INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Física y Matemática

Álgebra Moderna I

Apuntes Álgebra Moderna I

Profesor:
Escobar Gracia César Alberto

Alumnos:
Ramírez León Christian Yael
Silva Sierra Joshua Joaquín

5FM1

---

24 de diciembre de 2025

Índice general

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 $|A \setminus B = |A| - |B|$. □

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:

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

□

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

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

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

$$A = \{x \in \Omega : x \text{ cumple } C_1\}$$
$$B = \{x \in \Omega : x \text{ cumple } C_2\}$$

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:

$$C_1 : x \text{ sea divisible por } 3$$
$$C_2 : x \text{ sea divisible por } 5$$

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 $A_1, \ldots, A_n$ una colección finita de conjuntos finitos, definidos:

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

Definamos de este modo:

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

Por el principio de inclusión exclusión generalizado:

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

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:

$$\bar{a} + \bar{b} = \overline{a + b}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

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 $\varphi : \mathbb{N} \to \mathbb{N}$ 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) $\varphi(p^k) = p^{k-1}(p - 1), \quad k \in \mathbb{N}$

III) $\varphi(p^k q^t) = \varphi(p^k) \cdot \varphi(q^t), \quad k, t \in \mathbb{N}$

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 $p_1, \ldots, p_n \in \mathbb{N}$ primos distintos, sean $k_1, \ldots, k_n \in \mathbb{N} \cup \{0\}$:*

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

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 $\circ : G \times G \to G$, 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:

$$\overline{a + (-a)} = \bar{0}$$
$$\bar{a} + \overline{(-a)} = \bar{0}$$

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 $f : A \to V$, definamos la operación suma sobre $\mathcal{H}$ como:*

$$+ : \mathcal{H} \times \mathcal{H} \to \mathcal{H}$$
$$(f + g)(a) \mapsto f(a) + g(a) \quad \forall a \in A$$

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. *Considere $\mathbb{Z}/n\mathbb{Z}$, 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) $\forall \bar{a}, \bar{b}, \bar{c} \in G, \quad \bar{a}(\bar{b} \cdot \bar{c}) = \bar{a}(\overline{b \cdot c}) = \overline{a(b \cdot c)} = \overline{(ab)c} = \overline{(ab)} \cdot \bar{c} = (\bar{a}\bar{b})\bar{c}.$

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 $g \circ e' = g, \quad \forall g \in G$, 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 denotará $H \leq G$.*

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

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

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

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

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 $H = \langle S \rangle$. □

2.3. Grupo de permutaciones

Definición 2.3.1 (Grupo de Permutaciones)**.** *Sea X un conjunto no vacío, sea $\mathcal{H} = \{f : X \to X : f$ 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 $a_1, \ldots, a_n$, podemos representar con un arreglo bidimensional de renglones colocando:

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

Donde $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, 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:

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

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

Ejemplo 2.18. *S_3 es el grupo formado por los elementos:*

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

Donde:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \theta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

$\circ$	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 2.4. *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. □

CAPÍTULO 3

Productos Directos

3.1. Productos Directos

Definición 3.1.1. *Sea $(H, \circ), (K, *)$ dos grupos, definamos en $G = H \times K$, la función $\odot : G \times G \to G$, 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 3.1.2. *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 3.1. *El producto directo de una cantidad finita de grupos es asociativo (la igualdad se da salvo isomorfismo); es decir,*

$$(H_1 \times H_2) \times H_3 \cong H_1 \times (H_2 \times H_3) \qquad (\textit{Se escribe } H_1 \times H_2 \times H_3)$$

Verificarlo.

Teorema 3.1.1 (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 $n = p_1^{e_1} \dots p_k^{e_k}$ es la factorización en primos de n.*

Demostración. Sea $\varphi : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ 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: $n = |\mathbb{Z}_n| = |\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}| = p_1^{e_1} \dots p_k^{e_k}$. 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 $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$. □

Ejemplo 3.1. *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 $G \cong H \times K$.*

Demostración. 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 $\varphi : G \to H \times K$ 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 conmutan:

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

- 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. □

Corolario 3.1.1. *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). □

Teorema 3.1.2 (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 (biyeciones de G en sí mismo). Definimos la función $\varphi : G \to S_G$ dada por $\varphi(g) = f_g$, donde $f_g : G \to G$ 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 $h \in G$:

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

  De manera análoga, $f_{g^{-1}} \circ f_g = \mathrm{id}$. 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 $h \in G$:

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

  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 $\mathrm{Im}(\varphi)$. Dado que $\mathrm{Im}(\varphi)$ es un subgrupo de S_G, hemos demostrado que G es isomorfo a un subgrupo de permutaciones. □

Ejemplo 3.2. *Para ilustrar el teorema anterior, consideremos el grupo* $S_3 = \{id, \theta, \sigma, \theta\sigma, \sigma\theta, \theta^2\}$. *La función* $\varphi : S_3 \to S_{S_3}$ *asocia a cada* $g \in S_3$ *una permutación de los elementos de* S_3.

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

$$\begin{aligned} id &\mapsto \theta \\ \theta &\mapsto \theta^2 \\ \sigma &\mapsto \theta\sigma \\ \theta\sigma &\mapsto \theta^2\sigma \\ \sigma\theta &\mapsto \sigma \quad (\textit{pues } \theta\sigma\theta = \theta(\theta^{-1}\sigma) = \sigma) \\ \theta^2 &\mapsto id \end{aligned}$$

Corolario 3.1.2. *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 $G = \{a_1, \ldots, a_n\}$, definimos $\psi : S_X \to S_n$ dada por $f \mapsto \bar{f}$, en donde si $f(a_i) = a_j$, entonces $\bar{f}(i) = j$, con $X = \{a_1, \ldots, a_n\}$ y $\{1, \ldots, n\}$.

- ψ está bien definida: Pues si $f : X \to X$ 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 $j \in \{1, \ldots, n\}$, tenemos $a_j \in G$. Como f es biyectiva, $\exists a_i \in \{1, \ldots, n\}$ 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: $\psi(f) = \psi(g) \implies \bar{f} = \bar{g} \implies \bar{f}(i) = \bar{g}(i)\ \forall 1 \leq i \leq n \implies f(a_i) = g(a_i)\ \forall 1 \leq i \leq n \implies f = g$.

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

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

Teorema 3.1.3. *Sea G un grupo finito, $H \leq G$. $X = \{Hg \mid g \in G\} = (G/H)$ entonces existe $\varphi : G \to S_X$ un homomorfismo tal que $N = Ker\ \varphi$ es el mayor subgrupo normal en G contenido en H.*

Demostración. Sea $\varphi : G \to S_X$ definida por $\varphi(g) = f_g$ con $f_g : X \to X$ 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 $f_g(Hkg) = Hkgg^{-1} = Hk$.

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 3.1.3. *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 $H \neq G$). □

Corolario 3.1.4. *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 $|H| = \frac{|G|}{[G:H]} = \frac{p}{p} = 1$, 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). □

3.2. 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 $\{1, \ldots, n\}$ 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 3.2.1. *Un ciclo de longitud $1 \leq k \leq n$ en S_n es un elemento de S_n tal que existen $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ con $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ y $\sigma(j) = j \ \forall j \notin \{i_1, \ldots, i_k\}$.*

Note que en este caso:

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

Más aún:

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

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:

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

Si $k = 1$, $\sigma(i) = i\ \forall i$, es decir, $\sigma = id$ y se denota por $\sigma = (1) = (2) = \cdots = (k) = (n)$.
Si $k = 2$, $\sigma(i_1, i_2)$ y se llama una transposición. En este caso:

$$\sigma^2(i_1) = \sigma(i_2) = i_1$$
$$\sigma^2(i_2) = \sigma(i_1) = i_2$$

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 3.2.2. *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 3.3. *Consideremos S_5, entonces $\sigma = (1\ 2)$ y $\tau = (3\ 4\ 5)$ son disjuntos.*

Nota 3.2.1 (Nota). *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 3.2. *Si σ, τ son ciclos disjuntos, entonces $\sigma \circ \tau = \tau \circ \sigma$, es decir, conmutan.*

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 $s \notin \{i_1, \dots, i_k, j_1, \dots, j_l\}$:

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

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

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

Teorema 3.2.1 (Teorema)**.** *Sea $\theta \in S_n$, entonces θ se puede representar de manera única como producto de ciclos ajenos (disjuntos) salvo orden.*

Demostración. Sea $\{i_1, \ldots, i_k\}$ 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 $\{i_1, \ldots, i_k, i_{k+1}\}$. Considere que θ mueve a los elementos $\{i_1, \ldots, i_k, i_{k+1}\}$. Observe que $i_1, \theta(i_1), \theta^2(i_1), \ldots, \theta^{k+1}(i_1) \in \{i_1, \ldots, i_{k+1}\}$, por lo tanto $\{i_1, \theta(i_1), \ldots, \theta^{k+1}(i_1)\} \subseteq \{i_1, \ldots, i_{k+1}\}$, 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 $\sigma = (i_1, \theta(i_1), \ldots, \theta^{p-1}(i_1))$. $\{i_1, \theta(i_1), \ldots, \theta^{p-1}(i_1)\} \subseteq \{i_1, \ldots, i_{k+1}\}$ y definamos

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

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

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

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

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

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

Ahora τ mueve a los elementos $\{i_1, \ldots, i_{k+1}\} \setminus \{i_1, \sigma(i_1), \ldots, \sigma^{p-1}(i_1)\}$ 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

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

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 conmutan, por lo que podemos pensar que $i = 1 = j$, en este caso $\sigma_2, \ldots, \sigma_k, \tau_2, \ldots, \tau_l$ no mueven a i_1.

Además $\sigma_1 = (i_1, \sigma_1(i_1), \ldots, \sigma_1^{s-1}(i_1))$, $\tau_1 = (i_1, \tau(i_1), \ldots, \tau^{r-1}(i_1))$ 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 $\{i_1, \sigma(i_1), \ldots, \sigma^{k-1}(i_1)\}$ $\forall 1 < j \leq k$. Análogamente τ_j no mueve a ninguno de

$\{i_1, \tau(i_1), \ldots, \tau^{l-1}(i_1)\}$ $\forall 1 < j \leq l$. Por tanto para $m \in \mathbb{N}$

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

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 $\theta = \sigma_1 \ldots \sigma_k = \tau_1 \ldots \tau_l$ se obtiene $\sigma_2 \ldots \sigma_k = \tau_2 \ldots \tau_l$. Podemos suponer $k \leq l$. En cuyo caso realizando el mismo proceso obtenemos $\sigma_k = \tau_k$ y $Id = \tau_{k+1} \ldots \tau_l$. Como los τ_j son disjuntos a pares necesariamente $\tau_{k+1} \ldots \tau_l$ tienen longitud uno. Por lo tanto $l = k$. □

Corolario 3.2.1. *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 $\theta = \sigma_1 \ldots \sigma_k$ con los σ_i's ciclos disjuntos a pares y $n_i = o(\sigma_i)$ $m = [n_1, \ldots, n_k]$ entonces

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

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