ESTRUCTURAS ALGEBRAICAS
TEORÍA DE GRUPOS

Alberto Martín Aguilar

Mayo 2012

1Orientado para alumnos de 1º Grado en Matemáticas
Índice general

1. Grupos 3
   1.1. Definición y Propiedades elementales 3
   1.2. Subgrupos 4
   1.3. Grupos Cíclicos 5
   1.4. Teorema de Lagrange. Consecuencias 6
   1.5. Grupos abelianos Finitos 7
   1.6. Ejercicios 9

2. Homomorfismos 10
   2.1. Homomorfismo de Grupos 10
   2.2. Subgrupos Normales 11
   2.3. Grupo Cociente 12
   2.4. Teoremas de Isomorfía 13
   2.5. Clase de Conjugación. Ecuación de Clases 15
   2.6. Grupo de los automorfismos de un grupo cíclico 16
   2.7. Ejercicios 18

3. Ejemplos y clasificación de algunos grupos 19
   3.1. Grupo de Permutaciones 19
   3.2. Grupo Diédrico 21
   3.3. Clasificación de grupos 22
   3.4. Ejercicios 27

4. Teoremas de Sylow 28
   4.1. Producto Directo 28
   4.2. Producto Semidirecto 29
   4.3. Acciones sobre Grupos 30
   4.4. Teoremas de Sylow 32
   4.5. Aplicación del Teorema de Sylow. Apéndice 34
   4.6. Ejercicios 37
Capítulo 1

Grupos

1.1. Definición y Propiedades elementales

Definición 1.1.1 Sea $G$ un conjunto, $G \neq \emptyset$. Sea $*$ una operación binaria. Decimos que $G$ es un grupo respecto a la operación $*$, y se denota por $(G,*)$ si se verifican las siguientes condiciones:

$A1)$ $\forall x, y, z \in G \ (x * y) * z = x * (y * z)$ \quad Prop. Asociativa

$A2)$ $\exists e \in G \ | \ e * x = x * e = x \ \forall x \in G$ \quad El. neutro

$A3)$ $\forall x \in G, \ \exists y \in G \ | \ x * y = y * x = e$ \quad El. inverso

Estos son los llamados Axiomas de Grupo.

Nota 1.1.2 Diremos que $G$ es un grupo abeliano (conmutativo) si $\forall x, y \in G \ x * y = y * x$. Es decir, si la operación binaria $*$ es conmutativa.

Ejemplos

1. $\text{Gl}_n(\mathbb{R}) = \{ \text{Matrices } n \times n \ \mid \ |A| \neq 0 \}$ con respecto al producto forman un grupo abeliano si $n < 2$.

2. $(\mathbb{Q}^*, +), (\mathbb{R}, +), (\mathbb{C}, +)$

3. $C_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$. Sabemos que $\mathbb{C}$ es algebraicamente cerrado, luego el número de elementos de $C_n = n$.

4. $Q = \{ \pm 1, \pm i, \pm j, \pm k \}$ el Grupo de los Cuaternios.

5. $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ Grupo de Klein.

6. $\text{Aut}(G)$ Grupo de los automorfismos de un grupo G.

7. Grupo de los subconjuntos de un conjunto de $n$ elementos $B_n$. $|B| = 2^n$

Teorema 1.1.3 Si $G$ es un grupo con una operación binaria $*$, entonces se cumplen las leyes de cancelación por la izquierda (derecha) en $G$, es decir, $\forall a, b, c \in G$ si $a * b = a * c \ (b * a = c * a)$, entonces $b = c$. 
Demostración

Supongamos que \( a \ast b = a \ast c \). Por el 3º axioma, \( \exists a^{-1} \in G \). Luego:

\[
(a^{-1} \ast a) \ast b = (a^{-1} \ast a) \ast c \implies b = c
\]

De forma análoga se comprueba la ley de cancelación por la derecha.

**Teorema 1.1.4** Sea \( G \) un grupo con operación \( * \). Sean \( a \) y \( b \) elementos cualesquiera de \( G \), entonces las ecuaciones \( a \ast x = b \) e \( y \ast a = b \) tienen soluciones únicas.

**Demostración**

Consideremos la ecuación \( a \ast x = b \). Por los axiomas de grupo, podemos decir que una solución es \( x = a^{-1} \ast b \). Veamos que es única. Sean \( x_1, x_2 \in G \mid a \ast x_1 = b \) y \( a \ast x_2 = b \) Esto implica que \( a \ast x_1 = a \ast x_2 \) y por las leyes de cancelación, \( x_1 = x_2 \).

Se hace de igual forma para la otra ecuación.

### 1.2. Subgrupos

**Definición 1.2.1** Sea \((G, \ast)\) un grupo y sea \( H \subseteq G, H \neq \emptyset \). Decimos que \( H \) es un subgrupo de \( G \), y lo denotamos por \( H < G \) si:

i) \( \forall a, b \in H \Rightarrow a \ast b \in H \)

ii) \( e \in H \), donde \( e \) es el elemento neutro de \( G \).

iii) Si \( h \in H \), entonces \( h^{-1} \in H \)

**Proposición 1.2.2** Sea \((G, \ast)\) un grupo y sea \( H \subseteq G, H \neq \emptyset \). \( H \) es un subgrupo de \( G \) si y solo si \( \forall x, y \in G \Rightarrow x^{-1} \ast y \in H \).

**Demostración**

\[ \Rightarrow \text{Trivial} \]

\[ \Leftarrow \]

i) Sea \( x \in H \). Tomando \( y = x \); \( e = x^{-1} \ast x \in H \)

ii) Sea \( x \in H \). Tomando \( y = e \); \( x^{-1} = x^{-1} \ast e \in H \)

iii) Sean \( x, y \in H \). Según lo probado, \( x^{-1}, y \in H \Rightarrow (x^{-1})^{-1} \ast y = x \ast y \in H \)

**Ejemplos**

1. \((\mathbb{Q}^+, +) < (\mathbb{R}, +) < (\mathbb{C}, +)\)

2. \((\mathbb{Q}^*, \ast) < (\mathbb{R}^*, \ast) < (\mathbb{C}^*, \ast)\)
Definición 1.2.3 Sea G un grupo. Se define el centro de un grupo G y se denota por $Z(G)$ al conjunto:

$$Z(G) = \{ a \in G \mid a * x = x * a \ \forall x \in G \}$$

Definición 1.2.4 Si G es un grupo, entonces G es el subgrupo impropio de G y $\{ e \}$ es el subgrupo trivial de G. Todos los demás subgrupos serán llamados subgrupos propios de G.

Ejercicio: Sea G un grupo. Comprobar que $Z(G)$ es un subgrupo de G.

Definición 1.2.5 Sea X un conjunto. Se define el subgrupo generado por X y se denota por $<X>$:

$$<X> = \bigcap \{ H < G \mid X \subset H \}$$

$$<X> = \{ x_{i_1}^{e_1} \ldots x_{i_r}^{e_r} \mid e_j = \pm 1 ; x_{i_j} \in X \}$$

Definición 1.2.6 Se define el orden de un grupo, y se nota por $|G|$ como el número de elementos que contiene.

1.3. Grupos Cíclicos

Definición 1.3.1 Sea G un grupo y sea $a \in G$, entonces $H = \{ a^n \mid n \in \mathbb{Z} \}$ es un subgrupo de G generado por a y se denota por $H = < a >$. Además, si $G = < a >$ para un cierto $a \in G$, decimos que G es cíclico.

Ejemplos
1. $(\mathbb{Z}, +)$ es un grupo cíclico infinito.
2. $(\mathbb{Z}_7^*, *)$ es un grupo cíclico generado por 5

Proposición 1.3.2 Todo grupo cíclico es abeliano.

Demostración

Sea G = $< a >$. Sean $b, c \in G$. Entonces $\exists r, s \in \mathbb{Z} \mid b = a^r$ y $c = a^s$. Por tanto, $b * c = a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r = b * c \ \forall b, c \in G$.

Definición 1.3.3 Sea G un grupo y $a \in G$. Decimos que a tiene orden n (finito) y se denota por ord(a) = n, $n \in \mathbb{N}$ si $a^n = e$. Si no existe tal número, diremos que el orden de a es 0.

Teorema 1.3.4 Todo subgrupo de un grupo cíclico es cíclico

Demostración

Sea G = $< a >$ y sea H $\subset G$. Si $H = \{ e \}$, entonces H es un subgrupo cíclico. Supongamos que $H = \{ a^n \}$ para algún $n \in \mathbb{Z}^+$. Sea $m \in \mathbb{Z}^+$ minimal, tal que $a^m \in H$. Podemos afirmar que H está generado por $c = a^m$, esto es, $H = < a^m > = < c >$. Tenemos que demostrar que todo d $\in H$ es una potencia de c. Como $c \in H$ y $H \subset G$, entonces $c = a^n$ para algún $n \in \mathbb{Z}$. Por el algoritmo de la división, $n = mq + r$ para $0 \leq r < m$. 4
Sabemos que $a^n \in H, a^m \in H$. Luego $(a^m)^{-q} \in H$ y $a^n \in H$. Como $H$ es un subgrupo de $G$, $a^r = (a^m)^{-q}a^n \in H$. Lo cual es una contradicción ($m$ era minimal), $r = 0$ y $d = a^n = a^mq = c^q$.

**Corolario 1.3.5** Si $a$ es un generador de un grupo cíclico $G$ de orden $n$, entonces otros generadores de $G$ son los elementos de la forma $a^r$, donde $r$ y $n$ son primos relativos.

**Proposición 1.3.6** Sea $G = \langle a \rangle$ un grupo cíclico.

i) Todo subgrupo $H$ de $G$ es cíclico.

ii) Si $G$ es de orden $n > 0$, entonces todo subgrupo $H$ de $G$ es cíclico de orden un divisor de $n$.

iii) Además, para cada $m$ divisor de $n$, hay uno y solo uno subgrupo de orden $m$.

### 1.4. Teorema de Lagrange. Consecuencias

**Teorema de Lagrange 1.4.1** Sea $G$ un grupo finito de orden $n$, esto es $|G| = n$. Si $H < G$, entonces el orden de $H$ es un divisor del orden de $G$.

**Demostración**

Sea $G$ un grupo. $|G| = n$. Sea $G$ la unión de conjuntos disjuntos tales que todos ellos tienen el mismo número de elementos. Para cada $g \in G$, consideramos $gH = \{gh \mid h \in H\}$. Sea la aplicación:

$$
\varphi : H \rightarrow gH \text{ biyectiva.}
$$

$$
h \mapsto gh
$$

Entonces $\text{card}(gH) = \text{card}(H)$ $\forall g \in G$. Por tanto

$$
G = \bigcup_{x \in G} xH \Rightarrow |G| = \sum_{x \in G} |xH| = |G/H| \ast |H|
$$

**Corolario 1.4.2** Todo grupo de orden primo es cíclico.

**Demostración**

Sea $G$ un grupo de orden $p$, $p$ primo. Sea $a \in G$ distinto del elemento neutro. Sea $H = \langle a \rangle$, $|H| = m$. Por el T. de Lagrange, $|H| || G$ y como $p$ es primo y $m \geq 2$, $m = p$ y por tanto, $G$ es cíclico.

**Definición 1.4.3** Sea $G$ un grupo y $H < G$. Se define el índice de $G$ sobre $H$ y lo se denota por $[G : H]$, como el $n^o$ de subconjuntos distintos de $gH$.

**Observación:** Sea $G$ un grupo. Sea $a \in G$. Ord(a) es un divisor del orden de G.
Ejemplo de aplicación 1.4.4 Prueba que todo grupo de orden 4 es abeliano y encuentra cuántos hay salvo isomorfismos, y describlos.

Solución: Sea $G$ un grupo de orden 4. Por el Teo. de Lagrange, todo elemento de $G$ es un divisor de 4. Descartando que $G$ sea cíclico, encontramos que todo elemento distinto del neutro tiene orden 2. Luego $G$ es abeliano. Sea $a \in G, a \neq e$ y sea $H = \langle a \rangle$ el subgrupo generado por $a$. Dado que $H$ es un subgrupo propio, existe $b \in G$ tal que $b \notin H$. Claramente $G = H \cup Hb = \{e, a, b, ab\}$, con $ba = ab$. Podemos comprobar con ayuda de una tabla, que $G$ es el grupo de Klein.

1.5. Grupos abelianos Finitos

Definición 1.5.1 Sea $G$ un grupo, $|G| = n$. Definimos el exponente de $G$, y lo denotamos por $\exp(G)$, como $\exp(G) = \text{m.c.m}\{\text{ord}(a) \mid a \in G\}$.

Teorema 1.5.2 Sea $G$ un grupo finito de exponente $n$, entonces $G$ contiene un elemento (y por lo tanto, un subgrupo cíclico) de orden $n$.

Demostración

Por el Teorema de la Factorización, podemos expresar $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ como producto de potencias de primos. Para cada $1 \leq i \leq k$ sea $v_i = np_i^{\alpha_i - 1}$. Existe $a_i \in G$ tal que $a_i^{v_i} \neq e$. Sea ahora $b_i = a_i^{n/p_i^{\alpha_i}}$. Tenemos entonces que $\text{ord}(b_i) = p_i^{\alpha_i}$, y de aquí, $b = b_1...b_k$ tiene orden $n$.

Proposición 1.5.3 Sea $F$ un cuerpo. Sea $G < F, |G| < \infty$. Entonces $G$ es cíclico.

Demostración

Como $G$ es finito, $n = \exp(G)$. Por el Teorema anterior, $G$ contiene un subgrupo cíclico $C$ de orden $n$. Por otro lado, todo elemento de $G$ satisface la ecuación $x^n = e$. De donde, $|G| \leq n = |C|$. Esto implica que $G = C$, y por tanto, es cíclico.

Proposición 1.5.4 Sea $G$ un grupo finito de exponente 2. Entonces $G \cong B_2 \cong C_2^n$.

Teorema 1.5.5 Sea $A$ un grupo abeliano finito. Para cada primo $p$ que divide a $|A|$, consideramos $S_p$, que denota todos los elementos de $A$ de orden una potencia de $p$ (incluyendo el 0), entonces cada $S_p$ es un subgrupo de $A$ y $A$ es su suma directa.

Demostración

La comprobación de que $S_p$ es un subgrupo de $A$ es trivial. Sea $x \in A$, distinto del elem. neutro. $\text{Sea ord}(x) = n$, donde por el Teo. de Lagrange, $n \mid |A|$. Supongamos, que $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, donde cada $p_i$ son distintos y $\alpha_i \geq 1$. Escribimos, para cada $i \leq i \leq r$, $q_i = n/p_i^{\alpha_i}$. Obtenemos que el máximo común divisor de todos los $q_i$ es 1 y por la igualdad de Bezout, existen $k_1,k_2...k_r \in \mathbb{Z}$ tales que $k_1q_1 + ... + k_rq_r = 1$. Esto nos da que $x = (k_1q_1 + ... + k_rq_r)x = k_1q_1x + ... + k_rq_rx$. Cada $q_rx$ tiene orden un divisor de $p_i^{\alpha_i}$. Así $x$ puede ser expresado como suma de elementos con ordenes divisores de $p_1^{\alpha_1}, p_2^{\alpha_2},..., p_r^{\alpha_r}$ respectivamente. Por tanto, $x \in S_{p_1}, S_{p_2},..., S_{p_r} \leq A$. Así $S_p \nmid |A| = A$. 6
Finalmente, probaremos que A es la suma directa de los $S_p$. Esto se dará si para cada $q | A$, $S_q \cap S_p = p | A$ y $p \neq q \Rightarrow <0 >$. Pero esto es fácil de comprobar ya que cualquier elemento de $S_p$ tiene orden una potencia de $q$ mientras que cualquier elemento de $< S_p : p | A$ y $p \neq q >$ tiene orden un primo relativo con $q$. Luego el único elemento que pertenece a la intersección de ellos es el elemento neutro.

**Teorema 1.5.6** Sea $S_p$ un grupo abeliano finito. Entonces $S_p$ es la suma directa de grupos cíclicos (de orden potencia de un primo).

**Demostración**

Sea $s$ un elemento de orden $p^a$ maximal en $S_p$ y sea $T$ un subgrupo de $S_p$ que satisface que $< s > \cap T = < 0 >$. Entonces $< s,T > =< s > \oplus T$. Por tanto: i) $< s >$ y $T$ generan $< s,T >$; ii) $< s >$ y $T$ son normales en $< s,T >$; iii) $< s > \cap T = < 0 >$. Si $< s > \oplus T < S_p$, podemos encontrar un elemento $x \in S_p$ tal que $x \not\in < s > \oplus T$. Ya que $p^a x = 0$, $p^a x \in < s > \oplus T$. Entonces existe $\beta \in \mathbb{Z}^+$ de modo que $p\beta x \in < s > \oplus T$ pero $p^{\beta-1} x \not\in < s > \oplus T$. Llamamos $y = p^{\beta-1} x$. Ahora $py \in < s > \oplus T$. Por consiguiente, $py = ls + t$ ($l \in \mathbb{Z}, t \in T$). Entonces $0 = p^{\beta - 1} y = p^{\beta - 1} ls + p^{\beta - 1} t$. Así $p^{\beta - 1} ls \in < s > \oplus T = < 0 >$. Esto nos permite decir que $p \not| l$, $pk = l$, y por lo tanto, $p(y - ks) = py - ls = t \in T$. Sin embargo, $y - ks \not\in T$. Así $< T,y - ks > \supset T$. Consecuentemente, $< T,y - ks > \cap < s > \supset < 0 >$. Esto es, para algunos $m,x \in \mathbb{Z}$ y $v \in T$ tenemos que $0 \neq ms = v + n(y - ks)$. Como $p \not| n$, tenemos que $m,c.d(n,p) = 1$. Además, $ny = ms - v + nks \in < s > \oplus T$ y $py \in < s > \oplus T$. En consecuencia sería una contradicción si $y \not\in < s > \oplus T$. Por tanto, obtenemos finalmente que $< s > \oplus T = S_p$. Podemos utilizar un argumento similar para completar la demostración del teorema.

**Observaciones:**

1. Si $A$ es un grupo de orden potencia de un primo, no se puede descomponer como suma directa de dos o más grupos no triviales.

2. Ya que cada suma finita directa de los ciclos es un grupo abeliano finito, hemos caracterizado los grupos abelianos finitos con la mayor precisión como suma directa de grupos cíclicos. Con el propósito de efectuar una clasificación de estos grupos tenemos que explicar cómo distinguirlos. Esto se deduce de la cuestión: Dado un grupo abeliano $A$, ¿se puede descomponer como una única suma directa de grupos de orden potencia de un primo $p$? La respuesta inmediata es no; $A = < s > \oplus < t > = < s > \oplus < u >$, donde $< s >, < t >, < u >$ son cíclicos no podemos decir que $< t > = < u >$. Veremos un ejemplo más adelante.

**Teorema Fundamental de los Grupos Abelianos Finitos 1.5.7** Sea $A$ un grupo abeliano finito. Entonces para cualquiera dos descomposiciones de $A$ en suma directa de grupos cíclicos de orden un potencia de un primo, contiene el mismo número de sumandos de cada orden.

**Demostración**

Sea una descomposición de $A$ en una suma directa de grupos de orden potencia de un primo. Para cada $i$ definimos $B_i$ como la suma directa de todos los ciclos de orden $p^i$ en esa descomposición. Entonces $A = B_1 \oplus B_2 \oplus ... \oplus B_s$, y para cada $j \in \mathbb{Z}^+$, $p^j A = p^j B_1 \oplus p^j B_2 \oplus ... \oplus p^j B_s = p^j B_{j+1} \oplus ... \oplus p^j B_s$. (Es claro que $p^j A$ es un subgrupo de $A$). Ahora consideraremos el grupo factor $\frac{p^j A}{p^{j+1} A}$. Este grupo es isomorfo
a^{p}B_{j+1} \oplus \frac{a^{p}B_{j+2}}{p} \oplus \ldots \oplus \frac{a^{p}B_{s}}{p}, una suma directa de p-ciclos. Entonces el número de sumandos en la suma directa de ciclos es \( b_{j+1} + b_{j+2} + \ldots + b_{s} \) donde \( b_{i} \) es el número de sumandos cíclicos en \( B_{i} \). En consecuencia, en número total de sumandos cíclicos en \( \frac{p^{j}A}{p^{j+1}A} \) es igual al número de sumandos cíclicos en \( A \), que tiene de orden a

1.6. Ejercicios

1. Sea \( G \) un grupo. Probar que el elemento neutro y los inversos son únicos.

2. Sea \( G \) un conjunto no vacío dotado de un producto asociativo \( ab, a, b \in G \). Demuestra que \( G \) es un grupo si y sólo si para cualesquiera \( a, b \in G \), las ecuaciones \( ax = b \) y \( ya = b \) tienen soluciones. ¿Qué podemos decir además si \( G \) es un conjunto finito?

3. Sea \( A \) un anillo. Prueba que el conjunto de sus elementos inversibles \( Gr(A) \), es un grupo.

4. Sea \( G \) un grupo con elemento neutro \( e \). Si todo elemento \( a \in G \) verifica que \( a^{2} = e \), entonces \( G \) es abeliano.

5. Prueba que si \( a^{m} = e \), entonces \( \text{ord}(a) \) es un divisor de \( m \).

6. Prueba que \( \text{ord}(bab^{-1}) = \text{ord}(a) \)

7. Sea \( G \) un grupo y sean \( a, b \in G \). Si \( ab = ba \) y \( \text{ord}(a), \text{ord}(b) \) son primos relativos, entonces \( \text{ord}(ab) = \text{ord}(a)\text{ord}(b) \)

8. Prueba que en la tabla de multiplicación de un grupo finito cada elemento del grupo aparece una y una sola vez en cada fila y cada columna.

9. Sea \( G \) un grupo. Sea \( a \in G \) tal que \( \text{ord}(a) = n \). Prueba que el \( \text{ord}(a^{-1}) = n \).

10. Muéstrese que si \( H \) y \( K \) son subgrupos de un grupo abeliano \( G \), entonces \( \{hk \mid h \in H, k \in K \} \) es un subgrupo de \( G \).

11. Encontrar todos los subgrupos de \( C_{42} \).

12. Determine el retículo de los subgrupos de \( C_{8}, C_{4} \times C_{2}, C_{2} \times C_{2} \times C_{2}, D_{4} \) y \( Q \).

13. Sea \( G \) un grupo. Sean \( \{H_{i}\}_{i \in I} \) con \( H_{i} \in G \). Prueba que \( \bigcap_{i \in I} H_{i} \in G \).

14. Encuentra un grupo \( G \) que contenga a un subconjunto \( S \) tal que \( S \) sea un subgrupo respecto a una operación diferente de \( G \), pero no sea un subgrupo bajo la operación en \( G \).
Capítulo 2

Homomorfismos

2.1. Homomorfismo de Grupos

Definición 2.1.1 Sean $(G, \cdot)$ y $(G', \ast)$ dos grupos. Decimos que la aplicación $\varphi : G \rightarrow G'$ es un homomorfismo si se cumple que:

$$\varphi(x \cdot y) = \varphi(x) \ast \varphi(y) \ \forall x, y \in G.$$ 

Para abreviar notación, escribiremos la operación respecto de ambos grupos por yuxtaposición.

Ejercicio: Demostrar que:

1. $\varphi(e) = e'$
2. $\varphi(x^{-1}) = \varphi(x)^{-1}$

Donde e y e' denotan los elem. neutros de G y G' respectivamente.

Proposición 2.1.2 Sea $\varphi : G \rightarrow G'$ un homomorfismo de grupos. Entonces:

1. $\text{Im}(\varphi) = \{\varphi(x) | x \in G\} < G'$
2. $\text{Ker}(\varphi) = \{x \in G | \varphi(x) = e'\} < G$

Demostración

1) Veamos que si $\varphi(x), \varphi(y) \in G' \Rightarrow \varphi(xy^{-1}) \in \text{Im}(\varphi)$.

$$\varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) \in \text{Im}(\varphi)$$

Luego $\text{Im}(\varphi) < G$

2) Veamos que si $x, y \in \text{Ker}(\varphi) \Rightarrow x^{-1}y \in \text{Ker}(\varphi)$, es decir, $\varphi(x^{-1}y) = e'$. Sean $x, y \in \text{Ker}(\varphi) \Rightarrow \varphi(x) = e' ; \varphi(y) = e'$.

$$\varphi(x^{-1}y) = \varphi(x^{-1})\varphi(y) = \varphi(x)^{-1}\varphi(y) = e^{-1}e = e'.$$

Luego $\text{Ker}(\varphi) < G'$. 

9
Definición 2.1.3 Sea $\varphi : G \rightarrow G'$ un homomorfismo de grupos. Entonces:

1. Si $\varphi$ es inyectiva, se dirá que $\varphi$ es un monomorfismo.
2. Si $\varphi$ es sobreyectiva, se dirá que $\varphi$ es un epimorfismo.
3. Si $\varphi$ es biyectiva, se dirá que $\varphi$ es un isomorfismo y que $G$ y $G'$ son isomorfos.
4. Si $G = G'$, se dirá que $\varphi$ es un endomorfismo.
5. Si $\varphi : G \rightarrow G$ es biyectiva, se dirá que es un automorfismo.

Ejemplos:

Sean $G$ y $G'$ dos grupos.

1. $\varphi : G \rightarrow G'$
   
   $x \mapsto e$

   Este homomorfismo es el conocido como el homomorfismo trivial.

2. $\varphi : G \rightarrow G$
   
   $x \mapsto x$

   Conocido como el automorfismo identidad.

Ejercicio: Sea $G$ un grupo. Comprobar que para cada $b \in G$, la aplicación:

$\theta_b : G \rightarrow G$

$x \mapsto bxb^{-1}$

es un automorfismo de grupos. También llamado el automorfismo interno de $G$.

2.2. Subgrupos Normales

Definición 2.2.1 Sea $G$ un grupo y sea $N < G$. Diremos que $N$ es un subgrupo normal de $G$ y lo notaremos por $N \triangleleft G$ si:

$\forall g \in G, \forall x \in N \Rightarrow gxg^{-1} \in N$

Proposición 2.2.2 Si $\varphi : G \rightarrow G'$ es un homomorfismo, entonces $\ker(\varphi) \triangleleft G$.

Demostración

Por la Proposición 2.1.2, sabemos que $\ker(\varphi) \leq G$. Supongamos ahora que $n \in \ker(\varphi)$ y sea $g \in G$. Entonces $\varphi(g^{-1}ng) = \varphi(g^{-1})\varphi(n)\varphi(g) = \varphi(g^{-1})e'\varphi(g) = e'$. Por tanto, para cada $g \in G$, tenemos que $g^{-1}\ker(\varphi)g \subseteq \ker(\varphi)$.

Ejemplos: Sea $G$ un grupo.

1. Si $G$ es abeliano, entonces todos sus subgrupos son normales.
2. Sea \(H < G\) tal que \([G : H] = 2\). Dado \(g \notin H\) ⇒ \(G = H \cup Hg = H \cup gH\) con \(Hg \cap H = \emptyset\) (\(H \cap gH = \emptyset\)), entonces \(H \triangleleft G\).

**Definición 2.2.3** Sea \(G\) un grupo y sean \(N \triangleleft G\) y \(H < G\). Se define el menor conjunto de \(G\) que contiene a \(N\) y \(H\) como al conjunto:

\[N \triangleleft H = \{xy \mid \forall x \in N, \forall y \in H\}\]

**Lema 2.2.4** Sea \(G\) un grupo y sean \(N \triangleleft G\) y \(H < G\). Entonces \(H \triangleleft N \triangleleft G\).

**Demostración**
Sean \(x_1, x_2, y_1, y_2 \in H\). Veamos que \((x_1y_1)(x_2y_2)^{-1} \in NH\).
\[
x_1y_1(x_2y_2)^{-1} = x_1y_1y_2^{-1}x_2^{-1} = x_1yx_2^{-1}(y^{-1}y) = x_1(x_2^{-1}y^{-1})y = (x_1x)y \in NH
\]

donde \(y = y_1y_2^{-1} \in H\).

**Definición 2.2.5** Un grupo es simple si no tiene subgrupos normales propios no triviales.

### 2.3. Grupo Cociente

**Definición 2.3.1** Sea \(G\) un grupo y sean \(x, y \in G\). Definimos la relación de equivalencia:

\[x \sim y \iff xH = yH \iff x^{-1}y \in H\]

Para algún \(x \in G\), definimos \(\overline{x} = xH = \{xh \mid h \in H\}\)

**Ejercicio:** Comprobar que la relación es de equivalencia.

**Definición 2.3.2** Sea \(G\) un grupo y sea \(N \triangleleft G\). Consideramos el conjunto \(G/N = \{gN : g \in G\}\). Sea la operación:

\[\Psi : G/N \times G/N \to G/N \quad (g_1N, g_2N) \mapsto (g_1g_2)N\]

Veamos si con esta operación, podemos dotar al conjunto \(G/N\) de estructura de grupo. En primer lugar, veamos que la operación está bien definida y comprobemos después por la **Proposición 1.2.2** que es un grupo.

Sean \(x_1, x_2, y_1, y_2 \in G : x_1N = x_2N\) e \(y_1N = y_2N\). Entonces \(x_2 \in x_1N\) e \(y_2 \in y_1N\) ⇒ \(\exists z_1, z_2 \in N\) tales que \(x_2 = x_1z_1\) e \(y_2 = y_1z_2\). Por tanto, \(x_2y_2N = x_1z_1y_1z_2N = x_1y_1z_1z_2N = xyN\). La comprobación ahora de que posee estructura de grupo sería trivial.

Además sabemos que \(\text{ord}(G/N) = [G : N] = \frac{\text{ord}(G)}{\text{ord}(N)}\)

**Ejercicio:**

Sea \(G\) un grupo y \(N \triangleleft G\). Sea la aplicación:

\[
\pi : G \to G/N \quad g \mapsto gN
\]

Comprobar que \(\pi\) es un homomorfismo con \(\text{Ker}(\pi) = N\).
2.4. Teoremas de Isomorfía

1° Teorema de Isomorfía 2.4.1 Sean $G$ y $G'$ dos grupos y sea $\varphi : G \rightarrow G'$ un homomorfismo. Entonces:

$$G / \text{Ker} (\varphi) \cong \text{Im} (\varphi)$$

**Demostración**

Definimos la aplicación: Para simplificar la notación, $K = \text{Ker} (\varphi)$

$$\varphi : G / \text{Ker} (\varphi) \rightarrow \text{Im} (\varphi)$$

$aK(\varphi) \mapsto \varphi(a)$

1. Veamos que es un homomorfismo:

$$\varphi ((aK)(bK)) = \varphi ((ab)K) = \varphi (ab) = \varphi (a)\varphi (b) = \varphi (aK)\varphi (bK)$$

2. Claramente, $\varphi$ es sobreyectiva.

3. Veamos que es inyectiva $\iff \text{Ker} (\varphi) = \{ eK \}$

Sea $e' = \varphi (aK) = \varphi (a) \Rightarrow a \in K \Rightarrow e^{-1}a \in K \iff aK = eK = K$

2° Teorema de Isomorfía 2.4.2 Sea $G$ un grupo. Sea $N \triangleleft G$, $H < G$. Entonces:

1. $N \triangleleft NH$
2. $H \cap N \triangleleft H$
3. $\frac{NH}{N} \cong \frac{H}{H \cap N}$

**Demostración**

1. Por la definición de $NH$, sabemos que $N \subseteq NH$. Sea $h \in H, n \in N, y g \in G$. Entonces $ghn^{-1} = (gh^{-1})(g^{-1}) \in HN$, luego $N \triangleleft NH$.

2. Consideremos la aplicación:

$$\vartheta : H \rightarrow NH / N$$

$h \mapsto hN$

Veamos que es un homomorfismo con $\text{Ker} (\vartheta) = H \cap N$

$$\vartheta (gh) = ghN = (gN)(hN) = \vartheta (g)\vartheta (h) \forall g, h \in H$$

Finalmente, obtenemos que $\text{Ker} (\vartheta) = \{ h \in H \mid hN = N \} = N \cap H$. Por tanto, por el 1° Teorema de Isomorfía, se tiene que:

$$\frac{NH}{N} \cong \frac{H}{\text{Ker} (\vartheta)} \Rightarrow \frac{NH}{N} \cong \frac{H}{H \cap N}$$
Teorema de Isomorfía 2.4.3 Sea $G$ un grupo, $N \triangleleft G$, $K \triangleleft G$ tales que $N \subseteq K$. Entonces:
1. $K/N \triangleleft G/N$
2. $G/K \cong \frac{G}{N}$

Demostración

Sea la aplicación:

$\phi : G \to \frac{G}{K}$

$a \mapsto aK$ ($N/K)$

$\phi(ab) = [(ab)K(N/K) = [(aK)(bK)](N/K) = [(aK)(N/K)][(bK)(N/K)] = \phi(a)\phi(b)$

Por tanto, $\phi$ es un homomorfismo. El Ker$(\phi) = \{x \in G \mid \phi(x) = N/K\}$. Pero este conjunto, es exactamente $N$, por tanto, por el 1° Teorema de Isomorfía:

$G/K \cong \frac{G}{N}$

Notación:

1. $[\text{Ker}(\varphi); G] = \{H \leq G \mid \text{Ker}(\varphi) \subseteq H\}$
2. $[[e'], \text{Im}(\varphi)] = \{T \leq G' \mid T \subseteq \text{Im}(\varphi)\}$

Teorema de la Correspondencia: 2.4.4 Sean $G$ y $G'$ dos grupos y la aplicación $\varphi: G \to G'$ un homomorfismo de grupos. Definimos:

1. $\varphi_*(H) = \{\varphi(h) \mid h \in H\}$
2. $\varphi^*(T) = \{x \in G \mid \varphi(x) \in T\}$

Entonces:

1. $\varphi_*(\varphi_*(H)) = H \quad \forall H \in [\text{Ker}(\varphi), G]\$
2. $\varphi_*(\varphi^*(T)) = T \quad \forall T \in [[e'], \text{Im}(\varphi)]$

Demostración

Por la definición, sabemos que dichas aplicaciones están bien definidas. Vemos las igualdades por una doble contención:

1. \[
\subseteq \quad \text{Sea } h \in H \Rightarrow \varphi(h) \in \varphi_*(H) \iff h \in \varphi^*(\varphi_*(H))
\]

2. \[
\subseteq \quad \text{Sea } x \in \varphi^*(\varphi_*(H)) \iff \varphi(x) \in \varphi_*(H) \iff \exists h \in H \text{ tal que } \varphi(x) = \varphi(h) \iff \varphi(x)\varphi(h)^{-1} = e' \iff \varphi(xh^{-1}) = e' \iff xh^{-1} \in \text{Ker}(\varphi) \subseteq H \Rightarrow xh^{-1} = h' \in H \Rightarrow x = hh' \in H
\]
2. \[ y \in \varphi_*(\varphi^*(T)) \Rightarrow \varphi(x) = y \text{ donde } x \in \varphi^*(T) \iff \varphi(x) \in T \Rightarrow y \in T. \]

Ya que \( T \subset \text{Im}(\varphi) \), dado \( y \in T \), \( y \in \text{Im}(\varphi) \), \( y = \varphi(x) \), para algún \( x \in G \).

\[ T \ni y = \varphi(x) \Rightarrow x \in \varphi^*(T) \Rightarrow y = \varphi(x) \in \varphi_*(\varphi^*(T)). \]

**Corolario 2.4.5** Sea \( G \) un grupo y \( N \triangleleft G \). Consideramos la aplicación:

\[ \pi: G \longrightarrow G/N \]

\[ a \longmapsto aN \]

es un epimorfismo de grupos con \( \ker(\pi) = N \). Entonces los subgrupos del grupo cociente, son de la forma \( H/N \), donde \( H \leq G \), \( N \subseteq H \).

\[ [N, G] \longrightarrow \pi^* \pi^* [\{\pi(e)\}, G/N] \]

### 2.5. Clase de Conjugación. Ecuación de Clases

**Definición 2.5.1** Sea \( G \) un grupo finito. Definimos la relación:

\[ x \sim y \Leftrightarrow \exists a \in G \text{ tal que } y = axa^{-1} \]

Dejamos como ejercicio la comprobación de que la relación es de equivalencia, también conocida como la relación de conjugación. Dado \( x \in G \), denotamos por \( C_x \) a la clase de conjugación de \( x \), esto es, \( C_x = \{axa^{-1} \mid a \in G\} \). Como es relación de equivalencia, forman una partición en \( G \) tal que:

Para algunos \( C_x, C_y \) \[ \begin{cases} C_x = C_y \iff y = axa^{-1} \text{ para un cierto } a \in G. \\ C_x \cap C_y = \emptyset \end{cases} \]

\[ G = \bigcup_{j=1}^{n} C_{x_j} \quad C_{x_j} \cap C_{x_k} = \emptyset \quad \forall j \neq k \]

**Ecuación de clases**

\[ |G| = \sum_{j=1}^{n} \text{card}(C_{x_k}) = \sum_{j=1}^{n} |C_{x_j}| + \sum_{k=r+1}^{n} |C_{x_k}| \]

Sabemos que \( x \in C_x \). Además, \( C_x = \{x\} \Leftrightarrow x \in Z(G) \). Por tanto:

\[ |G| = |Z(G)| + \sum_{k=r+1}^{n} |C_{x_k}| \]

**Definición 2.5.2** Fijamos \( x \in G \). Definimos el normalizador de \( x \), y lo denotamos por \( N(x) \), al conjunto:

\[ N(x) = \{a \in G \mid axa^{-1} = x\} \]

**Ejercicio:** Comprobar que \( N(x) < G \)
Lema 2.5.3 Sea $G$ un grupo. Dado $a \in G$. Entonces $|C_x| = \frac{|G|}{|N(x)|}$

Demostración

Hay que demostrar que $C_x$ y $\{aN(x) \mid a \in G\}$ son equipotentes. Sea la aplicación:

$$\varphi : \{aN(x) \mid a \in G\} \rightarrow C_x$$

$$aN \mapsto axa^{-1}$$

Para cualquier $x, y \in G$, podemos ver que $x^{-1}Hx = y^{-1}Hy \Leftrightarrow xy^{-1} \in N(x) \Leftrightarrow N(x)x = N(x)y$.

Corolario 2.5.4 Sea $G$ un grupo de orden $p^n$ donde $p$ es primo y $n \geq 1$, entonces $p \mid |Z(G)|$.

Demostración

Si $|G| = p \ (n=1) \Rightarrow G$ es cíclico $\Rightarrow G$ es abeliano $\Rightarrow Z(G) = G$.

En general, por la ecuación de clases, $|C_{x_k}| = |G, N(x)| = \frac{|G|}{|N(x)|} = \frac{p^n}{p^m} \Rightarrow p \mid \frac{|G|}{|N(x)|}$

Corolario 2.5.5 Todo grupo de orden $p^2$ es abeliano ($p$ primo).

Demostración

Por el corolario anterior, $Z(G)$ no es trivial.

$$|Z(G)| = \left\{ \begin{array}{ll}
        p^2 & \text{si } Z(G) = G \\
        p & \text{si } Z(G) \neq G
      \end{array} \right.$$

Sea $a \in G \mid G/Z(G) = \{Z(G), aZ(G), \ldots, a^{p-1}Z(G)\}$ cuya unión es disjunta. Entonces:

$G = Z(G) \cup aZ(G) \cup \ldots \cup a^{p-1}Z(G)$. Para algunos $i, j$, y para $t, r \in Z(G)$, tenemos que

$x = a^i, y = a^j, t = a^t, r = a^r$. Pero entonces, $xy = a^i a^t = a^i a^t = a^i a^t = a^j a^t = yx$ y por tanto, $G$ es abeliano, es decir, $Z(G) = G$. Pero $|Z(G)| = |G| > p$, lo que es una contradicción.

2.6. Grupo de los automorfismos de un grupo cíclico

Proposición 2.6.1 Sea $G = < a >$ un grupo cíclico de orden $n$. Sea $\varphi \in \text{Aut}(G)$. ¿Cuáles son las posibles imágenes de $a$ mediante $\varphi$? $\varphi(a) = a^k$ ¿Cuáles son los posibles valores de $k$? $G = < a >$ $\Rightarrow \text{ord}(a) = n = \text{ord}(\varphi(a))$ $\Rightarrow |G| = n \quad \text{m.c.d}(k, n) = 1$

Ejemplos:

1. $\text{Aut}(C_5)$ $C_5 = < a >$ $\Rightarrow \text{ord}(a) = 5$. Como 5 es primo, los primos relativos con 5 son 1, 2, 3, 4, es decir, $|\text{Aut}(C_5)| = 4$

Sea $G = \text{Aut}(C_5)$. Las posibilidades para $G$ son $C_4$ ó $C_2 \times C_2$. Sea la aplicación:
Entonces $\text{Aut}(C_5) \cong C_4$

2. $\text{Aut}(C_7)$ \quad $C_7 = \langle a \rangle$ \quad $\text{ord}(a) = 7$. Como 7 es primo, los primos relativos con 5 son 1,2,3,4,5,6, es decir, $|\text{Aut}(C_7)| = 6$

Sea $G = \text{Aut}(C_7)$. Las posibilidades para G son $C_6$ ó $D_3$. Sea la aplicación:

$\varphi : C_7 \longrightarrow C_7$

$a \longmapsto a^3$

Entonces $\text{Aut}(C_7) \cong C_6$

3. $\text{Aut}(C_6)$ \quad $C_6 = \langle a \rangle$ \quad $\text{ord}(a) = 6$. Los primos relativos con 6 son 1,5, es decir, $|\text{Aut}(C_6)| = 2$

Sea $G = \text{Aut}(C_6)$. Sea la aplicación:

$\varphi : C_6 \longrightarrow C_6$

$a \longmapsto a^5$

Entonces $\text{Aut}(C_6) \cong C_2$

4. $\text{Aut}(C_{12})$ \quad $C_{12} = \langle a \rangle$ \quad $\text{ord}(a) = 12$. Los primos relativos con 12 son 1,5,7,11 es decir, $|\text{Aut}(C_{12})| = 4$

Sea $G = \text{Aut}(C_{12})$. Las posibilidades para G son $C_4$ ó $C_2 \times C_2$. Sea la aplicación:

$\varphi : C_{12} \longrightarrow C_{12}$

$a \longmapsto a^5$

Entonces $\text{Aut}(C_{12}) \cong C_2 \times C_2$

**Proposición 2.6.2** Sea $(A, +, \cdot)$ un anillo. Sea $Gr(A)$ el grupo de los elem. inversibles de $A$. Sea $(A, +)$ un grupo aditivo de A. Consideremos la aplicación:

$\theta : Gr(A) \longrightarrow \text{Aut}(A, +)$

$a \longmapsto \theta_a$

Donde $\theta_a = ax \quad (x \in A)$. Entonces $\theta$ es un monomorfismo de grupos.

**Demostración**

$\theta(a + b) = \theta_{a+b} = (a + b)x = ax + bx = \theta_a + \theta b = \theta(a) + \theta(b)$.

Sea $a \in \text{Ker}(\theta) \Rightarrow \theta(a) = 0 \Rightarrow ax = 0 \Leftrightarrow a = 0$ Luego es inyectiva, y $\theta$ es un monomorfismo de grupos.
Proposición 2.6.3 ¿Cuándo podemos afirmar que $\tau : Gr(A) \rightarrow Aut(A,+)$ es un isomorfismo de anillos?

Solución

Supongamos que el anillo $(A,+,\ast)$, el grupo aditivo $(A,+)$ es cíclico finito y que está generado por 1 (unidad de A). $(A,+)$ $\cong (\mathbb{Z}_n,+)$ 
Sea $f \in Aut(A,+)$. $f$ queda determinado por la imagen de 1. $f(1) = k1$, donde $k$ es primo relativo con $n$, $\text{mcd}(k,n) = 1$. Luego $Aut(A,+)$ $\cong Gr(A)$

Repasando los ejemplos anteriores:

1. $Aut(\mathbb{Z}_5,+)$ $\cong Gr(\mathbb{Z}_5,x,\ast)$ $\cong C_4$
2. $Aut(\mathbb{Z}_6,+)$ $\cong Gr(\mathbb{Z}_6,x,\ast)$ $\cong C_2$
3. $Aut(\mathbb{Z}_6,+)$ $\cong Gr(\mathbb{Z}_7,x,\ast)$ $\cong C_6$
4. $Aut(\mathbb{Z}_{12},+)$ $\cong Gr(\mathbb{Z}_{12},x,\ast)$ $\cong C_2 \times C_2$

En general, $Aut(\mathbb{Z}_p,+) \text{ donde p es primo, } \mathbb{Z}_p \cong C_{p-1}$

2.7. Ejercicios

1 Sea $\varphi : G \rightarrow G$ un automorfismo. Comprobar que cada $a \in G$, $\text{ord}(a) = n$ si y sólo si $\text{ord}(\varphi(a)) = n$

2 Sea $G$ un grupo. Probar que si $H$ es un subgrupo de $G$ y si $G$ no tiene otros subgrupos isomorfos a $H$, entonces $H$ es un subgrupo normal de $G$.

3 Sea $\varphi$ un homomorfismo de grupos. Demostrar que $\varphi(e) = e'$ y $\varphi(x^{-1}) = \varphi(x)^{-1}$.

4 Sea $G$ un grupo y sea $N \triangleleft G$. Sea la aplicación:

\[ \pi : G \rightarrow G/N \]
\[ g \mapsto gN \]

Comprobar que $\pi$ es un homomorfismo con $\text{Ker}(\pi) = N$.

5 Sea $G$ un grupo y sea $x \in G$. Probar que $N(x) < G$.

6 Sean $p_1, p_2, p_3$ tres números primos distintos. Consideremos la aplicación:

\[ f : \mathbb{Z} \rightarrow \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_3} \]
\[ x \mapsto (\overline{x}, \overline{x}, \overline{x}) \]

Demostrar que $f$ es un homomorfismo de grupos sobreexpecto. ¿Cuál es el núcleo de $f$?
Capítulo 3

Ejemplos y clasificación de algunos grupos

3.1. Grupo de Permutaciones

Definición 3.1.1 Una permutación de un conjunto $A$ es un aplicación biyectiva de $A$ en $A$.

Proposición 3.1.2 Sea $X$ un conjunto y sea $B(X) = \{\text{Aplicaciones biyectivas de } X\}$. Entonces $(B(X), \circ)$ tiene estructura de grupo.

Demostración

1. Asociativa: Trivial, ya que la composición de aplicaciones es asociativa.

2. Elemento neutro: La aplicación identidad.

3. Elemento inverso: Como la aplicación es biyectiva, sabemos que existe inversa.
   Si $a \in B(X) \Rightarrow \exists a^{-1} \in B(X)$ tal que $aa^{-1} = a^{-1}a = e$

Cuando $X$ es un conjunto finito, $X = \{1, 2, ..., n\}$. Normalmente llamaremos al conjunto $B(X) = S_n$ y además sabemos que $|S_n| = n!$

Notación Sea $S_n$ el grupo de las aplicaciones biyectivas de un conjunto $X$ de $n$ elementos, y sea $\sigma \in S_n$. Una permutación la vamos a denotar:

$$\sigma = \left( \begin{array}{cccc} 1 & 2 & 3 & \ldots & n \\ \sigma_1 & \sigma_2 & \sigma_3 & \ldots & \sigma_n \end{array} \right)$$

donde $\sigma_k = \sigma(k)$

Ejemplo:

Sea $A = \{1, 2, 3, 4, 5\}$ y las permutaciones:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$
Entonces:
\[ \rho \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} \]
También podemos denotar las permutaciones con notación cíclica \( \rho \sigma = (1, 2, 5, 3) \) y decir que tiene ciclo de longitud 4. En general, la permutación \( \tau = (x_1, x_2, ..., x_n) \) es un ciclo de longitud \( n \). Esto nos conduce a la siguiente definición.

**Definición 3.1.3** Una permutación \( \tau \) de un conjunto \( A \) es un ciclo de longitud \( n \) si existen \( a_1, a_2, ..., a_n \in A \) tales que
\[
\tau(a_1) = a_2 \quad \tau(a_2) = a_3 \quad ... \quad \tau(a_{n-1}) = a_n \quad \tau(a_n) = a_1
\]
y \( \tau(x) = x \) para cada \( x \in A \) tal que \( x \notin \{a_1, a_2, ..., a_n\} \).

**Definición 3.1.4** Un ciclo de longitud 2 es una transposición.

**Teorema de Cayley-Hamilton 3.1.5** Todo grupo finito \( G \) de orden \( n \) es isomorfo a un subgrupo de \( S_n \).

**Demostración**

Sea \( G = \{x_1, x_2, ..., x_n\} \) y consideremos las aplicaciones:
\[
\vartheta : G \rightarrow \text{Biyecc}(G) \quad \psi_a : G \rightarrow G \quad b \mapsto ab
\]

1. Veamos que \( \psi \) es inyectiva
\[
\psi_a(b) = \psi_a(c) \Rightarrow ab = ac \Rightarrow b = c
\]

2. Veamos que \( \psi \) es sobreyectiva

Sea \( b \in G \) \( \Rightarrow \exists x \in G \) \( \mid \psi_a(x) = b \Rightarrow x = a^{-1}b \).

Por tanto es biyectiva

3. \( \vartheta \psi_{ab}(x) = \psi_a \circ \psi_b(x) \)
\[
\psi_{ab} = abx = a(bx) = \psi_a(bx) = \psi_a(x) \circ \psi_b(x)
\]

4. Veamos que \( \vartheta \) es inyectiva

Sea \( a \in \text{Ker}(\vartheta) \) \( \Leftrightarrow \psi_a = e \Leftrightarrow \forall b \in G, \psi_a(b) = b \Leftrightarrow ab = b \Leftrightarrow abb^{-1} = bb^{-1} \Leftrightarrow a = e \forall b \in G \).

**Definición 3.1.6** Sea \( X = \{1, 2, ..., n\} \) un conjunto y sea \( \sigma \in S_n \) (\( S_n \) es el grupo de permutaciones de \( X \)). Dado \( x \in G \), se define la órbita de \( x \) como el conjunto:
\[
\sigma(x) = \{x, \sigma(x), \sigma^2(x), ..., \sigma^k(x)\}
\]

**Ejemplo:** Sea \( X = \{1, 2, 3, 4, 5\} \) y sea la permutación:
\[
\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}
\]
\[
\mu(1) = \{1, 5, 3\} \quad ; \quad \mu(4) = \{2, 4\}
\]
**Teorema 3.1.7** Toda permutación σ de \( S_n \) se puede expresar como composición (producto) de permutaciones cíclicas disjuntas.

**Demostración**

Supongamos, sin pérdida de generalidad, que \( A = \{1, 2, 3, ..., n\} \). Consideremos los elementos \( 1, \sigma(1), \sigma^2(1), \sigma^3(1), ... \). Como \( A \) es finito, sea \( r \) el mínimo que cumple \( \sigma^r(1) = 1 \), porque si \( \sigma^r(1) = \sigma^s(1) \) con \( 0 < s < r \), tendríamos que \( \sigma^{r-s}(1) = 1 \), con \( r - s < r \), que sería una contradicción. Por tanto, sea \( \tau_1 = (1, \sigma(1), \sigma^2(1), ..., \sigma^{r-1}(1)) \).

Sea \( i \) el primer elemento de \( A \) que no aparece en la notación cíclica de \( \tau_1 \). Repitiendo el argumento anterior, obtenemos un ciclo \( \tau_2 = (i, \sigma(i), \sigma^2(i), ..., \sigma^{f}(1)) \).

Obtenemos que \( \tau_1 \) y \( \tau_2 \) son disjuntos, ya que si tuvieran algún elemento en común serían la misma permutación. Siguiendo este procedimiento, podemos expresar \( \sigma \) como \( \sigma = \tau_1 \tau_2 ... \tau_m \).

**Corolario 3.1.8** El conjunto de las permutaciones cíclicas es un conjunto generador de \( S_n \).

**Teorema 3.1.9** Toda permutación cíclica se puede expresar como una composición de transposiciones.

**Ejemplos:**

1. Sea \( \tau \in S_6 \)

\[
\tau = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
6 & 4 & 1 & 5 & 2 & 3 \\
\end{pmatrix}
\]

Entonces \( \tau = (1, 6, 3)(2, 4, 5) = (1, 6)(6, 3)(2, 4)(4, 5) \)

2. Sea \( \rho \in S_9 \)

\[
\tau = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
3 & 7 & 5 & 9 & 1 & 6 & 2 & 4 & 8 \\
\end{pmatrix}
\]

Entonces \( \rho = (1, 3, 5)(2, 7)(4, 9, 8) = (1, 3)(3, 5)(2, 7)(4, 9)(9, 8) \)

**Definición 3.1.10** Una permutación de un conjunto finito es par o impar de acuerdo con que pueda expresarse como el producto de un número par de transposiciones o como producto de un número impar de transposiciones respectivamente.

**Definición 3.1.11** El subgrupo de \( S_n \) que consta de las permutaciones pares de \( n \) elementos es el grupo alternante \( A_n \) de \( n \) elementos.

### 3.2. Grupo Diédrico

**Definición 3.2.1** Si \( n \geq 2 \), el grupo diédrico \( D_n \) es un grupo de orden \( 2n \) presentado de la siguiente forma: \( D_n = \{1, a, a^2, ..., a^{n-1}, b, ba, ..., ba^{n-1}\} \), \( |a| = n \), \( |b| = 2 \) y además, \( aba = b \). De esta manera, quedan determinados todos los elementos de \( D_n \).

Esta última ecuación implica que \( a^k ba^k = b \) \( \forall k \in \mathbb{Z} \), y por tanto, \( a^k b = ba^{-k} = ba^{n-k} \) y \( |ba^k| = 2 \) \( \forall k \in \mathbb{Z} \). En particular, \( ab = ba^{n-1} \).
Ejemplos:
1. El grupo $D_3$ es isomorfo a $S_3$
2. El grupo $D_2$ es isomorfo al Grupo de Klein, ya que es abeliano $(ba = a^{-1}b = ab$, ya que $|a| = 2$)

Proposición 3.2.2 Sea $G$ un grupo de orden $2p$, donde $p$ es primo, $p > 2$. Entonces $G \cong C_{2p}$ ó $G \cong D_p$.

Demostración

Por el T° de Lagrange, para algún $x \in G$,ord$(x) = 1,2,p$ ó $2p$.

1. Si $\forall x \in G \ x^2 = e \Rightarrow G \cong C^2_2 \Rightarrow |G| = 2^n \neq 2p$. Sería una contradicción.

2. Si $\exists a \in G | \ ord(a) = 2p \Rightarrow G \cong C_{2p}$

3. Si $\exists a \in G | \ ord(a) = p$. Sea $H = \langle a \rangle = \{e, a, a^2,...a^{p-1}\}$

$[G : H] = \frac{|G|}{|H|} = 2 \Rightarrow \exists b \in G \setminus H : G = H \cup Hb \Rightarrow Hb^2 = H$

$\Rightarrow b^2 \in H \{ 1)b^2 = e \ 2)b^2 = a^k \ k = 1,...,p - 1 \Rightarrow G$ es cíclico $\Leftrightarrow ord(a) = 2p$

Sup. que $ord(b) \neq 2p$, entonces $ord(b) = p \Rightarrow p = 2r + 1$

$e = b^p = b^{2r+1} = b^{2r}b = (b^2)^rb = a^{kr}b \Rightarrow b = a^{-kr} \in H$ Contradicción. Por tanto, $ord(b) = 2p$. Falta por determinar $ba = ?$

Si $ba = \begin{cases} ab \rightarrow G \cong C_{2p} \\ a^{n-1}b \rightarrow G \cong D_p \end{cases}$

Sup. por el contrario que $ba = a^kb \ k > 1 \ k < p - 1 \Rightarrow \ mcd(k,p) = 1$

Por la igualdad de Bezout, $1 = kr + sp \Rightarrow s \in \mathbb{Z}, \ ba^n = a^k b \Rightarrow a = ba^k b \Rightarrow a^r = ba^k r = bab \Rightarrow a^k = a^r \Rightarrow a^{k^2} = a^k = a \Rightarrow a^{k^2 - 1} \Rightarrow p | (k^2 - 1) \Rightarrow p | (k + 1)(k - 1) \Rightarrow p | (k + 1)$ ó $p | (k - 1)$.

Pero $k+1 < p$ y $p$ es primo y $k - 1 \neq 0$. Luego es una contradicción si $ba = a^k b \ k > 1 \ k < p - 1$.

3.3. Clasificación de grupos

En este apartado clasificaremos grupos según su orden, y veremos que no hay más salvo isomorfismo.

Proposición 3.3.1 Los únicos grupos de orden 6 salvo isomorfismo son $C_6$ y $D_3$.

Demostración

Sea $G$ un grupo tal que $|G| = 6$. Por el T° de Lagrange, los posibles órdenes de sus elementos son $1,2,3$ y $6$.

1. $\exists a \in G | \ ord(a) = 6 \Rightarrow G \cong C_6$

2. $\exists a \in G | \ ord(a) = 6$
a) \[ \exists a \in G \mid \text{ord}(a) = 3 \implies \forall x \in G \ x^2 = e \implies |G| = 2^n \neq 6 \text{ Contradicción} \]

b) \[ \exists a \in G \mid \text{ord}(a) = 3 \]

Sea \( H = \langle e, a, a^2 \rangle \) Como \( |G : H| = 2 \implies \exists b \in G \setminus H \mid G = H \cup Hb \) con \( H \cap Hb = \emptyset \implies G = \langle e, b \rangle \) Para completar la tabla de multiplicación de \( G \), necesitamos saber cuánto es \( b^2 = ?? \) , \( ba = ?? \).

1) Si \( Hb^2 = Hb \implies b^2 = xb \implies x = b \in H \text{ Contradicción. Luego } Hb^2 = H \implies b^2 \in H = \{e, a, a^2\} \).

\[ b^2 = \begin{cases} 
  b^2 = e \\
  b^2 = a \\
  b^2 = a^2 
\end{cases} \]

Sup que \( \text{ord}(b) \neq 6 \implies \text{ord}(b) = 3 \implies e = b^3 = b^2b = a^k b \implies b = (a^k)^{-1} \in H \text{ Contradicción. Por tanto, } b^2 = e \)

2) Falta por determinar \( ba = ?? \)

\[ ba = \begin{cases} 
  ab \implies G \cong C_2 \times C_3 \cong C_6 \\
  a^2b \implies G \cong D_3 
\end{cases} \]

Proposición 3.3.2 Los únicos grupos de orden 8 salvo isomorfismo son \( C_8 \), \( D_4 \), \( C_4 \times C_2 \), \( C_2 \times C_2 \times C_2 \) y \( Q \).

Demostración

Sea \( G \) un grupo tal que \( |G| = 8 \). Por el Teorema de Lagrange, los posibles órdenes de sus elementos son 1, 2, 4 y 8.

1. \[ \exists a \in G \mid \text{ord}(a) = 8 \implies G \cong C_8 \]

2. \[ \exists a \in G \mid \text{ord}(a) = 8 \]

a) \[ \exists a \in G \mid \text{ord}(a) = 4 \implies \forall x \in G \ x^2 = e \implies G \cong C_2 \times C_2 \times C_2 \]

b) \[ \exists a \in G \mid \text{ord}(a) = 4 \]

Sea \( H = \langle e, a, a^2, a^3 \rangle \) Como \( |G : H| = 2 \implies \exists b \in G \setminus H \mid G = H \cup Hb \) con \( H \cap Hb = \emptyset \implies G = \langle e, b \rangle \) Para completar la tabla de multiplicación de \( G \), necesitamos saber cuánto es \( b^2 = ?? \) , \( ba = ?? \).

1) Si \( Hb^2 = Hb \implies b^2 = xb \implies x = b \in H \text{ Contradicción. Luego } Hb^2 = H \implies b^2 \in H = \{e, a, a^2, a^3\} \)

\[ b^2 = \begin{cases} 
  b^2 = e \\
  b^2 = a \quad b^2 = a^2 \\
  b^2 = a^3 
\end{cases} \]

a') Sup. que \( b^2 = a \; ; \; \text{ord}(a) = 4 \; ; \; \text{ord}(b) = 2 \). Falta por determinar \( ba = ?? \)

\[ ba = \begin{cases} 
  ab \implies G \text{ es abeliano } \implies G \cong C_4 \times C_2 \\
  a^3b \implies G \cong D_4 \\
  a^2b \implies G \cong ??? 
\end{cases} \]

Si \( ba = a^2b \implies a = ba^2b \; ; \; a^2 = ba^3b = b^2 = 3 \implies a^2 = e \text{ Contrad.} \]
\( b^2 = a \) ó \( b^2 = a^3 \) \( \Rightarrow \) \( \text{ord}(b) = 8 \)
\[ b^4 = a^2 = e \Rightarrow \text{ord}(b) > 4 \Rightarrow \text{ord}(b) = 8 \]

En ambos casos, \( G \cong C_8 \).
\( c' \) Sup. \( b^2 = a^2 \)
\[ b^4 = a^2 = e \Rightarrow \text{ord}(b) > 4 \Rightarrow \text{ord}(b) = 8 \]

\[ \downarrow \]

Proposición 3.3.3 Los únicos grupos de orden 10 salvo isomorfismo son \( C_{10} \) y \( D_5 \).

Demostración

Sea \( G \) un grupo tal que \( |G| = 10 \). Por el Tá de Lagrange, los posibles órdenes de sus elementos son 1, 2, 5 y 10.

1. \( \exists a \in G \mid \text{ord}(a) = 10 \Rightarrow G \cong C_{10} \)

2. \( \nexists a \in G \mid \text{ord}(a) = 10 \)

a) \( \exists a \in G \mid \text{ord}(a) = 2 \quad \forall x \in G \quad x^2 = e \Rightarrow |G| = 2^n \neq 10 \) Contradicción

b) \( \exists a \in G \mid \text{ord}(a) = 5 \)

Sea \( H = \langle a \rangle = \{e, a, a^2, a^3, a^4\} \) Como \( |G : H| = 2 \Rightarrow \exists b \in G \setminus H \mid G = H \cup Hb \cap Hb = \emptyset \Rightarrow G = \langle a, b \rangle = \{e, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\} \)

Para completar la tabla de multiplicación de \( G \), necesitamos saber cuanto es \( b^2 = ?? \) \( , ba = ?? \).

1) Si \( Hb^2 = Hb \Rightarrow b^2 = xb \Rightarrow x = b \in H \) Contrad. Luego \( Hb^2 = H \Rightarrow b^2 \in H = \{e, a, a^2, a^3, a^4\} \)

\[ b^2 = \begin{cases} 
  b^2 = e \\
  b^2 = a \\
  b^2 = a^2 \Rightarrow \text{Si } b^2 = a^k \quad k = 1, 2, 3, 4 \\
  b^2 = a^3 \\
  b^2 = a^4 
\end{cases} \]

Sup que \( \text{ord}(b) \neq 10 \Rightarrow \text{ord}(b) = 5 \quad e = b^5 = b^4b = a^2b \Rightarrow b = (a^2)^{-1} \in H \) Contradicción. Por tanto, \( b^2 = e \)

2) Falta por determinar \( ba = ?? \)

\[ ba = \begin{cases} 
  ab \Rightarrow G \cong C_2 \times C_5 \cong C_{10} \\
  a^4b \Rightarrow G \cong D_5 \\
  a^2b \Rightarrow \text{Vemos que lleva a una contrad.} \\
  a^3b \Rightarrow \text{Vemos que lleva a una contrad.} 
\end{cases} \]

Sup. \( ba = a^2b \Rightarrow a = ba^2b \Rightarrow a^3 = (ba^2b)^3 = ba^6b = bab = b(ba^2b)b = a^2 \Rightarrow a = e \) Contradicción.

De la misma forma obtenemos que \( ba = a^3b \) es una contradicción.
Proposición 3.3.4 Los únicos grupos de orden 14 salvo isomorfismo son $C_{14}$ y $D_7$.

Demostración

Sea $G$ un grupo tal que $|G| = 14$. Por el T de Lagrange, los posibles órdenes de sus elementos son 1, 2, 7 y 14.

1. $\exists \ a \in G \mid \text{ord}(a) = 14 \Rightarrow G \cong C_{14}$

2. $\not\exists \ a \in G \mid \text{ord}(a) = 14$

   a) $\exists \ a \in G \mid \text{ord}(a) = 2 \Rightarrow \forall x \in G \ x^2 = e = |G| = 2^a \neq 14$ Contradicción

   b) $\exists \ a \in G \mid \text{ord}(a) = 7$

   Sea $H = \langle a \rangle = \{e, a, a^2, a^3, a^4, a^5, a^6\}$. Como $|G : H| = 2 \Rightarrow \exists b \in G \setminus H$ y $G = H \cup Hb$ con $H \cap Hb = \emptyset \Rightarrow G = \langle a, b \rangle = \{e, a, a^2, a^3, a^4, a^5, a^6, b, ab, a^2b, a^3b, a^4b, a^5b, a^6b\}$. Para completar la tabla de multiplicación de $G$, necesitamos saber cuánto es $b^2 = ?$, $ba = ??$.

   1) Si $Hb^2 = Hb \Rightarrow b^2 = xb \Rightarrow x = b \in H$ Contrad. Luego $Hb^2 = H \Rightarrow b^2 \in H = \{e, a, a^2, a^3, a^4\}$

   $b^2 = \begin{cases} b^2 = e \\ b^2 = a \\ b^2 = a^2 \\ b^2 = a^3 \Rightarrow \text{Si } b^2 = a^k \ k = 1, 2, 3, 4, 5, 6 \\ b^2 = a^4 \\ b^2 = a^5 \\ b^2 = a^6 \\ b^2 = a^7 \\ b^2 = b^7 = b^6b = a^{3k}b \Rightarrow b = (a^{3k})^{-1} \in H$ Contradicción. Por tanto, $b^2 = e$.

   2) Falta por determinar $ba = ??$

   $ba = \begin{cases} ab \Rightarrow G \cong C_2 \ x \ C_7 \cong C_{14} \\ a^6b \Rightarrow G \cong D_7 \\ a^2b \Rightarrow \text{Veamos que lleva a una contrad.} \\ a^3b \Rightarrow \text{Veamos que lleva a una contrad.} \\ a^4b \Rightarrow \text{Veamos que lleva a una contrad.} \\ a^5b \Rightarrow \text{Veamos que lleva a una contrad.} \\ \end{cases}$

   $\sup ba = a^4b \Rightarrow a = ba^4b \Rightarrow a^2 = (ba^4b)^2 = ba^8b = bab = b(ba^4b)b = a^2 \Rightarrow a = e$ Contradicción.

Por un procedimiento análogo se demuestra que los otros llevan a una contradicción.

Ejercicio: Determinar los grupos abelianos cuyos órdenes sean un producto de potencias de exponentes de números primos.

Solución
Usaremos notación aditiva. Sea $G$ un grupo, $|G| = 24 = 2^3 * 3$. Sea $a = 8$ y $b = 3 \text{ m.c.d}(8,3) = 1$. Entonces $Z = 8Z + 3Z$. En particular, $1 = 8x + 3y = 8(2) + 3(-5)$

Se $a \in G$:

\[
\begin{cases}
G \text{ es abeliano} \\
|G| = 24
\end{cases}
\]

\[
a = (8 * 2) + (3 * 5)(-1)a = a_1 + a_2
\]

Entonces $3a_1 = 0$ (Teorema de Lagrange). De la misma forma, $8a_2 = 0$. Entonces $\text{ord}(a_2)$ divide a 8.

Sean $G(2) = \{a \in G \mid 2^3a = 0\}$; $G(3) = \{a \in G \mid 3a = 0\}$. Hemos visto que $G = G(2) + G(3)$. Por tanto, $G(2)$ y $G(3)$ son subgrupos de $G$. Sea $x \in G(2) \cap G(3)$. Entonces $\text{ord}(x) = 8$ y $\text{ord}(x) = 3$, es decir, $\text{ord}(x) = 1 \Leftrightarrow x = 0$. Luego $G = G(2) \oplus G(3)$

$|G(2)| \text{ divisor de 8 y } |G(3)| \text{ divisor de 3}$. Por tanto, $|G(2)| = 8$ y $|G(3)| = 3$, ya que sino fuera así el producto no sería 24.

**Pregunta:** ¿$H \times K \cong H \times L$ implica $K = L$? Veamos con un ejemplo que no:

Sean $Z_2 \times Z_2 = \{(0,0), (1,0), (0,1), (1,1)\}$

Sean $H = \{(0,0), (1,0)\} \cong Z_2$, $K = \{(0,0), (0,1)\} \cong Z_2$ y $L = \{(0,0), (1,1)\} \cong Z_2$.

Entonces $A = H \oplus K$ y $A = H \oplus L$, con $K \neq L$. 

25
3.4. Ejercicios

1 Encuentra la tabla de multiplicación de $D_4$, el grupo de simetrías de un cuadrado.

2 Di el orden y el inverso de los elementos de $D_4$

3

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 5 & 9 & 1 & 6 & 2 & 4 & 8 \end{pmatrix}$

$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 9 & 1 & 8 & 7 & 5 & 2 & 6 \end{pmatrix}$

Halla $\tau^{-1}, \tau\varphi, \varphi^{-1}\tau$ y expresar el resultado con notación cíclica.

4 Prueba que toda permutación puede ser escrita como producto de transposiciones, no necesariamente disjuntas

5

$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$

Halla la órbita de $\varphi$ en $x = 2$.

6 Dar otro ejemplo de grupos que verifiquen que $H \times K \cong H \times L$ y $K \neq L$

7 Determinar los grupos abelianos de orden 36

8 ¿Por qué $C_8 \not\cong C_4 \times C_2$?

9 Calcula el centro de $D_4$
Capítulo 4

Teoremas de Sylow

4.1. Producto Directo

Definición 4.1.1 Sea $G$ un grupo. Decimos que $G$ es un $p$-grupo si todo elemento de $G$ tiene orden potencia de un primo $p$.

Definición 4.1.2 Sea $G$ un grupo, $x \in G$. Llamamos centralizador de $x$, y lo denotamos por $\text{Cent}(x)$ al conjunto:

$$\text{Cent}(x) = \{g \in G \mid xg = gx\}$$

Ejercicio: Demostrar que $\forall x \in G; \text{Cent}(x) \triangleleft G$

Definición 4.1.3

1. Sea $H$ un subconjunto de un grupo $G$. El subconjunto $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$ es llamado el conjugado de $H$ por $g$ en $G$. Lo denotamos por $g^{-1}Hg = H^g$.

2. Si $H, K$ son subconjunto de un grupo $G$. Decimos que $K$ es conjugado por $H$ si existe un elemento $g$ de $G$ tal que $Hg = K$ o equivalente, si $K^g = H$.

Definición 4.1.4 Sean $G_1, G_2, \ldots, G_n$ grupos y sea $G = G_1 \times G_2 \times \ldots \times G_n$ el producto cartesiano de los conjuntos $G_i(1 \leq i \leq n)$. Se define el producto directo de los grupos $G_i(1 \leq i \leq n)$ con la operación $*$ tal que $(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)$, que se puede comprobar que es un grupo.

Teorema 4.1.5 El grupo $G$ contiene subgrupos $H_i(1 \leq i \leq n)$ tales que:

1. Para cada $i$, $H_i \cong G_i$.
2. Para cada $i$, $H_i \triangleleft G$.
3. $G = <H_1, H_2, \ldots, H_n>$
4. Para cada $i$, $H_i \cap <H_1, H_2, \ldots, H_{i-1}, H_{i+1}, \ldots, H_n> = <e>$

Demostración

Definimos $H_i = \{(e, e, \ldots, e, h_i, e, \ldots, e) \mid h_i \in G_i\}$ Es trivial comprobar que es un subgrupo.
1. La aplicación \((e,e,\ldots,h_i,e,\ldots,e)\) \(\mapsto h_i\) es claramente un isomorfismo. Luego \(H_i \cong G_i\).

2. La igualdad \((g_1,g_2,\ldots,g_i,\ldots,g_{i-1},g_n)^{-1}(e,e,\ldots,e,h_i,e,\ldots,e)(g_1,g_2,\ldots,g_i,\ldots,g_n)\)
   \(= (e,\ldots,e,g_i^{-1}h_ig_i,e,\ldots,e)\) muestra que \(H_i \triangleleft G\).

3. La igualdad \((g_1,g_2,\ldots,g_n) = (g_1,e,\ldots,e)(e,g_2,\ldots,e)(e,e,g_3,\ldots)(e,\ldots,g_n)\)
   muestra que \(G = \langle H_1,H_2,\ldots,H_n \rangle\).

4. Se deja como ejercicio.

**Notación:**

1. Cuando cada \(G_i\) de la definición sea abeliano y cuando usemos \(+\) para la operación binaria, entonces sustituiremos \(*\) por \(\oplus\). Por tanto, \(G\) será la suma directa de los \(G_i\) y \(G = G_1 \oplus G_2 \oplus \ldots \oplus G_n\).

2. En la primera definición, el grupo \(G\) fue formado mediante los grupos \(G_i\), que no eran subgrupos de \(G\), solo eran isomorfos a subgrupos \(H_i\) contenidos en \(G\). Por esta razón, \(G\) es también llamado el producto directo externo. Por el contrario, si \(G\) satisface las condiciones i),ii),iii) del **Teorema 4.1.5**, decimos que \(G\) es el producto directo interno de los \(H_i\).

**Teorema 4.1.6** Sea \(G_1,G_2\) dos grupos (no necesariamente abelianos) y sean \(N_1 \triangleleft G_1\) y \(N_2 \triangleleft G_2\). Entonces:

\[
\frac{G_1 \times G_2}{N_1 \times N_2} \cong \frac{G_1}{N_1} \times \frac{G_2}{N_2}
\]

**Demostración**

Sea la aplicación:

\[
\varphi : G_1 \times G_2 \to \frac{G_1}{N_1} \times \frac{G_2}{N_2}
\]

\[(a_1,a_2) \mapsto (a_1N_1,a_2N_2)\]

Esta aplicación es un epimorfismo con \(\ker(\varphi) = N_1 \times N_2\). Por el 1° Teorema de Isomorfía, obtenemos que \(\frac{G_1 \times G_2}{N_1 \times N_2} \cong \frac{G_1}{N_1} \times \frac{G_2}{N_2}\).

**4.2. Producto Semidirecto**

**Proposición 4.2.1** Sean \(H\) y \(K\) dos grupos cualesquiera. Sea la aplicación:

\[
\phi : K \to \text{Aut}(H)
\]

\(k \mapsto \phi_k(h) = h^k = khk^{-1}\)

es un homomorfismo de grupos. Entonces \(H \rtimes_{\phi} K = (H \times K, \phi)\) es un grupo.

**Demostración**

En primer lugar, demostraremos que la aplicación es un homomorfismo. y después comprobaremos los axiomas de grupo.

\[
\phi_k(ab) = (ab)^k = kabhk^{-1} = (kak^{-1})(bkh^{-1}) = \phi_k(a)\phi_k(b).
\]

Por tanto, es un homomorfismo. Comprobemos ahora que \((H \times K, \phi)\) tiene estructura de grupo.
Por tanto, Sean K, L y H grupos. Sean las aplicaciones: Teorema 4.2.1

definido por \( \theta \). Entonces existe un homomorfismo \( \theta \).

Veamos que:

La clave de la demostración es la siguiente:

\[ h^k = \phi_k(h) = \varphi_{\Theta k}(h) = h^{\Theta k} \]

Veamos que: \( \theta((h_1, k_1) \cdot (h_2, k_2)) = \theta(h_1^{\Theta k_1}, k_1 k_2) = (h_1 h^{\Theta k_1}, (k_1 k_2)) = (h_1 h_2^{\Theta k_1}, (\Theta(k_1))(\Theta(k_2))) = (h_1, \Theta(k_1)) \cdot (h_2, \Theta(k_2)) = \theta(h_1, k_1) \cdot \theta(h_2, k_2) \)

### 4.3. Acciones sobre Grupos

Definición 4.3.1 Sea G un grupo y sea X un conjunto. Se define la acción de G en X como una aplicación * : G × X → X tal que:

1. * (e, x) = x \ \forall x ∈ X, con e ∈ G el elemento neutro de G.
2. * (g_1 g_2, x) = * (g_1, * (g_2, x)) \ ∀ x ∈ X, g_1, g_2 ∈ G.
Nota: Normalmente, la acción de G sobre X se denotará por yuxtaposición.

Consecuencias

Sea G x X → X una acción de G sobre X. Consideremos la aplicación:

$$
\varphi : G \rightarrow \text{Bij}(X)
$$

$$
a \mapsto \varphi_a : X \rightarrow X
$$

$$
x \mapsto ax
$$

¿Es \(\varphi_a : X \rightarrow X\) biyectiva? Podemos comprobar que \(\forall a \in G\) la aplicación

$$
\varphi_a : X \rightarrow X
$$

$$
x \mapsto ax
$$

Posee inversa

$$
\varphi_{a^{-1}} : X \rightarrow X
$$

$$
x \mapsto a^{-1}x
$$

Luego es biyectiva.

Ejemplos

1. Sea G un grupo y consideremos X = G como conjunto.

$$
G \times G \rightarrow G
$$

$$
(a, x) \mapsto ax
$$

2. Sea G un grupo y consideremos X = G como conjunto.

$$
G \times G \rightarrow G
$$

$$
(a, x) \mapsto axa^{-1}
$$

3. Sea G un grupo y sea H ≤ G. Consideremos el conjunto: X = aHa^{-1} y la aplicación:

$$
G \times X \rightarrow X
$$

$$
(a, T) \mapsto aTa^{-1}
$$

Definición 4.3.2 Dado \(x \in X\). Se define la órbita de X (respecto de la acción dada) como el conjunto:

$$
\text{Orb}(x) = G \ast x = \{ax \mid a \in G\}
$$

Definición 4.3.3 Se define el estabilizador de un elemento \(x \in X\), y se denota por \(\text{Est}(x)\), como el conjunto:

$$
\text{Est}(x) = \{a \in G \mid ax = x\}
$$

Ejercicio: \(\text{Est}(x) \leq G\)

Proposición 4.3.4 Se la acción de G sobre X y sea \(x \in X\). Entonces:
Demostración

Sea la aplicación:

\[ G \rightarrow \text{Orb}(x) \]
\[ a \mapsto ax \]
\[ ax = bx \iff a^{-1}bx = a \iff a^{-1}b \in \text{Est}(x) \iff a\text{Est}(x) = b\text{Est}(x) \]

Luego el \( n \) de clases es el \( n \) de elementos de la órbita.

### 4.4. Teoremas de Sylow

#### Primer Teorema de Sylow 4.4.1

Sea \( G \) un grupo de orden \( p^\alpha s \), donde \( p \) es primo y no divide a \( s \), \( \alpha \geq 1 \). Entonces para cada \( \beta, 0 \leq \beta \leq \alpha \), \( G \) contiene un subgrupo de orden \( p^\beta \).

**Demostración**

1. Consideremos el caso en que \( G \) sea un grupo cíclico.

   \[ |G| = p^\alpha s, \text{ si } 0 \leq \beta \leq \alpha \Rightarrow p^\beta \text{ divide a } |G| \Rightarrow \exists S \leq G \text{ tal que } |S| = p^\beta \]

2. Supongamos que \( G \) no es un grupo abeliano finito. Demostraremos el resultado por inducción sobre el orden de \( G \). Por la ecuación de clases:

   \[ |G| = |Z(G)| + \sum_{k=1}^{l} |C_k| + \sum_{j=l+1}^{r} |C_j| = 1; |C_j| > 1 \]

   a) Supongamos que \( \exists \ l + 1 \leq j \leq r \mid p \text{ no divide a } |C_j| \).

   \[ |C_i| = |G : \text{Cent}(g)| = \frac{|G|}{|\text{Cent}(g)|} = p^\alpha s \iff p^\alpha \text{ divide a } |\text{Cent}(g)| \]

   donde \( C_i \) es la clase de conjugación de un cierto elemento \( g \).

   \[ |\text{Cent}(g)| = p^\alpha t, \text{ donde } t \text{ es un cierto divisor de } s. \text{ Sabemos que } |\text{Cent}(g)| < |G|, \text{ ya que } G \text{ no es abeliano.} \]

   Si \( |\text{Cent}(g)| = |G| \iff g \in Z(G) \iff C_i = \{g\}, \text{ y } |C_i| = 1. \text{ Por tanto, } |\text{Cent}(g)| = p^\alpha t \text{ donde } t < s. \text{ Ahora podemos utilizar la hipótesis de inducción, y por tanto:} \]

   \[ |\text{Cent}(g)| < |G| \Rightarrow \text{Cent}(g) \text{ contiene un subgrupo de orden } p^\alpha. \]

   b) Supongamos que \( p \text{ divide a } |C_j| \forall j \in \{l + 1, l + 2, ..., r\} \)

   **Por la ecuación de clases,**

   \[ |G| = |Z(G)| + \sum_{k=1}^{r} |C_k| = \sum_{k=1}^{l} |C_k| + \sum_{j=l+1}^{r} |C_j| \iff p \text{ divide a } |Z(G)| \]

31
Hemos visto antes que $Z(G)$ contiene un subgrupo de orden $p$. Sea $Y$ este subgrupo de orden $p$, $Y \leq Z(G) \Rightarrow Y \triangleleft G$. Como $Y \in Z(G)$, entonces $gYg^{-1} = Y$. Consideramos el grupo cociente $G/Y$. Para considerar el cociente, hay que ver que $Y$ es un subgrupo normal y que su orden es menor que el de $G$.

$$|G/Y| = [G : Y] = \frac{|G|}{|Y|} = \frac{p^\alpha s}{p} = p^{\alpha-1}s$$

**Definición 4.4.2** Sea $S \leq G \ | S | = p^\alpha \ S$ se llama $p$-subgrupo de Sylow.

Si llamamos $n_p$ al número de $p$-subgrupos de Sylow de $G$, entonces se cumple que:

1. $n_p$ es un divisor de $s$
2. $n_p \equiv 1 \ (\text{mod} \ p)$

**Definición 4.4.3** Sea $G$ un grupo y sean $X \subseteq G, Y \subseteq G$. Diremos que $Y$ es un conjugado de $X$ si $\exists \ a \in G \ | \ Y = aXa^{-1} = X^a$.

**Ejercicio:** Comprobar que la relación es de equivalencia.

**Lema 4.4.4** Sea $|G| = p^\alpha s$. Sea $P$ un $p$-subgrupo de Sylow de $G$. Sea $a \in G$ tal que

1. $\text{ord}(a) = p^\beta$ $\beta \leq \alpha$
2. $P^a = P$

Entonces $a \in P$.

**Demostración**

$aPa^{-1} = P \iff a \in \text{Nor}(P) \triangleright P$. Sea la aplicación:

$$\pi : \text{Nor}(P) \longrightarrow \text{Nor}(P)/P$$

$$\bar{b} \longmapsto \bar{b}$$

$$\bar{a} \in \frac{\text{Nor}(P)}{P} \iff \text{ord}(\bar{a}) = p^\lambda \ \lambda \leq \beta$$

$$\pi^{-1}(\bar{a}) \leq \text{Nor}(P) \ \ P \subseteq \pi^{-1}(\bar{a}) \leq \text{Nor}(P) \Longrightarrow a \in P$$

**Segundo Teorema de Sylow 4.4.5** Sea $G$ un grupo finito, $|G| = p^\alpha s$ donde $p$ es primo, $\alpha \geq 1$ y $p$ no divide a $s$. Sea $P$ $p$-subgrupo de Sylow de $G \ Leftrightarrow |P| = p^\alpha$.

Entonces todo $p$-subgrupo $Q$ de Sylow de $G$ es conjugado con $P$. $Q = P^a = aPa^{-1}$ para algún $a \in G$.

**Demostración**

Sea $P$ un $p$-subgrupo de Sylow y sea $K = \{P = P_0, P_1, ..., P_r\}$ que denota el conjunto de todos los conjugados distintos de $P$ en $G$. Claramente cada uno es un $p$-subgrupo de Sylow. Podemos decir que la relación $P_i \sim P_j \ Leftrightarrow P_i^a = P_j$ para algún $a \in P$. Sea $\{P\}$ su clase de equivalencia. Entonces el número de conjugados de $P$ es $|P : P \triangleleft N_G(P_0)|$ que es potencia de $p$. Podemos ver que el número de conjugados $P_1, ..., P_r$ se dividen en clases cada una un múltiplo de $p$ elementos. Por tanto, el número de conjugados de $P$ en $G$ es de la forma $1 + mp$.  

32
Supongamos por reducción al absurdo, que existe \( Q \) p-subgrupo de Sylow que no es conjugado a \( P \). Entonces \( |X| = rp \) y por tanto, \( 1 + mp = rp \). Lo cual, es una contradicción, ya que \( 1 = rp - mp = p(r-m) \) y \( r - m \neq 0 \) y \( p \) no divide a \( 1 \).

Proposición 4.4.6 Sea \( G \) un grupo y sea \( P \) un p-subgrupo de Sylow. Si \( n_p = 1 \), entonces \( P \triangleleft G \).

Demostración

Si \( n_p = 1 \), entonces existe un único conjugado con \( P \), y como \( P \) es un conjugado consigo mismo, entonces \( P \) es un subgrupo normal de \( G \).

Ejemplo: Un grupo \( G \) tal que \( |G| = 42 \) no es simple. \( 42 = 7 \cdot 3 \cdot 2 \)

1. \( p = 7 \) \( 42 = 7 \cdot 6 \) \( \text{m.c.d}(7,6) = 1 \)
2. \( p = 3 \) \( 42 = 3 \cdot 14 \) \( \text{m.c.d}(3,14) = 1 \)
3. \( p = 2 \) \( 42 = 21 \cdot 2 \) \( \text{m.c.d}(21,2) = 1 \)

Por el 1\(^{\circ} \) Teorema de Sylow, sabemos que hay al menos un subgrupo de orden 7, otro de orden 3 y otro de orden 2. Si consideramos \( p = 7 \) ¿Cuántos 7-subgrupos de Sylow puede poseer \( G \)?

\( n_7 \) es un divisor de 6
\( n_7 \equiv 1 \pmod{7} \)

Por tanto, \( n_7 = 1 \) y \( G \) no es simple. Podríamos haber hecho el mismo razonamiento con \( p = 2 \) ó \( p = 3 \) y haber comprobado si hay algún p-subgrupo.

Ejemplo: Un grupo \( G \) tal que \( |G| = 56 \) no es simple. \( 56 = 2^3 \cdot 7 \)

1. \( p = 7 \) \( 56 = 8 \cdot 7 \) \( \text{m.c.d}(8,7) = 1 \)
2. \( p = 2 \) \( 56 = 28 \cdot 2 \) \( \text{m.c.d}(28,2) = 2 \) Por el 1\(^{\circ} \) Teorema de Sylow, sabemos que hay al menos un subgrupo de orden 7 y otro de orden 2. Consideremos \( p = 7 \)

\( n_7 \) es un divisor de 8
\( n_7 \equiv 1 \pmod{7} \)

Luego, \( n_7 = 1 \) y \( G \) no es simple.

4.5. Aplicación del Teorema de Sylow. Apéndice

Proposición 4.5.1 Sea \( G \) un grupo de orden \( |G| = p^\alpha s \), donde \( p \) es primo y no divide a \( s \). Sea \( H \) un subgrupo de \( G \) tal que \( |H| = p^\beta \) donde \( \beta \leq \alpha \). Entonces \( H \) está contenido en un p-subgrupo de Sylow de \( G \).

Demostración

Sea \( X = \{ P \leq G \mid P \) es un p-subgrupo de Sylow de \( G \} \). Hemos probado que \( |X| \equiv 1 \pmod{p} \) y \( |X| \mid s \). Consideremos la acción del grupo \( H \) sobre \( H \) (por conjugación)
\[ HxX \rightarrow X \]
\[ (h,p) \mapsto hPh^{-1}, \quad h \in H. \]
\[ X = C_1 \cup C_2 \cup \ldots \cup C_m \] donde \( \{C_i\} \) son las distintas clases de conjugación del \( p \)-subgrupo \( P_i \) de Sylow.

\[ |C_i| = [H; \text{Est}(P_i)] = p^{n_i} \] donde \( \alpha_i \geq 0 \). \( \exists\) Cuándo \( |C_i| = 1 \? \iff \text{Est}(P_i) = H \? \] Sea \( p_i \in C_i = \{p_i^h \mid h \in H\} \). Entonces \( |C_i| = 1 \iff C_i = \{p_i\} \iff p_i^h = p_i \forall h \in H \Rightarrow h \in P_i \Rightarrow H \subseteq P_i \).

Sup, por reducción al absurdo, \( |C_j| > 1 \forall j = 1, 2, \ldots m \)
\[ \nmid p \mid |C_j| \forall j = 1, 2, \ldots m \implies p \mid |X|. \]

Y por tanto, una contradicción, ya que \( X \equiv 1 \pmod p \).

**Teorema 4.5.2** Cualquier grupo de orden 12 es isomorfo a:
\[
\mathbb{Z}_{12}, (\mathbb{Z}_2)^2 \times \mathbb{Z}_3, A_4, D_6 \text{ o el producto semidirecto no trivial } \mathbb{Z}_3 \rtimes \mathbb{Z}_4
\]

**Demostración**

Sea \( |G| = 12 = 2^2 \times 3 \) Aplicando el \( T^* \) de Sylow, obtenemos que:

\[ n_2 \mid 3 \text{ y } n_2 \equiv 1 \pmod 2 \quad n_3 \mid 4 \text{ y } n_3 \equiv 1 \pmod 3. \]

Queremos que \( n_2 = 1 \) ó \( n_3 = 1 \). Supongamos que \( n_3 \neq 1 \), entonces \( n_3 = 4 \). Un 3-subgrupo de Sylow tiene orden 3, luego hay dos 3-subgrupos diferentes con intersección el elemento neutro. Cada uno de los cuatro 3-subgrupos de Sylow tiene dos elementos de orden 3 que no está en ningún otro 3-subgrupo de Sylow. Lo cual, el número de elementos de \( G \) de orden 3 son \( 8 \) (2+4 = 8). Por tanto, hay 4 elementos de \( G \) que no tienen orden 3.

El 2-subgrupo de Sylow tiene orden 4 y no contiene elementos de orden 3, y por tanto, sólo existe un único 2-subgrupo de Sylow, es decir, \( n_2 = 1 \) si \( n_3 \neq 1 \).

Sea \( P \) un 2-subgrupo de Sylow y \( Q \) un 3-subgrupo de Sylow de \( G \), entonces \( P \circ Q \) es normal en \( G = PQ \) (si \( P \cap Q = \{e\} \) y tienen "tamaños apropiados"). Entonces \( P \cong \mathbb{Z}_4 \circ \mathbb{Z}_4 \cong (\mathbb{Z}_2)^2 \) y \( Q \cong \mathbb{Z}_3 \) por tanto, \( G \) es alguno de los siguientes productos semidirectos:

\[
\mathbb{Z}_4 \rtimes \mathbb{Z}_3, \quad (\mathbb{Z}_2)^2 \rtimes \mathbb{Z}_3, \quad \mathbb{Z}_3 \rtimes \mathbb{Z}_4, \quad \mathbb{Z}_3 \rtimes (\mathbb{Z}_2)^2
\]

Ya que los subgrupos de Sylow son abelianos, el producto semidirecto es abeliano. Determinaremos todos los productos semidirectos, salvo isomorfismo, calculando todas las posibles formas de actuar \( \mathbb{Z}_4 \) y \( (\mathbb{Z}_2)^2 \) bajo un automorfismo en \( \mathbb{Z}_3 \) y todas las posibles formas de actuar \( \mathbb{Z}_3 \) bajo un automorfismo sobre \( \mathbb{Z}_4 \) y \( (\mathbb{Z}_2)^2 \).

En primer lugar, necesitamos conocer el automorfismo de grupos de los siguientes grupos:

\[
\text{Aut}(\mathbb{Z}_4) \cong (\mathbb{Z}_4)^{\times}, \quad \text{Aut}((\mathbb{Z}_2)^2) \cong GL_2(\mathbb{Z}_2), \quad \text{Aut}(\mathbb{Z}_3) \cong (\mathbb{Z}_3)^{\times}
\]

Separaremos los casos dependiendo de si \( n_2 = 1 \) ó \( n_3 = 1 \). En primer lugar, supondremos \( n_2 = 1 \). Entonces el 2-subgrupo de Sylow es normal y el 3-subgrupo de Sylow actuando sobre él. Consideremos en primer lugar,

\[
\mathbb{Z}_4 \rtimes \mathbb{Z}_3, \quad (\mathbb{Z}_2)^2 \rtimes \mathbb{Z}_3
\]
En el primer producto semidirecto, el homomorfismo \( \mathbb{Z}_3 \rightarrow (\mathbb{Z}_4)^2 \) es trivial, ya que el dominio tiene orden 3 y el codomino tiene orden 2, luego el primer producto semidirecto tiene que ser el trivial: el producto directo de \( \mathbb{Z}_4 \times \mathbb{Z}_3 \) es cíclico de orden 12 (está generado por \((1,1)\).

En el segundo producto semidirecto, queremos saber todos los homomorfismos de \( \mathbb{Z}_3 \rightarrow GL_2(\mathbb{Z}_2) \). El homomorfismo trivial nos lleva al producto directo \((\mathbb{Z}_2)^2 \times \mathbb{Z}_3\). ¿Qué sabemos del homomorfismo trivial \( \mathbb{Z}_3 \rightarrow GL_2(\mathbb{Z}_2) \)? Dentro de \( GL_2(\mathbb{Z}_2) \) hay un subgrupo de orden 3:

\[
\left\{ \left( \begin{array}{cc} 1 & 0 \\
0 & 1 \\
1 & 1 \\
1 & 0 \end{array} \right) , \left( \begin{array}{cc} 0 & 1 \\
1 & 1 \\
1 & 0 \end{array} \right) \right\}
\]

Un homomorfismo no trivial \( \varphi : \mathbb{Z}_3 \rightarrow GL_2(\mathbb{Z}_2) \) está determinado mandando 1 mod 3 a una de las dos matrices \( A \) de orden 3. Las dos matrices de orden 3 en \( GL_2(\mathbb{Z}_2) \) son inversas una de otra, y la precomposición uno de estos homomorfismos \( \mathbb{Z}_3 \rightarrow GL_2(\mathbb{Z}_2) \) con la negación en \( \mathbb{Z}_3 \) se convierte en el otro homomorfismo, ya que convierte el valor en 1 mod 3 en el inverso de lo que era en un principio. Sin embargo, los dos homomorfismos no triviales \( \mathbb{Z}_3 \rightarrow GL_2(\mathbb{Z}_2) \) son la misma formación que un automorfismo de \( \mathbb{Z}_3 \) y en consecuencia, es isomórfico al producto semidirecto. Por lo que hay un isomorfismo con el producto semidirecto no trivial \((\mathbb{Z}_2)^2 \times \mathbb{Z}_3\), además de el producto trivial \((\mathbb{Z}_2)^2 \times \mathbb{Z}_3\).

Concretamente, el producto semidirecto no trivial \((\mathbb{Z}_2)^2 \times \mathbb{Z}_3\) es isomórfico a \( A_4 \), ya que mostramos que solo hay un grupo no abeliano de orden 12 con \( n_2 = 1 \) y \( A_4 \) se ajusta a esto,

Ahora, haremos el caso de \( n_2 \neq 1 \). Por lo tanto \( n_3 = 3 \) y \( n_3 = 1 \). Encontraremos dos grupos isomórficos, ambos no abelianos. Nuestro grupo es el producto semidirecto:

\[\mathbb{Z}_3 \rtimes \mathbb{Z}_4, \quad \mathbb{Z}_3 \rtimes (\mathbb{Z}_2)^2\]

Ya que \( n_2 = 1 \), el grupo no es abeliano, luego el producto semidirecto tampoco es abeliano. Buscamos homomorfismos no triviales \( \mathbb{Z}_4 \rightarrow Aut(\mathbb{Z}_3) = (\mathbb{Z}_3)^\times \) y \((\mathbb{Z}_2)^2 \rightarrow (\mathbb{Z}_3)^\times\). Hay solo un homomorfismo no trivial \( \mathbb{Z}_4 \rightarrow (\mathbb{Z}_3)^\times \) (1 mod 4 tiene que ir a -1 mod 3, y todos los elementos quedan determinados), que de hecho es c mod 4 → \((-1)^c\), por lo que tenemos un producto semidirecto no trivial \( \mathbb{Z}_3 \times \mathbb{Z}_4 \). Explicitamente, la operación del grupo es \((a,b)(c,d) = (a+(-1)^b c, b+d)\).

Tenemos 3 homomorfismos no triviales de \((\mathbb{Z}_2)^2 \rightarrow (\mathbb{Z}_3)^\times\), \((\mathbb{Z}_2)^2 \) tiene dos generadores, \((1,0)\) y \((0,1)\) y un homomorfismo no trivial \((\mathbb{Z}_2)^2 \rightarrow (\mathbb{Z}_3)^\times\) que manda los generadores a \pm 1, sin manda ambos a 1. Usando las matrices de orden 2 × 2 sobre \( \mathbb{Z}_2 \) para mover vectores no nulos en \((\mathbb{Z}_2)^2\), el tercer homomorfismo no trivial \((\mathbb{Z}_2)^2 \rightarrow (\mathbb{Z}_3)^\times\) puede ser transformado entre si bajo la composición de una de ellos con un automorfismo de \((\mathbb{Z}_2)^2\). Sin embargo, el tres productos semidirecto no trivial \( \mathbb{Z}_3 \rtimes (\mathbb{Z}_2)^2 \) son isomorfos, de esta manera todos los grupos no abelianos de orden 12 con \( n_3 = 1 \) y 2-subgrupos de Sylow isomorfos sobre \((\mathbb{Z}_2)^2\) son isomorfos. Concretamente, uno de estos grupos es \( D_6 \).

Si nos encontramos con un grupo de orden 12, podemos decidir cual de los 5 grupos es isomórfico diciendo si es abeliano o no, y en el caso de que no sea abeliano, si el 2-subgrupo de Sylow es normal (en este caso es isomorfo a \( A_4 \) o si el 3-subgrupo de Sylow es normal junto con 2-subgrupo de Sylow que son cíclicos o no son cíclicos (producto semidirecto no trivial \( \mathbb{Z}_3 \rtimes \mathbb{Z}_4 \) en el primer caso, \( D_6 \) en el segundo caso).
Otra manera de distinguir los tres grupos no abelianos de orden 12 es contando el número de elementos de orden 2: $D_6$ tiene 7 elementos de orden 2, $A_4$ tiene 3 elementos de orden 2 y $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ tiene un elemento de orden 2.

4.6. Ejercicios

1 Demostrar que si $|G| = 48$, entonces $G$ no es simple.

2 Demostrar que $\forall x \in G; \text{Cent}(x) \triangleleft G$.

3 Demostrar que $\text{Est}(x) \leq G$.

4 Sea $G$ un grupo y sean $X \subseteq G, Y \subseteq G$. Diremos que $Y$ es un conjugado de $X$ si $\exists a \in G \mid Y = aXa^{-1}$. Comprobar que la relación es de equivalencia.
Bibliografía

[1] **Antonio Fernández, Apuntes de clase**


[5] **Keith Conrad, Groups or order 12**