equiv 1 \pmod{p}$. Más aún

$$X = \{gPg^{-1} \mid g \in G\} = \{g \cdot P \mid g \in G\} = \mathcal{O}_P$$

Así,

$$\ell_p = |X| = |\mathcal{O}_P| = [G : St_G(P)] \mid |G|$$

□

Teorema 5.2.2 (Primer Teorema de Sylow). *Sea G un grupo de orden $|G| = p^s m$ con p primo, $(p, m) = 1$ entonces todo p -grupo Sylow tiene cardinalidad p^s .*

Demostración.

Sea P un p -Sylow de G . Para ver que $|P| = p^s$ basta probar que $[G : P] = m$ ($|G| = [G : P]|P|$) y para esto, basta ver que $([G : P], p) = 1$ pues si esto pasa $p^s m = |G| = [G : P]|P|$, $([G : P], p) = 1$, entonces $p^s \mid |P|$, además $|P| \mid |G| = p^s m$, luego, $|P| = p^s p^t$ y $|P| \leq p^s m$ (pues P es subgrupo), luego, $p^s p^t \ell = p^s m$ y $(p, m) = 1$, de donde $t = 0$ o $|P| = p^s$.

Veamos entonces que $([G : P], p) = 1$, tenemos que se sigue del teorema de Lagrange que $[G : P] = [G : N(P)][N(P) : P]$ así que basta ver $([G : N(P)], p) = 1$, $([N(P) : P], p) = 1$.

Pero por el teorema anterior $[G : N(P)] = [G : St_G(P)] = |\mathcal{O}_P| = \ell_p \equiv 1 \pmod{p}$, luego $([G : N(P)], p) = 1$.

Ahora, si $([N(P) : P], p) \neq 1$, $p \mid [N(P) : P]$ y como $P \trianglelefteq N(P)$, entonces p divide el orden del grupo $N(P)/P$, luego por el teorema de Cauchy, existe $\bar{X} = XP \in N(P)/P$ tal que $\bar{X}^p = \bar{e} = P$.

Observe que:

$$\langle \bar{X} \rangle = \frac{\langle X, P \rangle}{P} \leq \frac{N(P)}{P} \quad \text{y} \quad (\bar{X})^p = e$$

$$\begin{array}{ccc} N(P)/P & \longrightarrow & N(P) \\ \downarrow & & \downarrow \\ \langle \bar{X} \rangle & \longrightarrow & \langle X, P \rangle \\ \downarrow & & \downarrow \\ P = \bar{e} & \longrightarrow & P \end{array}$$

Por lo tanto, $\frac{\langle X, P \rangle}{P}$ es p -grupo, de donde $\langle X, P \rangle$ es p -grupo y

$$|\langle X, P \rangle| = [\langle X, P \rangle : P]|P| = \left| \frac{\langle X, P \rangle}{P} \right| |P|$$

Por la maximalidad de $P \subseteq \langle X, P \rangle$, $P = \langle X, P \rangle$ o $x \in P$ y $o(\bar{x}) = 1 \# C$ (Contradicción), luego $([N(P) : P], p) = 1$. De donde se concluye que $|P| = p^s$. \square

Ejemplo 5.6. Sea $|G| = pq$ con $p < q$ números primos. Calculamos la cantidad de q -subgrupos de Sylow, n_q :

$$n_q \equiv 1 \pmod{q} \quad \text{y} \quad n_q \mid p$$

Los divisores de p son $\{1, p\}$.

- Si $n_q = p$, entonces $p \equiv 1 \pmod{q}$, lo cual implica que $q \mid (p - 1)$. Esto es imposible pues $p < q$ (un número mayor no puede dividir a uno menor positivo).

Por lo tanto, $n_q = 1$. Sea Q el único q -Sylow de G , entonces $Q \trianglelefteq G$.

Ahora analicemos n_p :

$$n_p \equiv 1 \pmod{p} \quad \text{y} \quad n_p \mid q$$

Los divisores de q son $\{1, q\}$. Así que n_p puede ser 1 o q .

Sea P un p -Sylow de G . Como $Q \trianglelefteq G$ y $P \leq G$, y además $Q \cap P = \{e\}$ (pues $|Q| = q$, $|P| = p$ y son primos distintos), tenemos que:

$$|QP| = \frac{|Q||P|}{|Q \cap P|} = \frac{qp}{1} = pq = |G|$$

Por lo tanto $G = QP$. Como Q es normal y $Q \cap P = \{e\}$, G es un producto semidirecto:

$$G \cong Q \rtimes_{\varphi} P$$

donde $\varphi : P \rightarrow \text{Aut}(Q)$ es un homomorfismo.

Sabemos que $Q \cong \mathbb{Z}_q$, por lo que $\text{Aut}(Q) \cong \text{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}$. El orden del grupo de automorfismos es $|\text{Aut}(Q)| = q - 1$. El homomorfismo φ está determinado por la imagen de un generador de P . El orden de la imagen debe dividir tanto al orden de P (p) como al orden de $\text{Aut}(Q)$ ($q - 1$).

Caso 1: $p \nmid (q - 1)$. En este caso, $\gcd(p, q - 1) = 1$. El único elemento de orden que divide a p en $\text{Aut}(Q)$ es la identidad. Por lo tanto, φ es el homomorfismo trivial ($\varphi(g) = \text{Id}_Q$ para todo g). Esto implica que el producto es directo:

$$G \cong Q \times P \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$$

Así, si $p \nmid (q - 1)$, el único grupo de orden pq es el cíclico \mathbb{Z}_{pq} .

Caso 2: $p \mid (q - 1)$. Por el Teorema de Cauchy, como p divide al orden de $\text{Aut}(Q)$, existe un subgrupo de orden p en $\text{Aut}(Q)$. Esto permite definir un homomorfismo φ no trivial. Por lo tanto, existe un producto semidirecto no abeliano:

$$G \cong Q \rtimes P$$

Este grupo es único salvo isomorfismo (todos los homomorfismos no triviales dan lugar a grupos isomorfos en este caso). **Ejemplo:** S_3 tiene orden $6 = 2 \cdot 3$. Aquí $p = 2, q = 3$. Como $2 \mid (3 - 1)$, existe el grupo no abeliano $S_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

Ejemplo 5.7. Sea $|G| = 30 = 2 \cdot 3 \cdot 5$. Analicemos los subgrupos de Sylow:

- $n_5 \equiv 1 \pmod{5}$ y $n_5 \mid 6 \implies n_5 \in \{1, 6\}$.
- $n_3 \equiv 1 \pmod{3}$ y $n_3 \mid 10 \implies n_3 \in \{1, 10\}$.

Supongamos que G es simple (es decir, no tiene subgrupos normales propios). Entonces tendríamos $n_5 = 6$ y $n_3 = 10$ (pues si alguno fuera 1, ese Sylow sería normal).

Contemos los elementos:

- Si $n_5 = 6$, tenemos 6 subgrupos de orden 5. La intersección de cualesquiera dos de ellos es trivial (orden 1). Cada uno tiene $5 - 1 = 4$ elementos de orden 5. Total de elementos de orden 5: $6 \times 4 = 24$.
- Si $n_3 = 10$, tenemos 10 subgrupos de orden 3. Cada uno tiene $3 - 1 = 2$ elementos de orden 3. Total de elementos de orden 3: $10 \times 2 = 20$.

Sumando los elementos:

$$24 \text{ (orden 5)} + 20 \text{ (orden 3)} = 44 \text{ elementos}$$

Esto es imposible pues $|G| = 30$. Por lo tanto, nuestra suposición es falsa. Debe ocurrir que $n_5 = 1$ o $n_3 = 1$. Conclusión: Un grupo de orden 30 no puede ser simple (siempre tiene un subgrupo normal de orden 5 o de orden 3).

Ejemplo 5.8. Sea $|G| = 12 = 2^2 \cdot 3$.

- $n_3 \equiv 1 \pmod{3}$ y $n_3 \mid 4 \implies n_3 \in \{1, 4\}$.
- $n_2 \equiv 1 \pmod{2}$ y $n_2 \mid 3 \implies n_2 \in \{1, 3\}$.

Supongamos que G no es simple. Si $n_3 = 1$, ya terminamos ($P_3 \trianglelefteq G$). Supongamos entonces que $n_3 = 4$. El número de elementos de orden 3 es:

$$4 \times (3 - 1) = 8 \text{ elementos.}$$

Los elementos restantes son $12 - 8 = 4$. Estos 4 elementos deben formar el único 2-Sylow de G (que tiene orden 4). Por lo tanto, si $n_3 \neq 1$, obligatoriamente $n_2 = 1$.

En cualquier caso, G tiene un subgrupo normal (ya sea el 3-Sylow o el 2-Sylow).

Ejemplo 5.9. Sea $|G| = p^2q$ con p, q primos distintos. (El análisis suele ser similar: mostrar que no es simple contando elementos. Por ejemplo, si $p > q$, $n_p = 1$).

CAPÍTULO 6

Automorfismos de Grupos

6.1. Automorfismos de Grupos

Definición 6.1.1. Un **automorfismo** de un grupo G es un isomorfismo de G en sí mismo. Al conjunto de automorfismos se le denota por $\text{Aut}(G)$. Así:

$$\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ es un isomorfismo}\}$$

Observación 6.1. Si G es finito y $f : G \rightarrow G$ es un homomorfismo, entonces f es inyectivo si y solo si f es suprayectivo.

Demostración.

Como G es un grupo finito, denotemos su orden por $|G| = n < \infty$.

$\Rightarrow)$ Supongamos que f es inyectiva. Dado que f es una función inyectiva, la cantidad de elementos en su imagen es igual a la cantidad de elementos en su dominio. Es decir, $|\text{Im}(f)| = |G| = n$. Sabemos que $\text{Im}(f) \subseteq G$. Dado que $\text{Im}(f)$ es un subconjunto de G y tiene la misma cardinalidad finita que G , necesariamente $\text{Im}(f) = G$. Por lo tanto, f es suprayectiva.

$\Leftarrow)$ Supongamos que f es suprayectiva. Consideraremos el núcleo de f , $\ker(f)$. Por el Primer Teorema de Isomorfía, sabemos que:

$$G / \ker(f) \cong \text{Im}(f)$$

Tomando cardinalidades:

$$\frac{|G|}{|\ker(f)|} = |\text{Im}(f)|$$

Como f es suprayectiva, $\text{Im}(f) = G$, por lo que $|\text{Im}(f)| = |G|$. Sustituyendo en la ecuación:

$$\frac{|G|}{|\ker(f)|} = |G|$$

Como $|G|$ es finito y no nulo, podemos dividir ambos lados por $|G|$, obteniendo:

$$\frac{1}{|\ker(f)|} = 1 \implies |\ker(f)| = 1$$

El único subgrupo de orden 1 es el trivial, por lo tanto $\ker(f) = \{e\}$. Sabemos que un homomorfismo es inyectivo si y solo si su núcleo es trivial. Concluimos que f es inyectiva. \square

Proposición 6.1.1. *Sea G un grupo y $a \in G$. Definimos $f_a : G \rightarrow G$ por $f_a(g) = aga^{-1}$. Se verifica que f_a es un isomorfismo.*

Demuestração.

i) f_a es homomorfismo: Sean $g_1, g_2 \in G$.

$$f_a(g_1g_2) = a(g_1g_2)a^{-1} = ag_1(a^{-1}a)g_2a^{-1} = (ag_1a^{-1})(ag_2a^{-1}) = f_a(g_1)f_a(g_2)$$

ii) f_a es inyectiva:

$$f_a(g) = f_a(g_1) \iff aga^{-1} = ag_1a^{-1} \iff g = g_1$$

iii) f_a es sobreyectiva: Dado $y \in G$, existe $x = a^{-1}ya \in G$ tal que:

$$f_a(x) = f_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = (aa^{-1})y(aa^{-1}) = eye = y$$

Por lo tanto, f_a es un isomorfismo de G en sí mismo (un automorfismo). \square

Definición 6.1.2. *Al conjunto de los automorfismos de la forma f_a se les llama automorfismos internos de G , y se denota por $Im(G)$.*

$$Im(G) = \{f_a : G \rightarrow G \mid f_a(g) = aga^{-1}, \text{ para algún } a \in G\}$$

Observación 6.2. *Aut(G), con la operación de composición de funciones, es un grupo.*

Demuestração.

Sabemos que la composición de biyecciones es una biyección y la composición de homomorfismos es un homomorfismo. Sean $f, g \in Aut(G)$. Entonces $f \circ g$ es biyectiva y es homomorfismo, luego $f \circ g \in Aut(G)$. La asociatividad se hereda de la composición de funciones. La identidad es $Id_G(x) = x$, que trivialmente es un automorfismo. Si $f \in Aut(G)$, su función inversa f^{-1} también es un isomorfismo, por lo que $f^{-1} \in Aut(G)$. \square

Ejemplo 6.1. *Si G es un grupo, definamos $\varphi : G \rightarrow Aut(G)$ como $\varphi(g) = f_g$, donde $f_g : G \rightarrow G$ está dado por $f_g(a) = gag^{-1}$. Entonces φ es un homomorfismo.*

En efecto:

$$f_{gg_1}(a) = (gg_1)a(gg_1)^{-1} = g(g_1ag_1^{-1})g^{-1} = gf_{g_1}(a)g^{-1} = f_g(f_{g_1}(a)) = (f_g \circ f_{g_1})(a)$$

Por lo tanto:

$$\varphi(gg_1) = f_{gg_1} = f_g \circ f_{g_1} = \varphi(g) \circ \varphi(g_1)$$

La imagen de φ es justamente $Im(G)$.

Teorema 6.1.1. *Sea G un grupo, entonces $\text{Im}(G) \trianglelefteq \text{Aut}(G)$ y*

$$G/Z(G) \cong \text{Im}(G)$$

Demostración.

Sea $\varphi : G \rightarrow \text{Aut}(G)$ dada por $\varphi(g) = f_g$ (como en el ejemplo anterior). Entonces, φ es un homomorfismo con imagen $\text{Im}(G)$. Además:

$$\begin{aligned} g \in \ker \varphi &\iff \varphi(g) = \text{Id}_G \iff f_g(a) = a, \forall a \in G \\ &\iff gag^{-1} = a, \forall a \in G \iff ga = ag, \forall a \in G \iff g \in Z(G) \end{aligned}$$

Por lo tanto, $\ker \varphi = Z(G)$. Por el Primer Teorema de Isomorfía:

$$G/\ker \varphi = G/Z(G) \cong \text{Im}(\varphi) = \text{Im}(G)$$

Ahora, para ver la normalidad ($\text{Im}(G) \trianglelefteq \text{Aut}(G)$), sea $f_g \in \text{Im}(G)$ y $h \in \text{Aut}(G)$. Para $a \in G$:

$$(h \circ f_g \circ h^{-1})(a) = h(f_g(h^{-1}(a))) = h(gh^{-1}(a)g^{-1})$$

Como h es un homomorfismo:

$$= h(g)h(h^{-1}(a))h(g^{-1}) = h(g)ah(g)^{-1} = f_{h(g)}(a)$$

Luego, $h \circ f_g \circ h^{-1} = f_{h(g)}$. Como $h(g) \in G$, entonces $f_{h(g)} \in \text{Im}(G)$. De donde concluimos que $\text{Im}(G) \trianglelefteq \text{Aut}(G)$. \square

Observación 6.3. *Si $G \cong G_1$, entonces $\text{Aut}(G) \cong \text{Aut}(G_1)$.*

Demostración.

Sea $\psi : G \rightarrow G_1$ un isomorfismo. Definamos $\Psi : \text{Aut}(G) \rightarrow \text{Aut}(G_1)$ dada por:

$$f \mapsto h_f = \psi \circ f \circ \psi^{-1}$$

Es decir, $\Psi(f) = \psi \circ f \circ \psi^{-1}$. Demostraremos que Ψ es un isomorfismo, en efecto:

1. Ψ está bien definida: Es decir, $\psi \circ f \circ \psi^{-1} \in \text{Aut}(G_1)$. En efecto, claramente $\psi \circ f \circ \psi^{-1}$ es biyectiva (composición de biyecciones). Además, para $g_1, g_2 \in G_1$:

$$\begin{aligned} h_f(g_1g_2) &= (\psi \circ f \circ \psi^{-1})(g_1g_2) = \psi(f(\psi^{-1}(g_1g_2))) \\ &= \psi(f(\psi^{-1}(g_1)\psi^{-1}(g_2))) \quad (\text{pues } \psi^{-1} \text{ es hom.}) \\ &= \psi(f(\psi^{-1}(g_1)) \cdot f(\psi^{-1}(g_2))) \quad (\text{pues } f \text{ es hom.}) \\ &= \psi(f(\psi^{-1}(g_1))) \cdot \psi(f(\psi^{-1}(g_2))) \quad (\text{pues } \psi \text{ es hom.}) \\ &= h_f(g_1)h_f(g_2) \end{aligned}$$

Por lo tanto, $h_f \in \text{Aut}(G_1)$.

2. Ψ es homomorfismo: Sean $f, \rho \in \text{Aut}(G)$.

$$\Psi(f \circ \rho) = h_{f \circ \rho} = \psi \circ (f \circ \rho) \circ \psi^{-1}$$

Por otro lado:

$$\Psi(f) \circ \Psi(\rho) = (\psi \circ f \circ \psi^{-1}) \circ (\psi \circ \rho \circ \psi^{-1}) = \psi \circ f \circ (\psi^{-1} \circ \psi) \circ \rho \circ \psi^{-1}$$

Como $\psi^{-1} \circ \psi = Id_G$, esto se reduce a:

$$= \psi \circ f \circ \rho \circ \psi^{-1} = h_{f \circ \rho}$$

Luego, $\Psi(f \circ \rho) = \Psi(f) \circ \Psi(\rho)$.

3. Ψ es inyectiva:

$$\Psi(f) = \Psi(\rho) \iff \psi \circ f \circ \psi^{-1} = \psi \circ \rho \circ \psi^{-1}$$

Componiendo con ψ^{-1} a la izquierda y ψ a la derecha:

$$\iff \psi^{-1}(\psi \circ f \circ \psi^{-1})\psi = \psi^{-1}(\psi \circ \rho \circ \psi^{-1})\psi \iff f = \rho$$

4. Ψ es sobreyectiva: Sea $g \in \text{Aut}(G_1)$. Existe $f = \psi^{-1} \circ g \circ \psi \in \text{Aut}(G)$ tal que:

$$\Psi(f) = \psi \circ (\psi^{-1} \circ g \circ \psi) \circ \psi^{-1} = (\psi \circ \psi^{-1}) \circ g \circ (\psi \circ \psi^{-1}) = g$$

Por lo tanto, $\text{Aut}(G) \cong \text{Aut}(G_1)$. □

Observación 6.4. *El recíproco es falso.*

Demuestra.

Sea $G = S_3$. Sus elementos son:

$$S_3 = \{e, \theta = (123), \theta^2 = (132), \sigma = (12), \tau = (13), \rho = (23)\}$$

Sabemos que S_3 es generado por θ y σ ($\langle \theta, \sigma \rangle = S_3$) con las relaciones $\theta^3 = e, \sigma^2 = e, \sigma\theta = \theta^2\sigma$. Cualquier automorfismo $f \in \text{Aut}(S_3)$ queda determinado por sus valores en los generadores. Además, un isomorfismo preserva el orden de los elementos.

Los elementos de orden 3 son $\{\theta, \theta^2\}$. Los elementos de orden 2 son $\{\sigma, \tau, \rho\}$. Por lo tanto, para $f(\theta)$ tenemos 2 opciones (θ ó θ^2) y para $f(\sigma)$ tenemos 3 opciones (σ, τ ó ρ). En total hay a lo más $2 \times 3 = 6$ automorfismos.

Sabemos que $\text{Im}(S_3) \cong S_3/Z(S_3)$. Como $Z(S_3) = \{e\}$, entonces $\text{Im}(S_3) \cong S_3$, por lo que $|\text{Im}(S_3)| = 6$. Como $\text{Im}(S_3) \leq \text{Aut}(S_3)$ y $|\text{Aut}(S_3)| \leq 6$, concluimos que:

$$\text{Aut}(S_3) = \text{Im}(S_3) \cong S_3$$

(Nota: Existen grupos no isomorfos a S_3 , como $\mathbb{Z}_2 \times \mathbb{Z}_2$, cuyo grupo de automorfismos es isomorfo a S_3 , mostrando que el recíproco falla). □

Teorema 6.1.2. Sean H_1 y H_2 grupos finitos tales que $\gcd(|H_1|, |H_2|) = 1$. Entonces:

$$\text{Aut}(H_1 \times H_2) \cong \text{Aut}(H_1) \times \text{Aut}(H_2)$$

Demostración.

Identificamos a H_1 con el subgrupo $H_1 \times \{e_2\}$ y a H_2 con $\{e_1\} \times H_2$ dentro de $G = H_1 \times H_2$.

Sea $f \in \text{Aut}(H_1 \times H_2)$. Probemos que $f(H_1) = H_1$ y $f(H_2) = H_2$.

Sea $(h, e_2) \in H_1$. Su orden k divide a $|H_1|$. Aplicando f , el elemento $f(h, e_2)$ debe tener el mismo orden k . Sea $f(h, e_2) = (x, y) \in H_1 \times H_2$. Entonces el orden de (x, y) es $(|x|, |y|) = k$. Esto implica que $|y|$ divide a k , y por tanto $|y|$ divide a $|H_1|$. Pero $y \in H_2$, por lo que $|y|$ divide a $|H_2|$. Como $(|H_1|, |H_2|) = 1$, la única posibilidad es que $|y| = 1$, es decir, $y = e_2$. Por lo tanto, $f(h, e_2) = (x, e_2) \in H_1$.

Esto demuestra que $f(H_1) \subseteq H_1$. Por ser f inyectiva y H_1 finito, $f(H_1) = H_1$. Análogamente se demuestra que $f(H_2) = H_2$.

Dado que f preserva los subgrupos H_1 y H_2 , podemos definir las restricciones: $f|_{H_1} : H_1 \rightarrow H_1$ y $f|_{H_2} : H_2 \rightarrow H_2$. Estas restricciones son automorfismos de H_1 y H_2 respectivamente.

Definimos la función $\Psi : \text{Aut}(H_1 \times H_2) \rightarrow \text{Aut}(H_1) \times \text{Aut}(H_2)$ dada por:

$$\Psi(f) = (f|_{H_1}, f|_{H_2})$$

Ψ es un homomorfismo. En efecto:

Sean $f, g \in \text{Aut}(H_1 \times H_2)$.

$$\Psi(f \circ g) = ((f \circ g)|_{H_1}, (f \circ g)|_{H_2}) = (f|_{H_1} \circ g|_{H_1}, f|_{H_2} \circ g|_{H_2})$$

(Esto es válido porque $g(H_1) = H_1$, así que la composición se restringe bien).

$$= (f|_{H_1}, f|_{H_2}) \cdot (g|_{H_1}, g|_{H_2}) = \Psi(f) \cdot \Psi(g)$$

Ψ es biyectiva. En efecto:

- **Inyectiva:** Si $\Psi(f) = (Id_{H_1}, Id_{H_2})$, entonces $f(h, e_2) = (h, e_2)$ y $f(e_1, k) = (e_1, k)$. Para un elemento arbitrario $(h, k) \in H_1 \times H_2$:

$$f(h, k) = f((h, e_2)(e_1, k)) = f(h, e_2)f(e_1, k) = (h, e_2)(e_1, k) = (h, k)$$

Luego $f = Id_{H_1 \times H_2}$, así que $\ker \Psi$ es trivial.

- **Sobreyectiva:** Dado $(\alpha, \beta) \in \text{Aut}(H_1) \times \text{Aut}(H_2)$, definimos $f : H_1 \times H_2 \rightarrow H_1 \times H_2$ como $f(h, k) = (\alpha(h), \beta(k))$. Es fácil verificar que f es un automorfismo y que $\Psi(f) = (\alpha, \beta)$.

Por lo tanto, $\text{Aut}(H_1 \times H_2) \cong \text{Aut}(H_1) \times \text{Aut}(H_2)$. \square

Teorema 6.1.3. *Sea G un grupo cíclico de orden n . Entonces:*

$$\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

Donde $(\mathbb{Z}/n\mathbb{Z})^$ es el grupo multiplicativo de las unidades módulo n . En particular, $|\text{Aut}(G)| = \varphi(n)$, donde φ es la función de Euler.*

Demostración.

Sea $G = \langle g \rangle$ un grupo cíclico de orden n . Sea $f \in \text{Aut}(G)$. Como G es cíclico, f queda completamente determinado por la imagen del generador g . Sea $f(g) = g^{c_f}$ para algún entero c_f . Como f es un automorfismo, $f(g)$ debe ser otro generador de G . Sabemos que g^k es un generador de G si y solo si $\gcd(k, n) = 1$. Por lo tanto, $\gcd(c_f, n) = 1$, lo que implica que la clase $\overline{c_f}$ pertenece a $(\mathbb{Z}/n\mathbb{Z})^*$.

Definimos la función $\Psi : \text{Aut}(G) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ dada por:

$$\Psi(f) = \overline{c_f} \quad \text{donde } f(g) = g^{c_f}$$

1. Ψ es un homomorfismo: Sean $f_1, f_2 \in \text{Aut}(G)$ con $f_1(g) = g^{c_{f_1}}$ y $f_2(g) = g^{c_{f_2}}$.

$$(f_1 \circ f_2)(g) = f_1(f_2(g)) = f_1(g^{c_{f_2}}) = (f_1(g))^{c_{f_2}} = (g^{c_{f_1}})^{c_{f_2}} = g^{c_{f_1}c_{f_2}}$$

Por lo tanto, el exponente asociado a la composición es el producto de los exponentes:

$$\Psi(f_1 \circ f_2) = \overline{c_{f_1}c_{f_2}} = \overline{c_{f_1}} \cdot \overline{c_{f_2}} = \Psi(f_1)\Psi(f_2)$$

2. Ψ es inyectiva:

$$\Psi(f) = \overline{1} \implies c_f \equiv 1 \pmod{n} \implies f(g) = g^1 = g$$

Como el automorfismo fija al generador, fija a todo el grupo. Luego $f = \text{Id}_G$.

3. Ψ es sobreyectiva: Sea $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$. Entonces $\gcd(k, n) = 1$. Definimos $f : G \rightarrow G$ por $f(x) = x^k$. Como $\gcd(k, n) = 1$, la aplicación $x \mapsto x^k$ es una biyección en el grupo cíclico finito y es un homomorfismo ($f(xy) = (xy)^k = x^ky^k$ pues G es abeliano). Así, $f \in \text{Aut}(G)$ y $\Psi(f) = \overline{k}$.

Por lo tanto, $\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$. □

Corolario 6.1.1. *Si p es un número primo, entonces:*

$$\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$$

Demostración.

Aplicando el teorema anterior con $G = \mathbb{Z}_p$ (cíclico de orden p), tenemos:

$$\text{Aut}(\mathbb{Z}_p) \cong (\mathbb{Z}/p\mathbb{Z})^*$$

El orden de este grupo es $\varphi(p) = p - 1$. Sabemos por la teoría de grupos finitos (específicamente por la existencia de raíces primitivas módulo p) que el grupo multiplicativo de un cuerpo finito \mathbb{Z}_p es siempre cíclico. Por lo tanto:

$$(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1} \cong \mathbb{Z}_{p-1}$$

Así concluimos que $\text{Aut}(\mathbb{Z}_p)$ es isomorfo al grupo cíclico de orden $p - 1$. \square

Teorema 6.1.4. *Sea G un grupo cíclico de orden n . Entonces:*

$$\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

Donde $(\mathbb{Z}/n\mathbb{Z})^$ es el grupo multiplicativo de las unidades módulo n . En particular, $|\text{Aut}(G)| = \varphi(n)$, donde φ es la función de Euler.*

Demostración.

Sea $G = \langle g \rangle$ un grupo cíclico de orden n . Sea $f \in \text{Aut}(G)$. Como G es cíclico, f queda completamente determinado por la imagen del generador g . Sea $f(g) = g^{c_f}$ para algún entero c_f . Como f es un automorfismo, $f(g)$ debe ser otro generador de G . Sabemos que g^k es un generador de G si y solo si $\gcd(k, n) = 1$. Por lo tanto, $\gcd(c_f, n) = 1$, lo que implica que la clase $\overline{c_f}$ pertenece a $(\mathbb{Z}/n\mathbb{Z})^*$.

Definimos la función $\Psi : \text{Aut}(G) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ dada por:

$$\Psi(f) = \overline{c_f} \quad \text{donde } f(g) = g^{c_f}$$

1. Ψ es un homomorfismo: Sean $f_1, f_2 \in \text{Aut}(G)$ con $f_1(g) = g^{c_{f_1}}$ y $f_2(g) = g^{c_{f_2}}$.

$$(f_1 \circ f_2)(g) = f_1(f_2(g)) = f_1(g^{c_{f_2}}) = (f_1(g))^{c_{f_2}} = (g^{c_{f_1}})^{c_{f_2}} = g^{c_{f_1}c_{f_2}}$$

Por lo tanto, el exponente asociado a la composición es el producto de los exponentes:

$$\Psi(f_1 \circ f_2) = \overline{c_{f_1}c_{f_2}} = \overline{c_{f_1}} \cdot \overline{c_{f_2}} = \Psi(f_1)\Psi(f_2)$$

2. Ψ es inyectiva:

$$\Psi(f) = \overline{1} \implies c_f \equiv 1 \pmod{n} \implies f(g) = g^1 = g$$

Como el automorfismo fija al generador, fija a todo el grupo. Luego $f = \text{Id}_G$.

3. Ψ es sobreyectiva: Sea $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$. Entonces $\gcd(k, n) = 1$. Definimos $f : G \rightarrow G$ por $f(x) = x^k$. Como $\gcd(k, n) = 1$, la aplicación $x \mapsto x^k$ es una biyección en el grupo cíclico finito y es un homomorfismo ($f(xy) = (xy)^k = x^ky^k$ pues G es abeliano). Así, $f \in \text{Aut}(G)$ y $\Psi(f) = \overline{k}$.

Por lo tanto, $\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$. \square

Corolario 6.1.2. *Si p es un número primo, entonces:*

$$\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$$

Demostración.

Aplicando el teorema anterior con $G = \mathbb{Z}_p$ (cíclico de orden p), tenemos:

$$\text{Aut}(\mathbb{Z}_p) \cong (\mathbb{Z}/p\mathbb{Z})^*$$

El orden de este grupo es $\varphi(p) = p - 1$. Sabemos por la teoría de grupos finitos (específicamente por la existencia de raíces primitivas módulo p) que el grupo multiplicativo de un cuerpo finito \mathbb{Z}_p es siempre cíclico. Por lo tanto:

$$(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1} \cong \mathbb{Z}_{p-1}$$

Así concluimos que $\text{Aut}(\mathbb{Z}_p)$ es isomorfo al grupo cíclico de orden $p - 1$. □

Ejemplo 6.2. *Sea G un grupo y hagamos actuar G en sí mismo por conjugación. Entonces esta es una acción como grupo.*

Definimos $\tilde{\varphi} : G \times G \rightarrow G$ por $\tilde{\varphi}(g, g_1) = gg_1g^{-1}$. Ya se tiene que es una acción (visto en el capítulo anterior). Veamos que actúa por automorfismos:

$$\begin{aligned} (k_1 k_2)^g &= \tilde{\varphi}(g, k_1 k_2) = g(k_1 k_2)g^{-1} = gk_1(g^{-1}g)k_2g^{-1} \\ &= (gk_1g^{-1})(gk_2g^{-1}) = \tilde{\varphi}(g, k_1)\tilde{\varphi}(g, k_2) = k_1^g k_2^g \end{aligned}$$

Por lo tanto, la conjugación preserva el producto.

Observación 6.5. *Sean H y K grupos. Entonces H actúa en K como grupo si y solo si $\varphi : H \rightarrow \text{Aut}(K)$ es un homomorfismo. (Nota: $\text{Aut}(K) \leq S_K$).*

En efecto, \Rightarrow) Si H actúa como grupo en K , existe $\tilde{\varphi} : H \times K \rightarrow K$ que cumple las condiciones i), ii) de acción y la condición de compatibilidad iii). Definamos $\varphi : H \rightarrow \text{Aut}(K)$ por $\varphi(h) = f_h$, donde $f_h : K \rightarrow K$ está dada por $f_h(k) = \tilde{\varphi}(h, k)$.

1. φ está bien definida: Como $\tilde{\varphi}$ es acción, la función $\varphi : H \rightarrow S_K$ dada por $h \mapsto f_h$ es un homomorfismo de grupos (propiedad general de acciones). Basta ver que la imagen cae en $\text{Aut}(K)$, es decir, que $f_h \in \text{Aut}(K)$ para todo h . Sabemos que f_h es biyectiva (por ser acción). Además:

$$\begin{aligned} f_h(k_1 k_2) &= \tilde{\varphi}(h, k_1 k_2) = (k_1 k_2)^h = k_1^h k_2^h \\ &= \tilde{\varphi}(h, k_1)\tilde{\varphi}(h, k_2) = f_h(k_1)f_h(k_2) \end{aligned}$$

Luego, f_h es homomorfismo y por tanto $f_h \in \text{Aut}(K)$. Así φ está bien definida.

\Leftarrow) Recíprocamente, sea $\varphi : H \rightarrow \text{Aut}(K)$ un homomorfismo. Definamos $\tilde{\varphi} : H \times K \rightarrow K$ por $\tilde{\varphi}(h, k) = (\varphi(h))(k)$. Notemos que como $\varphi(h) \in \text{Aut}(K)$, denotemos $f_h = \varphi(h)$, entonces $\tilde{\varphi}(h, k) = f_h(k)$.

Verifiquemos que es acción como grupo:

- $k^e = \tilde{\varphi}(e, k) = (\varphi(e))(k) = \text{Id}_K(k) = k$. (Pues φ es homomorfismo, $\varphi(e) = \text{Id}$).
- $(k^{h_1})^{h_2} = \tilde{\varphi}(h_2, k^{h_1}) = f_{h_2}(f_{h_1}(k)) = (f_{h_2} \circ f_{h_1})(k)$. Como φ es homomorfismo, $f_{h_2} \circ f_{h_1} = \varphi(h_2) \circ \varphi(h_1) = \varphi(h_2 h_1) = f_{h_2 h_1}$. Luego, $= f_{h_2 h_1}(k) = k^{h_2 h_1}$.

- $(k_1 k_2)^h = f_h(k_1 k_2) = f_h(k_1) f_h(k_2)$ (pues $f_h \in \text{Aut}(K)$). $= k_1^h k_2^h$.

□

Ejemplo 6.3. Sea G un grupo y $K \trianglelefteq G$. Entonces G **no** actúa necesariamente en K como grupo por multiplicación a la izquierda. Es decir, sea $\tilde{\varphi}(g, k) = gk$.

Aunque $\tilde{\varphi}(e, k) = ek = k$ y $\tilde{\varphi}(g_1 g_2, k) = (g_1 g_2)k = g_1(g_2 k)$, la propiedad de automorfismo falla:

$$(k_1 k_2)^g = g(k_1 k_2)$$

mientras que:

$$k_1^g k_2^g = (gk_1)(gk_2) = gk_1 gk_2$$

En general $gk_1 k_2 \neq gk_1 gk_2$ (esto implicaría $e = g$, lo cual no es cierto para todo g). Además, gk no necesariamente está en K si K no es el grupo total (aunque si tomamos $K = G$, falla la condición de homomorfismo a menos que G sea trivial).