Universidad de Granada

Álgebra II

Pedro Ramos Suárez

Doble Grado de Ingeniería Informática y Matemáticas

14 de junio de 2021

Índice

1. Combinatoria y teoría elemental de grafos

2. Grupos: definición y ejemplos

Definición

Un grupo G es un conjunto no vacío junto con una operación interna $\cdot : G \times G \to G$ satisfaciendo:

① Propiedad asociativa:

$$(ab)c = a(bc) \ \ \forall a, b, c \in G$$

Muchas veces escribiremos $abc := (ab)c = a(bc)$.

② Existencia de elemento neutro 1:

$$1a = a1 = a \ \ \forall a \in G$$

③ Existencia de inversos:

$$\forall a \in G \ \ \exists a^{-1} \in G \text{ tal que } aa^{1} = 1$$

Si además verifica la propiedad conmutativa ($ab = ba \ \ \forall a, b \in G$) entonces el grupo es abeliano o conmutativo.

Proposición

Sea G un grupo. Entonces:

① En G hay un único elemento neutro: la unidad o el uno de G.

② Cada elemento tiene un único inverso.

③ Para cada $a \in G$, $(a^{-1})^{-1} = a$.

④ Para cualesquiera $a, b \in G$, las ecuaciones $ax = b$ y $ya = b$ tienen solución y además es única: $x = a^{-1}b$ y $y = ba^{-1}$.

⑤ Si a es un elemento tal que $aa = 1$, entonces $a = 1$.

⑥ Sea $n \geq 1$ y $a_1, ..., a_n$. Definimos:

$$\prod_{i=1}^{1} a_i = a_1$$

$$\prod_{i=1}^{n} a_i = a_n \prod_{i=1}^{n-1} a_i$$

Demostración

① Supongamos que existe otro elemento neutro $e \in G$. Entonces $1 = 1e = e$.

② Supongamos que para $a \in G$ existe otro inverso, $a' \in G$. Entonces $a' = a'1 = a'aa^{-1} = 1a^{-1} = a^{-1}$.

Proposición: Propiedad asociativa generalizada

Sean $a \in G$ grupo y $n \geq 2$, entonces para cada m con $1 \leq m < n$ tenemos:

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{m} a_i \prod_{i=m+1}^{n} a_i$$

Demostración

El caso inicial es la propiedad asociativa. El caso general se demuestra por inducción.

Proposición

Sea $a \in G$ grupo. Para $n \geq 1$, tenemos que:

$$(\prod_{i=1}^{n} a_i)^{-1} = \prod_{i=1}^{n} a_{n+i-1}^{-1}$$

Demostración

Por inducción. El caso inicial es trivial. Veamos el caso $n+1$:

$$(\prod_{i=1}^{n+1} a_i)(\prod_{i=1}^{n+1} a_{n+2-i}^{-1}) = (\prod_{i=1}^{n} a_i \cdot a_{n+1})(a_{n+1}^{-1} \prod_{i=2}^{n+1} a_{n+2-i}) = \prod_{i=1}^{n} a_i \prod_{i=1}^{n} a_{n+1-i} = 1$$

Definición

Sea $a \in G$ grupo. Definimos las potencias como:

$$a^n = \prod_{i=1}^{n} a$$

Proposición

Sea G un grupo. Se verifican las siguientes propiedades de las potencias:

① Sean $a \in G$ y $r, s > 0$. Se verifica:

$$a^r a^s = a^{r+s}$$

② Para todo $a \in G$ y todo $n \geq 1$ se verifica:

$$(a^n)^{-1} = (a^{-1})^n$$

Para cada $n \geq 1$ definimos $a^{-n} := (a^n)^{-1} = (a_{-1})^n)$.

③ Para todo $a \in G$ y cualesquiera $r, s \in \mathbb{Z}$ se cumple:

$$a^r a^s = a^{r+s}$$

$$(a^r)^s = a^{rs}$$

Demostración

③ Comencemos con $a^r a^s = a^{r+s}$.

- $r = 0$ ó $s = 0$. Caso obvio.
- $r, s > 0$. Estamos en ①.
- Si $r, s < 0$:

$$a^{-r}a^{-s} = (a^{-1})^r(a^{-1})^s = (a^{-1})^{r+s} = a^{-r-s}$$

- Si $r > 0, s < 0$.
  - Para $r \geq s \Rightarrow r - s \geq 0$:

$$a^r a^{-s} = (a^{r-s}a^s)a^{-s} = a^{r-s}a^s a^{-s} = a^{r-s}$$

  - Para $r \leq s \Rightarrow r - s \leq 0$:

$$a^r a^{-s} = (a^{-(r-s)}a^s)a^{-s} = a^{-(r-s)}a^s a^{-s} = a^{-(r-s)}$$

- Si $r < 0, s > 0$. Análogo al caso anterior.

Por lo que $a^r a^s = a^{r+s}$.

Veamos ahora $(a^r)^s = a^{rs}$. Para $r \in \mathbb{Z}$:

- $s \geq 1$:

$$(a^r)^s = a^r a^r ...^{s-veces}...a^r = a^{r+...^{s-veces}...+r} = a^{rs}$$

- $s = 0$:

$$(a^r)^s = (a^r)^0 = 1 = a^{r0} = a^{rs}$$

- $s < 0$

$$(a^r)^{-s} = [(a^r)^s]^{-1} = (a^{rs})^{-1} = a^{-rs} = a^{r(-s)}$$

Nota

Hay que tener en cuenta que estamos usando notación multiplicativa. En notación aditiva $\prod$ pasa a ser $\sum$. Por ejemplo, si $n \geq 1$, a^n pasa a ser (na) y si $n = 0$ tendríamos $(0a = 0)$.

Proposición

Sea G un conjunto, $G \neq \emptyset$, y $\cdot : G \times G \to G, (a, b) \to ab$ operación interna tal que:

① $(ab)c = a(bc) \;\; \forall a, b, c \in G$.

② $\exists 1 \in G$ tal que $a1 = a \;\; \forall a \in G$.

③ Para cada $a \in G, \;\; \exists a^{-1} \in G$ tal que $aa^{-1} = 1$.

Entonces G es un grupo.

Demostración

Tenemos que demostrar que $1a = a$ y $a^{-1}a = 1$.

$$1a =_{(3)} (aa^{-1})a =_{(1)} a(a^{-1}a) = a1 =_{(2)} a$$

2.1. Anillos

Un anillo es una terna $(A, +, \cdot)$ tal que $(A, +)$ es un grupo abeliano y con respecto al producto se verifica:

- $(ab)c = a(bc) \;\; \forall a, b, c \in A$.
- $\exists 1 \in A$ tal que $a1 = a = 1a$.
- Distributiva: $a(b + c) = ab + ac \;\; \forall a, b, c \in A$.

$(A, +, \cdot)$ es conmutativo si $ab = ba \;\; \forall a, b \in A$.

Definición

$u \in A$ se dice unidad si $\exists u^{-1} \in A$ tal que $uu^{-1} = 1 = u^{-1}u$.

Proposición

Si A es un anillo:

- $(A, +)$ es un grupo abeliano.
- $(A^{\times}, \cdot)$ es un grupo, donde $A^{\times} = \mathcal{U}(A) = \{u \in A | u \text{ es unidad}\}$.

Ejemplos

-

$$\mathbb{Z} \to \begin{cases} (\mathbb{Z}, +) \text{ es un grupo abeliano.} \\ \mathbb{Z}^{\times} = \{1, -1\} \text{ es un grupo abeliano con el producto.} \end{cases}$$

- $$\mathbb{Q} \to \begin{cases} (\mathbb{Q}, +) \text{ es un grupo abeliano.} \\ \mathbb{Q}^\times = \mathbb{Q} - \{0\} \text{ es un grupo abeliano con el producto.} \end{cases}$$

- $$\mathbb{R} \to \begin{cases} (\mathbb{R}, +) \text{ es un grupo abeliano.} \\ \mathbb{R}^\times = \mathbb{R} - \{0\} \text{ es un grupo abeliano con el producto.} \end{cases}$$

- $$\mathbb{C} \to \begin{cases} (\mathbb{C}, +) \text{ es un grupo abeliano.} \\ \mathbb{C}^\times = \mathbb{C} - \{0\} \text{ es un grupo abeliano con el producto.} \end{cases}$$

  $z = a + bi \neq 0 \iff a \neq 0$ ó $b \neq 0 \iff r = |z| = \sqrt{a^2 + b^2} \neq 0, \;\; a, b \in \mathbb{R}$.
  $z = r(cos\theta + isen\theta)$ representación módulo-argumento de z.
  θ (argumento) es el ángulo determinado $cos\theta = \frac{a}{\sqrt{a^2+b^2}}$ y $sen\theta = \frac{b}{\sqrt{a^2+b^2}}$.
  $z' = r'(cos\theta' + isen\theta') \Rightarrow zz' = rr'(cos(\theta + \theta') + isen(\theta + \theta'))$
  $z^{-1} = \frac{1}{z} = \frac{1}{r}(cos\theta + isen\theta)$.

Anillo de matrices cuadradas

Sean K un cuerpo y $n \geq 2$. $\mathcal{M}_n(K)$ es el anillo de matrices cuadradas de orden n con entradas en K.

Nos da lugar a dos grupos:

- $(\mathcal{M}_n(K), +)$ abeliano.
- $GL_n(K) := \mathcal{M}_n(K)^\times = \{B \in \mathcal{M}_n(K) : B \text{ es regular}\} =$
  $= \{B \in \mathcal{M}_n(K) : det(B) \neq 0\}$ es un grupo en general no abeliano.

Si K es un cuerpo finito, entonces $GL_n(K)$ es también finito.

Definición

Si G es un grupo con un número finito de elementos, al cardinal de G lo llamaremos orden de G y lo denotaremos por $|G|$.

Tabla de Cayley

$G = \{1, x_1, ..., x_r\}$.

$\cdot$	1	x_1	x_2	$...$	x_r
1	1	x_1	x_2	$...$	x_r
x_1	x_1	x_1^2	x_1x_2	$...$	x_1x_r
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_r	x_r	x_r^2	x_rx_2	$...$	x_r^2

Definición

$\mathbb{Z}_n = {}^{\mathbb{Z}}/_{n\mathbb{Z}} = \{0, 1, ..., n-1\}$ anillo conmutativo.
$(\mathbb{Z}_n, +)$ es un grupo abeliano. $\mathbb{Z}_n^{\times} = \mathcal{U}(\mathbb{Z}_n) = \{r \in \mathbb{Z}_n : mcd(r,n) = 1\}$ es un grupo abeliano u $|\mathbb{Z}_n^{\times}| = \varphi(n)$ donde φ es la función de Euler.

$\varphi : \mathbb{N} - \{0\} \to \mathbb{N}$ tal que $\varphi(n) := card\{r \in \mathbb{N} : 0 \leq r \leq n-1 \text{ y } mcd(n,r) = 1\}$.
Si $p \in \mathbb{Z}$ es primo, $e \geq 1$, $\varphi(p^e) = p^{e-1}(p-1)$.
$mcd(n,m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$.
Si $n = p_1^{e_1}...p_k^{e_k}$ factorización en primos, entonces
$\varphi(n) = p_1^{e_1-1}...p_k^{e_k-1}(p_1-1)...(p_k-1)$.

Relación 1: Ejercicio 1

$\mathbb{Z}_8^{\times} = \{r \in \mathbb{Z}_8 : mcd(r,8) = 1\} = \{1,3,4,7\}$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Relación 1 : Ejercicio 3

Calcular el inverso de 7 en $Z_{37}^{\times}$.

$|\mathbb{Z}_{37}^{\times}| = \varphi(37) = 37 - 1 = 36$.
$mcd(7,37) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$ tal que $1 = a \cdot 7 + b \cdot 37$.

		u	v					
	37	1	0	37	=	$1 \cdot 37$	+	$0 \cdot 7$
5	7	0	1	7	=	$0 \cdot 37$	+	$1 \cdot 7$
3	2	1	-5	2	=	$1 \cdot 37$	-	$5 \cdot 7$
2	1	-3	16	1	=	$-3 \cdot 37$	+	$16 \cdot 7$

$1 \equiv a \cdot 7 \quad mod(37) \Rightarrow 7^{-1} = 16$

Definición

Sea $n \geq 2$ y sea:
$$\mathcal{M}_n := \{z \in \mathbb{C}^{\times} | z^n = 1\}$$

$\mathcal{M}_n$ con el producto es un grupo.
$z, z' \in \mathcal{M}_n$ entonces $(zz')^n = z^n z'^n = 1 \Rightarrow zz' \in \mathcal{M}_n$.

El producto de números complejos es una operación interna en $\mathcal{M}_n$.
$1 \in \mathcal{M}_n$ y es el uno de $\mathcal{M}_n$.
$z \in \mathcal{M}_n \Rightarrow \frac{1}{z} \in \mathcal{M}_n$ pues $(\frac{1}{z})^n = \frac{1^n}{z^n} = \frac{1}{1} = 1$.

$\mathcal{M}_n$ con el producto es un grupo abeliano y que se llama el grupo de las raíces n-ésimas de la unidad $(x^n - 1)$.

$$\mathcal{M}_n = \{\xi_k = cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n} | 0 \leq k \leq n-1\}$$

Es claro que $\xi_k^n = cos(2k\pi) + isen(2k\pi) = 1 + 0i = 1 \Rightarrow \xi_k \in \mathcal{M}_n$.

n=3 $\mathcal{M}_3 = \{\xi_0 = 1, \xi_1 = cos\frac{2\pi}{3} + isen\frac{2\pi}{3}, \xi_2 = cos\frac{4\pi}{3} + isen\frac{4\pi}{3}\} =$
$= \{1, cos(120) + isen(120), cos(240) + isen(240)\} =$
$= \{1, -cos(60) + isen(60), -cos(60) - isen(60)\}$.
n=4 $\mathcal{M}_4 = \{\xi_0 = 1, \xi_1 = cos\frac{2\pi}{4} + isen\frac{2\pi}{4}, \xi_2 = cos\frac{4\pi}{4} + isen\frac{4\pi}{4},$
$\xi_3 = cos\frac{6\pi}{4} + isen\frac{6\pi}{4}\} = \{1, i, -1, -i\}$

$$\mathcal{M}_n := \{z \in \mathbb{C}^* | z^n = 1\} = \{\xi_k = cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n} | 0 \leq k \leq n-1\}$$

$\xi_k = cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n} \in \mathcal{M}_n$
$\xi_t = cos\frac{2t\pi}{n} + isen\frac{2t\pi}{n} \in \mathcal{M}_n$
$\xi_k \cdot \xi_t = cos\frac{2(k+t)\pi}{n} + isen\frac{2(k+t)\pi}{n}$
$k + t = n \cdot q + r \quad 0 \leq r < n$
$\frac{2(k+t)\pi}{n} = \frac{2(nq+r)\pi}{n} = q2\pi + \frac{2r\pi}{n}$

2.2. Grupos Simétricos

Sea X un conjunto no vacío. Definimos el grupo de permutaciones de X como:

$$S(X) := \{\alpha : X \to X \mid \alpha \text{ es biyectiva}\}$$

con operación (con producto) dado por la composición de aplicaciones.

El uno en $S(X)$ es la aplicación $id_X : X \to X \;\; id_X(x) = x \;\; \forall x \in X$.

Para todo elemento $\alpha \in S(X)$, $\exists \alpha^{-1} : X \to X$ tal que $\alpha\alpha^{-1} = id_X = \alpha^{-1}\alpha$.

En el caso particular de que $X = \{1, 2, 3, ..., n\} (n \geq 2)$, al conjunto $S(X)$ lo denotaremos por S_n y lo llamaremos el n-ésimo grupo simétrico.

$$S_n = \{\alpha : \{1, 2, 3, ..., n\} \to \{1, 2, 3, ..., n\} \mid \alpha \text{ es biyectiva } \}$$

con operación dada por la composición.

S_n es un grupo finito con $|S_n| = n!$.

Notación matricial

$\alpha, \beta \in S_n$

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & ... & n \\ \beta(1) & \beta(2) & ... & \beta(n) \end{pmatrix}$$

$$\alpha \cdot \beta = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha\beta(1) & \alpha\beta(2) & ... & \alpha\beta(n) \end{pmatrix}$$

Ejemplo

En S_5.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

$$\alpha \cdot \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha(\beta(2)) & \alpha(\beta(4)) & \alpha(\beta(3)) & \alpha(\beta(1)) & \alpha(\beta(5)) \end{pmatrix} =$$

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

$$\beta \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

Nota

En general, S_n no es abeliano.
Con la notación matricial, el uno:

$$id_x = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ 1 & 2 & 3 & ... & n \end{pmatrix}$$

Si $\alpha \in S_n$, entonces $\alpha^{-1} \in S_n$ está determinada.

$$a^{-1}(y) = x \iff \alpha(x) = y$$

Ejemplo

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \in S_5$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

Definición

Dos permutaciones $\alpha, \beta \in S_n$ diremos que son disjuntas si los elementos (de X) que mueve una de ellas quedan fijos por la otra (α mueve a $x \in X$ si $\alpha(x) \neq x$). Es decir, si se tiene:

① $\alpha(x) \neq x \Rightarrow \beta(x) = x$

② $\beta(x) \neq x \Rightarrow \alpha(x) = x$

Nota: ① $\iff$ ②.

Ejemplo

En S_6.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 4 & 5 & 3 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$$

son disjuntas.

Proposición

Si $\alpha, \beta \in S_n$ son disjuntas entonces:

$$\alpha \cdot \beta = \beta \cdot \alpha$$

Demostración

Hemos de ver que $\alpha\beta(x) = \beta\alpha(x) \ \ \forall x \in X$. Tenemos 3 casos:

① $x \in X$ sea tal que $\alpha(x) \neq x \Rightarrow \beta(x) = x$ y entonces $\alpha(\beta(x)) = \alpha(x)$.
Si $\alpha(x) \neq x \Rightarrow \alpha(\alpha(x)) \neq \alpha(x) \Rightarrow \beta(\alpha(x)) = \alpha(x)$
Por lo que $\alpha\beta(x) = \beta\alpha(x)$.

② $x \in X$ sea tal que $\beta(x) \neq x$. Entonces, intercambiando los papeles de α y β en el caso 1, llegamos a que $\beta\alpha(x) = \beta(x) = \alpha\beta(x)$.

③ $x \in X$ sea tal que $\alpha(x) = x = \beta(x)$. Entonces:
$\alpha\beta(x) = \alpha(x) = x = \beta(x) = \beta\alpha(x)$.

Definición

Una permutación $\alpha \in S_n$ diremos que es un ciclo si $\exists x_1, x_2, ..., x_r \in X$ $(2 \leq r \leq n)$ tal que:

$$\alpha(x_1) = x_2$$

$$\alpha(x_2) = x_3$$

$$\vdots$$

$$\alpha(x_{n-1}) = x_n$$
$$\alpha(x_n) = x_1$$

y

$$\alpha(x) = x \quad \forall x \notin \{x_1, x_2, ..., x_n\}$$

Diremos que α es un ciclo de longitud r o un r-ciclo.
La identidad id_X puede considerarse un ciclo de longitud 1.
Escribiremos $\alpha = (x_1\ x_2\ ...\ x_r)$.
Un r-ciclo tiene r expresiones:

$$\alpha = (x_1\ x_2\ ...\ x_r) = (x_2\ x_3\ ...\ x_r\ x_1) = ... = (x_r\ x_1\ ...\ x_{r-1})$$

Ejemplo

En S_5:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 3 & 5 & 1 \end{pmatrix}$$

es un ciclo.

$$\alpha = (1\ 4\ 3\ 6) = (4\ 3\ 6\ 1) = (3\ 6\ 1\ 4) = (6\ 1\ 4\ 3)$$

Ejercicio

Sean $\alpha = (x_1\ ...\ x_r)$ y $\beta = (y_1\ ...\ x_s)$ dos ciclos en S_n.
Entonces α y β son disjuntas $\iff \{x_1, ..., x_r\} \cap \{y_1, ..., y_s\} = \emptyset$.
Por ejemplo, en S_4, $\alpha = (1\ 2)$ y $\beta = (3\ 4)$ son disjuntos ($\{1, 2\} \cap \{3, 4\} = \emptyset$).
Demostrar.

Teorema

Toda permutación de S_n, distinta de id_X, se expresa de forma única (salvo el orden) como producto de ciclos disjuntos.
Es decir, dado $\alpha \in S_n, \alpha \neq id_X$, existen únicos ciclos $\alpha_1, ..., \alpha_m \in S_n$ disjuntos dos a dos, tal que $\alpha = \alpha_1\alpha_2...\alpha_m$.

Demostración

Existencia: $\alpha \in S_n, \alpha \neq id$. Sea $s = |\{x \in X : \alpha(x) \neq x\}|$.
Como $\alpha \neq id_X$ entonces $\exists x \in X$ tal que $\alpha(x) \neq x$. Si $\alpha(x) = y, y \neq x \Rightarrow \alpha(y) \neq \alpha(x) = y \Rightarrow s \geq 2$.
Hacemos inducción en s. Primer paso es que $s = 2$, es decir, que existen únicamente dos elementos $x, y \in X$ que son movidos por α ($\alpha(z) = z\ \ \forall z \neq x, y$).
Entonces $\alpha(x) = y$ y $\alpha(y) = x$, es decir, $\alpha = (x\ y)$.

Sea $s > 2$ y supongamos el resultado cierto para toda permutación que mueva menos de s elementos.
Elegimos $x \in X$ tal que $\alpha(x) \neq x$. La sucesión $x, \alpha(x), \alpha^2(x), \alpha^3(x), ...$ necesariamente es finita, es decir, $\exists k, k' \;\; k > k'$ tal que $\alpha^k(x) = \alpha^{k'}(x)$, es decir, $\alpha^{k-k'}(x) = x$.
Sea r el menor tal que $\alpha^r(x) = x$ ($r \geq 2$).
Consideramos el siguiente ciclo: $\alpha_1 = (x \; \alpha(x) \; ... \; \alpha^{r-1}(x)) \in S_n$.
Definimos $\alpha' \in S_n$ como sigue:

$$\alpha'(y) = \begin{cases} y & y \in \{x, \alpha(x), ..., \alpha^{r-1}(x)\} \\ \alpha(y) & y \notin \{x, \alpha(x), ..., \alpha^{r-1}(x)\} \end{cases}$$

① α_1 y α' son permutaciones disjuntas.
② $\alpha = \alpha_1\alpha'$.
Vamos a verlo.

- $y \in \{x, \alpha(x), ..., \alpha^{r-1}(x)\}$.
  $(\alpha \; \alpha')(y) = \alpha_1(y) = \alpha(y)$.
  $y = \alpha^j(x) \quad 0 \leq j \leq r-1$.
  $\alpha_1(y) = \alpha^{j+1}(x) = \alpha(\alpha^j(x)))\alpha(y)$.
- $y \notin \{x, \alpha(x), ..., \alpha^{r-1}(x)\}$.
  $(\alpha_1 \; \alpha')(y) = \alpha_1(\alpha(y)) = \alpha(y)$.
  $\alpha(y) \notin \{x, \alpha(x), ..., \alpha^{r-1}(x)\}$.

α' mueve $s - r$ elementos. Como $s - r < s$ por hipótesis de inducción, $\exists \alpha_2, ..., \alpha_m$ ciclos disjuntos dos a dos tal que:

$$\alpha' = \alpha_2 ... \alpha_m$$

$$\alpha = \alpha_1\alpha' = \alpha_1\alpha_2 ... \alpha m$$

Unicidad: $\alpha = \alpha_1\alpha_2...\alpha_m$ ciclos disjuntos y $\alpha = \beta_1\beta_2...\beta_{m'}$ ciclos disjuntos. vamos a ver que $m = m'$ y $\alpha_i = \beta_i \;\; \forall i = 1, ..., m$.
$\alpha_1 = (x \; \alpha_1(x) \; \alpha_1^2(x) \; ...) = (x \; \alpha(x) \; \alpha^2(x) \; ...)$
$\alpha_1(x) = \alpha(x)$ (pues α_1 es disjunto con $\alpha_2, \alpha_3, ..., \alpha_m$).
Como $\alpha(x) \neq x$ existe un único β_j tal que $\beta_j(x) \neq x$ y $\beta_k(x) = x \;\; \forall k \neq j$ pues $\alpha = \beta_1\beta_2...\beta_{m'}$ es una expresión como producto de ciclos disjuntos.
Podemos suponer que $j = 1$, es decir, $\beta_1(x) \neq x$ (que permutaciones disjuntas conmutan).
$\beta_1 = (x \; \beta_1(x) \; \beta_1^2 \; ...) = (x \; \alpha(x) \; \alpha^2(x) \; ...)$ pues $\beta_1(x) = \alpha(x)$. Por tanto, $\alpha_1 = \beta_1$.

$$\alpha = \alpha_1\alpha_2 ... \alpha_m$$

$$\alpha = \alpha_1\beta_2 ... \beta_{m'}$$

Hacemos inducción en m. Si $m = 1$, entonces $m' = 1$, porque si $m' > 1$:

$$\alpha_1 = \alpha_1\beta_2 ... \beta_{m'} \Rightarrow id_X = \beta_2 ... \beta_{m'}$$

es una contradicción. Es decir, $m' = 1$.
Supongamos $m > 1$ y cierto para $m = 1$.

$$\alpha_1\alpha_2...\alpha_m = \alpha_1\beta_2...\beta_{m'} \Rightarrow \alpha_2...\alpha_m = \beta_2...\beta_{m'} \Rightarrow$$

$$\Rightarrow \begin{cases} m - 1 = m' - 1 \Rightarrow m = m' \\ \alpha_i = \beta_i \ \ \forall i = 2, ..., m \end{cases}$$

Relación 1: Ejercicio 12

Sean $\alpha_1, \alpha_2 \in S_7$.

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{pmatrix}$$

$$\alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}$$

Calcular $\alpha_1\alpha_2, \alpha_2\alpha_1, \alpha_2^2$. Expresarlos como producto de ciclos disjuntos.

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix}$$

$$\alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1\,5 \end{pmatrix} \begin{pmatrix} 2 & 7 & 3 & 6 & 4 \end{pmatrix}$$

$$\alpha_1\alpha_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{pmatrix} =$$

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

Relación 1: Ejercicio 13

En S_9:

$$P_1 = \begin{pmatrix} 1 & 3 & 2 & 8 & 5 & 9 \end{pmatrix} \begin{pmatrix} 2 & 6 & 3 \end{pmatrix} =$$

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

Relación 1: Ejercicio 19

Describid todos los ciclos de S_4 y expresar todos los elementos distintos de la identidad de S_4 como producto de ciclos disjuntos.

- Ciclos de longitud 2:

$$\begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix}$$

- Ciclos de longitud 3:

$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 2\end{pmatrix},$$

$$\begin{pmatrix}1 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 3\end{pmatrix}, \begin{pmatrix}2 & 3 & 4\end{pmatrix}, \begin{pmatrix}2 & 4 & 3\end{pmatrix}$$

- Ciclos de longitud 4:

$$\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 4 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix},$$

$$\begin{pmatrix}1 & 3 & 4 & 2\end{pmatrix}, \begin{pmatrix}1 & 4 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 4 & 3 & 2\end{pmatrix}$$

- No son ciclos:

$$\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}$$

Añadiendo id_{S_4}, tenemos $4! = 24$ ciclos.

Proposición

Sea $n \geq 2$. En S_n se tiene:

① $(x_1\ x_2\ ...\ x_r)^{-1} = (x_r\ x_{r-1}\ ...\ x_2\ x_1)$.

② Para todo $\alpha \in S_n$:

$$\alpha(x_1\ x_2\ ...\ x_r)\alpha^{-1} = (\alpha(x_1)\ \alpha(x_2)\ ...\ \alpha(x_r)$$

③ $(x_1\ x_2\ ...\ x_r) = (x_1\ x_2)(x_2\ x_3)...(x_{r-1}\ x_r)$

④ Dado un r-ciclo $(x_1\ x_2\ ...\ x_r)$ se verifica que para todo $1 \leq k < r$, $(x_1\ ...\ x_r)^k \neq id$ y $(x_1\ ...\ x_r)^r = id$

Demostración

④ Si $1 \leq k < r$ se verifica $(x_1 \ ... \ x_r)^k(x_1) = x_{k+1}$ y lo vemos por inducción en k.
Si $k = 1$, es claro $(x_1 \ .... \ x_r)(x_1) = x_2$.
Sea $k > 1$.

$$(x_1 \ ... \ x_r)^k(x_1) = [(x_1 \ ... \ x_r)(x_1 \ ... \ x_r)^{k-1}](x_1) =$$

$$= (x_1 \ ... \ x_r)(x_{k-1+1}) = x_{k+1}$$

Puesto que $k < r \Rightarrow k+1 \leq r$ y entonces $(x_1 \ ... \ x_r)^k(x_1) = x_{k+1} \neq x_1$, y en definitiva $(x_1 \ ... \ x_r)^k \neq id$.

$$(x_1 \ ... \ x_r)^r(x_1) = (x_1 \ ... \ x_r)(x_1 \ ... \ x_r)^{r-1}(x_1) = (x_1 \ ... \ x_r)(x_r) = x_1$$

$$(x_1 \ ... \ x_r)^r = id$$

Sea $2 \leq i \leq r$:

$$(x_1 \ ... \ x_r)^r(x_i) = (x_1 \ ... \ x_r)^r(x_1 \ ... \ x_r)^{i-1}(x_1) =$$

$$= (x_1 \ ... \ x_r)^{i-1}(x_1 \ ... \ ...x_r)^r(x_1) = (x_1 \ ... \ x_r)^{i-1}(x_1) = x_i$$

Si $x \notin \{x_1, ..., x_r\}$, entonces $(x_1 \ ... \ x_r)^r(x) = x$.

$$(x_1 \ ... \ x_r)^r = id$$

2.3. Grupos Diédricos

Sea $n \geq 3$ y P_n el polígono regular de n lados.

Se define el n-ésimo grupo diédrico, que denotaremos por D_n, como el grupo de las isometrías (ó movimientos que preservan la distancia) del plano real $\mathbb{R}^2$ que globalmente dejan fijo a P_n.

$$D_n = \{T : \mathbb{R}^2 \to \mathbb{R}^2 \mid T \text{ es isometría y } T(P_n) = P_n\}$$

donde la operación es la composición.

Vamos a ver que D_n es un grupo finito con $|D_n| = 2n$.

P_n polígono regular de n lados, lo centramos en el origen (tomamos un sistema de coordenadas tal que esté en el origen) y suponemos centrado de radio 1. Entonces los vértices de P_n son:

$$v_0, v_1, ..., v_{n-1} \text{ donde } v_k = (cos\frac{2k\pi}{n}, sen\frac{2k\pi}{n})$$

En particular, $v_0(1, 0)$.

Reconocemos $2n$ elementos en D_n que son:

- Para cada $0 \leq k \leq n-1$, sea R_k el giro centrado en el origen y amplitud $\frac{2k\pi}{n}$ $(R_0 = id)$.

$$R_k = \mathbb{R}^2 \to \mathbb{R}^2 \qquad (x,y) \to (x,y) \begin{pmatrix} cos\frac{2k\pi}{n} & sen\frac{2k\pi}{n} \\ -sen\frac{2k\pi}{n} & cos\frac{2k\pi}{n} \end{pmatrix}$$

- $s_0, s_1, .., s_{n-1}$ los n ejes de simetría de P_n que son:
  - Si n es impar, las rectas que unen cada vértice con el origen.
  - Si n es par, las rectas que unen cada vértice con el origen y las que unen los puntos medios de cada lado con el origen (hay n ya que la recta que une un vértice con el origen es la misma que la que une el vértice opuesto con el origen, y análogo con los puntos medios).

  Sea S_k la simetría respecto al eje s_k.

$$S_k = \mathbb{R}^2 \to \mathbb{R}^2 \qquad (x,y) \to (x,y) \begin{pmatrix} cos\frac{2k\pi}{n} & sen\frac{2k\pi}{n} \\ sen\frac{2k\pi}{n} & -cos\frac{2k\pi}{n} \end{pmatrix}$$

Proposición

$D_n = \{R_0, R_1, ..., R_{n-1}, S_0, S_1, ..., S_{n-1}\}$

Demostración

1. Todo movimiento del plano está totalmente determinado por la imagen de 3 puntos no alineados.
2. Si $T \in D_n$ entonces aplica vértices en vértices.

$$T|_{\{v_0,v_1,...,v_{n-1}\}} : \{v_0, ..., v_{n-1}\} \to \{v_0, v_1, ..., v_{n-1}\}$$

define una permutación de los vértices.

Si n es par y v_i un vértices de P_n y sea v_j el vértice opuesto.

$$\forall (p,q) \in P_n \times P_n \qquad d(p,q) \leq d(v_i, v_j)$$

Como T preserva distancias y $T(P_n) = P_n$.

$$\forall (p,q) \in P_n \times P_n \qquad d(p,q) \leq d(T(v_i), T(v_j)) = d(v_i, v_j) \Rightarrow$$

$$\Rightarrow T(v_i), T(v_j) \in \{v_0, v_1, ..., v_n\}$$

Si n es impar y v_i un vértices de P_n y sean v_j, v_k los vértices opuestos.

$$\forall (p,q) \in P_n \times P_n \qquad d(p,q) \leq d(v_i, v_j)$$

y entonces $T(v_i), T(v_j), T(v_k) \in \{v_0, v_1, ..., v_k\}$

$$T|_{\{v_0,v_1,...,v_{n-1}\}} : \{v_0, ..., v_{n-1}\} \to \{v_0, v_1, ..., v_{n-1}\}$$

y $T|_{\{v_0,v_1,...,v_{n-1}\}}$ es inyectiva (T preserva distancias) $\Rightarrow R|_{\{v_0,v_1,...,v_{n-1}\}}$ es biyectiva.

3. Si $T \in D_n$ entonces $T(0,0) = (0,0)$ $\qquad O = (0,0)$
porque O es el único punto del plano que equidista de todos los vértices.

4. Si $T \in D_n$, entonces T está completamente determinado por $T(v_0)$ y $T(v_1)$, ya que O, v_0 y v_1 son 3 puntos no alineados y $T(v) = v$.
Si $T, T' \in D_n$ tal que $\begin{cases} T(v_0) = T'(v_0) \\ T(v_1) = T'(v_1) \end{cases} \Rightarrow T = T'$.

5. Si $T \in D_n$ entonces $T(v_0)$ y $T(v_1)$ son vértice adyacentes porque los vértices adyacentes de P_n son los de mínima distancia entre los pares de vértices de P_n.

6. $D_n = \{R_0 = id, R_1, ..., R_{n-1}, S_0, ..., S_{n-1}\}$.
Sea $T \in D_n$ y supongamos que $T(v_0) = v_k$ $\ 0 \leq 1 \leq n-1$.
Si $T(v_1) = v_{k+1}$ (entendiendo v_0 si $k = n-1$) $\Rightarrow_{(4)} T = R_k$ porque $R_k(v_0) = v_k$ y $R_k(v_1) = v_{k+1}$.
Si $T(v_1) = v_{k-1}$ (entendiendo v_{n-1} si $k = 0$) $\Rightarrow_{(4)} T = S_k$ porque $S_k(v_0) = v_k$ y $S_k(v_2) = v_{k-1}$.

Veamos otra forma de trabajar con los grupos D_n (puramente algebraica).

Ejemplo

$n = 4 \qquad D_4 = \{R_0 = id, R_1, R_2, R_3, S_0, S_1, S_2, S_3\}$.

- $R_0 = id$.
- $R_1 =$ giro de amplitud 90 °.
- $R_2 =$ giro de amplitud 180 °.
- $R_3 =$ giro de amplitud 270 °.
- $S_0 =$ simetría respecto al eje s_0 $\quad (x = 0)$.
- $S_1 =$ simetría respecto al eje s_1 $\quad (x = y)$.
- $S_2 =$ simetría respecto al eje s_2 $\quad (y = 0)$.
- $S_3 =$ simetría respecto al eje s_3 $\quad (y = -x)$.

$$r = R_1, r^2 = R_2, r^3 = R_3, r^4 = 1, s = S_0$$

① $rs = S_1$.

② $r^2s = S_2$.

③ $r^3s = S_3$.

Demostración de ①:

$$\begin{cases} rs(v_0) = r(v_0) = v_1 = s_1(v_0 \\ rs(v_1) = r(v_3) = v_0 = s_1(v_1 \end{cases} \Rightarrow rs = s_1$$

Demostrar ② y ③ queda como ejercicio.

$$D_4 = \{1, r, r^2, r^3, rs, r^2s, r^3s\}$$

Se verifica además que $sr = r^3s$. Demostración:

$$\begin{cases} sr(v_0) = v_3 = s_3(v_0) \\ sr(v_1) = v_2 = s_3(v_1) \end{cases} \Rightarrow sr = s_3 = r^3s$$

$\cdot$	1	r	r^2	r^3	s	rs	r^2s	r^3s
1	1	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	1	rs	r^2s	r^3s	s
r^2	r^2	r^3	1	r	r^2s	r^3s	s	rs
r^3	r^3	1	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	1	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	1	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	1	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	1

Corolario

Sea $n \geq 3$ $\quad D_n = \{1, R_1, R_2, ..., R_{n-1}, S_0, S_1, ..., S_{n-1}\}$.
Si llamamos

$$r = R_1 \text{ giro centrado en el origen y amplitud } \frac{2\pi}{n}$$

$$s = S_0 \text{ simetría respecto al eje y=0}$$

Entonces se verifica:

$$R_k = r^k \qquad 0 \leq k \leq n-1$$

$$S_k = r^ks \qquad 0 \leq k \leq n-1$$

Además, se tiene

$$① \qquad r^n = 1 = s^2 \text{ y } sr = r^{n-1}s$$

Es decir:

$$D_n = \{1, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s\}$$

Proposición

Para todo $1 \leq k \leq n-1$ se tiene que:

$$② \qquad sr^k = r^{n-k}s$$

y entonces podemos escribir la tabla del grupo D_n haciendo uso únicamente de las identidades

Demostración

Veamos ②. Hacemos inducción en k.
Para $k = 1$ se tiene por ①.
Supuesto cierto para k:

$$sr^{k+1} = sr^k r = r^{n-k}sr = r^{n-k}r^{n-1}s = r^{2n-(k+1)}s =$$

$$= r^n r^{n-(k+1)}s = r^{n-(k+1)}s$$

y se tiene ②.
Notemos que ② es consecuencia de ①.

Notemos además que otra forma de escribir ② es:

$$sr^k = r^{-k}s$$

porque $r^{-k} = (r^k)^{-1} = r^{n-k}$ ya que $r^k r^{n-k} = r^n = 1$.

Proposición

Describir la tabla de D_n es decir:

$$r^i \cdot r^j = r^{i+k} = r^{res(i+j;n)}$$

$$r^i \cdot r^j s = r^{i+j}s = r^{res(i+j;n)}s$$

$$r^i s \cdot r^j = r^i r^{-j}s = r^{i-j}s = r^{res(i-j;n)}s$$

$$r^i s \cdot r^j s = r^i r^{-j}ss = r^{i-j} = r^{res(i-j;n)}$$

Diremos que D_n está generado por r y s, y escribiremos

$$D_n =< r, s \mid r^n = 1 = s^2;\ sr = r^{n-1}s >$$

A las identidades:

$$r^n = 1 = s^2 \qquad sr = r^{n-1}s$$

las llamaremos identidades fundamentales.

Nota

Los grupos diédricos D_n NO son abelianos.

$sr = r^{n-1}s$ y como $n \geq 3$ entonces $sr \neq rs$

2.4. Grupo de los cuaternios

El grupo de los cuaternios, que denotaremos por Q_2, es dado por:

$$Q_2 = \{1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, -1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, -i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, -j = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, k = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, -k = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\}$$

con operador dado por el producto de matrices.

$$\begin{aligned} 1^{-1} &= 1 & \qquad (-1)^{-1} &= -1 \\ i^{-1} &= -i & (-i)^{-1} &= i \\ j^{-1} &= -j & (-j)^{-1} &= j \\ j^{-1} &= -k & (-k)^{-1} &= k \end{aligned}$$

Proposición

Se verifica (identidades fundamentales):

a) $i^2 = j^2 = k^2 = 1 \qquad (-1)^2 = 1$

b) $i(-1) = -i = (-1)i$

c) $j(-1) = -j = (-1)j$

d) $k(-1) = -k = (-1)k$

e) $ij = k$

La demostración queda como ejercicio.

Proposición

Prescindiendo de la descripción de los elementos de Q_2 como matrices, y utilizando únicamente las identidades anteriores $a), b), c), d), e)$, tenemos que en Q_2 se verifica:

$$jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j$$

Se puede entonces escribir la tabla de Q_2 prescindiendo de sus descripciones como matrices.

Demostración

Veamos que $jk = i$:.
Por $e)$ sabemos que:
$ij = k \Rightarrow ijk = k^2 \Rightarrow ijk = -1 \Rightarrow i^2jk = i(-1) = (-1)jk = (-1)i \Rightarrow$
$\Rightarrow (-1)^2jk = (-1)^2i \Rightarrow jk = i$

Veamos que $ki = j$.
Como $jk = i \Rightarrow jki = i^2 = -1 \Rightarrow j^2ki = j(-1) \Rightarrow (-1)ki = (-1)j \Rightarrow$
$\Rightarrow (-1)^2ki = (-i)^2j \Rightarrow ki = j$

Vemos que $ji = -k$.
Como $ki = j \Rightarrow ki^2 = ji \Rightarrow k(-1) = ji \Rightarrow -k = ji$.

Definición

$$Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$$

Verificando las identidades:

$$(-1)^2 = 1 \qquad i^2 = j^2 = k^2 = -1$$

$$a(-1) = -1 = (-1)a \qquad a = i, j, k$$

$$ij = k$$

2.5. El grupo de Klein

Definición

Sean G y H dos grupos. Definimos el producto directo de$G$ y H como el grupo dado por el producto cartesiano:

$$G \times H = \{(x, y) : x \in G, \qquad y \in H\}$$

y con producto definido como sigue:

$$(x, y) \cdot (x', y') := (xx', yy')$$

Es fácil ver que en efecto $G \times H$ es un grupo con la operación anterior, donde uno es $(1, 1)$ y para cada $(x, y) \in G \times H$, su inverso $(x, y)^{-1} = (x^{-1}, y^{-1})$.

Si G y H son finitos, entonces $G \times H$ es finito con:

$$|G \times H| = |G||H|$$

Definición

Definimos el grupo de Klein, que denotaremos por K (ó V en algunos libros), como el producto directo de μ_2 con μ_2, donde μ_2 es el grupo de las raíces cuadradas de la unidad.

$$K := \mu_2 \times \mu_2 = \{(1,1),(1,-1),(-1,1),(-1,-1)\}$$

$$(\mu_2 = \{x \in \mathbb{C}^* : x^2 = 1\} = \{1,-1\})$$

$$|K| = 4$$

Ejercicio

Escribid la tabla del grupo de Klein.

2.6. Homomorfismos

Definición

Sean G y G' dos grupos. Un homomorfismo de grupos de G en G' es una aplicación:

$$f : G \to G'$$

tal que verifica:

$$f(ab) = f(a)f(b) \qquad \forall a,b \in G$$

Si f es inyectiva, diremos que f es un monomorfismo.
Si f es sobreyectiva, diremos que f es un epimorfismo.
Si f es biyectiva, diremos que f es un isomorfismo.

Ejemplos

1. Para todo grupo G, la identidad $1_G : G \to G$ es un isomorfismo.
2. $n \geq 2, K$ cuerpo, la aplicación:

$$det : GL_n(K) \to K^*$$

   es un homomorfismo.
3. $f : \mathbb{R} \to \mathbb{R}^* \qquad f(x) = e^x$ es un homomorfismo.
4. Para todo $n \geq 2$:

$$p : \mathbb{Z} \to \mathbb{Z}_{\ltimes} \text{ proyección}$$

   tal que $p(k) = res(k;n)$, es un homomorfismo.

Proposición

Sea $f : G \to G'$ un homomorfismo de grupos. Entonces:

1. $f(1) = 1$.
2. $f(a^{-1}) = f(a)^{-1} \quad \forall a \in G$.

Proposición

Sean $f : G \to G'$ y $g : G' \to G''$ dos aplicaciones. Entonces:

1. Si f y g son homomorfismos $\Rightarrow g_o f$ es un homomorfismo.
2. Si f y g son monomorfismos (respectivamente, epimorfismos, isomorfismos) $\Rightarrow g_o f$ es monomorfismo (respectivamente, epimorfismo, isomorfismo).

Proposición

Sea $f : G \to G'$ un homomorfismo. Entonces:
f es ismorfismo $\iff \exists g : G' \to G$ tal que $f_o g = id_{G'}$, $g_o f = id_G$ y g es un homomorfismo de grupos.

Además, en tal caso, g es única y se denota por $f^{-1} : G' \Rightarrow G$.

Demostración

$\Leftarrow$) Obvio.
$\Rightarrow$) $f : G \to G'$ isomorfismo. Entonces f es una aplicación biyectiva y por tanto $\exists g : G' \to G$ tal que:

$$f_o g = id_{G'} \qquad \text{y} \qquad g_o f = id_G$$

Veamos que $g : G' \to G$ es un homomorfismo de grupos:
$\forall x', y' \in G' \qquad g(x', y') =^? g(x')g(y')$
$g(x', y') \in G \Rightarrow f(g(x'y')) = (f_o g)(x'y') = x'y'$
$g(x')g(y') \in G \Rightarrow f(g(x')g(y')) = f(g(x'))f(g(y')) =$
$= (f_o g)(x')(f_o g)(y') = x'y'$
$f(g(x'y)) = f(g(x')g(y')) \Rightarrow g(x'y') = g(x')g(y')$

Corolario

En la clase de todos los grupos, la relación binaria "ser isomorfos" es una relación de equivalencia.

Demostración

Dados dos grupos G y G' diremos que G es isomorfo a G' si existe un isomorfismo $f : G \to G'$ y escribiremos $G \cong G'$.

"Ser isomorfos" es una relación binaria en la clase de todos los grupos.

Puesto que $1_G : G \to G$ es un isomorfismo $\Rightarrow G \cong G$ para todo G (propiedad reflexiva).

Si $G \cong G'$ es porque $\exists f : G \to G'$ isomorfismo $\Rightarrow f^{-1} : G' \to G$ es un isomorfismo $\Rightarrow G' \cong G$ (propiedad simétrica).

Si $G \cong G'$ y $G' \cong G''$, $\exists f : G \to G'$ isomorfismo y $\exists g : G' \to G''$ isomorfismo $\Rightarrow g_o f : G \to G''$ isomorfismo $\Rightarrow G \cong G''$ (propiedad transitiva).

Por lo que "ser isomorfos" es relación de equivalencia.

Teorema

Todos los grupos de orden 2 son isomorfos entre si. Es decir, hay sólo una clase de equivalencia que la representaremos por el grupo:

$$\mu_2 = \{1, -1\}$$

Demostración

$$G = \{1, a\} \qquad\qquad H = \{1, b\}$$

Definimos:

$$f : G \to H,\ \ f(1) = 1,\ \ f(a) = b$$

f es un homomorfismo de grupos y entonces es isomorfismo.

$$f(xy) = f(x)f(y) \qquad \forall x, y \in G$$

Es obvio que se tiene si $x = 1$ ó $y = 1$.
Si $x = y = 1$, entonces $xy = a^2 = 1$ ($a^2 \neq a$ pues $a^2 = a \Rightarrow a = 1$).

$\cdot$	1	a
1	1	a
a	a	1

$$\begin{cases} f(xy) = f(a^2) = f(1) \\ f(x)f(1) = f(a)f(a) = b^2 = 1 \end{cases} \Rightarrow f(aa) = f(a)f(a)$$

2.7. Ejercicios

Relación 1: Ejercicio 5

En el conjunto $\mathbb{Q}^{\times} := \{\mathbf{q} \in \mathbb{Q} | \mathbf{q} \neq \mathbf{0}\}$ de los números racionales no nulos, se considera la operación de división, dada por $(\mathbf{x}, \mathbf{y}) \to \frac{\mathbf{x}}{\mathbf{y}} = \mathbf{x}\mathbf{y}^{-1}$. ¿Nos da esta operación una estructura de grupo en $\mathbb{Q}^{\times}$?

La operación no es asociativa (comprobar), por lo que no es un grupo.

Relación 1: Ejercicio 6

Sea G un grupo en el que $\mathbf{x}^2 = \mathbf{1}$ para todo $\mathbf{x} \in \mathbf{G}$. Demostrar que el grupo G es abeliano.

$x, y \in G \Rightarrow x^2 = 1 = y^2$ y también $(xy)^2 = 1 \Rightarrow xyxy = 1 \Rightarrow$
$\Rightarrow x^2yxy^2 = xy \Rightarrow 1yx1 = xy \Rightarrow yx = xy \Rightarrow G$ abeliano.

Otras formas:
$xyyx = xy^2x = xx = x^2 = 1$
$yx = (xy)^{-1} = xy$.

Relación 1: Ejercicio 7

Sea G un grupo. Demostrar que son equivalente:

1. **G es abeliano.**
2. **$\forall \mathbf{x}, \mathbf{y} \in \mathbf{G}$ se verifica que $(\mathbf{xy})^2 = \mathbf{x}^2\mathbf{y}^2$.**
3. **$\forall \mathbf{x}, \mathbf{y} \in \mathbf{G}$ se verifica que $(\mathbf{x}, \mathbf{y})^{-1} = \mathbf{x}^{-1}\mathbf{y}^{-1}$.**

1 $\Rightarrow$ 2 Es obvio.
2 $\Rightarrow$ 3 $(x^{-1}y^{-1})^2 = x^{-1}x^{-1}y^{-1}y^{-1} \Rightarrow x(x^{-1}y^{-1}x^{-1}y^{-1})y =$
$= x(x^{-1}x^{-1}y^{-1}y^{-1})y \Rightarrow y^{-1}x^{-1} = x^{-1}y^{-1} \Rightarrow (xy)^{-1} = x^{-1}y^{-1}$
3 $\Rightarrow$ 1 Puesto que $(xy)^{-1} = x^{-1}y^{-1} \Rightarrow xyx^{-1}y^{-1} = 1 \Rightarrow xyx^{-1}y^{-1}yx = yx \Rightarrow xy = yx \Rightarrow G$ es abeliano.

Relación 1: Ejercicio 9

Si $\mathbf{a}, \mathbf{b} \in \mathbb{R}, \mathbf{a} \neq \mathbf{0}$, demostrar que el conjunto de las aplicaciones $\mathbf{f} : \mathbb{R} \to \mathbb{R}$, tales que $\mathbf{f}(\mathbf{x}) = \mathbf{ax} + \mathbf{b}$, es un grupo con la composición como ley de composición.

$f(x) = ax + b \qquad g(x) = a'x + b \qquad a, a' \neq 0$
$(g_o f)(x) = g(ax + b) = a'(ax + b) + b' = a'ax + a'b + b' \Rightarrow g_o f \in G$

Es asociativa y existe uno (demostrar). Además, hay que comprobar que $f : \mathbb{R} \to \mathbb{R}, f(x) = ax + b$ entonces $f^{-1} : \mathbb{R} \to \mathbb{R}$ es $f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$.

Relación 1: Ejercicio 10

① **Demostrar que $|\mathbf{GL_2}(\mathbb{Z}_\mathbf{2})| = \mathbf{6}$, describiendo explicitamente todos los elementos que forman este grupo.**

② **Sean**

$$\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Demostrar que:

$$\mathbf{GL_2}(\mathbb{Z}_\mathbf{2}) = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

③ **Escribir, utilizando la representación anterior, la tabla de multiplicar de $\mathbf{GL_2}(\mathbb{Z}_\mathbf{2})$**

①

$$GL_2(\mathbb{Z}_2) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\}$$

③ Es la misma tabla que la de D_3 (con $r = \alpha$ y $s = \beta$).

Relación 1: Ejercicio 21

① **Demostrar que la aplicación**

$$\mathbf{1} \to \mathbf{1}, -\mathbf{1} \to \mathbf{4}, \mathbf{i} \to \mathbf{2}, -\mathbf{i} \to \mathbf{3},$$

da un isomorfismo entre el grupo $\mu_\mathbf{4}$ de las raíces cuárticas de la unidad y el grupo $\mathbb{Z}_\mathbf{5}^\times$ de las unidades en $\mathbb{Z}_\mathbf{5}$

② **Encontrar otro isomorfismo entre estos dos grupos que sea distinto del anterior.**

② Otro isomorfismo:

$$g : \mu_4 \to \mathbb{Z}_5^\times \text{ isomorfismo de grupos}$$

$g(1) = 1$ pues g ha de ser homomorfismo.
Probamos $g(-1) = 2$, y como g es homomorfismo debe cumplirse:

$$g((-1)(-1)) = g(-1)g(-1) \Rightarrow g(1) = 2 \cdot 2 \Rightarrow 1 \neq 4 \text{ (en } \mathbb{Z}_5)$$

luego $g(-1) \neq 2$. Como $g(1) = g(-1)g(-1) = 1$, sabemos que $g(-1) = 4$ (ya que $4 \cdot 4 = 16 = 1$ (en $\mathbb{Z}_5$).
Comprobad que con $g(i) := 3$ y $g(-i) := 2$, g es un homomorfismo de grupos (y por lo cual isomorfismo al ser biyectivo) y, obviamente, $g \neq f$.

Relación 1: Ejercicio 26

① **Demostrar que los grupos multiplicativos $\mathbb{R}^*$ (de los reales no nulos) y $\mathbb{C}^*$ (de los complejos no nulos) no son isomorfos.**

② **Demostrar que los grupos aditivos $\mathbb{Z}$ y $\mathbb{Q}$ no son isomorfos.**

① Lo demostramos por reducción al absurdo.
Supongamos que existe:

$$f : \mathbb{C}^* \to \mathbb{R}^* \text{ isomorfismo}$$

Sea $f(i) = a$. Entones $f(1) = f(i^4) = f(i)^4 = a^4$ (ya que es isomorfismo) $\Rightarrow a = 1$ ó $a = -1$.
$a \neq 1$ ya que $i \neq 1 \Rightarrow f(i) \neq f(1) = 1$.
Por lo que $f(i) = -1$. Pero $f(-1) = f(i^2) = f(i)f(i) = (-1)(-1) = 1 = f(1) \Rightarrow f(-1) = f(1)$. Contradicción.

② Análogo al anterior.
Supongamos que existe:

$$g : \mathbb{Z} \to \mathbb{Q} \text{ isomorfismo}$$

Sea $g(1) = \frac{a}{b}$. Entonces para $n \in \mathbb{Z}$ se tendrá que $n > 0$:

$$g(n) = g(1 + ...^{n \text{ veces}}... + 1) = g(1) + ...^{n \text{ veces}}... + g(1) = n\frac{a}{b}$$

$$g(-n) = -g(n) = -n\frac{a}{b}$$

Elegimos $p \in \mathbb{Z}$ primo tal que $p \nmid b$ y consideramos $\frac{1}{p} \in \mathbb{Q}$. Como g es isomorfismo, es sobreyectiva, luego $\exists n \in \mathbb{Z}$ tal que:

$$g(n) = n\frac{a}{b} = \frac{1}{p} \Rightarrow pna = b \Rightarrow p \mid b$$

Por lo que llegamos a una contradicción.

Relación 1: Ejercicio 28

Demostrar que no existe ningún cuerpo K tal que sus grupos $(\mathbf{K}, +)$ y $(\mathbf{K}^*, \cdot)$ sean isomorfos.

Definición: Sea K un cuerpo, se define su característica como el menor entero positivo n tal que $n \cdot 1 = 0$.
Si no existe ningún entero positivo n verificando $n \cdot 1 = 0$, se dice que K tiene característica 0.

$$Car(\mathbb{R}) = Car(\mathbb{Q}) = Car(\mathbb{C}) = 0$$

$$Car(\mathbb{Z}_p) = p \qquad p \text{ primo}$$

Supongamos que existe:

$$f : K^* \to K \text{ isomorfismo}$$

$$f(xy) = f(x) + f(y) \quad \forall x, y \in K^* \qquad f(1) = 0$$

$0 = f(1) = f((-1)(-1)) = f(-1) + f(-1) = 2f(-1) \Rightarrow 2f(-1) = 0$
Si $Car(K) \neq 2 \Rightarrow f(-1) = 0 \Rightarrow f(-1) = f(1)$ (Contradicción, ya que f es inyectiva).
Supongamos que $Car(K) = 2$. Consideramos:

$$f^{-1} : K \to K^* \text{ es también ismorfismo}$$

$$f^{-1}(x + y) = f^{-1}(x)f^{-1}(y) \quad \forall x, y \in K \qquad f^{-1}(0) = 1$$

Sea $a \in K^*$ arbitrario. Como f^{-1} es sobreyectiva, $\exists b \in K$ tal que $f^{-1}(b) = a$.

$a^2 = f^{-1}(b)f^{-1}(b) = f^{-1}(b + b) = f^{-1}(2b) = f^{-1}(0) = 1 \Rightarrow a^2 = 1 \Rightarrow a = 1$

Por tanto $K^* = \{1\}$, con lo que $K = \{0, 1\}$, y por tanto no son conjuntos biyectivos (Contradicción).

3. Subgrupos. Generadores. Retículos

3.1. Subgrupos

Definición

Sea G un grupo. Un subgrupo de G es un subconjunto $H \subseteq G,\ \ H \neq \emptyset$ y que verifica:

1. Para cualesquiera $x, y \in H,\ \ xy \in H$.
2. $1 \in H$.
3. Para todo $x \in H,\ \ x^{-1} \in H$.

Por tanto H con el producto en G, tiene también estructura de grupo.
Cuando H sea un subgrupo de G, lo escribiremos de la forma $H \leqslant G$.

Ejemplos

1. Para todo grupo G, el conjunto $\{1\}$ y G son subgrupos de G. Estos subgrupos los llamaremos subgrupos impropios de G. El subgrupo $\{1\}$ se llama el subgrupo trivial de G.

   Los demás subgrupos, si los hay, se llaman subgrupos propios. Si H es un subgrupo propio de $H \Rightarrow \{1\} \leqslant H \leqslant G$.
2. $\mathbb{Q}^* \leqslant \mathbb{R}^* \leqslant \mathbb{C}^*$.
3. $\forall n \geq 1 \qquad \mu_n \leqslant \mathbb{C}^*$.
4. Si $m, n \geq 1$ y $m \mid n \Rightarrow \mu_m \leqslant \mu_n$.

Proposición

Sea G un grupo y $H \subseteq G,\ \ H \neq \emptyset$.
Entonces:

$$H \text{ es un subgrupo de G} \iff \text{Para cualesquiera } x, y \in H, xy^{-1} \in H$$

Demostración

$\Rightarrow$) Es clara.
$\Leftarrow$) Como $H \neq \emptyset$, elegimos $x \in H$. Entonces tomando $y = x$, por hipótesis, $xy^{-1} = xx^{-1} = 1 \in H$ y, por tanto, se tiene 2.
Sea $x \in H$ y consideremos $1 \in H$. Entonces, por hipótesis, $1 \cdot x^{-1} = x^{-1} \in H$. Se tiene así 3.
Sean $x, y \in H \Rightarrow xy^{-1} \in H \Rightarrow^{(\text{hipótesis})} x(y^{-1})^{-1} = xy \in H$ y, por tanto, se tiene 1.

Proposición

Sea G un grupo finito y $H \subseteq G, \;\; H \neq \emptyset$. Entonces:

$$H \text{ es un subgrupo de } G \iff \text{Para cualesquiera } x, y \in H, xy \in H$$

Demostración

$\Rightarrow$) Es clara.
$\Leftarrow$) Por hipótesis se verifica ①.
Sea $x \in H$. Consideramos:

$$x, x^2, x^3, ..., x^n, ...$$

todos son elementos de H, por hipótesis. Puesto que G es finito, podemos asegurar que $\exists n, m, \;\; n \neq m$ tal que $x^n = x^m$. Supongamos $n > m$ y entonces:

$$x^n x^{-m} = x^m x^{-m} = 1$$

Es decir, $x^{n-m} = 1$ y $n - m > 0$, por lo que entonces $1 = x^{n-m} \in H$.
Se tiene entonces ②.
Si $x^{n-m} = 1 \Rightarrow x^{-1} = x^{n-m-1}$ y como $n - m > 0 \Rightarrow n - m - 1 \geq 0$ y así $x^{-1} = x^{n-m-1} \in H$ y se tiene ③.

Ejemplo

① Sea $n \geq 3$. En $D_n = \{1, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\}$ se tiene:

$$C = \{1, r, ..., r^{n-1}\} \leqslant D_n$$

ya que $r^n = 1 = s^2, sr = r^{n-1}s \Rightarrow r^i r^j = r^{\text{res}(i+j;n)} \in C$.

Para cada $0 \leq k \leq n-1$:

$$h_k = \{1, r^k s\} \leqslant D_n$$

$\cdot$	1	$r^k s$
1	1	$r^k s$
$r^k s$	$r^k s$	1

$$r^k s \cdot r^k s = r^k r^{-k} s s = 1$$

El conjunto $X = \{1, s, rs, ..., r^{n-1}s\}$ NO es un subgrupo de D_n porque la operación no es interna en X ($s \cdot rs = srs = r^{n-1}ss = r^{n-1} \notin X$).

② En S_4:

$$K = \{id, \alpha_1 = (1\,2)(3\,4), \alpha_2 = (1\,3)(2\,4), \alpha_3 = (1\,4)(2\,3)\}$$

es un subgrupo de S_4.

$\cdot$	1	α_1	α_2	α_3
1	1	α_1	α_2	α_3
α_1	α_1	α_2	α_3	1
α_2	α_2	α_3	1	α_1
α_3	α_3	1	α_1	α_2

se llama el subgrupo de Klein de S_4.

Proposición

Sea $f : G \to G'$ un homomorfismo de grupos. Entonces:

i) Si $H \leqslant G \Rightarrow f_*(H) \leqslant G'$.
$(f_*(H)) := \{f(x) \mid x \in H\} \subseteq G')$

ii) Si $H' \leqslant G' \Rightarrow f^*(H') \leqslant G$.
$(f^*(H')) := \{x \in H \mid f(x) \in H'\} \subseteq G)$

iii) $Ker(f) := \{x \in G \mid f(x) = 1\} \leqslant G$.
$Img(f) := \{f(x) \mid x \in G\} \leqslant G'$.

iv) f es monomorfismo $\iff Ker(f) = \{1\}$.
f es epimorfismo $\iff Img(f) = G'$.

Demostración

i) $H \leqslant G \Rightarrow f_*(H) \subseteq G'$ y $f_*(H) \neq \emptyset$ pues $H \neq \emptyset$.
Sean $x', y' \in f_*(H) \Rightarrow \exists x, y \in H$ tal que $x' = f(x),\ \ y' = f(y)$.

$$x'(y')^{-1} = f(x)f(y)^{-1} =^{(1)} f(x)f(y^{-1}) = f(xy^{-1}) \in^{(2)} f_*(H)$$

(1) ya que f es homomorfismo.
(2) ya que $x, y \in H \Rightarrow xy^{-1} \in H$.

ii) $H' \leqslant G'$ entones $f^*(H') \subseteq G$ y, como $f(1) = 1 \in H' \Rightarrow 1 \in f^*(H')$, entonces $f^*(H') \neq \emptyset$.
Sean $x, y \in f^*(H') \Rightarrow f(x), f(y) \in H' \Rightarrow^{(3)} f(x)f(y)^{-1} \in H' \Rightarrow f(xy^{-1}) \in H' \Rightarrow xy^{-1} \in f^*(H')$.
(3) ya que $H' \leqslant G'$.

iii) $Ker(f) = f^*(\{1\}) \leqslant G$.
$Img(f) = f_*(G) \leqslant G'$.

iv) Ejercicio.

3.2. Grupos Alternados

Sea $n \geq 2$. Si $(x_1\ x_2\ ...\ x_r)$ es un r-ciclo en S_n, entonces:

$$(x_1\ x_2\ ...\ x_r) = (x_1\ x_2)(x_2\ x_3)...(x_{r-1}\ x_r)$$

Todo ciclo se expresa como producto de transposiciones, pero dicha expresión no es única:

$$(1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4) = (1\ 3)(1\ 2)(3\ 4) = (2\ 4)(1\ 3)(2\ 4)(1\ 2)(3\ 4)$$

Como consecuencia, todo elemento de S_n se expresa como producto de transposiciones ($id = (1\ 2)(1\ 2)$).
Dicha expresión no es única.

Teorema

Sea $n \geq 2$ y $\alpha \in S_n$. Supongamos que:

$$\alpha = \tau_1\tau_2...\tau_s, \quad \tau_i \text{ transposición } \forall i$$

y

$$\alpha = \tau_1'\tau_2'...\tau_r', \quad \tau_j' \text{ transposición } \forall j$$

Entonces $s \equiv r \bmod(2)$.

Demostración

Lo probamos primero para $\alpha = id$. Como:

$$id = (1\ 2)(1\ 2)$$

Entonces basta demostrar que si:

$$(*) \qquad id = \tau_1\tau_2...\tau_r \Rightarrow r \equiv 0 \bmod(2)$$

Hacemos inducción en r.
El primer caso es $r = 2$ y es claro que se verifica.
Supongamos $r > 2$ y el resultado cierto para cualquier expresión de id como producto de menos de r transposiciones.

Elegimos $m \in \{1, 2, ..., n\}$ que aparezca en alguna de las transposiciones $\tau' s$.
Sea τ_j la 1ª en la que aparece m. Será $\tau_j = (m\ x)$.
Aseguramos que $j < r$ porque si $j = r$:

$$id(X) = \tau_1\tau_2...\tau_r(x) = \tau_1\tau_2...\tau_{r-1}(m) =^{(1)} m \neq x$$

(1) pues m no aparece en $\tau_1, ..., \tau_{r-1}$.
Esto es una contradicción. Así $j < r$ y podemos considerar τ_{j+1}:

1. $\tau_j\tau_{j+1} = (m\ x)(m\ x) = id$.
2. $\tau_j\tau_{j+1} = (m\ x)(m\ y) = (x\ y)(m\ x) = \tau_j'\tau_{j+1}'$.

3. $\tau_j\tau_{j+1} = (m\ x)(y\ z) = (y\ z)(m\ x) = \tau'_j\tau'_{j+1}$.
4. $\tau_j\tau_{j+1} = (m\ x)(x\ y) = (x\ y)(m\ y) = \tau'_j\tau'_{j+1}$.

Sustituyendo en la expresión de $id(*)$ obtenemos en el primer caso:

$$id = \tau_1...\tau_{j-1}\tau_{j+2}...\tau_r \Rightarrow r-2 \equiv 0 \bmod(2)$$

y en los otros 3:

$$id = \tau_1...\tau_{j-1}\tau'_j\tau'_{j+1}\tau j+2...\tau_r$$

donde la primera aparición de m se traslada al lugar $j+1$.
Repitiendo el proceso las veces que haga falta y teniendo en cuenta que no puede ser que m aparezca por primera vez en la última transposición, en algún momento nos encontraremos en la situación 1ª. Es decir, en nº finito de pasos, llegamos a que:

$$id = \tau'_1...\tau'_{r-2} \text{ con } \tau'_i \text{ tansposición } \forall i$$

Por hipótesis de inducción, $r-2 \equiv 0 \bmod(2) \Rightarrow r \equiv 0 \bmod(2)$.

Sean:

$$\alpha = \tau_1\tau_2...\tau_r \qquad \tau_i \text{ transposiciones } \forall i$$

$$\alpha = \tau'_1\tau'_2...\tau'_s \qquad \tau'_j \text{ transposiciones } \forall j$$

Entonces:

$$\tau_1\tau_2...\tau_r = \tau'_1\tau'_2...\tau'_s \Rightarrow id = \tau_1\tau_2...\tau_r(\tau'_1\tau'_2...\tau'_s)^{-1} =$$

$$= \tau_1\tau_2..\tau_r(\tau'_s)^{-1}...(\tau'_2)^{-1}(\tau'_1)^{-1} = \tau_1\tau_2...\tau_r\tau'_s...\tau'_2\tau'_1$$

Entonces $r+s \equiv 0 \bmod(2)$.

Definición

Sea $n \geq 2$. Una permutación $\alpha \in S_n$ diremos que es par (respectivamente, impar) si se expresa como un número par de transposiciones (respectivamente, número impar).

Ejemplo

$id \in S_n$ es permutación par.
Cualquier transposición es impar.
$(x_1\ x_2\ x_3) = (x_1\ x_2)(x_2\ x_3)$ es par.
Como $(x_1\ x_2\ ...\ x_r) = (x_1\ x_2)(x_2\ x_3)...(x_{r-1}\ x_r)$, $(x_1\ ...\ x_r)$ es par (respecto a impar) $\iff$ r es impar (respecto a par).

Definición

Sea $n \geq 2$ y $\alpha \in S_n$. Definimos la signatura de α, que denotamos por $s(\alpha)$, como:

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

Proposición

Se tiene:

$$s : S_n \to \mu_2 = \{1, -1\}$$

es un homomorfismo de grupos.

Demostración

Sean $\alpha, \beta \in S_n$. Sea $\alpha = \tau_1\tau_2...\tau_r$ una expresión de α como producto de transposiciones y $\beta = \tau_1'\tau_2'...\tau_s'$ una expresión de β.

Entonces $s(\alpha) = (-1)^r$ y $s(\beta) = (-1)^s$.

$$\alpha\beta = \tau_1\tau_2...\tau_r\tau_1'\tau_2'...\tau_s' \Rightarrow s(\alpha\beta) = (-1)^{r+s}$$

$$s(\alpha\beta) = (-1)^{r+s} = (-1)^r(-1)^s = s(\alpha)s(\beta)$$

Definición

Sea $n \geq 2$. Definimos el n-ésimo grupo alternado, que denotaremos por A_n, como:

$$A_n := \{\alpha \in S_n \mid s(\alpha) = 1\}$$

que es un subgrupo de S_n pues $A_n = Ker(s)$.

Ejemplo

$n = 2$ $S_2 = \{id, (1\ 2)\}$ y $A_2 = \{id\}$.
$n = 3$ $S_3 = \{id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$.
$A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$.
$n = 4$ $A_4 = \{id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4),$
$(2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

Proposición

$\forall n \geq 2$ se verifica que:

$$|A_n| = \frac{n!}{2}$$

Demostración

Consideramos $\tau = (1\ 2) \in S_n$ y sea:

$$(1\ 2)A_n := \{(1\ 2)\alpha \mid \alpha \in A_n\}$$

Es claro que todos los elementos de $(1\ 2)A_n$ son permutaciones impares.
Si $\sigma \in S_n$ es una permutación impar, entonces $\sigma \in (1\ 2)A_n$ porque $\sigma = (1\ 2)(1\ 2)\sigma$ (y $(1\ 2)\sigma \in A_n$).

Consecuentemente el conjunto $(1\ 2)A_n$ es el conjunto de las permutaciones impares de S_n.
Así tenemos:

$$A_n \cup (1\ 2)A_n = S_n \qquad\qquad A_n \cap (1\ 2)A_n = \emptyset$$

$\Rightarrow |S_n| = |A_n| + |(1\ 2)A_n|$

Por otro lado, la aplicación:

$$\lambda : A_n \to (1\ 2)A_n \text{ tal que } \lambda(\alpha) := (1\ 2)\alpha$$

es biyectiva y entones $|A_n| = |(1\ 2)|$.

Tenemos que $|S_n| = |A_n| + |(1\ 2)A_n| = 2|A_n| \Rightarrow |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Definición

Para G un grupo, denotaremos por $Sub(G)$ a la familia de todos los subgrupos de G.

$$Sub(G) = \{H \subseteq G \mid H \text{ es un subgrupo de } G\}$$

Se tiene que $Sub(G)$ es un conjunto ordenado por la inclusión.

$Sub(G)$ es un retículo.

Definición

Un conjunto $(X, \leq)$ ordenado se dice un retículo si $\forall x, y \in X$, existe $\inf\{x, y\}$ y existe el $\sup\{x, y\}$.

Proposición

Sea G un grupo y $\{H_i\}_{i\in I}$ una familia de subgrupos de G. Entonces:

$$\bigcap_{i\in I} H_i \text{ es también un subgrupo de } G$$

Todos los elementos contienen al menos al 1, por lo que no es vacío.

Demostración

Ejercicio.

Corolario

$Sub(G)$ es un retículo.

Demostración

Sean $H_1, H_2 \in Sub(G)$.

- $\text{ínf}\{H_1, H_2\} = H_1 \cap H_2$.
  Si $K \leqslant H_1$ y $K \leqslant H_2 \Rightarrow K \leqslant H_1 \cap H_2$.
- $\sup\{H_1, H_2\} = \bigcap\limits_{K \in Sub(G)} K \in Sub(G)$.

Denotación

Denotaremos $\sup\{H_1, H_2\} = H_1 \vee H_2$.

La unión de subgrupos no es en general un subgrupo. Ejemplo:

$$G = D_3 = \{r, s \mid r^3 = 1 = s^2, sr = r^2 s\} = \{1, r, r^2, r^3, s, rs, r^2 s\}$$

$H_1 = \{1, s\}, H_2 = \{1, rs\}$
$H_1 \cup H_2 = \{1, s, rs\}$ no es un subgrupo de D_3 ($(rs)s = rs^2 = r \notin H_1 \cup H_2$).

$s, rs \in H_1 \vee H_2 \Rightarrow (rs)s = rs^2 = r \in H_1 \vee H_2$.
Si $r, s \in H_1 \vee H_2 \Rightarrow G \leqslant H_1 \cup H_2 \Rightarrow H_1 \cup H_2 = G$.

Notación

Sea G un grupo y X, Y subconjuntos no vacíos de G.
Denotamos por XY al conjunto:

$$XY := \{xy \mid x \in X, y \in Y\}$$

Si $X = \{a\}$ escribiremos $aY = \{ay \mid y \in Y\}$.
Si $Y = \{b\}$ escribiremos $Xb = \{xb \mid x \in X\}$.

Proposición

Sean $H_1, H_2 \in Sub(G)$ tal que

$$H_1 H_2 = H_2 H_1$$

Entonces:

1. $H_1 H_2$ es un subgrupo de G.
2. $H_1 \vee H_2 = H_1 H_2$.

Demostración

$H_1, H_2 \in Sub(G)$ tal que $H_1H_2 = H_2H_1$.

① Sean $x, y \in H_1H_2 \Rightarrow x = h_1h_2, y = h'_1h'_2$ donde $h_1, h'_1 \in H_1, h_2, h'_2 \in H_2$.
$xy^{-1} = h_1h_2(h'_1h'_2)^{-1} = h_1h_2(h'_2)^{-1}(h'_1)^{-1})$.
$\begin{cases} h_2, h'_2 \in H_2 \\ h'_1 \in H_1 \end{cases} \Rightarrow h_2(h'_2)^{-1} \in H_2 \Rightarrow h_2(h'_2)^{-1}(h'_1)^{-1}) \in H_2H_1 = H_1H_2 \Rightarrow \exists k_1 \in H_1, k_2 \in H_2$ tal que $h_2(h'_2)^{-1}(h'_1)^{-1} = k_1k_2$.
Entones:
$$xy^{-1} = h_1k_1k_2 \in H_1H_2$$
Por tanto H_1H_2 es un subgrupo de G.

② $H_1 \leqslant H_1H_2, H_2 \leqslant H_1H_2$
$(h_1 = h_1 \cdot 1 \in H_1H_2)$.
$(h_2 = 1 \cdot h_2 \in H_1H_2)$.
Si $k \in Sub(G)$ tal que $H_1 \leqslant K$ y $H_2 \leqslant L \Rightarrow H_1H_2 \leqslant K$.
Por tanto, $H_1 \vee H_2 = H_1H_2$.

Corolario

Si G es abeliano, entonces $\forall H_1, H_2 \in Sub(G), \quad H_1 \vee H_2 = H_1H_2$.

Ejemplo

En S_4 sean:

$$K = \{id, \alpha_1 = (1\ 2)(3\ 4), \alpha_2 = (1\ 3)(2\ 3)\} \leqslant S_4$$

$$H = \{id, (1\ 2)\} \leqslant S_4$$

$$\begin{aligned} KH = \ & \{id, \alpha_1 = (1\ 2)(3\ 4), \alpha_2 = (1\ 3)(2\ 3), (1\ 2), \alpha_1(1\ 2) = (3\ 4), \\ & \alpha_2(1\ 2) = (1\ 4\ 2\ 3), \alpha_3(1\ 2) = (1\ 3\ 2\ 4)\}. \\ HK = \ & \{id, \alpha_1, \alpha_2, \alpha_3, (1\ 2), (1\ 2)\alpha_1 = (3\ 4), (1\ 2)\alpha_2 = (1\ 3\ 2\ 4), \\ & (1\ 2)\alpha_3 = (1\ 4\ 2\ 3)\}. \end{aligned}$$

$KH = HK \Rightarrow KH \in Sub(G)$ y $K \vee H = KH$.

3.3. Subgrupos cíclicos

Definición

Sea G un grupo y $X \subseteq G, X \neq \emptyset$. Definimos el subgrupo generado por X como el menor subgrupo de G que contiene X. Lo denotaremos por $< X >$ y es claro que:

$$< X > = \bigcap_{K \in Sub(G) | X \subseteq K} K$$

Definición

Sea G un grupo y $X \subseteq G, X \neq \emptyset$ (X subconjunto de G, no necesariamente subgrupo). Una palabra en los elementos de X es una expresión de la forma:

$$x_1^{n_1} x_2^{n_2} ... x_k^{n_k}$$

donde $k \geq 1; n_1, n_2, ..., n_k \in \mathbb{Z}$ y $x_1, x_2, ..., x_k \in X$.

Diremos que dicha palabra es reducida si $x_i \neq x_{i+1}$.

Proposición

Sea G un grupo y $X \subseteq H, X \neq \emptyset$. Entonces:

$$< X >= \{x_1^{n_1} ... x_k^{n_k} \mid x_i \in X, n_1 \in \mathbb{Z}, k \geq 1\}$$

Además, si G es finito, entonces:

$$< X >= \{x_1^{n_1} ... x_k^{n_k} \mid x_i \in X, n_1 \geq 0, k \geq 1\}$$

Demostración

$X \subseteq \{x_1^{n_1} ... x_k^{n_k} \mid x_i \in X, n_1 \in \mathbb{Z}, k \geq 1\} \neq \emptyset$.
Sean x, y dos palabras en los elementos de $X \Rightarrow x = x_1^{n_1} ... x_k^{n_k}$ $y = y_1^{t_1} ... t_s^{t_s}$
$x_i, y_j \in X, n_i, t_j \in \mathbb{Z}, s, k \geq 1 \Rightarrow xy^{-1} = x_1^{n_1} ... x_k^{n_k} (y_1^{t_1} ... y_s^{t_s})^{-1} =$
$= x_1^{n_1} ... x_k^{n_k} y_s^{-t_s} ... y_1^{-t_1}$ que claramente es una palabra en elementos de X.
Se tiene pues que el conjunto de las palabras es un subgrupo de G que claramente es el menor subgrupo de G que contiene a X.

Sea G es finito. El conjunto:

$$\{x_1^{n_1} ... x_k^{n_k} \mid x_i \in X, n_1 \geq 0, k \geq 1\}$$

es cerrado para productos y como G es finito, es un subgrupo de G. Como es el más pequeño que contiene a X, entonces:

$$< X >= \{x_1^{n_1} ... x_k^{n_k} \mid x_i \in K, n_i \geq 0, k \geq 1\}$$

Definición

Sea G un grupo y $X \subseteq G, X \neq \emptyset$. Si $< X >= G$, diremos que X es un conjunto de generadores del grupo G.

Un grupo G diremos que es finitamente generado si $\exists X \subseteq G, X \neq \emptyset, X$ finito tal que $G =< X >$.

Todo grupo finito es finitamente generado.

Si $X = \{a\} \subset G$, al subgrupo generado por X, que denotaremos por $< a >$, lo llamaremos el subgrupo cíclico generado por el elemento a.

$$< a >= \{a^n \mid n \in \mathbb{Z}\} \text{ (siempre es abeliano)}$$

y si G es finito, entonces:

$$< a >= \{a^n \mid n \geq 0\}$$

El grupo G se dice cíclico si $\exists a \in G$ tal que $G =< a >$.

Ejemplos

- $D_n =< r, s > \quad \forall n \geq 3$ es finitamente generado.
- $Q_2 =< i, j >$
  ($Q_2 = \{1, -1, i, -i, j, -j, k, -k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = -1,$
  $ij = k, (-1)a = -a = a(-1)\ a = i, j, k\}$).
- $n \geq 2\ \ S_n =< (i\ j) \mid 1 \leq i < j \leq n >$.
- $\mathbb{Z} =< 1 >=< -1 >$ ya que:

$$< 1 >= \{n \cdot 1 \mid n \in \mathbb{Z}\} = \mathbb{Z}$$

$$< -1 >= \{n \cdot (-1) \mid n \in \mathbb{Z}\} = \mathbb{Z}$$

- $\mathbb{Z} \cdot \mathbb{Z} \quad (a, b) + (a', b') = (a + a', b + b')$

$$\mathbb{Z} \cdot \mathbb{Z} =< (1, 0), (0, 1) >= \{n_1(1, 0) + n_2(0, 1) \mid n_1, n_2 \in \mathbb{Z}\} =$$

$$= \{(n_1, n_2) \mid n_1, n_2 \in \mathbb{Z}\}$$

- $\forall n, \quad \mu_n = \{\xi_k = \cos(\frac{2k\pi}{n}) + i\,\text{sen}(\frac{2k\pi}{n}) \mid 0 \leq k \leq n - 1\}$ es un grupo cíclico generado por $\xi_1 = \cos(\frac{2\pi}{n}) + i\,\text{sen}(\frac{2\pi}{n})$.

$$\mu_n =< \xi_1 >$$

$$\xi_k \xi_r = \xi_{\text{res}(k+r;n)}$$

  Es fácil ver que $\xi_1^k = \xi_k\ \ \forall k = 0, ..., n - 1$.

- $S_n =< (i\ j) \mid 1 \leq i < j \leq n >$
  Se verifica que $S_n =< (1\ 2), (1\ 3), ..., (1\ n) >$ pues para todo $1 \leq i < j \leq n$ se tiene que:

$$(i\ j) = (1\ i)(1\ j)(1\ i)$$

  $S_n =< (i\ j) \mid 1 \leq i < j \leq n > \leqslant < (1\ 2), ..., (1\ n) > \Rightarrow$
  $\Rightarrow S_n =< (1\ 2), (1\ 3), ..., (1\ n) >$

Relación 2: Ejercicio 4

Demostrar que $\mathbb{Z}_7^\times = \{1,2,3,4,5,6\}$ es cíclico.

$$< 2 >= \{2^n \mid n \geq 0\}$$
$$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 1$$
$\forall n \geq 4$ si $n = 3q + r,\ \ 0 \leq r < 2 \Rightarrow 2^n = 2^{3q}2^r = 2^r$
$$< 2 >= \{1,2,4\} \lneq \mathbb{Z}_7^\times$$

$$< 3 >= \{3^n \mid n \geq 0\} = \{1,3,2,6,4,5\} = \mathbb{Z}_7^\times$$
$$3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 2 \quad 3^3 = 6 \quad 3^4 = 4 \quad 3^5 = 5$$

También se verifica:
$$\mathbb{Z}_7^\times =< 5 >$$

Relación 2: Ejercicio 5

Demostrar que:
$$S_n =< (1\ 2), (2\ 3), ..., (n-1\ n) >$$

Se deduce que $\forall i = 2,3,...,n$:

$$(1\ i)(i\ i+1)(1\ i) = (1\ i+1)$$

Entonces por inducción de verifica (demostrar) que:

$$\{(1\ 2), (1\ 3), ..., (1\ n)\} \leqslant< (1\ 2), (2\ 3), ..., (n-1\ n) >$$

Relación 2: Ejercicio 6

Demostrar que:
$$S_n =< \sigma = (1\ 2\ ...\ n), \tau = (1\ 2) >$$

Para todo $i \geq 1$:

$$\sigma(i\ i+1)\sigma^{-1} = (\sigma(i)\ \sigma(i+1)) = (i+1\ i+2)$$

Por inducción, se verifica (demostrar) que:

$$\{(1\ 2), (2\ 3), ..., (n-1\ n)\} \leqslant< \sigma, \tau >$$

Proposición

① Sea G un grupo y sean X, Y subconjuntos de G. Entonces si $H =< X >$ y $K =< Y >$:
$$H \vee K =< X \cup Y >$$

② Sea $f : G \to G'$ un homomorfismo de grupos y sea X un subconjunto de G. Entonces:
$$f_*(< X >) =< f_*(X) >$$
En particular, la imagen directa de un subgrupo cíclico de G es un subgrupo cíclico de G'.

Demostración

Ejercicio.

Ejercicio

Sea $f : G \to G'$ un homomorfismo de grupos y sea X' un subconjunto de G'.
¿Qué relación hay entre $< f^*(X') >$ y $f^*(< X' >)$?

Sea G un grupo y $H \leqslant G$ un subgrupo.

$$< H >= H$$

3.4. Conjuntos cocientes

Definición

Sea G un grupo y $H \leqslant G$ un subgrupo.
Definimos en G dos relaciones binarias asociadas a H como sigue: Dados $x, y \in G$:
$$x \sim_I y \overset{def}{\iff} y^{-1}x \in H$$
$$x \sim_D y \overset{def}{\iff} xy^{-1} \in H$$

Proposición

$\sim_I, \sim_D$ son relaciones de equivalencia en G.

Denotaremos por ${}^G/_H$ al conjunto cociente de G por $\sim_I$.
Denotaremos por ${}^H/_G$ al conjunto cociente de G por $\sim_D$.

$${}^G/_H = \{[x]_i \mid x \in G\} \qquad {}^H/_G = \{[x]_D \mid x \in G\}$$
$$[x]_I := \{y \in G \mid y \sim_I x\} = \{y \in G \mid x^{-1}y \in H\} = xH = \{xh \mid h \in H\}$$

Si $y \in xH$ entonces $\exists h \in H$ tal que $y = xh \Rightarrow x^{-1}y = x^{-1}xh = h \in H \Rightarrow y \in [x]_I$.
Recíprocamente, si $y \in [x]_I \Rightarrow x^{-1}y \in H$ y por tanto, $y = x(x^{-1}y) \in xH$.

$[x]_I = xH$ se llama la clase lateral de x por la izquierda módulo H.
$[x]_D = Hx$ se llama la clase lateral de x por la derecha módulo H.

$$
{}^{G}/_{H} = \{xH \mid x \in G\}
$$
$$
{}^{H}/_{G} = \{Hx \mid x \in G\}
$$

Proposición

1. $x \in xH$ y $x \in Hx$.
2. $xH = yH \iff y^{-1}x \in H$.
   $Hx = Hy \iff xy^{-1} \in H$.
3. $xH \neq yH \iff xH \cap yH = \emptyset$.
   $Hx \neq Hy \iff Hx \cap Hy = \emptyset$.
4. ${}^{G}/_{H}$ es una partición de G.
   ${}^{H}/_{G}$ es una partición de G.
5. Los conjuntos xH y Hx son biyectivos a H, para todo $x \in G$.
6. Existe una biyección entre ${}^{G}/_{H}$ y ${}^{H}/_{G}$.

Demostración

5. $t : H \to xH \qquad t(h) = xh$ es biyectiva.
   $s : H \to Hx \qquad s(h) = hx$ es biyectivo.
6. Sea $\lambda : {}^{G}/_{H} \to {}^{H}/_{G} \quad \lambda(xH) := Hx^{-1}$.
   $xH = yH \iff y^{-1}x \in H \iff (y^{-1}x)^{-1} = x^{-1}y = x^{-1}(y^{-1})^{-1} \in H \iff Hx^{-1} = Hy^{-1}$

Definición

Sea G un grupo finito y H subgrupo de G. Definimos el índice de H en G como el cardinal del conjunto ${}^{G}/_{H}$ (= cardinal de ${}^{H}/_{G}$). Lo denotaremos por $[G : H]$, y así:
$[G : H] =$ nº de clases laterales a izquierda módulo $H =$ nº de clases laterales a derecha módulo H.

Teorema de Lagrange

Sea G un grupo finito y $H \leqslant G$ un subgrupo. Entonces:

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

Demostración

Supongamos $[G : H] = r$ y sea:

$$^{G}/_{H} = \{x_1H, x_2H, ..., x_rH\}$$

Por ④ de la proposición anterior:

$$\begin{cases} G = \bigcup\limits_{i=1}^{r} x_iH \\ x_iH \cap x_jH = \emptyset \quad \forall i \neq j \end{cases} \Rightarrow |G| = \sum_{i=1}^{r} |x_iH| = \sum_{i=1}^{r} |H| =$$

$$= r|H| = [G : H]|H|$$

Ejemplo

$G = S_3$ y $H = A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$.

$$|^{S_3}/_{A_3}| = [S_3 : A_3] = \frac{|S_3|}{|A_3|} = 2$$

$$S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

$$^{S_3}/_{A_3} = \{idA_3 = A_3,$$

$$(1\ 2)A_3 = \{(1\ 2), (1\ 2)(1\ 2\ 3) = (2\ 3), (1\ 2)(1\ 3\ 2) = (1\ 3)\}\}$$

$$^{A_3}/_{S_3} = \{A_3id = A_3,$$

$$A_3(1\ 2) = \{(1\ 2), (1\ 2\ 3)(1\ 2) = (1\ 3), (1\ 3\ 2)(1\ 2) = (2\ 3)\}\}$$

$\forall \alpha \in S_3 \qquad \alpha A_3 = A_3\alpha$
$G = S_3 \qquad H = \{id, (2\ 3)\} \leqslant S_3$

$$|^{S_3}/_{H}| = \frac{|S_3|}{|H|} = \frac{6}{2} = 3$$

$$^{S_3}/_{H} = \{idH = H, (1\ 2)H = \{(1\ 2), (1\ 2)(2\ 3) = (1\ 2\ 3)\}\}$$

$$^{H}/_{S_3} = \{Hid = H, H(1\ 2) = \{(1\ 2), (2\ 3)(1\ 2) = (1\ 2\ 3)\}\}$$

$$H(1\ 3) = \{(1\ 3), (2\ 3)(1\ 3) = (1\ 2\ 3)\}$$

$(1\ 2)H \neq H(1\ 2) \qquad (1\ 3)H \neq H(1\ 3)$.

Corolario

Sea G un grupo finito.
Si H es un subgrupo de $G \Rightarrow |H| \mid |G|$.

En general, no es cierto el recíproco y más adelante veremos algún ejemplo.

3.5. Orden

Definición

Sea G un grupo y $a \in G$.
Definimos el orden de a, que denotaremos por $ord(a)$ como el menor entero positivo n tal que $a^n = 1$.
Si no existe $n > 0$ tal que $a^n = 1$, diremos que a tiene orden infinito y escribiremos $ord(a) = \infty$.

Es claro que si G es un grupo finito entonces todos sus elementos tienen orden finito.
Es claro que $ord(1) = 1$ y de hecho:

$$ord(a) = 1 \iff a = 1$$

Ejemplos

① En $\mathbb{Z}$ el único elemento de orden n es el 0.

② En $\mu_n, \xi_1 = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n}$ tiene orden n.

$$ord(\xi_1) = n$$

③ Si $\alpha = (x_1 \, ... \, x_k) \in S_n$ entonces $ord(\alpha) = k$.

Relación 2: Ejercicio 16

Listar los órdenes de los elementos de Q_2.

$$Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$$

$$\begin{cases} ord(1) = & 1 \\ ord(-1) = & 2 \\ ord(i) = ord(-i) = & 4 \\ ord(j) = ord(-j) = & 4 \\ ord(k) = ord(-k) = & 4 \end{cases}$$

Listar los órdenes de los elementos de D_4:

$$D_4 =< r, s \mid r^4 = 1 = s^2, sr = r^3s >= \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

Orden 1 = $\{1\}$.
Orden 2 = $\{r, r^2, r^3, s, rs, r^2s, r^3s\}$.

Proposición

Sea G un grupo y $a \in G$:

1. Si $ord(a) = n > 0 \Rightarrow < a >= \{1, a, ..., a^{n-1}\}$
2. Si $ord(a) = \infty \Rightarrow < a > \cong \mathbb{Z}$

Demostración

Sabemos que

$$< a >= \{a^k \mid k \in \mathbb{Z}\}$$

1. $ord(a) = n \qquad \{1, a, ..., a^{n-1}\} \subset < a >$
   Dado $k \in \mathbb{Z}, \exists ! q, r, \in \mathbb{Z}$ tal que:

   $$k = nq + r \text{ y } 0 \leq r < n$$

   $a^k = a^{nq}a^r = a^r \in \{1, a, ..., a^{n-1}\}$
   $< a >= \{1, a, ..., a^{n-1}\}$ donde:

   $$a^r a^s = a^{textres(r+s;n)}$$

   En particular:

   $$| < a > | = ord(a)$$

2. $ord(a) = \infty \;\; (\nexists k \in \mathbb{Z}, k \neq 0 \text{ tal que } a^k = 1)$
   Definimos $f : \mathbb{Z} \to < a >= \{a^k \mid k \in \mathbb{Z}\}$

   $$f(k) := a^k$$

   $f(k + k') = a^{k+k'} = a^k a^{k'} = f(k)f(k')$
   f es homomorfismo de grupos, claramente es epimorfismo.
   $ker(f) = \{k \in \mathbb{Z} \mid f(k) = 1\} = \{k \in \mathbb{Z} \mid a^k = 1\} = \{0\}$
   f es también monomorfismo, f es isomorfismo.

Corolario

Sea G un grupo finito y $a \in G$. Entonces $ord(a)$ es un divisor de $|G|$.

$$ord(a) \mid |G|$$

Corolario

Si H y H' son grupos cíclicos finitos y $|H| = |H'| \Rightarrow H \cong H'$

Demostración

$$\begin{cases} H =< a > \\ H' =< b > \end{cases} \Rightarrow \qquad |H| = n = |H'| \Rightarrow ord(a) = n = ord(b)$$

$$\begin{cases} H = \{1, a, ..., a^{n-1}\} \\ H' = \{1, b, ..., b^{n1}\} \end{cases} \Rightarrow H \cong H'$$

Corolario

Hay sólo una clase de isomorfismo de grupos cíclicos de orden n. Un representante es μ_n.

De forma abstracta, representaremos al cíclico de orden n por C_n y escribiremos:

$$C_n =< a \mid a^n = 1 >= \{1, a, ..., a^{n-1}\}$$
$$a^r a^s = a^{textres(r+s;n)}$$

Teorema

Sea G un grupo con $ord(G) = p$, siendo p un número primo. Entonces $G \cong C_p$.
Consecuentemente cualesquiera dos grupos de orden p son isomorfos.

Demostración

$|G| = p \quad p \geq 2$. Elegimos $a \in G, a \neq 1$.
Entonces: $\begin{cases} ord(a) \mid |G| = p \\ a \neq 1 \Rightarrow ord(a) \neq 1 \\ p \text{ primo} \end{cases} \Rightarrow ord(a) = p \Rightarrow |< a >| = p = |G| \Rightarrow < a >= G$

Proposición

Sea $C_n =< x \mid x^n = 1 > \quad n \geq 2$.
$C_n = \{1, x, ..., x^{n-1}\} \quad x^r x^s = x^{\mathrm{res}(r+s;n)}$

1. $x^m = 1 \iff n \mid m$
2. $ord(x^k) = \frac{n}{mcd(n,k)}$
3. x^k es un generador de $C_n \iff mcd(n, k) = 1$
4. El número de generadores distintos de C_n es exactamente $\varphi(n)$, siendo φ la función de Euler.

Demostración

① $\Leftarrow$ Clara.
$\Rightarrow x^m = 1$
Dividimos m entre n: $m = nq + r \quad 0 \leq r < n \Rightarrow$
$$\begin{cases} 1 = x^r \\ 0 \leq r < n \\ ord(x) = n \end{cases} \Rightarrow r = 0 \Rightarrow m = nq$$

② $ord(x^k) = \frac{d}{mcd(n,k)} \qquad d = mcd(n,k), n = dn', k = dk'$
$(x^k)^{n'} = x^{kn'} = x^{dk'n'} = x^{nk'} = 1^{k'} = 1$
Sea $m > 0$ tal que $(x^k)^m = x^{km} = 1 \Rightarrow n \mid km$
$\exists t \in \mathbb{Z}$ tal que $\begin{cases} km = nt \\ dk'm = dn't \end{cases} \Rightarrow k'm = n't \Rightarrow \begin{cases} n0 \mid k'm \\ mdc(n', k') = 1 \end{cases} \Rightarrow$
$\Rightarrow n' \mid m$

③ Consecuencia inmediata de ②.

Definición

$\varphi(n) := card\{1 \leq k \leq n \mid mcd(n,k) = 1\}$

$\varphi(p^e) = p^{e-1}(p-1) \qquad p$ primo.
Si $mcd(n,m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$.
Si $n = p_1^{e_1} ... p_k^{e_k} \Rightarrow \varphi(n) = p_1^{e_1 - 1} ... p_k^{e_k - 1}(p_1 - 1)...(p_k - 1)$

Nota

El orden del producto de dos elementos en general no tiene por qué ser igual al producto de los órdenes.

Relación 2: Ejercicio 17

G grupo, $a, b \in G$ tal que son de orden finito y:

$$ab = ba$$

$$mcd(ord(a), ord(b)) = 1$$

Entonces:

① $< a > \cap < b >= \{1\}$

② $ord(ab) = ord(a)ord(b)$

① $x \in < a > \cap < b > \Rightarrow \begin{cases} x \in < a > \\ x \in < b > \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} ord(x) | ord(< a >) = ord(a) \\ ord(x) | ord(< b >) = ord(b) \end{cases} \Rightarrow ord(x) = 1 \Rightarrow x = 1$

② $ord(a) = n \qquad ord(b) = m$
$(ab)^{nm} =^{(ab=ba)}= a^{nm}b^{nm} = 1 \cdot 1 = 1$
$1 = (ab)^k = a^k b^k \Rightarrow a^k = (b^k)^{-1} \in < a > \cap < b >= \{1\} \Rightarrow$
$\begin{cases} a^k = 1 \Rightarrow n \mid k \\ b^k = 1 \Rightarrow m \mid k \end{cases} \Rightarrow mcm(n, m) = nm \mid k$

Ejemplo

$G = \mathbb{Z}_8^\times = \{1, 3, 5, 7\} \qquad ab = ba$
$\begin{cases} a = 3 \quad ord(a) = 2 \\ b = 5 \quad ord(b) = 2 \end{cases} \Rightarrow mcd(ord(a), ord(b)) = 2 \neq 1$
$ab = 7 \quad ord(7) = 2 \neq ord(3)ord(5) = ord(a)ord(b)$

Teorema

Sea $n \geq 2$ y $\alpha, \beta \in S_n$ dos permutaciones disjuntas. Entonces:

$$ord(\alpha\beta) = mcm(ord(\alpha), ord(\beta))$$

Como consecuencia, si $\alpha \in S_n, \alpha \neq id$ entonces $ord(\alpha) = mcm$ de las longitudes de los ciclos disjuntos en que descompone.

Demostración

$\alpha, \beta \in S_n$ disjuntas.
Veamos que $\forall k \geq 1, \alpha^k$ y β^k también son disjuntas.

En efecto, sea $x \in \{1, 2, ..., n\}$ tal que $\alpha^k(x) \neq x$.
Entonces será $\alpha(x) \neq x \Rightarrow \beta(x) = x \Rightarrow \beta^k(x) = x$.

Sea $r = ord(\alpha), s = ord(\beta)$ y sea $m = mcm(r, s)$:

$$(\alpha\beta)^m = \alpha^m\beta^m = id \cdot id = id$$

Sea k tal que $id = (\alpha\beta)^k = \alpha^k\beta^k$, como α^k y β^k son disjuntas, entonces $\alpha^k = id = \beta^k$.
Pues si $\alpha^k \neq id$, sea x tal que $\alpha^k(x) \neq x \Rightarrow \beta^k(x) = x$:

$$(\alpha^k\beta^k)(x) = \alpha^k(x) \neq x \text{ (Contradicción ya que } \alpha^k\beta^k = id)$$

$\begin{cases} \alpha^k = id \Rightarrow r \mid k \\ \beta^k = id \Rightarrow s \mid k \end{cases} \Rightarrow m = mcm(r, s) \mid k.$

3.6. Ejercicios

Relación 2: Ejercicio 18

$\sigma = (1\ 8\ 10\ 4)(2\ 8)(5\ 1\ 4\ 8) \in S_{15}$
La expresión de G en ciclos dusjuntos es:

$$\sigma = (2\ 10\ 4)(5\ 8)$$

$ord(\sigma) = mcm(3, 2) = 6.$

Relación 2: Ejercicio 20

G un grupo generado por $a, b (a \neq b)$ tal que:

- $ord(a) = 2 = ord(b)$
- $ab = ba$

Entonces $G = \{1, a, b, ab\}$ y G es $\cong$ al grupo de Klein.

$G =< a, b >=^{(ab=ba)}= \{a^r b^s \mid r, s \in \mathbb{Z}\} =^{(ord(a)=ord(b)=2)}=$
$= \{a^r b^s \mid 0 \leq r \leq 1, 0 \leq s \leq 1\} = \{1, a, b, ab\}$

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

$\mu_2 \times \mu_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$
$f : \mu_2 \times \mu_2 \to G$
$(1, 1) \to 1$
$(1, -1) \to a$
$(-1, 1) \to b$
$(-1, -1) \to ab$

$K =< a, b \mid a^2 = 1 = b^2; ab = ba >$ Grupo de Klein.

Relación 2: Ejercicio 23

Resuelto en vídeo (07/04/2021).

Teorema

$C_n =< x \mid x^n = 1 >= \{1, x, ..., x^{n-1}\}, n \geq 2$

① Para cada divisor positivo d de n, $< x^{\frac{n}{d}} > \leqslant C_n$ tiene orden d. Por tanto, $< x^{\frac{n}{d}} >= C_d$.

② Sea $H \leqslant C_n$, $H \neq \{1\}$ y sea:

$$s = \text{mín}\{r \geq 1 \mid x^r \in H\}$$

Entonces s es un divisor de n y $H =< a^s >$

③ Denotemos por $Div(n) = \{d \leq 1 \mid d|n\}$. Entonces la aplicación:

$$Div(n) \to Sub(C_n$$
$$d \mapsto < x^{\frac{n}{d}} >$$

es biyectiva.

④ Sean $d_1, d_2 \in Div(n)$.

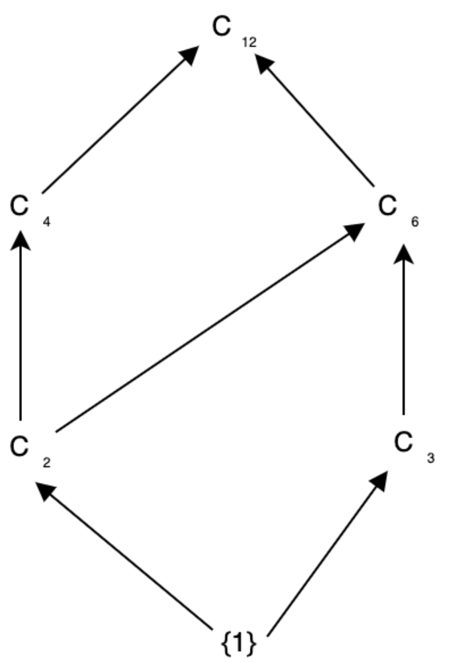
$$d_1 \mid d_2 \iff < x^{\frac{n}{d_1}} > \leqslant < x^{\frac{n}{d_2}} >$$

Ejemplo

$n = 12$ $\qquad$ $C_{12} =< x \mid x^{12} >$

$$Div(12) = \{1, 2, 3, 4, 6, 12\}$$

$Sub(C_{12}) = \{< x^{12} = \{1\}, < x^6 >= C_2, < x^4 >= C_3, < x^3 >= C_4, < x^2 >= C_6, < x >= C_{12}\}$



Demostración

① $d \mid n, d \geq 1, < x^{\frac{n}{d}} >$
Puesto que $ord(x^{\frac{n}{d}}) = \frac{n}{mcd(n,\frac{n}{d})} = \frac{n}{mcd(n,s)} = \frac{n}{s} = d$ (ya que $\frac{n}{d} = s$).
Entonces $| < x^{\frac{n}{d}} > | = d$.
Es decir, $< x^{\frac{n}{d}} >= C_d$.

② $H \leqslant C_n, H \neq 1$
$s = \min\{r \geq 1 \mid x^r \in H\}$
Puesto que $s \in \{r \geq 1 \mid x^r \in H\} \Rightarrow x^s \in H \Rightarrow < x^s > \leqslant H$
Sea $x^m \in H$. Dividimos m entre s, $m = sq + t, 0 \leq t < s$:
$x^m = x^{sq}x^t \Rightarrow x^t = x^m(x^{sq})^{-1} \Rightarrow x^t \in H$ (ya que $x^m \in H, x^{sq} \in H$).
$\begin{cases} x^t \in H \\ 0 \leq t < s & \Rightarrow t = 0 \\ s \text{ es el mínimo de } A \end{cases}$
Entonces $m = sq$ con lo que:

$$x^m = x^{sq} \in < x^s > \Rightarrow H \leqslant < x^s >$$

Por tanto $< x^s >= H$.

Puesto que $x^n = 1 \in H$ entonces $s \mid n$ por el mismo razonamiento anterior. $H =< x^s >, s \mid n \Rightarrow n = sd \Rightarrow s = \frac{n}{d} \Rightarrow H =< x^{\frac{n}{d}} >$.

Relación 2: Ejercicio 28

$Sub(C_{p^n})$ siendo p un número primo y $n \geq 1$.

$$C_{p^n} =< x \mid x^{p^n} = 1 >$$

$Div(p^n) = \{p^k \mid 0 \leq k \leq n\}$
$Sub(C_{p^n}) = \{< x^{p^{n-k}} >= C_{p^k} \mid 0 \leq k \leq n >$

Relación 2: Ejercicio 27

Describir $Sub(S_3)$ y $Sub(D_4)$.

$$S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

Puesto que $|S_3| = 6$ entonces sus posibles subgrupos tendrán orden 1, 2, 3 ó 6.

Orden 1 $\{1\}$
Orden 2 Como todo grupo de orden 2 es cíclico generado por un elemento de orden 2, hay tres subgrupos de orden 2: $C_2 =< (1\ 2) >= \{id, (1\ 2)\}$, $C_2' =< (1\ 3) >= \{id, (1\ 3)\}, C_2'' =< (2\ 3) >= \{id, (2\ 3)\}$.

Orden 3 Como todo grupo de orden 3 es cíclico: $C_3 =< (1\ 2\ 3) >= \{id, (1\ 2\ 3), (1\ 2\ 3)^2 = (1\ 3\ 2)\} =< (1\ 3\ 2) >= \{id, (1\ 3\ 2), (1\ 3\ 2)^2 = (1\ 2\ 3)\}$.

Orden 6 S_3

$$D_4 =< r, s \mid r^4 = 1 = s^2, sr = r^3s >= \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

$|D_4| = 8$ y entonces buscamos subgrupos de orden 1, 2, 4 y 8.

Orden 1 $\{1\}$.

Orden 2 Generados por elementos de orden 2 de D_4.
$C_2 =< r^2 >= \{1, r^2$ $\quad C_2' =< s >= \{1, s\}$ $\quad C_2'' =< r^2s >= \{1, r^2s\}$
$C_2''' =< rs >= \{1, rs\}$ $\quad C_2^{IV} =< r^3s >= \{1, r^3s\}$.

Orden 4 Como los grupos de orden 4 son salvo isomorfismo C_4 o tipo Klein. Los cíclicos de orden 4 son los generados por elementos de orden 4 en D_4, que son r y r^3.
$C_4 =< r >= \{1, r, r^2, r^3\} =< r^3 >$.
Para buscar los subgrupos en D_4 que son tipo Klein, tenemos que buscar dos elementos de orden 2 que conmutan entre sí.
r^2, s tienen orden 2 y $sr^i = r^{-i}s$.
$K = \{1, r^2, s, r^2s\} \leqslant D_4$.
r^2, rs tienen orden 2 y $r^2(rs) = (rs)r^2$.
$K' = \{1, r^2, rs, r^3s\} \leqslant H$.

Orden 8 D_4.

Proposición

Sea $C_n =< x \mid x^n = 1\}$.

1. $< x^m >=< x^{mcd(m,n)} >$.
2. $< x^{m_1}, x^{m_2}, x^{m_3}, ..., x^{m_k} >=< x^{mcd(m_1,m_2,m_3,...,m_k,n)} >$

Demostración

1. Sea $d = mcd(m, n)$, Tendremos que $n = ds$. Sabemos que $\exists!$ subgrupo cíclico de C_n de orden s que es $< x^{\frac{n}{s}} >=< x^d >$.
$$| < x^m > | = ord(x^m) = \frac{n}{mcd(n, m)} = \frac{n}{d} = s$$
Por tanto, $< x^m >=< x^d >$.
2. $H =< x^{m_1}, x^{m_2}, ..., x^{m_k} >\leqslant C_n$
Sea $d = mcd(m_1, m_2, ..., m_k, n)$.
Puesto que $d \mid m_i \Rightarrow x^{mi} \in< x^d > \quad \forall i = 1, ..., k$
Por tanto $H \leqslant< x^d >$.
Por el Teorema de Bezout, $\exists t_1, t_2, ..., t_k, t \in \mathbb{Z}$ tal que:
$$d = m_1t_1 + m_2t_2 + ... + m_kt_k + nt$$

Entonces:
$$x^d = x^{m_1 t_1} x^{m_2 t_2} ... x^{m_k t_k} \in H$$
con lo que $< x^d > \leqslant H$.

4. Grupos cocientes. Teoremas de isomorfía

4.1. Subgrupos normales

Definición

Sea G un grupo y N un subgrupo de G. Diremos que N es un subgrupo normal en G si:

$$aN = Na \qquad \forall a \in G$$

Es decir, las clases laterales a izquierda coinciden con las laterales a derecha.

Si N es normal en G lo indicaremos por $N \trianglelefteq G$.

Ejemplos

① Si G es abeliano, todo subgrupo suyo es normal.

② Para todo G, $\{1\}$ y G son normales.

③ Sea $G = D_4$ y $N =< r >= \{1, r, r^2, r^3\}$
$D_4 =< r, s \mid r^4 = 1 = s^2, sr = r^3 s >$
${}^{D_4}/_{N} = \{N, sN\}$ $\qquad$ ${}^{N}/_{D_4} = \{N, Ns\}$
$sN = \{s, sr, sr^2, sr3\} = \{s, r^3 s, r^2 s, rs\} = Ns$
Por tanto $N \trianglelefteq D_4$.

Sea $H =< s >= \{1, s\} \leqslant D_4$. No es normal en D_4:

$$rH = \{r, rs\} \neq Hr = \{r, sr\} = \{r, r^3 s\}$$

Teorema

Sea G un grupo y $N \leqslant G$. Son equivalentes los siguientes enunciados:

① N es un subgrupo normal en G.

② $aNa^{-1} = N \qquad \forall a \in G$.

③ $aNa^{-1} \leqslant N \qquad \forall a \in H$.

Es decir, N es un subgrupo normal de G si y sólo si coincide a todos sus conjugados ó, si y sólo si contiene a todos sus conjugados.
Para $N \leqslant G$ y $a \in G$, el subgrupo de G:

$$aNa^1 = \{axa^{-1} \mid x \in N\}$$

se llama el subgrupo conjugado de N por el elemento a.

Demostración

① $\Rightarrow$ ② $\Rightarrow$ ③ Es fácil.

③ $\Rightarrow$ ① Sea $a \in G$, tenemos que ver que

$$aN = Na$$

Lo vemos por doble inclusión.
Sea $x \in aN \Rightarrow \exists n \in N$ tal que $x = an$.
Entonces $xa^{-1} = ana^{-1} \in aNa^{-1} \leqslant N \Rightarrow \exists n' \in N$ tal que $x = n'a \in Na$.
Tenemos pues que $aN \leqslant Na$.
Sea $y \in Na \Rightarrow \exists m \in N$ tal que $y = ma$.
Entonces $a^{-1}y = a^{-1}ma \in a^{-1}Na \leqslant N \Rightarrow \exists m' \in N$ tal que $a^{-1}y = m' \Rightarrow y = am' \in aN$.
Por tanto, $Na \leqslant aN$.

Ejemplos

① Sea $f : G \to G'$ un homomorfismo de grupos. $Ker(f) = \{x \in G \mid f(x) = 1\}$.
Sea $a \in G$ y $x \in Ker(f)$:

$$f(axa^{-1}) = f(a)f(x)f(a)^{-1})f(a)f(a)^{-1} = 1 \Rightarrow axa^{-1} \in Ker(f)$$

Luego $aKer(f)a^{-1} \leqslant Ker(f) \quad \forall a \in G$
Entonces $Ker(f) \trianglelefteq G$.

② Sea $G = S_4$ y:

$$K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Sea $\alpha \in S_4$:

$$\alpha(1\ 2)(3\ 4)\alpha^{-1} = \alpha(1\ 2)\alpha^{-1}\alpha(3\ 4)\alpha^{-1} = (\alpha(1)\alpha(2))(\alpha(3)\alpha(4)) \in^{*} K$$

$*$ $\Rightarrow \alpha$ es biyectiva.

Análogamente, por el mismo argumento:

$$\alpha)1\ 3)(2\ 4)\alpha^{-1} \in K, \alpha(1\ 4)(2\ 3) \in K$$

$$\alpha id\alpha^{-1} = id \in K$$

Por tanto, $\alpha K\alpha^{-1} \leqslant K \quad \forall \alpha \in S_4 \Rightarrow K \trianglelefteq S_4$.

Proposición

Sea G un grupo y $X \subset G$ un subconjunto de G no vacío. Sea $N =< X >$.

$$N \trianglelefteq G \iff axa^{-1} \in N \quad \forall a \in G\ \forall x \in X$$

Demostración

$\Leftarrow$ Obvio.
$\Rightarrow$ Sea $a \in G$ y sea:

$$\varphi_a : G \to G \qquad \varphi_a(y) := aya^{-1}$$

Es fácil ver (ejercicio) que φ_a es un homomorfismo de grupos.

$$aNa^{-1} = (\varphi_a)_*(N) = (\varphi_a)_*(< X >) =$$

$$=< (\varphi_a)_*(X) >=< aXa^{-1} >\leqslant N$$

Por tanto $N \trianglelefteq G$.

Proposición

$\forall n \geq 2 \qquad A_n \trianglelefteq S_n$

Demostración

Utilizaremos que A_n está generado por:

$$X = \{(x_1, x_2, x_3) \mid x_1, x_2, x_3 \in \{1, 2, ..., n\}\}$$

Sea $\alpha \in S_n$ y $(x_1\ x_2\ x_3) \in X$, entonces:

$$\alpha(x_1\ x_2\ x_3)\alpha^{-1} = (\alpha(x_1)\alpha(x_2)\alpha(x_3)) \in X \subset A_n$$

Por tanto, $A_n \trianglelefteq S_n$:

$$(x\ y)(z\ t) = (x\ y\ z)(y\ <\ t)$$

$$(x\ y)(y\ z) = (x\ y\ z)$$

Relación 3: Ejercicio 3

Sea G finito y $H \leqslant G$ tal que $[G : H] = 2 \Rightarrow H \trianglelefteq G$.

$[G : H] = 2 \Rightarrow \begin{cases} G/H = \{H, aH\} & a \notin H \\ H/G = \{H, Ha\} \end{cases}$

Como $\begin{cases} G = H \cup aH \\ G = H \cup Ha \end{cases}$ y ambas uniones son disjuntas $\Rightarrow H = H$ y $aH = Ha$.
Entonces $H \trianglelefteq G$.

Por tanto $A_n \trianglelefteq S_n\ \ \forall n \geq 2$ pues $[S_n : A_n] = 2$. También obtenemos que en:

$$D_n =< r, s \mid r^n = 1 = s^2, sr = r^{n-1}s >$$

el grupo $N =< r > \trianglelefteq D_n$ pues $[D_n : N] = \frac{|D_n|}{|N|} = \frac{2n}{n} = 2$.

Relación 3: Ejercicio 4

Describid el retículo de subgrupos de A_4.

$A_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3),$
$(2\ 3\ 4), (2\ 4\ 3)\}$

$|A_4| = 2 \Rightarrow$ Tendrá posiblemente subgrupos en orden 1, 2, 3, 4, 6 ó 12.

$K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq A_4$.

A_4 no tiene subgrupos de orden 6.

Supongamos que $\exists N \leqslant A_4$ tal que $|N| = 6$. Entonces $[A_4 : N] = \frac{|A_4|}{|N|} = \frac{12}{6} = 2 \Rightarrow N \trianglelefteq A_4$.
Como $|N| = 6, N$ ha de contener un ciclo de longitud 3. Supongamos:

$$(1\ 2\ 3) \in N \Rightarrow (1\ 2\ 3) = (1\ 3\ 2) \in N$$

Sea $\alpha = (1\ 2)(3\ 4) \in A_4$, como $N \trianglelefteq A_4$, entonces:

$$\alpha(1\ 2\ 3)\alpha^{-1} = (2\ 1\ 4) = (1\ 4\ 2) \in N \Rightarrow (1\ 4\ 2)^{-1} = (1\ 2\ 4) \in N$$

Sea $\beta = (1\ 3)(2\ 4) \in A_4$, como $N \trianglelefteq A_4$, entonces:

$$\beta(1\ 2\ 3)\beta^{-1} = (3\ 4\ 1) = (1\ 3\ 4) \in N \Rightarrow (1\ 3\ 4)^{-1} = (1\ 4\ 3) \in N$$

Como $id \in N$, pues N es un subgrupo, resulta $|N| \geq 7$ (Contradicción).

Los subgrupos normales de A_4 son $\{1\}, A_4, yK$.
Los de orden 2 y los de orden 3 no son normales en A_4.

$$C_2 = \{id, (1\ 2)(3\ 4)\} \leqslant A_4$$

Sea $\alpha = (1\ 2\ 3)$, entonces:

$$\alpha(1\ 2)(3\ 4)\alpha^{-1} = \alpha(1\ 2)\alpha^{-1}\alpha(3\ 4)\alpha^{-1} = (2\ 3)(1\ 4) = (1\ 4)(2\ 3) \notin C_2$$

$\alpha C_2 \alpha^{-1} \nleqslant C_2 \Rightarrow C_2 \ntrianglelefteq A_4$

$\begin{cases} C_2 \leqslant K \\ K \text{ es abeliano} \end{cases}$ entonces $C_2 \trianglelefteq K$.

4.2. Grupo Cociente

Definición

Sea G un grupo y $N \trianglelefteq G$. Consideramos:

$$G/N = \{aN \mid a \in G\}$$

Definimos en ${}^{G}/_{N}$ la siguiente operación binaria:

$$ {}^{G}/_{N} \times {}^{G}/_{N} \to {}^{G}/_{N} $$

$$ (aN, bN) \mapsto (aN)(bN) := abN $$

Por ser N un subgrupo normal de G, esta operación está bien definida. En efecto:

$$ \begin{cases} aN = a_1 N \\ bN = b_1 N \end{cases} \Rightarrow abN = a_1 b_1 N $$

$aN = a_1 N \iff a_1^{-1} a \in N \iff \exists n \in \mathbb{N}$ tal que $a_1^{-1} a = n \iff a = a_1 n$
$bN = b_1 N \iff \exists m \in N$ tal que $b = b_1 m$.
Entonces $ab = a_1 n b_1 m$.
Como $nb_1 \in Nb_1 = b_1 N \Rightarrow \exists n' \in N$ tal que $nb_1 = b_1 n'$.
Entonces $ab = a_1 n b_1 m = a_1 b_1 n' m \Rightarrow (a_1 b_1)^{-1}(ab) \in N \Rightarrow abN = a_1 b_1 N$.

Resulta que ${}^{G}/_{N}$ con este producto tiene estructura de grupo, con uno dado por $1N = N$ y donde para cada $aN \in {}^{G}/_{N}, (aN)^{-1} = a^{-1}N$.
Este grupo lo llamaremos el grupo cociente de G por N.

Se tiene un epimorfismo de grupos:

$$ p : G \to {}^{G}/_{N} \qquad p(a) := aN $$

que llamaremos la proyección canónica.

Teorema

Sea $f : G \to G'$ un homomorfismo de grupos. Sea $N \trianglelefteq G$ tal que $N \leqslant Ker(f)$, entonces:

① Existe un único homomorfismo:

$$ \bar{f} : {}^{G}/_{N} \to G' $$

tal que $\bar{f}_o p = f$.

$$ \begin{tikzcd} G \arrow[r, "p"] \arrow[dr, "f"'] & G/N \arrow[d, "\bar{f}"] \\ & G' \end{tikzcd} $$

② $\bar{f}$ es epimorfismo $\iff$ f es epimorfismo.

③ $\bar{f}$ es monomorfismo $\iff N = Ker(f)$.

$\bar{f}$ se llama el homomorfismo inducido por f en el grupo cociente ${}^{G}\!/_{N}$.

Demostración

$$f : G \to G'$$
$$N \trianglelefteq G \text{ tal que } N \leqslant Ker(f)$$

① Definimos:

$$\bar{f} : {}^{G}\!/_{N} \to G' \text{ por } \bar{f}(aN) := f(a)$$

Veamos $\bar{f}$ está bien definido:
Si $aN = bN \iff b^{-1}a \in N \Rightarrow b^{-1}a \in Ker(f) \Rightarrow f(b^{-1}a) = f(b^{-1})f(a) = 1 \Rightarrow f(a) = f(b)$.
Es fácil ver que $\bar{f}$ es un homomorfismo así como que $\bar{f}_o p = f$.

Supongamos que $g : {}^{G}\!/_{N} \to G'$ homomorfismo tal que $g_o p = f$.

$$\bar{f} : {}^{G}\!/_{N} \to G'$$

Sea $aN \in {}^{G}\!/_{N}$, entonces:

$$g(aN) = g(p(a)) = (g_o p)(a) = f(a) = \bar{f}(aN)$$

Por tanto, $\bar{f} = g$.

② Puesto que $Img(\bar{f}) = Img(f)$. $\begin{cases} \bar{f} : {}^{G}\!/_{N} \to G' \\ \bar{f}(aN) = f(a) \end{cases}$ entonces $\bar{f}$ es epimorfismo $\iff Img(\bar{f}) = G' \iff Img(f) = G' \iff f$ es epimorfismo.

③ $\bar{f}$ es monomorfimos $\iff N = Ker(f)$.

$\Rightarrow$ Tenemos que ver que $Ker(f) \leqslant N$. Sea $a \in Ker(f) \Rightarrow f(a) = 1$
Como $\bar{f}(aN) = f(a) = 1 \Rightarrow aN \in Ker(\bar{f}) \overset{*}{=} \{N\} \Rightarrow$
$\Rightarrow aN = N \Rightarrow a \in N$
$* \Rightarrow \bar{f}$ es monomorfismo.

$\Leftarrow$ Si $N = Ker(f), \bar{f} : {}^{G}\!/_{N} \to G'$.
Sea $aN \in {}^{G}\!/_{N}$ tal que $\bar{f}(aN) = f(a) = 1$. Entonces:

$$a = Ker(f) = N \Rightarrow aN = N$$

Así pues $Ker(\bar{f}) = \{N\}$ y $\bar{f}$ es monomorfismo.

Corolario: Primer Teorema de Isomorfia

Sea $f : G \to G'$ un homomorfismo de grupos.
Entonces f induce un isomorfismo:

$$^{G}/_{Ker(f)} \equiv Img(f) \qquad aKer(f) \mapsto f(a)$$

Demostración

Consideramos $f : G \to Img(f)$ y aplicamos el teorema anterior a este homomorfismo tomando $N = Ker(f)$.
f induce un homomorfismo:

$$\bar{f} : {}^{G}/_{Ker(f)} \to Img(f) \qquad \bar{f}(aKer(f)) = f(a)$$

$\bar{f}$ es epimorfismo por ②.
Como $N = Ker(f), \bar{f}$ es monomorfismo por ③.

Relación 3: Ejercicio 12

G y H finitos y $mcd(|G|, |H|) = 1$.
Probar que si $f : G \to H$ es un homomorfismo entonces $f(a) = 1 \ \ \forall a \in G$.

$^{G}/_{Ker(f)} \equiv Img(f) \Rightarrow \frac{|G|}{|Ker(f)|} = |^{G}/_{Ker(f)} = |Img(f)| \Rightarrow$
$\Rightarrow |G| = |Ker(f)||Img(f)|$
$\begin{cases} \text{En particular, } |Img(f)| \text{ es divisor de } |G| \\ Img(f) \leqslant H \Rightarrow |Img(f)| \text{ es divisor de } |H| \end{cases} \Rightarrow |Img(f)| = 1 \Rightarrow$
$\Rightarrow Img(f) = \{1\}$
Por tanto $f(a) = 1 \ \ \forall a \in G$

Corolario

Si $f : G \to G'$ es un homomorfismo y G y G' son finitos, entonces:

$$|G| = |Img(f)||Ker(f)|$$

Vamos a estudiar quien es $Sub(^{G}/_{N})$ en relación con $Sub(G)$.

Proposición

Sea G un grupo y $N \trianglelefteq G$. Entonces:

① Si $H \in Sub(G)$ tal que $N \leqslant H$ entones $N \trianglelefteq H$ y $^{H}/_{N} \in Sub(^{G}/_{N})$.

② Si $H_1, H_2 \in Sub(G)$ tal que $N \trianglelefteq H_i \ \ i = 1, 2$, entonces:

$$^{H_i}/_{N} = {}^{H_2}/_{N} \iff H_1 = H_2$$

③ Sea $L \in Sub(^G/_N)$ entonces existe un único $H \in Sub(G)$ tal que $N \trianglelefteq H$ y $L = {}^H/_N$.

$Sub(^G/_N) = \{^H/_N \mid N \trianglelefteq H \leqslant G\}$

Demostración

① Si $aNa^{-1} \leqslant N \ \ \forall a \in G$ entonces $aNa^{-1} \leqslant N \ \ \forall a \in H$ pues $H \leqslant G$, con lo que $N \trianglelefteq H$.
Podemos pues considerar ${}^H/_N \leqslant {}^G/_N$ claramente.
Así ${}^H/_N \in Sub(^G/_N)$.

② $\Leftarrow$ Es obvio.
$\Rightarrow$ $H_1, H_2 \leqslant G$ tal que $N \trianglelefteq H_1 \ \ \forall i = 1, 2$
${}^{H_1}/_N = {}^{H_2}/_N$
Sea $a \in H_1 \Rightarrow aN \in {}^{H_1}/_N = {}^{H_2}/_N \Rightarrow \exists b \in H_2$ tal que $aN = bN \iff b^{-1}a \in N \leqslant H_2$.

$$\begin{cases} b^{-1}a \in H_2 \\ b \in H_2 \end{cases} \Rightarrow a = b(b^{-1}a) \in H_2$$

Tenemos que $H_1 \leqslant H_2$. De la misma forma se demuestra que $H_2 \leqslant H_1$ y entonces $H_1 = H_2$.

③ $L \leqslant {}^G/_N$
Consideramos la proyección canónica:

$$p : G \to {}^G/_N \qquad p(a) = aN$$

$L \leqslant {}^G/_N$ entonces $p^*(L) \leqslant G$.
Sea $H = p^*(L) = \{a \in G \mid p(a) \in L\} = \{a \in G \mid aN \in L\} \leqslant G$. Sea $a \in N \Rightarrow p(a) = aN = N \in L \Rightarrow a \in H$
por tanto $N \leqslant H$.

Veamos que $L = {}^H/_N$.
Es claro que ${}^H/_N \leqslant L$.
Recíprocamente, si $aN \in L \Rightarrow a \in H \Rightarrow aN \in {}^H/_N$, es decir, $L \leqslant {}^H/_N$.
La unicidad es consecuencia de ②.

Segundo Teorema de Isomorfia

Sea G un grupo y $N \trianglelefteq G$.
Sea $H \in Sub(G)$ tal que $N \leqslant H$.
Entonces:

$${}^H/_N \trianglelefteq {}^G/_N \iff H \trianglelefteq G$$

Además en tal caso:

$${}^G/_H \equiv {}^{(G/N)}/_{(H/N)}$$

Demostración

$N \trianglelefteq G$ y $H \leqslant G$ con $N \trianglelefteq H$.

$\Leftarrow$) $H \trianglelefteq G$ y tenemos que ver que $H/N \trianglelefteq G/N$.
Sean $aN \in H/N, xN \in G/N$, es decir, $a \in H$.
$(xN)(aN)(xN)^{-1} = (xax^{-1})N \in H/N$
$\begin{cases} a \in H \\ x \in G \\ H \trianglelefteq G \end{cases} \Rightarrow xHx^{-1} \leqslant H$ y por tanto $xax^{-1} \in H$.
Es decir, $(xN)H/N(xN)^{-1} \leqslant H/N \forall xN \in G/N \Rightarrow H/N \trianglelefteq G/N$.

$\Rightarrow$) Suponemos que $H/N \trianglelefteq G/N$. Consideramos las proyecciones canónicas:

$$G \xrightarrow{p} G/N \xrightarrow{q} (G/N)/(H/N)$$

Sea $f = q_o p : G \to (G/N)/(H/N)$.

$$f(a) = (aN)H/N$$

f es un epimorfismo por ser composición de epimorfismos.

$$Ker(f) = \{a \in G \mid f(a) = H/N\} = \{a \in G \mid (aN)H/N = H/N\} =$$

$$= \{a \in G \mid aN \in H/N\}$$

Veamos que $H = Ker(f)$ por doble inclusión. Es claro que $H \leqslant Ker(f)$. Sea $a \in Ker(f)$ entonces $aN \in H/N \Rightarrow \exists b \in H$ tal que $aN = bN \iff \begin{cases} b^{-1}a \in N \leqslant H \\ b \in H \end{cases} \Rightarrow a = b(b^{-1}a) \in H$.
Por tanto $Ker(f) \leqslant H$.
Consecuentemente, $H = Ker(f) \Rightarrow H \trianglelefteq G$.
Además, aplicando el 1º Teorema de Isomorfia a f:

$$G/Ker(f) \equiv Img(f)$$

es decir,

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

pues f es epimorfimo.

Tercer Teorema de Isomorfia

Sea G un grupo y $N, K \in Sub(G)$ con $N \trianglelefteq G$. Entonces:

(1) KN es un subgrupo de G y $N \trianglelefteq KN$.

(2) $K \cap N \trianglelefteq K$.

(3) Existe un isomorfismo:

$$K/K \cap N \equiv KN/N$$

Demostración

(1) Para demostrar que $KN \leqslant G$, basta con ver que $KN = NK$ y esta igualdad es inmediata puesto que $N \trianglelefteq G$.
Por tanto $KN \in Sub(G)$.
Es claro que $N \leqslant KN (x \in N, x = 1 \cdot x \in KN)$ y $N \trianglelefteq G$, entonces $N \trianglelefteq KN$.

(2) y (3) Consideramos los homomorfismos:

$$K \overset{i}{\hookrightarrow} G \overset{p}{\to} {}^{G}/_{N}$$

y sea $g = p_o i : K \to {}^{G}/_{N}$.

$$g(a) = aN \;\; \forall a \in K$$

$Ker(g) = \{a \in K \mid g(a) = N\} = \{a \in K \mid aN = N\} = \{a \in K \mid a \in N\} = K \cap N$
y entonces $K \cap N \trianglelefteq K$ y tenemos (2).
Además, por el 1º Teorema de Isomorfia aplicada a g:

$$^{K}/_{K \cap N} \equiv Img(g)$$

$Img(g) = \{g(a) \mid a \in K\} = \{aN \mid a \in K\} \overset{?}{=} {}^{KN}/_{N}$
Puesto que $K \leqslant KN$, es claro que $Img(g) \leqslant {}^{KN}/_{N}$.
Recíprocamente, sea $xN \in {}^{KN}/_{N}$ es decir $x \in KN$.
Si $x \in KN \Rightarrow \exists a \in K$ y $\exists b \in N$ tal que $x = ab$.
Entonces:

$$xN = (ab)N = (aN)(bN) \overset{b \in N}{=} (aN)N = aN \overset{a \in K}{\in} Img(g)$$

$^{KN}/_{N} \leqslant Img(g)$

$$^{K}/_{K \cap N} \equiv {}^{KN}/_{N}$$

Relación 3: Ejercicio 14

G un grupo, $N \trianglelefteq G$ tal que N y $^{G}/_{N}$ son abelianos. $H \leqslant G$.
Demostrad que $\exists K \trianglelefteq H$ tal que K y $^{H}/_{K}$ son abelianos.

$G, N, H \in Sub(G), N \trianglelefteq G$.
$N \cap H \trianglelefteq H$ y $^{NH}/_{N} \equiv {}^{H}/_{N \cap H}$ (3º Teorema de Isomorfia).
Tomamos $K = N \cap H \leqslant H$.
Como $K \leqslant N$ y N abeliano $\Rightarrow K$ es abeliano.
Por otro lado $^{H}/_{K} = {}^{H}/_{N \cap K} \equiv {}^{HN}/_{N} \leqslant {}^{G}/_{N}$
Como $^{G}/_{N}$ es abeliano, entonces $^{HN}/_{N}$ es abeliano $\Rightarrow {}^{H}/_{K}$ es abeliano.

Relación 3: Ejercicio 15

G grupo finito, $K, N \in Sub(G)$ con $N \trianglelefteq G$. Suponemos que $|K|$ y $[G : N]$ son primos relativos.
Demostrad que $K \leqslant N$.

Sabemos que

$$^{K}/_{K \cap N} \equiv {}^{KN}/_{N} (3^{\text{o}} \text{ Teorema de Isomorfia})$$

entonces

$$[K : K \cap N] = [KN : N] = r$$

Como

$$^{KN}/_{N} \leqslant {}^{G}/_{N} \Rightarrow r = |^{KN}/_{N}| \mid |^{G}/_{N}| = [G : N]$$

Por otro lado

$$r = [K : K \cap N] = \frac{|K|}{|K \cap N|} \Rightarrow |K| = r \cdot |K \cap N| \Rightarrow r \mid |K|$$

Como $mcd(|K|, [G : N]) = 1$, entonces $r = 1$.
Tenemos entonces $|^{K}/_{K \cap N}| = 1 \Rightarrow K = K \cap N$.

Definición

Sea G un grupo. Se define su centro como:

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

Propiedades

- $Z(G) \trianglelefteq G$ (Relación 3: Ejercicio 6)
- G es abeliano $\iff Z(G) = G$.

Relación 3: Ejercicio 8

Demostrar que $Z(A_3) = A_3$ y $Z(A_n) = \{id\} \ \ \forall n \geq 4$.

$A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\} =< (1\ 2\ 3) >$ es abeliano y entonces $Z(A_3) = A_3$.

Sea $n \geq 4$ y sea $\sigma \in A_n, \sigma \neq id$ entonces $\exists \alpha \in A_n$ tal que $\sigma\alpha \neq \alpha\sigma$.
Si $\sigma \neq id$ entonces $\exists i, j \in \{1, 2, ..., n\}$ tal que $\sigma(i) = j$ siendo $j \neq i$.
Elegimos $k, l \in \{1, 2, ..., n\}$ tal que $k \neq l$ y $\{k, e\} \cap \{i, j\} \neq \emptyset$ (odemos elegirlos porque $n \geq 4$).
Sea $\alpha = (k\ k\ l) \in A_n$

$$\begin{cases} \sigma\alpha(i) = \sigma(i) = j \\ \alpha\sigma(i) = \alpha(j) = k \end{cases} \Rightarrow \sigma\alpha(i) \neq \alpha\sigma(i) \Rightarrow \sigma\alpha \neq \alpha\sigma \Rightarrow \sigma \notin Z(A_n)$$

Consecuentemente $Z(A_n) = \{id\} \ \ \forall n \geq 4$

Relación 3: Ejercicio 9

Demostrar que:

a) $Z(D_n) = \{1, r^m\}$ si $n = 2m$

b) $Z(D_n) = \{1\}$ si $n = 2m + 1$

a) $n = 2m$
$D_n =< r, s \mid r^n = 1 = s^2, sr = r^{-1}s >= \{1, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\}$
Observamos primero que $r^k s \notin Z(D_n) \forall k = 0, ..., n-1$

$$r(r^k s) = r^{k+1}s \qquad (r^k s)r = r^k r^{-1}s = r^{k-1}s$$

$r^{k+1}s = r^{k-1}s \iff r^{k+1} = r^{k-1} \iff r = r^{-1} \iff r^2 = 1 \iff$
$ord(r) = 2 \neq n$ (Contradicción)

$$r(r^k s) \neq (r^k s)r \Rightarrow r^k s \notin Z(D_n) \forall k = 0, ..., n-1$$

Obviamente $r^k r^j = r^j r^k \ \ \forall j = 0, ..., n-1$.
Por tanto decir que $r^k \in Z(D_n)$ es decir

$$r^k(r^j s) = (r^j s)r^k \iff r^{k+j}s = r^j r^{-k}s = r^{j-k}s \iff$$

$$\iff r^{k+j} = r^{j-k} \ \ \forall j \iff r^k = r^{-k} \iff (r^k)^2 = 1 \iff$$

$$\iff ord(r^k) = 2$$

Sabemos que $ord(r^k) = \frac{n}{mcd(n,k)}$

$$r^k \in Z(D_n) \iff \frac{n}{mcd(n,k)} = 2 \iff n = 2mcd(n,k)$$

Como $n = 2m$

$$2m = 2mcd(2m,k) \iff m = mcd(2m,k) \iff k = m$$

$$Z(D_{2m}) = \{1, r^m\}$$

Definición

Sea G un grupo. Un automorfismo de G es un isomorfismo $f : G \to G$

$$Aut(G) = \{f : G \to G \mid f \text{ es automorfismo}\}$$

$Aut(G)$ con la composición es un grupo.

Relación 3: Ejercicio 18

Sea $n \geq 2$ y $C_n =< x \mid x^n = 1 >= \{1, x, ..., x^{n-1}\}$.
Sea G un grupo arbitrario. Demostrar que:

(1) Si $\theta : C_n \to G$ es un homomorfismo de grupo con $\theta(x) = g(g \in G)$ entonces

$$ord(g) \mid n \text{ y } \theta(x^k) = g^k \;\; \forall k = 0, ..., n-1$$

Puesto que θ es un homomorfismo

$$1 = \theta(1) = \theta(x^n) = \theta(x)^n = g^n$$

Por tanto g es un elemento de G de orden finito y además, $ord(g) \mid n$.

(2) Demostrar que para cada $g \in G$ tal que $ord(g) \mid n$ existe un único homomorfismo de grupos.

$$\theta_g : C_n \to G \text{ tal que } \theta_g(x) = g$$

Definimos $\theta_g : C_n \to G$ por $\theta_g(x^k) := g^k \;\; k = 0, ..., n-1$.
Veamos que θ_g es un homomorfismo.

$x^k, x^r \in C_n$ hemos de ver que $\theta_g(x^k \cdot x^r) = \theta_g(x^k)\theta_g(x^r)$

$$\theta_g(x^k \cdot x^r) = \theta_g(x^{\text{res}(k+r;n)}) = g^{\text{res}(k+r;n)} = g^s$$

donde $s = \text{res}(k + r; n)$.
Sea $ord(g) = t$

$$\theta_g(x^k) \cdot \theta_g(x^r) = g^k \cdot g^r = g^{\text{res}(x+r;t)}$$

$s = tq + h \quad h = \text{res}(s; t) \quad 0 \leq h \leq t - 1$
$s = \text{res}(k + r; n)$ entonces $k + r = nq' + s \quad 0 \leq s \leq n - 1$
Como $ord(g) = t \mid n \Rightarrow n = tq''$.
$k + r = nq' + s = tq''q' + s = tq''q' + tq + h = t(q''q' + q) + h$ con $0 \leq h \leq t - 1 \Rightarrow \text{res}(k + r; t) = h = \text{res}(s; t)$

Entonces $\theta_g(x^k x^r) = \theta_g(x^k)\theta_g(x^r)$.

La unidad es consecuencia de (1).

(3) Sea $g \in G$ tal que $ord(g) \mid n$. Demostrar que $\theta_g : C_n \to G$ es monomorfismo $\iff ord(g) = n$.

$$\theta_g : C_n \to G \;\; \theta_g(x^k) = g^k \;\; \forall k$$

$\Rightarrow$) Suponemos que θ_g es monomorfismo $\Rightarrow Ker(\theta_g) = \{1\}$.
Sea $t = ord(g)$, entonces $g^t = 1$.
Entonces:

$$1 = g^t = \theta(x^t) \Rightarrow x^t \in Ker(\theta_g) = \{1\} \Rightarrow x^t = 1 \overset{ord(x)=n}{\Rightarrow} n \mid t$$

Como $t \mid n \Rightarrow n = t$.

$\Leftarrow)$ $ord(g) = n \quad \theta_g : C_n \to G, \theta_g(x^k) = g^k$

Sea $x^k \in Ker(\theta_g) \Rightarrow \theta_g(x^k) = g^k = 1 \Rightarrow \begin{cases} n \mid k \\ 0 \leq k \leq n-1 \end{cases} \Rightarrow$

$\Rightarrow k = 0$, es decir, $x^k = 1$.

Por tanto $Ker(\theta_g) = \{1\} \Rightarrow \theta_g$ es monomorfismo.

(4) Demostrar que existe un isomorfismo

$$U(\mathbb{Z}_n) \equiv Aut(C_n)$$

dado por $r \mapsto f_\sigma : C_n \to C_n, f_r(x) = x^r$.

En particular $Aut(C_n)$ es abeliano y tiene $\varphi(n)$ elementos (φ función de Euler).

$$U(\mathbb{Z}_n) = \{r \mid 1 \leq r \leq n-1 \text{ y } mcd(n,r) = 1\}$$

Entonces para $r \in U(\mathbb{Z}_n), x^r$ es un generador de C_n pues $ord(x^r) = \frac{n}{mcd(n,r)} = \frac{n}{1} = n$.

Por (2) $f_r : C_n \to C_n, f_r(x) = x^r (f_r(x^k = x^{kr})$ y (3), es un monomofrismo.

Como $Img(f_r) =< f_r(x) >=< x^r >= C_n$, entonces f_r también es epimorfismo.

Tenemos pues una aplicación

$$f : U(\mathbb{Z}_{\ltimes} \to Aut(C_n), r \mapsto f_r$$

f es un homomorfismo de grupos.

$$f(rs) = f_{rs} : C_n \to C_n$$

$$f(r)_o f(s) = f_r o f_s : C_n \to C_n$$

$$(f_r o f_s)(x) = f_r(x^s) = x^{rs} = x^{\text{res}(rs;n)}$$

$$f(rs)(x) = f(\text{res}(rs;n))(x) = x^{\text{res}(rs;n)}$$

Por (1) y (2) es fácil ver que f es isomorfismo.

Relación 3: Ejercicio 19

$Aut(C_8)$, demostrar que es isomorfo al grupo de Klein.

$$\{f_1, f_3, f_5, f_7\} = Aut(C_8) \equiv U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$$

$$f_k : C_8 \to C_8 \quad f_k(x) = x^k \quad k = 1, 3, 5, 7$$

Para $k = 1, f_1 = id$.

f_3, f_5, f_7 tienen orden 2.

$$(f_3^2)(x) = f_3(f_3(x)) = f_3(x^3) = (x^3)^3 = x^9 = x \Rightarrow f_3^2 = id \Rightarrow ord(f_3) = 2$$

$$ord(f_5) = 2 = ord(f_7)$$

Relación 3: Ejercicio 20

Vídeo del 21/04/2021.

4.3. Producto directo de grupos

Definición

Sean $G_1, G_2, ..., G_n (n \geq 2)$ grupos. Definimos su producto directo como el grupo cuyos elementos son los del producto cartesiano:

$$\prod_{i=1}^{n} G_i = G_1 \times ... \times G_n = \{(x_1, x_2, ..., x_n) \mid x_i \in G_i, i = 1, ..., n\}$$

y con operación definida como sigue

$$(x_1, ..., x_n) \cdot (y_1, ..., y_n) := (x_1 y_1, x_2 y_2, ..., x_n y_n)$$

Es fácil ver que en efecto $\prod_{i=1}^{n} G_i$ es un grupo con uno la n-tupla $(1, 1, ..., 1)$ y donde:

$$(x_1, x_2, ..., x_n)^{-1} = (x_1^{-1}, x_2^{-1}, ..., x_n^{-1})$$

Se tiene para cada $k = 1, ..., n$ homomorfismo

$$p_k : \prod_{i=1}^{n} G_i \to G_k \qquad p_k(x_1, x_2, ..., x_n) = x_k$$

que se llama la proyección k-ésima. También se tiene un homomorfismo.

$$j_k : G_k \to \prod_{i=1}^{n} G_i \qquad j_j(x_k) = (1, ..., x_k, ..., 1)$$

que se llama la inyección k-ésima.

Es claro que las proyecciones son epimorfismos y las inyecciones son monomorfismos.

Además se verifica:

- $G_k \equiv Img(j_k) \;\; \forall k = 1, ..., n$
- $Img(j_k) \trianglelefteq \prod_{i=1}^{n} G_i \;\; \forall k = 1, ..., n$.
  Así, G_k es isomorfo a un subgrupo normal del producto directo.
- Sea dado $H_k \in Sub(G_k)$ para $k = 1, ..., n$.
  Entonces $\prod_{k=1}^{n} H_k$ es un subgrupo de $\prod_{k=1}^{n} G_k$.

Proposición

Sean $G_1, G_2, ..., G_n$ grupos finitos. Entonces:

(1) $\prod_{i=1}^n G_i$ es también finito y
$$|\prod_{i=1} PnG_i| = \prod_{i=1}^{n} |G_i|$$

(2) Sea $(x_1, x_2, ..., x_n) \in \prod_{i=1}^n G_i$, entonces
$$ord((x_1, x_2, ..., x_n)) = mcm(ord(x_1), ord(x_2), ..., ord(x_n))$$
Supongamos que $mcd(|G_i|, |G_j|) = 1 \ \ \forall i \neq j$.

(3) Si cada G_i es cíclico entonces $\prod_{i=1}^n G_i$ es cíclico.

(4) Si $L \leqslant \prod_{i=1}^n G_i$ entonces existen $H_1 \leqslant G_1, H_2 \leqslant G_2, ..., H_n \leqslant G_n$ tal que
$$L = \prod_{i=1}^{n} H_i$$

Demostración

(2) $(x_1, x_2, ..., x_n) \in \prod_{i=1}^n G_i$ y sea $t_i = ord(x_i), i = 1, ..., n$
Sea $t = mcm(t_1, t_2, ..., t_n)$
$$(x_1, x_2, ..., x_n)^t = (x_1^t, x_2^t, ..., x_n^t) = (1, 1, ..., 1)$$
Sea $m \geq 1$ tal que
$$(x_1^m, x_2^m, ..., x_n^m) = (x_1, x_2, ..., x_n)^m = (1, 1, ..., 1) \Rightarrow$$
$$\Rightarrow x_i^m = 1 \ \ \forall i = 1, ..., n, ord(x_i) = t_i \Rightarrow \begin{cases} t_i \mid m \ \ \forall i = 1, ..., n \\ t = mcm(t_1, ..., t_n) \end{cases} \Rightarrow$$
$\Rightarrow t \mid m$
$ord((x_1, x_2, ..., x_n)) = mcm(ord(x_1), ..., ord(x_n))$.

(3) $mcd(|G_i|, |G_j|) = 1 \quad \forall i \neq j$
Supongamos que $G_i =< a_i > \quad i = 1, ..., n$
Consideramos el elemento
$$a = (a_1, a_2, ..., a_n) \in \prod_{i=1}^{n} G_i$$
Por (2)
$$ord(a) = mcm(ord(a_1), ord(a_2), ..., ord(a_n)) =$$
$$= mcm(|G_1|, |G_2|, ..., |G_n|) \overset{mcd(|G_i|,|G_j|)=1}{=} |G_1||G_2|...|G_n|$$
Entonces $< a >= \prod_{i=1}^n G_i$ y entonces cíclico.

(4) $mcd(|G_i|, |G_j|) = 1 \;\; \forall i \neq j$
Hacemos inducción en n.
Caso $n = 2$: $L \leqslant G_1 \times G_2$.
Queremos buscar $H_1 \leqslant G_1, H_2 \leqslant G_2$ tal que $L = H_1 \times H_2$.

$$p_1 : G_1 \times G_2 \to G_1, (x_1, x_2) \mapsto x_1$$

$$p_2 : G_1 \times G_2 \to G_2, (x_1, x_2) \mapsto x_2$$

Sea $H_1 = (p_1)_*(L) \leqslant G_1, H_2 = (p_2)_*(L) \leqslant G_2$.
Sea $(x_1, x_2) \in L \Rightarrow \begin{cases} p_1(x_1, x_2) = x_1 \in (p_1)_*(L) = H_1 \\ p_2(x_1, x_2) = x_2 \in (p_2)_*(L) = H_2 \end{cases} \Rightarrow (x_1, x_2) \in$
$H_1 \times H_2$
Por tanto $L \leqslant H_1 \times H_2$.
Recíprocamente, $r = |G_1|, s = |G_2|$
$mcd(r, s) = 1$, elegimos $a, b \in \mathbb{Z}$ tal que

$$1 = ar + bs$$

Sea $x_1 \in H_1 = (p_1)_*(L)$ entonces $\exists y_2 \in G_2$ tal que $(x_1, y_2) \in L$

$$(x_1, y_2) \in L \Rightarrow (x_1, y_2)^{bs} \in L$$

$(x_1, y_2)^{bs} = (x_1^{bs}, y_2^{bs}) = (x_1^{bs}, 1) = (x_1^{1-ar}, 1)$

$$y \in G_2 \Rightarrow ord(y_2) \mid |G_2| = s$$

$= (x_1^1 \cdot x_1^{-ar}, 1) = (x_1, 1)$

$$x_1 \in G_1 \Rightarrow ord(x_1 \mid |G_1| = r$$

Así si $x_1 \in H_1 \Rightarrow (x_1, 1) \in L, x_2 \in H_2 \Rightarrow (1, x_2) \in L$.
Sea $(x_1, x_2) \in H_1 \times H_2 \Rightarrow x_1 \in H_1$ y $x_2 \in H_2 \Rightarrow (x_1, 1), (1, x_2) \in L \Rightarrow$
$(x_1, 1)(1, x_2) = (x_1, x_2) \in L$.
Así $L = H_1 \times H_2$.
Sea $n > 2$, y el resultado cierto para $n - 1$.
Sea $L \leqslant \prod_{i=1}^{n} G_i = (\prod_{i=1}^{n-1} G_i) \times G_n$
como $mcd(|\prod_{i=1}^{n-1} G_i| = \prod_{i=1}^{n-1} |G_i|, |G_n|) = 1$, por el caso anterior $\exists K \leqslant \prod_{i=1}^{n} G_i$ y $\exists H_n \leqslant G_n$ tal que $L = K \times H_n$.
Por hipótesis de inducción, si $K \leqslant \prod_{i=1}^{n-1} G_i, \exists H_i \leqslant G_i, i = 1, ..., n-1$ tal que

$$K = H_1 \times ... \times H_{n-1}$$

Combinando, obtenemos que

$$L = H_1 \times ... \times H_n$$

Corolario

Sean $n, m \geq 1$.

$$C_n \times C_m \equiv C_{nm} \iff mcd(n,m) = 1$$

Supongamos dado un grupo G y dados

$$H_1, H_2, ..., H_n \in Sub(G)$$

Consideramos $H_1 \times H_2 \times ... \times H_n$. Tenemos una aplicación:

$$\phi : H_1 \times H_2 \times ... \times H_n \to G$$

$$\phi((x_1, x_2, ..., x_n)) := x_1 x_2 ... x_n$$

Se verifica:

Proposición

$$\phi \text{ es un isomorfismo } \iff \begin{cases} (a) \quad H_i \trianglelefteq G \;\; \forall i = 1, ..., n \\ (b) \quad H_1 H_2 ... H_n = G \\ (c) \quad (H_1 ... H_{i-1}) \cap H_i = \{1\} \;\; \forall i = 2, ..., n-1 \end{cases}$$

En estas condiciones se dice que el grupo es producto directo interno de los subgrupos $H_1, H_2, ..., H_n$.

Demostración

$\Rightarrow$) $\phi : H_1 \times ... \times H_n \to G, \qquad \phi(x_1 ... x_n) = x_1 x_2 ... x_n$ es isomorfismo.
En particular es epimorfismo y entonces:

$$Img(\phi) = H_1 H_2 ... H_n = G$$

y se tiene (b).
Entonces como para cada $k = 1, ..., n$.

$$Img(j_k) \leqslant \prod_{i=1}^{n} H_i \Rightarrow \phi_*(Img(j_k)) = H_k \leqslant Img(\phi) = G$$

$j_j : H_k \to \prod_{i=1}^{n} H_i$ la k-ésima inyección canónica. Por tanto se tiene (a).
Veamos (c). Sea $x \in (H_1 ... H_{i-1}) \cap H_i \;\; 2 \leq i \leq n-1$.
Como $x \in H_1 H_2 ... H_{i-1}$, existirán $h_1 \in H_1, ..., h_{i-1} \in H_{i-1}$ tal que $x = h_1 ... h_{i-1}$.
Entonces $x = \phi((h_1, h_2, ..., h_{i-1}, 1, ..., 1))$.
Como $x \in H_i$, podemos considerar el elemento $(1, 1, ..., 1, \overset{i}{x}, 1, ..., 1) \in$

$H_1 \times H_2 \times ... \times H_n$ y $\phi((1,...,1,x,1,...,1)) = x$. Entones como ϕ es monomorfismo, tendremos que:

$$(h_1, h_2, ..., h_{i-1}, 1, ..., 1) = (1, ..., 1, \overset{i}{x}, 1, ..., 1) \Rightarrow h_i = 1 \ \forall i \text{ y } x = 1$$

Tenemos que $(H_1...H_{i-1}) \cap H_i = \{1\} \qquad 2 \leq i \leq n$.

$\Leftarrow)$ Suponemos que se verifican $(a),(b)$ y $(c) \overset{?}{\Rightarrow} \phi : H_1 \times ... \times H_n \to G \ \ \phi(h_1, h_2, ..., h_n) = h_1 h_2 ... h_n$ es isomorfismo.
Primero veamos que $\forall i \neq j$, los elementos de H_i conmutan con los elementos de H_j.
Supongamos $i < j$ y sean $h_i \in H_i, h_j \in H_j$.
Consideramos el elemento $a = h_i h_j h_i^{-1} h_j^{-1} \in G$.

Como $H_i \trianglelefteq G$ entonces $\begin{cases} h_j h_i^{-1} h_j^{-1} \in H_i \\ h_i \in H_i \end{cases} \Rightarrow a \in H_i$.

Como $H_j \trianglelefteq G$ entonces $\begin{cases} h_i h_j h_i^{-1} \in H_j \\ h_j^{-1} \in H_j \end{cases} \Rightarrow a \in H_j$.

Por tanto $\begin{cases} a \in H_i \cap H_j \\ i < j \Rightarrow H_i \leqslant H_1 H_2 ... H_{j-1} \end{cases} \Rightarrow a \in (H_1 H_2 ... H_{j-1} \cap H_j$

Entonces utilizando la condición $(c), (a) = 1$. Es decir:

$$h_i h_j h_i^{-1} h_j^{-1} = 1 \Rightarrow h_i h_j = h_j h_i$$

Veamos primero que ϕ es homomorfismo.
$\phi((h_1, h_2, ..., h_n \cdot (k_1, k_2, ..., k_n)) = \phi((h_1 k_1, h_2 k_2, ..., h_n k_n)) =$
$= h_1 k_1 h_2 k_2 ... h_n k_n = h_1 h_2 k_1 k_2 h_3 k_3 ... h_n k_n = h_1 h_2 h_3 k_1 k_2 k_3 ... h_n k_n =$
$= ... = h_1 h_2 ... h_n k_1 k_2 ... k_n = \phi((h_1, ..., h_n)) \cdot \phi((k_1, ..., k_n))$
Por definición de ϕ:

$$Img(\phi) = H_1 H_2 ... H_n \overset{(b)}{=} G \Rightarrow \phi \text{ es epimorfismo}$$

Sea $(h_1, h_2, ..., h_n) \in Ker(\phi) \Rightarrow \phi((h_1, ..., h_n)) = 1$, es decir,
$h_1 h_2 ... h_n = 1 \Rightarrow h_1 h_2 ... h_{n-1} = h_n^{-1} \in (H_1..Hn-1) \cap H_n \overset{(c)}{=} \{1\} \Rightarrow h_n = 1$.
$h_1 h_2 ... hn - 1 = 1 \Rightarrow h_1 h_2 ... h_{n-2} = h_{n-1}^{-1} \in (H_1 ... H_{n-2}) \cap H_{n-1} \overset{(c)}{=} \{1\}$.
En un número finito de pasos llegamos a que $h_1 = h_2 = ... = h_n = 1$, es decir, $(h_1, h_2, ..., h_n) = (1, 1, ..., 1)$ y ϕ es monomorfismo.

Ejercicio

Sea $f : G \to G'$ un homomorfismo de grupos y $N \trianglelefteq G$. Demostrad que $f_*(N) \trianglelefteq Img(f)$.

Ejercicio

Sean $H, K \in Sub(G)$. Probar que $H \subset HK, K \subset HK$.

Relación 3: Ejercicios 21, 26 y 27

Vídeo del 26/04/2021.

5. Grupos resolubles

Definición

Sea G un grupo. Una de cadena de subgrupos de G en la forma:

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_{n-1} \trianglelefteq H_n = H$$

la llamaremos una serie normal de G.

Cada H_i se llama término i-ésimo de la serie $i = 0, ..., n$.
Cada H_i/H_{i-1} se llama factor i-ésimo de la serie $i = 1, ..., n$.

La serie se dice propia si $H_{i-1} \underset{\neq}{\trianglelefteq} H_i \ \forall i = 1, ..., n$ (es decir, todas las inclusiones son propias). En tal caso diremos que la serie tiene longitud n.

Definición

Dadas dos series:

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_{n-1} \trianglelefteq H_n = G \quad (1)$$

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq ... \trianglelefteq K_{m-1} \trianglelefteq K_m = G \quad (2)$$

Diremos que la serie (2) es un refinamiento de la serie (1) si:

(I) $n \leq m$.

(II) Para cada $j \in \{0, ..., n\}$ existe un $k \in \{0, ..., m\}$ tal que $H_j = K_r$.
(Es decir, todos los grupos de la serie (1) aparecen en la serie (2)).

Si $n \lneq m$ (es decir, la serie (2) tiene más grupos que la serie (1)) diremos que el refinamiento es propio.

Ejemplo

$G = S_4$
Son series normales propias de S_4:

- $\{id\} \trianglelefteq A_4 \trianglelefteq S_4$.
- $\{id\} \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$
  $K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$.
- $\{id\} \trianglelefteq C_2 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$
  $C_2 =< (1\ 2)(3\ 4) >= \{id, (1\ 2)(3\ 4)\}$.

La 3ª es un refinamiento propio de la 1ª y la 2ª.
La 2ª es un refinamiento propio de la 1ª.
La 1ª tiene longitud 2, la 2ª longitud 3 y la 3ª tiene longitud 4.

Nota

En una serie normal de un grupo G

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

H_{i-1} es normal en H_i, pero no tiene por qué ser normal en H_j para $j \geq i+1$.

Definición

Sea G un grupo. Una serie normal propia de G que no admite refinamientos propios la llamaremos una serie de composición de G.
A los factores de una serie de composición los llamaremos factores de composición de G.

Nota

No todo grupo tiene series de composición.

Por ejemplo, $\mathbb{Z}$ no tiene series de composición porque cualquier serie normal propia de $\mathbb{Z}$ puede refinarse propiamente.
En efecto sea

$$\{0\} = H_0 \underset{\neq}{\trianglelefteq} H_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_n = \mathbb{Z}$$

Si $n = 1, \{0\} = H_0 \underset{\neq}{\trianglelefteq} H_1 = \mathbb{Z}$, consideramos $K = m\mathbb{Z}, m \geq 2$, entonces

$$\{0\} = H_0 \underset{\neq}{\trianglelefteq} K \underset{\neq}{\trianglelefteq} H_1 = \mathbb{Z}$$

es un refinamiento propio de la serie.

Si $n > 1$ entonces $H_1 \underset{\neq}{\trianglelefteq} \mathbb{Z}, H_1 \underset{\neq}{\trianglelefteq} \{0\}$ entonces $H_1 = m\mathbb{Z}$ para $m \geq 2$.
Consideramos $K = 2m\mathbb{Z}$, entonces:

$$\{0\} = H_0 \underset{\neq}{\trianglelefteq} K \underset{\neq}{\trianglelefteq} H_1 \underset{\neq}{\trianglelefteq} H_2 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_n = \mathbb{Z}$$

es un refinamiento de la serie dada.

Definición

Un grupo G diremos que es simple si no es trivial y no admite subgrupos normales propios ó, en otros términos, sus únicos subgrupos normales son $\{1\}$ y G.

En el caso abeliano se tiene:

Proposición

Sea G un grupo abeliano.
G es simple $\iff$ G es finito de orden un número primo.

Demostración

$\Leftarrow$) $|G| = p, p$ primo $\Rightarrow G \cong C_p =< x \mid x^p = 1 >$
Si $H \leqslant G \Rightarrow |H| \mid |G| = p \Rightarrow \begin{cases} |H| = 1 \Rightarrow H = \{1\} \\ |H| = p \Rightarrow H = G \end{cases}$

$\Rightarrow$) G es simple y abeliano entonces G no tiene subgrupos propios.
Como G no es trivial, elegimos $x \in G, x \neq 1$ y consideramos $< x > \neq \{1\}$.
$\begin{cases} \{1\} \neq < x > \trianglelefteq G \\ G \text{ simple} \end{cases} \Rightarrow G =< x >$
Supongamos $ord(x) = \infty$, entonces $G \cong \mathbb{Z}$ que no es simple.
Por tanto necesariamente $ord(x)$ es finito.
Supongamos $ord(x) = m$. Como $G =< x >$ entonces $|G| = | < x > | = ord(x) = m$ y así G es un grupo finito.
Sea $n \in \mathbb{Z}, n \mid m(n > 0)$ y consideramos el elemento $x^n \in< x >= G$ y el subgrupo $< x^n >$.
$\begin{cases} < x^n > \leq G \\ G \text{ es simple} \end{cases} \Rightarrow \begin{cases} < x^n = \{1\} = x^n = 1 \\ < x^n >= G =< x > \end{cases}.$
En el primer caso $ord(x^n) = \frac{m}{n} = 1 \Rightarrow n = m$.
En el segundo caso $ord(x^n) = \frac{m}{n} = ord(x) = m \Rightarrow n = 1$.
Entonces m es un número primo.

Teorema

Sea G un grupo y:

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_{n-1} \trianglelefteq H_n = G \qquad (1)$$

una serie normal de G.
Dicha serie es de composición $\iff$ ${}^{H_i}/_{H_{i-1}}$ es simple $\forall i = 1, ..., n$.

Demostración

$\Rightarrow$) Suponemos que la serie (1) es de composición.
En particular es una serie propia y entones $H_{i-1} \underset{\neq}{\trianglelefteq} H_i \;\; \forall i = 1, ..., n \Rightarrow$ ${}^{H_i}/_{H_{i-1}}$ es no trivial $\forall i = 1, ..., n$.
Sabemos que los subgrupos normales de ${}^{H_i}/_{H_{i-1}}$ son de la forma ${}^{K}/_{H_{i-1}}$ donde

$$H_{i-1} \trianglelefteq K \trianglelefteq H_i$$

Entonces $\exists i \in \{1, ..., n\}$ tal que ${}^{H_i}/_{H_{i-1}}$ no es simple, estaríamos diciendo que $\exists K \leqslant G$ tal que

$$H_{i-1} \underset{\neq}{\trianglelefteq} K \underset{\neq}{\trianglelefteq} H_1 ({}^{H_{i-1}}/_{H_{i-1}} \neq {}^{K}/_{H_{i-1}} \underset{\neq}{\trianglelefteq} {}^{H_i}/_{H_{i-1}})$$

Pero entonces la serie

$$\{1\} = H_0 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_{i-1} \underset{\neq}{\trianglelefteq} K \underset{\neq}{\trianglelefteq} H_i \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_n = G$$

es un refinamiento propio de la serie (1), en contradicción con que (1) es de composición.

$\Leftarrow$) $1 = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_n = G$
Suponemos que ${}^{H_i}/_{H_{i-1}}$ son simples $\forall i = 1, ..., n$
$\forall i \; {}^{H_i}/_{H_{i-1}} \neq 1 \Rightarrow H_{i-1} \underset{\neq}{\trianglelefteq} H_i \;\; \forall i = 1, ..., n.$
Luego la serie es normal, propia.

Suponemos que

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq ... \trianglelefteq K_m = G \qquad (2)$$

es un refinamiento propio de la serie (1).
Entonces $n < m$ y todos los grupos de la serie (1) aparecen en la serie (2).
Como $n < m$, existe $l \in \{0, ..., m\}$ tal que $K_l \neq H_i \;\; \forall i \in \{0, 1, ..., 1\}$.
Sea $t \in \{0, ..., m\}$ el mayor subíndice tal que K_t no aparece en la serie (1).
Notemos que $0 < t < m$ pues $K_0 = \{1\} = H_0$ y $K_m = G = H_n$.
Podemos entonces considerar K_{t+1} y, por la elección de t,
$\exists r \in \{0, ..., n\}$ tal que $K_{t+1} = H_r$.
Entonces tenemos la siguiente situación

$$H_{r-1} \underset{\neq}{\trianglelefteq} K_t \underset{\neq}{\trianglelefteq} K_{t+1} = H_r \Rightarrow$$

$$\Rightarrow 1 \neq {}^{K_t}/_{H_{r-1}} \underset{\neq}{\trianglelefteq} {}^{H_r}/_{H_{r-1}}$$

Consecuentemente, la serie (1) no admite refinamientos propioes.

Ejemplo

$G = S_4$
$1 \underset{\neq}{\trianglelefteq} A_4 \underset{\neq}{\trianglelefteq} S_4$
Sus factores son ${}^{A_4}/_1 = A_4$ no es simple.
La serie no es de composición.

$1 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4 \qquad K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(3\ 2)\}$
Sus factores son ${}^{S_4}/_{A_4}, {}^{A_4}/_{K}, {}^{K}/_{1} = K$ (no es simple).
La serie no es de composición.

$1 \trianglelefteq C_2 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4 \qquad C_2 =< (1\ 2)(3\ 4) >= \{id, (1\ 2)(3\ 4)\}$
$|{}^{S_4}/_{A_4}| = 2 \Rightarrow {}^{S_4}/_{A_4} \cong C_2$ y entonces simple.
$|{}^{A_4}/_{K}| = 3 \Rightarrow {}^{A_4}/_{K} \cong C_3$ y entonces simple.
$|{}^{K}/_{H}| = 2 \Rightarrow {}^{K}/_{H} \cong C_2$ y entonces simle.
${}^{H}/_{1} = H \cong C_2$ y entonces simple.
Consecuentemente la serie es de composición.

Teorema

Todo grupo finito tiene una serie de composición.

Demostración

Sea G finito.
Hacemos inducción en $|G|$.
Si $|G| = 2 \Rightarrow G \cong C_2$ y por tanto G es simple.
Entonces $1 \underset{\neq}{\trianglelefteq} G$ es una serie de composición de G.

Supongamos que $|G| > 2$ y el resultado es cierto para todo grupo de orden menor que $|G|$.
Sea:

$$\triangle = \{K \in Sub(G) \mid K \underset{\neq}{\trianglelefteq} G\}$$

$\triangle \neq \emptyset$, $\triangle$ es un conjunto finito.
Elegimos $K \in \triangle$ tal que $|K|$ sea el mayor de los órdenes de los elementos de $\triangle$.
Se tiene que ${}^{G}/_{K}$ es un grupo simple.
En efecto, como $K \underset{\neq}{\trianglelefteq} G, {}^{G}/_{K}$ es no trivial y si $L \trianglelefteq {}^{G}/_{K} \Rightarrow L = {}^{H}/_{K}$ con $K \trianglelefteq H \trianglelefteq G$.
Si $H \neq K$ entonces necesariamente $H = G$ porque en caso contrario, $H \underset{\neq}{\trianglelefteq} G, H \in \triangle$ y $|K| < |H|$ pues $K \underset{\neq}{\trianglelefteq} H$ (contradicción por la elección de K).
Si $H \neq K \Rightarrow H = G \Rightarrow L = {}^{G}/_{K}$.
Si $H = K \Rightarrow L = \{1\}$.
Es decir, ${}^{G}/_{K}$ es simple.

Como $K \underset{\neq}{\trianglelefteq} G \Rightarrow |K| \lneq |G|$ y por hipótesis de inducción, K tiene una serie de composición.

$$1 = K_0 \underset{\neq}{\trianglelefteq} K_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} K_r = K \text{ serie de composición de } K$$

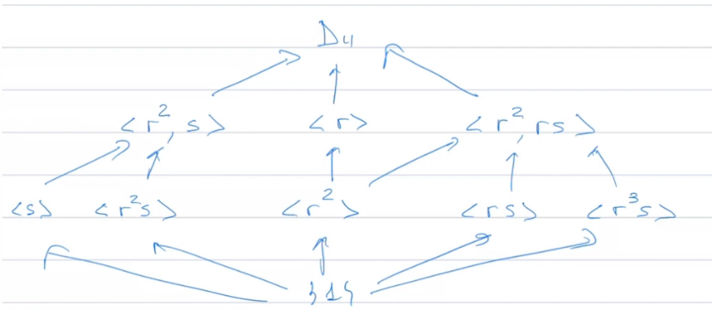
Entonces

$$1 = K_0 \underset{\neq}{\trianglelefteq} K_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} K_r = K \underset{\neq}{\trianglelefteq} K_{r+1} = G$$

es una serie de composición de G.

Ejemplo

$G = D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$



Subgrupos normales son

$$< r^2, s > \qquad < r > \qquad < r^2, rs >$$

pues son de índice dos en D_4.
$Z(D_4) = \{1, r^2\} =< r^2 >$ y entonces $< r^2 > \trianglelefteq D_4$
El resto de subgrupos de orden 2 de D_4 no son normales en D_4

$$< s >= \{1, s\} \qquad r \in D_4$$

$$rsr^{-1} = rsr^3 = rr^{-3}s = r^{-2}s = r^2s \notin < s >$$

Por tanto

$$r < s > r^{-1} \nsubseteq < s > \Rightarrow < s > \underset{\neq}{\ntrianglelefteq} D_4$$

De igual forma para los otros tres:

$$< r^2, s > \underset{\neq}{\trianglelefteq} D_4$$

$$< r > \underset{\neq}{\trianglelefteq} D_4$$

$$< r^2, rs > \underset{\neq}{\trianglelefteq} D_4$$

$$1 \underset{\neq}{\trianglelefteq} < s > \underset{\neq}{\trianglelefteq} < r^2, s > \underset{\neq}{\trianglelefteq} D_4$$

$$1 \underset{\neq}{\trianglelefteq} < r^2 > \underset{\neq}{\trianglelefteq} < r^2, s > \underset{\neq}{\trianglelefteq} D_4$$

$$1 \underset{\neq}{\trianglelefteq} < r^3 s > \underset{\neq}{\trianglelefteq} < r^2, s > \underset{\neq}{\trianglelefteq} D_4$$

$$1 \underset{\neq}{\trianglelefteq} < r^2 s > \underset{\neq}{\trianglelefteq} < r > \underset{\neq}{\trianglelefteq} D_4$$

$$1 \underset{\neq}{\trianglelefteq} < r^2 > \underset{\neq}{\trianglelefteq} < r^2, rs > \underset{\neq}{\trianglelefteq} D_4$$

$$1 \underset{\neq}{\trianglelefteq} < rs > \underset{\neq}{\trianglelefteq} < r^2, rs > \underset{\neq}{\trianglelefteq} D_4$$

$$1 \underset{\neq}{\trianglelefteq} < r^3 s > \underset{\neq}{\trianglelefteq} < r^2, rs > \underset{\neq}{\trianglelefteq} D_4$$

Factores de la 1ª serie son:

$$D_4 / < r^2, s > \cong C_2 \qquad < r^2, s > / < s > \cong C_2 \qquad < s > / 1 = < s > \cong C_2$$

De forma análoga, se observa que los elementos de las demás series son, salvo isomorfismo, C_2.

Definición

Sea G un grupo y

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_n = G$$

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq ... \trianglelefteq K_m = G$$

dos series normadas de G. Diremos que son equivalentes o isomorfas si

(I) $n = m$

(II) $\exists \sigma \in S_n$ tal que $H_i / H_{i-1} \cong K_{\sigma(i)} / K_{\sigma(i)-1} \;\; \forall i = 1, ..., n$.

Teorema de Jordan-Holder

Sea G un grupo que admite una serie de composición. Entonces:

a) Toda serie normal de G admite un refinamiento que es una serie de composición.

b) Cualesquiera dos series de composición de G son equivalentes.

Lema (Teorema de refinamiento de Schreier)

Cualesquiera dos series normales de un grupo G admiten refinamientos equivalentes.

Lema

Si una serie normal de un grupo G es equivalente a una serie de composición de G, entonces dicha serie es también de composición.

Demostración (Teorema de Jorda-Holder)

Sea

$$1 = G_0 \underset{\neq}{\trianglelefteq} G_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} G_n = G$$

una serie de composición de G.

a) Sea $1 = H_0 \underset{\neq}{\trianglelefteq} H_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_r = G$ una serie normal de G.
Por el Teorema de refinamiento de Schreier, ambas series admiten refinamientos equivalentes.
Como la serie primera es de composición, todo refinamiento suyo coincide con ella misma. Entonces la serie

$$1 = H_0 \underset{\neq}{\trianglelefteq} H_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_r = G$$

tiene un refinamiento equivalente a una serie de composición y entonces, por el segundo lema, dicho refinamiento es también una serie de composición de G.

b) Es consecuencia inmediata del Teorema de refinamiento de Schreier.

Definición

Sea G un grupo finito. Definimos la longitud de G, que denotaremos por $l(G)$, como la longitud de cualquiera de sus series de composición.

Definimos los factores de composición de G como los factores de sus series de composición. Al conjunto de dichos factores lo denotaremos por $fact(G)$.

Ejemplos

1. $G = S_2 \cong C_2$.
   $1 \underset{\neq}{\trianglelefteq} S_2$ es una serie de composición de S_2.
   Entonces:
   $$l(S_2) = 1 \qquad fact(S_2) = \{C_2\}$$

2. S_3
   $1 \underset{\neq}{\trianglelefteq} A_3 \underset{\neq}{\trianglelefteq} S_3$ es una serie de composición de S_3 pues:
   $$\begin{cases} S_3/A_3 \cong C_2 \\ A_3/1 = A_3 \cong C_3 \end{cases}$$
   Entonces $l(S_3) = 2 \qquad fact(S_3 = \{C_2, C_3\}$.

3. S_4
   $1 \trianglelefteq C_2 \underset{\neq}{\trianglelefteq} K \underset{\neq}{\trianglelefteq} A_4 \underset{\neq}{\trianglelefteq} S_4$ serie de composición.

$$l(S_4) = 4$$

$$fact(S_4) = \{{}^{S_4}/_{A_4} \cong C_2, {}^{A_4}/_{K} \cong C_3 {}^{K}/_{C_2} \cong C_2, {}^{C_2}/_{1} = C_2\}$$

4. $G = D_3 = \{1, r, r^2, s, rs, r^2s\}$
   $1 \trianglelefteq < r > \trianglelefteq D_3$ serie de composición de D_3

$$l(D_3) = 2 \qquad fact(D_3 = \{{}^{D_3}/_{< r >} \cong C_2, < r > \cong C_3\}$$

5. $G = D_4$
   $1 \underset{\neq}{\trianglelefteq} < s > \underset{\neq}{\trianglelefteq} < r^2, s > \underset{\neq}{\trianglelefteq} D_4$ es una serie de composición.

$$l(D_4) = 3$$

$$fact(D_4) = \{{}^{D_4}/_{< r^2, s >} \cong C_2, \ {}^{< r^2, s >}/_{< s >} \cong C_2, < s > \cong C_2\}$$

Relación 4: Ejercicio 12

Vídeo del 28/04/2021.

Proposición

Sea G un grupo finito y N subgrupo normal propio de G. Entonces:

$$l(G) = l(N) + l({}^{G}/_{N})$$

$$fact(G) = fact(N) \cup fact({}^{G}/_{N})$$

Demostración

Como N un subgrupo normal propio de G, entonces la serie

$$1 \underset{\neq}{\trianglelefteq} N \underset{\neq}{\trianglelefteq} G$$

es una serie normal propia de G.

Por el Teorema de Jordan-Hölder se puede refinar hasta una serie de composición de G.
Sea:

$$1 = K_0 \underset{\neq}{\trianglelefteq} K_1 \underset{\neq}{\trianglelefteq} \ldots \underset{\neq}{\trianglelefteq} K_r = N \underset{\neq}{\trianglelefteq} K_{r+1} \underset{\neq}{\trianglelefteq} \ldots \underset{\neq}{\trianglelefteq} K_n = G$$

dicho refinamiento.
Entonces:

$$1 = K_0 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} K_r = N \text{ es una serie de composición de } N$$

y

$$1 = {}^{K_r}/_{N} \underset{\neq}{\trianglelefteq} {}^{K_{r-1}}/_{N} \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} {}^{K_n}/_{N} = {}^{G}/_{N}$$

es una serie de composición de ${}^{G}/_{N}$.
Entonces se deduce el resultado.

Teorema de Abel

Para cada $n \geq 5$ el grupo A_n es un grupo simple.

Demostración

$n \geq 5$ y sea $N \trianglelefteq A_n$, $N \leq 1$.
Vamos a demostrar que $N = A_n$.

Como $N \neq 1$, elegimos en N un $\alpha \in N, \alpha \notin id$ y que mueve el menor nº de elementos de $\{1, 2, ..., n\} \Rightarrow$ veamos que α es un 3-ciclo, es decir, que mueve exactamente 3 elementos.
Supongamos que α no es un 3-ciclo, es decir, que mueve más de 3 elementos.

Caso 1: α mueve exactamente 4 elementos, entonces $\alpha = (x_1\ x_2)(x_3\ x_4)$ (pues los ciclos de longitud 4 son permutaciones impares).
Sea $x_5 \in \{1, 2, ..., n\}$ tal que $x_5 \neq x_i$ $i = 1, 2, 3, 4$ (que podemos hacerlo pues $n \geq 5$) y sea $\beta = (x_3\ x_4\ x_5) \in A_n$.
Entonces $\beta^{-1} N \beta \leqslant N$ pues $N \trianglelefteq A_n$, con lo que $\beta^{-1}\alpha^{-1}\beta \in N$.
Entonces $\sigma = \beta^{-1}\alpha^{-1}\beta\alpha \in N$.
Resulta que σ mueve menos elementos que α en contra de la elección de α.

$$\sigma = (x_3\ x_5\ x_4)(x_1\ x_2)(x_3\ x_4) = (x_3\ x_4\ x_5)$$

Caso 2: α mueve 5 o mas elementos.
Elegimos $x_1, x_2, x_3, x_4, x_5 \in \{1, ..., n\}$ elementos movidos por α y suponemos que $\alpha(x_1) = x_2$.
Consideramos $\beta = (x_3\ x_4\ x_5) \in A_n$, entonces como en el caso anterior.

$$\sigma = \beta^{-1}\alpha^{-1}\beta\alpha \in N$$

Vemos que σ mueve menos elementos que α, o σ deja fijos mas elementos que α.
En efecto, si $j \in \{1, ..., n\}$ tal que $\alpha(j) = j$ entonces $j \neq x_i$ $\forall i = 1, ..., 5$ y

$$\sigma(j) = \beta^{-1}\alpha^{-1}\beta\alpha(j) = \beta^{-1}\alpha^{-1}\beta(j) = \beta^{-1}\alpha^{-1}(j) = \beta^{-1}(j) = j$$

Pero además:

$$\sigma(x_1) = \beta^{-1}\alpha^{-1}\beta\alpha(x_1) = \beta^{-1}\alpha^{-1}\beta(x_2) = \beta^{-1}\alpha^{-1}(x_2) =$$
$$= \beta^{-1}(x_1) = x_1$$

Por tanto σ mueve menos elementos que α en contradicción con la elección de α.

Consecuentemente $\alpha = (x_1\ x_2\ x_3) \in N$.
Sea $k \neq x_i$ $i = 1,2,3$ y sea $\gamma = (x_1\ x_2)(x_3\ k) \in A_n$.
Entonces $\gamma N \gamma^{-1} \leqslant N$ por ser $N \trianglelefteq A_4$ y entones $\gamma\alpha^{-1}\gamma^{-1} \in N$.
Es fácil ver
$$\sigma\alpha^{-1}\sigma^{-1} = (x_1\ x_2\ k) \in N$$
Entonces $\{(x_1\ x_2\ k) \mid k \neq x_1, x_2\} \subset N$ y aplicando el lema anterior

$$A_n =< (x_1\ x_2\ k) \mid k \neq x_1, x_2 >\leqslant N \Rightarrow A_n = N$$

Corolario

Para $n \geq 5$, la longitud de S_n es 2 y $fact(S_n) = \{A_n, C_2\}$.

Demostración

Por el teorema de Abel, la serie

$$1 \underset{\neq}{\trianglelefteq} A_n \underset{\neq}{\trianglelefteq} S_n$$

es una serie de composición de S_n pues sus factores son ${}^{S_n}/_{A_n} \cong C_2$ y ${}^{A_n}/_1 = A_n$ y por tanto simples.
Entonces:
$$l(S_n) = 2 \qquad fact(S_n) = \{A_n, C_2\}$$

Lema

Sea $n \geq 3$ y $x_1, x_2 \in \{1, 2, ..., n\}$ con $x_1 \neq x_2$.
Entonces:
$$A_n =< (x_1\ x_2\ k) \mid k \neq x_1\ \ i = 1,2 >$$

Demostración

Sabemos que A_n está generado por todos los ciclos de longitud 3.
Sea:
$$H =< (x_1\ x_2\ k \mid k \neq x_1, x_2 >\leqslant A_n$$
Demostraremos que para cualquier $(i\ j\ k)$ 3-ciclo se verifica que $(i\ j\ k) \in H$.

Como

$$(x_1\ x_2\ k) = (x_2\ k\ x_1) = (k\ x_1\ x_2) \in H$$

Como $(x_1\ x_2\ k)^{-1} = (k\ x_2\ x_1) \in H$

$$(x_1\ k\ x_2) = (k\ x_2\ x_1) \in H$$

Sea $\alpha = (i\ j\ k)$ un 3-ciclo.

Caso 1: $\{x_1, x_2\} \leqslant \{i, j, k\} \Rightarrow$ por la observación anterior, $(i\ j\ k) \in H$.

Caso 2: $x_1 \in \{i, j, k\} \wedge x_2 \notin \{i, j, k\}$.
Si $i = x_1$ entones:
$a)\alpha = (x_1\ j\ k) = (x_1\ x_2\ k)^{-1}(x_1\ x_2\ j)(x_1\ x_2\ k) \in H$
Si $j = x_1$ entonces
$b)\alpha = (i\ x_1\ k) = (x_1\ k\ i) \in H$ por el caso anterior a).
Si $k = x_1$ entonces
$c)\alpha = (i\ j\ x_1) = (x_1\ i\ j) \in H$ por el primer caso a).

Caso 3: $x_i \notin \{i, j, k\} \wedge x_2 \in \{i, j, k\}$
Se procede de forma análoga al caso 2 y se concluye entonces $\alpha \in H$.

Caso 4: $x_1, x_2 \notin \{i, j, k\}$.

$$\alpha = (i\ j\ k) = (x_1\ x_2\ i)(x_2\ j\ k)(x_1\ x_2\ i)^{-1} \in H$$

Por tanto H contiene todos los 3-ciclos y entonces $H = A_n$.

5.1. Grupos resolubles

Definición

Un grupo G se dice resoluble si tiene una serie normal

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_n = G$$

tal que H_i/H_{i-1} es abeliano $\forall i = 1, ..., n$.

Es claro que si G es un grupo abeliano entonces G es resoluble pues la serie

$$1 \trianglelefteq H_0 \trianglelefteq H_1 = G$$

tiene sus factores abelianos ($H_1/H_0 = G$).

Teorema

Sea G un grupo finito. Son equivalentes los siguientes enunciados:

(I) Los factores de composición de G son cíclicos de orden un número primo.

(II) G es resoluble.

Demostración

$(i) \Rightarrow (ii)$ Es inmediato.

$(ii) \Rightarrow (i)$ Suponemos G resoluble, sea

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$$

serie normal de G con ${}^{G_i}/_{G_{i-1}}$ abeliano $\forall i = 1, ..., n$.
Como G es finito, podemos aplicar el Teorema de Jordan-Hölder, la serie anterior puede refinarse a una serie de composición de G.
Sea $1 = H_0 \underset{\neq}{\trianglelefteq} H_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_m = G$ serie de composición de G que refina a la anterior.
Veamos que ${}^{H_r}/_{H_{r-1}}$ es abelaino $\forall r = 1, ..., m$. Elegimos un r, y existirá un $i \in \{1, ..., n\}$ tal que $H_r \leqslant G_i$ (usando que la serie de composición es un refinamiento)

Caso 1: $H_{r-1} = G_{i-1}$ entonces

$${}^{H_r}/_{H_{r-1}} = {}^{H_r}/_{G_{i-1}} \leqslant {}^{G_i}/_{G_{i-1}} \text{ que es abeliano}$$

$$\Rightarrow {}^{H_r}/_{H_{r-1}} \text{ también es abeliano}$$

Caso 2: $H_{r-1} \neq G_{i-1}$ entonces

$$G_{i-1} \trianglelefteq H_{r-1} \underset{\neq}{\trianglelefteq} H_r \leqslant G_i$$

Entonces

$${}^{H_r}/_{H_{r-1}} \overset{2^{\text{o}} \text{ Teorema de Isomorfia}}{\cong} {}^{{}^{H_r}/_{G_{i-1}}}/_{{}^{H_{r-1}}/_{G_{i-1}}}$$

es abeliano porque ${}^{H_r}/_{G_{i-1}}, {}^{H_{r-1}}/_{G_{i-1}}$ son subgrupos de ${}^{G_i}/_{G_{i-1}}$ que es abeliano.
Como ${}^{H_r}/_{H_{r-1}}$ es simple y abeliano $\Rightarrow {}^{H_r}/_{H_{r-1}}$ es cíclico de orden primo $\forall r = 1, ..., m$.

Corolario

S_n es resoluble $\iff n \leq 4$.

Demostración

$\Leftarrow$) Si $n \leq 4 \Rightarrow n = 2, 3$ ó 4.
$\begin{cases} fact(S_2) = \{C_2\} \\ fact(S_3) = \{C_2, C_3\} \\ fact(S_4) = \{C_2, C_2, C_2, C_3\} \end{cases} \Rightarrow$ son resolubles por el teorema anterior.

$\Rightarrow$) Si $n \geq 5$ entonces $fact(S_n) = \{C_2, A_n\}$.
Como A_n no es cíclico de orden primo entonces S_n no es resoluble por el Teorema anterior.

Ejemplo

Hemos visto que:

$$fact(D_3) = \{C_2, C_3\}$$

$$fact(D_4) = \{C_2, C_2, C_2\}$$

$$fact(D_6) = \{C_3, c_2, C_2\}$$

entonces D_3, D_4 y D_6 son resolubles.

Proposición

1) Sea G un grupo resoluble y $H \leqslant G$, entonces H es resoluble.
2) Sea G un grupo resoluble y $N \trianglelefteq G$ entonces ${}^{G}/_{N}$ es resoluble.
3) Sea G un grupo y $N \trianglelefteq G$ tal que N y ${}^{G}/_{N}$ son resolubles, entonces G es resoluble.

Demostración

Haremos uso de los siguientes resultados (Ejercicio).

(a) Sean $N, N', H \leqslant G$ con $N \trianglelefteq N' \Rightarrow N \cap H \trianglelefteq N' \cap H$.

(b) $H, H', N \leqslant G$ con $\begin{cases} H \trianglelefteq H' \\ N \trianglelefteq G \end{cases} \Rightarrow NH \trianglelefteq NH'$

1) Sea $1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ serie normal de G con ${}^{G_i}/_{G_{i-1}}$ abeliano, $i = 1, ..., n$.
   Sea $H \leqslant G$. Por (a), obtenemos una serie normal

   $$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq ... \trianglelefteq G_n \cap H = G \cap H = H$$

   de H.
   Sea $i \in \{1, ..., n\}$, aplicamos el 3º Teorema de isomorfia a G_i y a los subgrupos

   $$K = G_i \cap H \leqslant G_i$$

   $$N = G_{i-1} \trianglelefteq G$$

   Entonces ${}^{K}/_{N \cap K} \cong {}^{KN}/_{N}$, es decir

   $${}^{G_i \cap H}/_{G_{i-1} \cap H} = {}^{G_i \cap H}/_{G_{i-1} \cap G_i \cap H} \cong {}^{G_{i-1}(G_i \cap H)}/_{G_{i-1}}$$

   Puesto que ${}^{G_{i-1}(G_i \cap H)}/_{G_{i-1}} \leqslant {}^{G_i}/_{G_{i-1}}$ y entonces abeliano.

   Consecuentemente H tiene una serie normal con factores abelianos. Es decir, H es resoluble.

2) $N \trianglelefteq G, G$ resoluble.
Sea $1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ serie normal de G con ${}^{G_i}/_{G_{i-1}}$ abeliano, $i = 1, ..., n$.

Por (b), $G_{i-1}N \trianglelefteq G_iN \ \ \forall i = 1, ..., n$.
Además N es normal en todo G_iN pues N es normal en G y entonces, tomando cociente

$$1 = {}^{G_0N}/_N \trianglelefteq {}^{G_1N}/_N \trianglelefteq ... \trianglelefteq {}^{G_nN}/_N = {}^{GN}/_N = {}^{G}/_N$$

es una serie normal de ${}^{G}/_N$. Sus factores $i = 1, ..., n$

$${}^{G_iN/N}/_{G_{i-1}N/N} \overset{2^{\text{o}}\text{ Teorema de Isomorfia}}{\cong} {}^{G_iN}/_{G_{i-1}N}$$

Aplicamos el tercer teorema de isomorfia a
$K \qquad G_i \trianglelefteq G_iN$
$N \qquad G_{i-1}N \trianglelefteq G_iN$

$${}^{G_i}/_{(G_{i-1}N)\cap G_i} \cong {}^{G_i(G_{i-1}N)}/_{G_{i-1}N} = {}^{G_iN}/_{G_{i-1}N}$$

$${}^{G_i}/_{(G_{i-1}N)\cap G_i} \overset{2^{\text{o}}\text{ Teorema de Isomorfia}}{\cong} {}^{G_i/G_{i-1}}/_{(G_{i-1})N)\,\cap\, G_i/G_{i-1}}$$

y por tanto abeliano al ser cociente de ${}^{G_i}/_{G_{i-1}}$ que es abeliano.

Consecuentemente ${}^{G}/_N$ tiene una serie normal con factores abelianos. Es decir, ${}^{G}/_N$ es resoluble.

3) $N \trianglelefteq G$, N y ${}^{G}/_N$ resolubles.
Sean $1 = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_r = N$ serie normal de N tal que ${}^{N_i}/_{N_{i-1}}$ es abeliano $\forall i = 1, ..., r$.
Sean

$$1 = {}^{N}/_N \trianglelefteq {}^{H_1}/_N \trianglelefteq ... \trianglelefteq {}^{H_s}/_N = {}^{G}/_N$$

serie normal de ${}^{G}/_N$ tal que ${}^{H_j/N}/_{H_{j-1}/N} \cong {}^{H_j}/_{H_{j-1}}$ es abeliano $\forall j = 1, ..., s$.

Entonces es inmediato que

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_r = N \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_s = G$$

es una serie normal cuyos factores son abelianos. Por tanto G es resoluble.

Corolario

Para todo $n \geq 3$, el grupo diédrico D_n es resoluble.

Demostración

$D_n =< r, s \mid r^n = 1 = s^2, sr = r^{-1}s >$
Consideramos $N =< r >\cong G_n$.
$N \trianglelefteq D_n$ pues $[D_n : N] = 2$.

N es abeliano y entonces resoluble. ${}^{D_n}/_{N} \cong C_2$ abeliano y entonces resoluble $\Rightarrow D_n$ es resoluble.

5.2. Conmutadores

Definición

Sea G un grupo y sean $x_1 y \in G$. Definimos el conmutador de x e y, denotado $[x, y]$, como el elemento:

$$[x.y] := xyx^{-1}y^{-1}$$

Definimos el subgrupo conmutador (ó también llamado primer subgrupo derivado) de G, denotado por $[G, G]$, como el subgrupo generado por los conmutadores. Esto es:

$$[G, G] :=< [x, y] \mid x, y \in G >$$

Proposición

Sea G un grupo. Entonces:

(1) $[G, G] \trianglelefteq G$:

(2) $[G, G] = 1 \iff G$ es abeliano,

(3) ${}^{G}/_{[G,G]}$ es un grupo abeliano.

(4) Si $N \trianglelefteq G$, entonces ${}^{G}/_{N}$ es abeliano $\iff [G, G] \leqslant N$.

Al cociente ${}^{G}/_{[G,G]}$ se le llama el abelianizado de G.

Demostración

(1) Puesto que $\{[x, y] \mid x, y \in G\}$ generan $[G, G]$, para ver que $[G, G] \trianglelefteq G$ basta ver que $a[x, y]a^{-1} \in [G, G] \forall a \in G$. Esto último es claro porque

$$a[x, y]a^{-1} = [axa^{-1}, aya^1] \in [G, G]$$

(2) Es inmediato.

(3) Sean $x[G, G], y[G, G] \in {}^{G}/_{[G,G]}$.

$$(x[G, G])(y[G, G]) = (xy)[G, G]$$

$$(y[G, G])(x[G, G]) = yx[G, G]$$

Como

$$(yx)^{-1}xy = x^{-1}y^{-1}xy = [x^{-1}, y^{-1}] \in [G, G]$$

$\Rightarrow (xy)[G,G] = yx[G,G]$ y se tiene que ${}^{G}/_{[G,G]}$ es abeliano.

(4) $N \trianglelefteq G$.
${}^{G}/_{N}$ es abeliano $\iff$
$\iff (xy)N = (xN)(yN) = (yN)(xN) = (yx)N \;\; \forall x, y \in G \iff$
$\iff (yx)^{-1}(xy) = x^{-1}y^{-1}xy = [x^{-1}, y^{-1}] \in N \;\; \forall x, y \in G \iff$
$\iff \{[x,y] \mid x, y \in G\} \subset N$

Relación 4: Ejercicio 3

Vídeo del 05/05/2021.

Definición

Sea G un grupo. Para cada $n \geq 0$ definimos el n-ésimo subgrupo derivado de G, por recurrencia, como sigue:

$$G^{(0)} := G$$

$$G^{(n+1)} := [G^{(n)}, G^{(n)}] \forall n \geq 0$$

Notemos que tenemos la siguiente serie:

$$... \trianglelefteq G^{(n+1)} \trianglelefteq G^{(n)} \trianglelefteq ... \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

que en general no tiene porque ser finita.
Sus factores son:

$${}^{G^{(n)}}/_{G^{(n+1)}} = {}^{G^{(n)}}/_{[G^{(n)}, G^{(n)}]} \text{ abelianos}$$

Esta serie se conoce por la serie derivada de G.

Teorema

Sea G un grupo.
G es resoluble $\iff \exists n$ tal que $G^{(n)} = 1$.

Demostración

$\Leftarrow$) Inmediato.
$\Rightarrow$) Supongamos G resoluble y sean

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_n = G$$

serie normal de G con ${}^{H_i}/_{H_{i-1}}$ abeliano $\forall i = 1, ..., n$.
Veamos que para todo $i \geq 1, G^{(i)} \leqslant H_{n-1}$, por inducción en i.

Sea $i = 1$. Puesto que: ${}^{G_n}/_{H_{n-1}} = {}^{G}/_{H_{n-1}}$ es abeliano $\Rightarrow [G, G] = G^{(1)} \leqslant H_{n-1}$ y se tiene el resultado para $i = 1$.
Supuesto cierto para i, esto es $G^{(i)} \leqslant H_{n-i}$, veamoslo para $i + 1$.
Puesto que ${}^{H_{n-i}}/_{H_{n-i-1}}$ es abeliano $\Rightarrow [H_{n-i}, H_{n-1}] \leqslant H_{n-(i+1)}$
$G^{(i)} \leqslant H_{n-i} \Rightarrow [G^{(i)}, G^{(i)}] = G^{(i+1)} \leqslant [H_{n-i}, H_{n-i}] \leqslant H_{n-(i+1)}$
tenemos pues $G^{(i+1)} \leqslant H_{n-(i+1)}$.
Tomando $i = n$, $G^{(n)} \leqslant H_{n-n} = H_0 = 1 \Rightarrow G^{(n)} = 1$.

5.3. Ejercicios

Relación 4: Ejercicio 2

Vídeo del 10/05/2021.

Relación 4: Ejercicio 4

Vídeo del 10/05/2021.

Relación 4: Ejercicio 6

Vídeo del 10/05/2021.

Ejercicio

Si G es un grupo y $N \trianglelefteq G$ tal que N y ${}^{G}/_{N}$ son finitos, entonces G es finito.

Vídeo del 10/05/2021.

Relación 4: Ejercicio 11

Vídeo del 10/05/2021.

Relación 4: Ejercicio 15

Vídeo del 10/05/2021.

6. G-conjuntos y p-grupos

Definición

Sea G un grupo y X un conjunto no vacío. Una acción de G sobre X (por la izquierda) es una aplicación:

$$G \times X \to X \qquad (g, x) \mapsto^{g} x$$

que verifica las dos siguientes propiedades:

1) ${}^{1}x = x \quad \forall x \in X$.
2) ${}^{gh}x =^{g} ({}^{h}x) \quad \forall g, h \in G\ \ \forall x \in X$.

Al elemento ${}^{g}x$ lo leeremos como el resultado de hacer actuar el elemento g sobre el elemento x.
Diremos que G actúa sobre X (por la izquierda) ó que X es un G-conjunto.
$G =$ dominio de operadores.
A la acción $G \times X \to X$ aplicación G-estructura de X.
Trabajaremos siempre con acciones por la izquierda.

Para cada $g \in G$, podemos definir la siguiente aplicación:

$$\phi(g) : X \to X \qquad \phi(g)(x) :=^{g} x$$

La condición 1) nos dice:

$$\phi(1) = id_X : X \to X$$

La condición 2) nos dice que, dados $g, h \in G$:

$$\phi(g, h) = \phi(g)_o \phi(h)$$

En particular:

$$\phi(gg^{-1}) = id_X = \phi(g)_o \phi(g^{-1})$$
$$\phi(g^{-1}g) = id_X = \phi(g^{-1})_o \phi(g)$$

Es decir, $\phi(g) : X \to X$ es biyectiva con $\phi(g)^{-1} = \phi(g^{-1})$. Entonces tenemos definido un homomorfismo de grupos:

$$\phi : G \to S(X) \qquad g \mapsto \phi(g) : X \to X \quad \phi(g)(x) =^{g} x$$

donde $S(X)$ es el grupo de permutaciones del conjunto X.
Este homomorfismo la llamaremos representación de G por permutaciones asociada a la acción.

Recíprocamente: Sea G un grupo y X un conjunto no vacío. Supongamos dado un homomorfismo:

$$f : G \to S(X)$$

Entonces podemos definir una acción de G sobre X como sigue:

$$G \times X \to X \qquad (g,x) \mapsto^g x := f(g)(x)$$

La condición 1) se deduce de que $f(1) = id_X$.
La condición 2) se deduce de que $f(gh) = f(g)_o f(h)$.
Además, es fácil ver que la representación de G es asociada a esta acción es el homomorfismo de f.

Definición

Una acción de G sobre un conjunto X diremos que es fiel si el núcleo de $\phi : G \to S(X)$ es trivial.

$$Ker(\phi) = \{g \in G \mid \phi(g) = id_X\} = \{g \in G \mid \phi(g)(x) = x \ \ \forall x \in X\} =$$

$$= \{g \in G \mid^g x = x \ \ \forall x \in X\}$$

Ejemplos

1) Dado G un grupo y $X \neq \emptyset$. La aplicación

$$G \times X \to X \qquad (g,x) \mapsto^g x := x$$

es una acción de G sobre X que llamaremos la acción trivial de G sobre X.
La representación asociada es el homomorfismo trivial:

$$\phi : G \to S(X) \qquad g \mapsto id_X \Leftarrow \phi(g)(x) =^g x = x \ \ \forall x \in X$$

$Ker(\phi) = G$.

2) Supongamos X un G-conjunto y $H \leqslant G$ un subgrupo de G. Entonces X también es un H-conjunto con acción

$$H \times X \to X$$

definida como la de $G \times X \to X$ restringiéndose a los elementos de H.
Esta acción se llama la acción por restricción.
Si $\phi : G \to S(X)$ es la representación de G, entonces la de H no es otra que la composición:

$$H \overset{i}{\hookrightarrow} G \overset{\phi}{\to} S(X)$$

3) $G = S_n$ y $X = \{1, 2, ..., n\}$. Entonces:

$$S_n \times X \to X \qquad (\sigma, i) \mapsto^{\sigma} i := \sigma(i)$$

es una acción de S_n sobre X cuya representación asociada

$$id_{S_n} = \phi : S_n \to S(X) = S_n$$

Por tanto se trata de una acción fiel.

4) $G = D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$ y $X = \{1, 2, 3, 4\}$. Sea

$$\phi : D_4 \to S(X) = S_4$$

$$\phi(r^i) = (1\ 2\ 3\ 4)^i \qquad 0 \le i \le 3$$

$$\phi(r^is) = (1\ 2\ 3\ 4)^i(2\ 4) \qquad 0 \le i \le 3$$

ϕ es un homomorfismo de grupos (ejercicio).

Tenemos entonces una acción:

$$D_4 \times \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

$$g_j := \phi(g)(j) \qquad g \in D_4, j \in \{1, 2, 3, 4\}$$

g_j es precisamente el resultado de aplicar al vértice j el movimiento que corresponde a g.

$$r_j = \phi(r)(j) = (1\ 2\ 3\ 4)(j)$$

$Ker(\phi) = \{1\}$ y entonces es fiel.

5) $G = S_n \qquad X$ cualquier conjunto, $X \neq \emptyset$.
Consideramos $X^n = X \times \overset{n}{\ldots} \times X$.
Definimos una acción de S_n sobre X^n como sigue:

$$S_n \times X^n \to X^n$$

$$(\sigma, (x_1, x_2, ..., x_n)) \mapsto^{\sigma} (x_1, x_2, ..., x_n) := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, ..., x_{\sigma^{-1}(n)})$$

Veamos la propiedad 2:
$\sigma, \tau \in S_n$

$$^{\sigma\tau}(x_1, x_2, ..., x_n) =^{\sigma} (^{\tau}(x_1, x_2, ..., x_n))$$

$$^{\sigma\tau}(x_1, x_2, ..., x_n) = (x_{(\sigma\tau)^{-1}(1)}, x_{(\sigma\tau)^{-1}(2)}, ..., x_{(\sigma\tau)^{-1}(n)}) =$$

$$= (x_{\tau^{-1}\sigma^{-1}(1)}, x_{\tau^{-1}\sigma^{-1}(2)}, ..., x_{\tau^{-1}\sigma^{-1}(n)})$$

$$^{\tau}(x_1, x_2, ..., x_n) = (x_{\tau^{-1}(1)}, x_{\tau^{-1}(2)}, ..., x_{\tau^{-1}(n)}) = (y_1, ..., y_n)$$

$$y_j = x_{\tau^{-1}(j)} \qquad j = 1, ..., n$$

$$^{\sigma}(^{\tau}(x_1, x_2, ..., x_n)) =^{\sigma} (y_1, y_2, ..., y_n) = (y_{\sigma^{-1}(1)}, y_{\sigma^{-1}(2)}, ..., y_{\sigma^{-1}(n)})$$

Ahora $y_{\sigma^{-1}(j)} = x_{\tau^{-1}\sigma^{1}(j)} \quad \forall j = 1, ..., n$
$= (x_{\tau^{-1}\sigma^{-1}(1)}, x_{\tau^{-1}\sigma^{-1}(2)}, ..., x_{\tau^{-1}\sigma^{-1}(n)})$.

La aplicación:

$$S_n \times X^n \to X^n$$

$$(\sigma, (x_1, ..., x_n)) \to (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

en general no es acción.

6) Sea G un grupo y $X = G$, entonces podemos definir una acción de G sobre G llamada la acción por traslación y dada como sigue:

$$G \times G \to G \qquad (g, h) \mapsto^{g} (h) := gh$$

Si $\varphi : G \to S(G)$ es la representación asociada.

$$Ker(\phi) = \{g \in G \mid \phi(g) = id_G\} = \{g \in G \mid \phi(g)(h) =$$

$$= h \;\; \forall h \in G\} = \{g \in G \mid^{g} h = h \;\; \forall h \in G\} =$$

$$= \{g \in G \mid gh = h \;\; \forall h \in G\} = \{1\}$$

Es decir, esta acción es fiel.
Si G es finito y $|G| = n$, entonces $S(G) \cong S_n$ y como

$$\phi : G \to S(G) \cong S_n$$

es un monomorfismo, aplicando el 1º Teorema de isomorfia

$$G \cong Img(\phi)$$

7) Sea G un grupo y $H \leqslant G$ subgrupo. Entonces

$$G \times {}^{G}/_{H} \to {}^{G}/_{H}$$

$$(g, xH) \mapsto^{g} (xH) := gxH$$

También

$$G \times {}^{H}/_{G} \to {}^{H}/_{G}$$

$$(g, Hx) \mapsto^{g} (Hx) := Hxg^{-1}$$

es una acción

8) Sea G un grupo y consideremos $X = G$. Entonces la aplicación:

$$G \times G \to G \qquad (g,h) \mapsto^g h := ghg^{-1}$$

es una acción que llamaremos la acción por conjugación de G sobre sí mismo.

$$\phi : G \to S(G)$$

$$g \mapsto \phi(g) : G \to G$$

$$\phi(g)(h) =^g h = ghg^{-1}$$

Es decir, $\phi(g) = \varphi_g$ es el automorfismo interno definido por el elemento $g \in G$.

$$Img(\phi) = Int(G) \leqslant Aut(G)$$

$$Ker(\phi) = \{g \in G \mid \varphi_g = id_G\} = \{g \in G \mid \varphi_g(h) = h \ \ \forall h \in G\} =$$

$$= \{g \in G \mid ghg^{-1} = h \ \ \forall h \in G\} = \{g \in G \mid gh = hg \ \ \forall h \in G\} = Z(G)$$

9) Sea G un grupo y consideremos el conjunto $X = Sub(G)$.
Entonces:

$$G \times Sub(G) \to Sub(G)$$

$$(g,H) \mapsto^g H := gHg^{-1}$$

es una acción.

Teorema de Cayley

Todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.

Definición

Sea G un grupo y X un G-conjunto y sea

$$G \times X \to X \qquad (g,x) \mapsto^g x$$

la acción.
Podemos definir en X la siguiente relación binaria, denotada por $\sim$:
Dados $x, y \in X$

$$x \sim y \overset{def}{\iff} \exists g \in G \text{ tal que } y =^g x$$

Esta relación binaria es una relación de equivalencia.
En efecto:

Simétrica Supongamos que $x \sim y \Rightarrow \exists g \in G$ tal que $y =^g x$

$$y =^g x \Rightarrow^{g^{-1}} (y) =^{g^{-1}} ({}^g x) \underset{2)}{=}^{(g^{-1}g)} x =^1 x \underset{1)}{=} x \Rightarrow y \sim x$$

De la misma forma se demuestran la propiedad reflexiva y transitiva.

Definición

Para cada $x \in X$, definimos la órbita de x, que denotaremos por $\theta(x)$, como la clase de equivalencia de x por la relación de equivalencia anterior. Entonces

$$\theta(x) = \{y \in X \mid x \sim y\} = \{y \in X \mid y =^g x \text{ para } g \in G\} = \{^g x \mid g \in G\}$$

Tenemos que

1) $\theta(x) = \theta(y) \iff x \sim y \iff \exists g \in G$ tal que $y =^g x$.
2) $\theta(x) \neq \theta(y) \iff \theta(x) \cap \theta(y) = \emptyset$.
3) El conjunto de todas las órbitas, es decir, $X/\sim$, es una partición de X.

$$X = \cup_{x \in X} \theta(x) \text{ unión disjunta}$$

Una acción diremos que es transitiva si tiene una única órbita (si $X/\sim$ es unitario. Es decir,

$$\theta(x) = \theta(y) \qquad \forall x, y \in X$$

o, en otros términos, si

$$\forall x, y \in X \quad \exists g \in G \text{ tal que } y =^g x$$

Definición

Sea G un grupo y X un G-conjunto. Para cada $x \in X$ definimos el estabilizador de x en G como:

$$Stab_G(x) := \{g \in G \mid^g x = x\}$$

Se verifica que $Stab_G(x)$ es un subgrupo de G (ejercicio). También llamado el grupo de isotropia de x en G.

Proposición

Sea G un grupo y X un G-conjunto. Sean $x, y \in X$, entonces

$$\theta(x) = \theta(y) \iff Stab_G(x), Stab_G(y) \text{ son subgrupos conjugados de } G$$

($H, K \leqslant G, H$ y K se dicen conjugados si $\exists g \in G$ tal que $H = gkg^{-1}$)

Demostración

Suponemos que $\theta(x) = \theta(y) \Rightarrow x \sim y \Rightarrow \exists g \in G$ tal que $y =^g x \Rightarrow^{g^{-1}} y = x$.
Veamos que $gStab_G(x)g^{-1} = Stab_G(y)$.

Lo vemos por doble inclusión.
Sea $h \in Stab_G(x) \Rightarrow^h x = x$.
Consideramos ghg^{-1} y lo hacemos actuar sobre y

$$^{(ghg^{-1})}y =^{gh} (^{g^{-1}}y) =^{(gh)} x =^g (^h x) =^g x = y$$

$$\Rightarrow ghg^{-1} \in Stab_G(y)$$

Tenemos que $gStab_G(x)g^{-1} \leqslant Stab_G(y)$.
Por el mismo razonamiento anterior y puesto que $x =^{g^{-1}} y$, tendremos que:

$$g^{-1}Stab_G(y)g \leqslant Stab_G(x) \Rightarrow Stab_G(y) \leqslant gStab_G(x)g^{-1}$$

Consecuentemente:

$$Stab_G(y) = gStab(x)g^{-1}$$

Teorema

Sea G un grupo finito y X un G-conjunto. Entonces, para cada $x \in X$, la órbita de x es un conjunto finito, teniéndose que

$$|\theta(x)| = [G : Stab_G(x)]$$

En particular $|\theta(x)|$ es un divisor de $|G|$.

Demostración

$$\{gStab_G(x) \mid g \in G\} = {}^{G}\!/_{Stab_G(x)} \xrightarrow{\lambda} \theta(x) = \{^g x \mid g \in G\}$$

Definimos $\lambda(gStab_G(x)) :=^g x$.

$$gStab_G(x) = hStab_G(x) \iff h^{-1}g \in Stab_G(x) \iff {}^{(h^{-1}g}x = x \iff$$

$$\iff {}^g x =^h x$$

Por tanto λ está bien definida y además λ es inyectiva.
Obviamente, por definición, λ es sobreyectiva.

Por tanto λ es biyectiva.
Como ${}^{G}\!/_{Stab_G(x)}$ es finito por ser G finito, entonces $\theta(x)$ es finito y

$$|\theta(x)| = [G : Stab_G(x)]$$

Relación 6: Ejercicio 1

Vídeo del 12/05/2021.

Definición

Sea G un grupo y X un G-conjunto. Un elemento $x \in X$ diremos que es un elemento fijo por la acción si ${}^g x = x \;\; \forall g \in G$. El conjunto de los elementos fijos lo denotaremos por $Fix(X)$

$$Fix(X) = \{x \in X \mid^g x = x \;\; \forall g \in G\}$$

Notemos que

$$x \in Fix(X) \iff \theta(x) = \{x\} \iff Stab_G(x) = G$$

.

Sea G un grupo finito y X un G-conjunto finito. El conjunto ${}^X/_\sim$ también es finito. Supongamos:

$${}^X/_\sim = \{\theta(x_1), \theta(x_2), ..., \theta(x_r)\}$$

Sabemos que $X = \cup_{i=i}^r \theta(x_i)$ unión disjunta $\Rightarrow$

$$|X| = \sum_{i=1}^r |\theta(x_i)| = |Fix(X)| + \sum_{x \notin Fix(X)} |\theta(x_i)| =$$

$$= |Fix(X)| + \sum_{x_i \notin Fix(X)} [G : Stab_G(x_i)]$$

Ejemplo

1) Sea G un grupo cualquiera y consideramos la acción de G sobre sí mismo por traslación

$$G \times G \to G \qquad {}^g h := gh$$

Sea $h \in G$

$$\theta(h) = \{{}^g h \mid g \in G\} = \{gh \mid g \in G\} = G$$

Por tanto $\forall h, h' \in G$, se tiene que $\theta(h) = \theta(h')$, es decir, esta acción es transitiva.

$$Stab_G(h) = \{g \in G \mid^g h = h\} = \{g \in G \mid gh = h\} = \{1\}$$

$$Fix(G) = \{h \in G \mid^g h = h \;\; \forall g \in G\} = \{h \in G \mid gh = h \;\; \forall g \in G\} = \emptyset$$

2) Sea G un grupo y consideramos la acción de G sobre sí mismo por conjugación
$$G \times G \to G \qquad {}^g h = ghg^{-1}$$
$h \in G$
$$\theta(h) = \{ {}^g h \mid g \in G\} = \{ghg^{-1} \mid g \in G\}$$
se llama la clase de conjugación del elemento h en G y se denota por $cl(h)$.
$$Stab_G(h) = \{g \in G \mid {}^g h = h\} = \{g \in G \mid ghg^{-1} = h\} =$$
$$= \{g \in G \mid gh = hg\} \leqslant G$$
se llama el centralizador de h en G y se denota por $c_G(h)$.
$$Fix(G) = \{h \in G \mid {}^g h = h \ \ \forall g \in G\} =$$
$$= \{h \in G \mid ghg^{-1} = h \ \ \forall g \in G\} = \{h \in G \mid gh = hg \ \ \forall g \in G\} = Z(G)$$
Supongamos que G es un grupo finito.
$$G/\sim = \{cl(h_1), cl(h_2), ..., cl(h_r)\}$$
Entonces
$$|G| = |Z(G)| + \sum_{h_i \notin Z(G)} |cl(h_i)| = |Z(G)| + \sum_{h_i \notin Z(G)} [G : c_g(h_i)]$$
(Fórmula de las clases)

Relación 6: Ejercicio 9

Vídeo del 12/05/2021.

Relación 6: Ejercicio 7

Vídeo del 17/05/2021.

Definición

Sea p un número primo. Un grupo finito G no trivial diremos que es un p-grupo si todo elemento de G tiene orden una potencia de p.

Ejemplos

1) Para cada $n \geq 1, C_{p^n} =< x \mid m^{p^n} = 1 >$ es un p-grupo.
Porque si $a \in C_{p^n} \Rightarrow ord(a) \mid |C_{p^n}| = p^n \Rightarrow ord(a) = p^k \;\; 0 \leq k \leq n$.

2) Para cada $n \geq 2$, el producto directo

$$G = C_p \times C_p \times \overset{n}{\cdots} \times C_p$$

es un p-grupo.
Si $(x_1, ..., x_n) \in G$

$$ord((x_1, ..., x_n)) = mcm(ord(x_1), ..., ord(x_n)) = p^k \;\; 0 \leq k \leq 1$$

Así todo elemento de G tiene orden una potencia de p.

3) Si G es un grupo con $|G| = p^n$ para $n \geq 1$ entonces, razonando como en el ejemplo 1, G es un p-grupo.

Teorema de Cauchy

Sea G un grupo finito. Para cada primo p divisor de G existe $x \in G$ tal que $ord(x) = p$ (entonces $\exists H =< x >\leqslant G$ tal que $|H| = p$).

Demostración

Sea $|G| = n$ y $p \mid n$, p número primo.
Sea X definido como sigue:

$$X := \{(x_1, x_2, ..., x_p) \in G^p \mid x_1 x_2 ... x_p = 1 \Rightarrow x_1 = (x_2 ... x_p)^{-1}\}$$

Como $|G| = n \Rightarrow |X| = n^{p-1}$.
Consideramos $\sigma = (1\ 2\ ...\ p) \in S_p$ y $H =< \sigma >= \{1, \sigma, \sigma^2, ..., \sigma^{p-1}\}$. Definimos una acción de H sobre X como sigue:

$$H \times X \to X$$

$$^{\sigma^0}(x_1, ..., x_p) := (x_1, ..., x_p)$$

$$1 \leq j \leq p-1 \qquad ^{\sigma^j}(x_1, ..., x_p) := (x_{j+1}, ..., x_p, x_1, ..., x_j)$$

(Ejercicio: Demostrad que en efecto tenemos una acción)
Sea $(x_1, ..., x_p) \in X$

$$O((x_1, ..., x_p)) = \{^{\sigma^j}(x_1, ..., x_p) \mid 0 \leq j \leq p-1\} =$$

$$= \{(x_1, ..., x_p), (x_2, ..., x_p, x_1), (x_3, ..., x_p, x_1, x_2), ..., (x_p, x_1, ..., x_{p-1})\}$$

$|O((x_1,...,x_p))|$ divide a $|H| = p \Rightarrow |O((x_1,...,x_p)) = 1$ ó p.
Los elementos con $|O(x_1,...,x_p)| = 1$ son precisamente $(x_1,...,x_p) \in Fix(X)$.

$$(x_1,...,x_p) \in Fix(X) \iff x_1 = x_2 = ... = x_p$$

Puesto que $(1,1,...,1) \in Fix(X)$, entonces $Fix(X) \neq \emptyset$.
Sabemos

$$|X| = |Fix(X)| + \sum_{(x_1,...,x_p) \notin Fix(X)} |O(x_1,...,x_p)|$$

Si $(x_1,...,x_p) \notin Fix(X) \Rightarrow |O(x_1,...,x_p)| = p$.
Sea $r = |Fix(X)|$ y $s =$ nº de elementos $\notin Fix(X)$.

$$n^{p-1} = |x| = r + ps \Rightarrow \begin{cases} r = n^{p-1} - ps \\ p \mid n \end{cases} \Rightarrow p \mid r \Rightarrow r \geq 2$$

Decir que $r \geq 2$ significa que $\exists(x,x,...,x) \in Fix(X)$ y
$(x,x,...,x) \neq (1,1,...,1) \iff x \neq 1$.
Entonces como $(x,x,...,x) \in X$, por definición de X, $x...x = x^p = 1 \quad x \neq 1$.
Concluimos pues $\exists x \in X$ tal que $ord(x) = p$.

Corolario

Sea G un grupo finito no trivial.

$$G \text{ es un } p\text{-grupo} \iff |G| = p^n \text{ para algún } n \geq 1$$

Demostración

- $\Leftarrow$ Ejemplo 3.
- $\Rightarrow$ Sea $|G| = m (m \geq 1)$.
  Sea a un divisor primo de $m \Rightarrow$ por el teorema de Cauchy $\exists x \in G$ tal que $ord(x) = q$.
  Por otro lado, como G es un p-grupo entonces $ord(x) = p^k \;\; k \geq 1$.
  Consecuentemente:

  $$q = p^k \Rightarrow k = 1 \text{ y } p = q$$

  Si el único divisor primo de m es $p \Rightarrow m = p^n$ para algún $n \geq 1$.

Teorema de Burnside

Sea G un p-grupo finito. Entones $|Z(G)| \geq p$. En particular, $Z(G)$ no es trivial.

Demostración

Como G es un p-grupo, supongamos que $|G| = p^n, n \geq 1$.

Si G es abeliano $\Rightarrow Z(G) = G$ y se tendría el resultado.

Si G no es abeliano, por la fórmula de las clases

$$|Z(G)| = |G| - \sum_{h \notin Z(G)} |cl(h)|$$

Si $h \notin Z(G) \Rightarrow |cl(h)| > 1$ y como $|cl(h)| = [G : c_G(h)]$, es decir, $|cl(h)| \mid |G| = p^n$, entonces $|cl(h)| = p^k \ \ k > 0$. Consecuentemente, p es un divisor de $\sum_{h \notin Z(G)} |cl(h)|$. Como $p \mid |G|$, obtenemos que:

$$p \mid |Z(G)| \Rightarrow |Z(G)| \geq p$$

Corolario

Sea p un número primo y G un grupo con $|G| = p^2$. Entonces G es abeliano.

Demostración

Por el teorema de Burnside, $|Z(G)| \geq p$. Con lo que $|Z(G)| = p$ ó $|Z(G)| = p^2$.
Supongamos que $|Z(G)| = p$, entonces $\exists a \in G$ tal que $a \notin Z(G)$

$$c_G(a) \leqslant G \qquad c_G(a) = \{g \in G \mid ag = ga\}$$

Es claro que $Z(G) \lneqq c_G(a) \Rightarrow |c_G(a)| = p^2 \Rightarrow c_G(a) = G \Rightarrow a \in Z(G)$ (Contradicción).
Por tanto, $Z(G)| = p^2 = |G| \Rightarrow Z(G) = G \Rightarrow G$ es abeliano.

Corolario

Si G es un p-grupo finito entonces G es resoluble.

Demostración

Sea $|G| = p^n, n \geq 1$. Hacemos inducción en n.
Si $n = 1$, es decir, $|G| = p \Rightarrow G \cong C_p$ y por tanto resoluble.
Sea $n > 1$ y el resultado cierto para todo p-grupo de orden menor que p^n. Si G es abeliano $\Rightarrow G$ es resoluble y lo tendriamos. Supongamos G no abeliano.

$$1 \underset{\neq}{\trianglelefteq} Z(G) \underset{\neq}{\trianglelefteq} G$$

$\Rightarrow |Z(G)| = p^k \qquad 1 \leq k < n$.
Por hipótesis de inducción, $Z(G)$ es resoluble. Por otro lado

$$|{}^{G}/_{Z(G)}| = p^{n-k} \quad 1 \leq n - k < n$$

y entonces, por hipótesis de inducción $^{G}/_{Z(G)}$ es resoluble.

$$\begin{cases} Z(G) \trianglelefteq G \text{ resoluble} \\ ^{G}/_{Z(G)} \text{ resoluble} \end{cases} \Rightarrow G \text{ es resoluble.}$$

Definición

Sea G un grupo finito y p un número primo.
Un subgrupo H de G que sea p-grupo lo llamaremos un p-subgrupo de$G$.

Observación

El teorema de Cauchy nos dice que para cada primo p divisor de $|G|$ existe un $H \leqslant G, |H| = p$ y entonces un p-subgrupo.

6.1. Teoremas de Sylow

Primer teorema de Sylow

Sea G un grupo finito con $|G| = n$. Sea p un número primo divisor de n.
Entonces para cada potencia p^i con $p^i \mid n$ existe $H \leqslant G$ tal que $|H| = p^i$.

Demostración

Hacemos inducción en i.
Para $i = 1$, el resultado se sigue del Teorema de Cauchy.
Sea $i > 1$ y supongamos el resultado cierto para todo grupo finito con orden divisible por $p^j, j < i$.
Veamoslo para $i > 1.|G| = n$ y $p^i \mid n$ buscamos $H \leqslant G$ tal que $|H| = p^i$.
Hacemos inducción $|G|$. Como $p^i \mid n$ el primer caso es $|G| = p^i$ y entonces basta tomar $H = G$. Supongamos que $|G| = n > p^i$ y el resultado cierto para todo grupo de orden menor que n y divisible por p^i.

Caso 1 $\exists K \not\leqslant G$ tal que $p \nmid [G : K]$.
Como
$$\begin{cases} |G| = [G : K]|K| \\ p^i \mid |G| \\ p \nmid [G : K] \end{cases} \Rightarrow p^i \mid |K|$$

$$\begin{cases} p^i \mid |K| \\ K \not\leqslant G \Rightarrow |K| < |G| = n \end{cases} \underset{\text{por hipótesis de inducción}}{\Rightarrow} \exists H \leqslant K \text{ tal que}$$
$|H| = p^i$. Claramente $H \leqslant G$ y se tiene el resultado.

Caso 2 Para todo $K \leqslant G, p \mid [G : K]$.
Por la fórmula de las clases
$$|Z(G)| = |G| - \sum_{h \notin Z(G)} [G : c_G(h)]$$

$p \mid |G|$ y $p \mid \sum[G : c_G(h)] \Rightarrow p \mid |Z(G)|$.
Aplicamos el Teorema de Cauchy a $Z(G)$ y entonces $\exists N \leqslant Z(G)$ tal que $|N| = p$.
Como $N \leqslant Z(G) \Rightarrow N \trianglelefteq G$ (Ejercicio).
Podemos pues considerar ${}^{G}/{}_{N}$. Como $|N| = p$ y $p^i \mid |G| \Rightarrow p^{i-1} \mid |{}^{G}/{}_{N}|$.
Por hipótesis de inducción en la portencia de p,

$$\exists L \leqslant {}^{G}/{}_{N} \text{ tal que } |L| = p^{i-1}$$

$\Rightarrow L = {}^{H}/{}_{N} \quad N \trianglelefteq H \trianglelefteq G$.
$|{}^{H}/{}_{N}| = p^{i-1} \Rightarrow |H| = |{}^{H}/{}_{N}||N| = p^{i-1}p = p^i$.

Definición

Sea G un grupo finito y p un número divisor de G.
Sea p^k la máxima potencia de p que divide a $|G|$ (es decir, $|G| = p^k m$, $mcd(p, m) = 1$).
Los p-subgrupos de G de orden p^k se llaman p-subgrupos de Sylow de G.

Corolario

Todo grupo G tiene p-subgrupos de Sylow, para cada p divisor de $|G|$.

Ejemplos

1) $n \geq 2$ y $C_n =< x \mid x^n = 1 >$.
Sea $n = p_1^{t_1} p_2^{t_2} ... p_k^{t_k}$ la factorización de n en primos.
Para cada $1 \leq i \leq k$, los p_i-subgrupos de Sylow tienen orden $p_i^{t_i}$. Sólo hay uno que es

$$C_{p_i^{t_i}} =< x^{s_i} > \qquad s_i = p_1^{t_1} p_2^{t_2} ... p_{i-1}^{t_{i-1}} p_{i+1}^{t_{i+1}} ... p_k^{t_k}$$

2) $G = A_4, |A_4| = 12 = 3 \cdot 2^2$
Los 3-subgrupos de Sylow de A_r tienen orden 3 y entonces cíclicos de orden 3.

$$\mathcal{P}_1 =< (1\ 2\ 3) >, \mathcal{P}_2 =< (1\ 2\ 4) >, \mathcal{P}_3 < (1\ 3\ 4) >, \mathcal{P}_4 =< (2\ 3\ 4) >$$

Los 2-subgrupos de Sylow de A_4 tienen orden 4 y sólo tiene uno que es

$$K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Si $\mathcal{P}$ es un p-subgrupo de Sylow de G

$$|G| = p^k m \quad mcd(m, p) = 1$$

Entonces $|\mathcal{P}| = p^k$ y por tanto $[G : \mathcal{P}] = m \Rightarrow mcd(|\mathcal{P}|, [G : \mathcal{P}]) = 1$.

Lema

Sea G un grupo finito, p un número primo divisor de $|G|$ y $\mathcal{P}$ un p-subgrupo de Sylow de G.
Sea $H \leqslant G$ un p-subgrupo de G tal que $H \leqslant N_G(\mathcal{P})$, entonces $H \leqslant \mathcal{P}$.

Demostración

$\mathcal{P} \trianglelefteq N_G(\mathcal{P})$ Aplicamos el tercer teorema.
$H \leqslant N_G(\mathcal{P})$ de isomorfía y entonces:

$$^{H}/_{H \cap \mathcal{P}} \cong {}^{H\mathcal{P}}/_{\mathcal{P}}$$

Con lo que $r = [H : H \cap \mathcal{P}] = [H\mathcal{P} : \mathcal{P}]$.

$$r \mid |H| \overset{H \text{es un p-grupo}}{\Rightarrow} r = p^t \quad t \geq 0$$

Consideramos $\mathcal{P} \leqslant H\mathcal{P} \leqslant G$

$$\Rightarrow [G : \mathcal{P}] = [G : H\mathcal{P}][H\mathcal{P} : \mathcal{P}] = [G : H\mathcal{P}] \cdot r \Rightarrow r \mid [G : \mathcal{P}]$$

$\mathcal{P}$ subgrupo de Sylow $mcd([G : \mathcal{P}], |\mathcal{P}|) = 1$

$$\Rightarrow mcd(r, p) = 1$$

$$\begin{cases} mcd(r,p) = 1 \\ r = p^t \;\; t \geq 0 \end{cases} \quad \Rightarrow t = 0 \text{ y } r = 1.$$

Tenemos que $1 = [H : H \cap \mathcal{P}] \Rightarrow H = H \cap \mathcal{P} \Rightarrow H \leqslant \mathcal{P}$.

Segundo Teorema de Sylow

Sea G un grupo finito y p un número primo divisor de $|G|$. Supongamos que $|G| = p^k m$ con $mcd(p, m) = 1$. Entonces:

(a) Todo p-subgrupo de G está contenido en algún p-subgrupo de Sylow de G.

(b) Cualesquiera dos p-subgrupos de Sylow de G son conjugados (es decir, si $\mathcal{P}_1, \mathcal{P}_2$ son dos p-subgrupos de Sylow de G entonces $\exists g \in G$ tal que $\mathcal{P}_2 = g\mathcal{P}_1 g^{-1}$).

(c) Si $n_p :=$ número de p-subgrupos de Sylow de G, se tiene que

$$n_p \mid m \qquad \text{y} \qquad n_p \equiv 1 \bmod(p)$$

Demostración

$|G| = p^k m \qquad mcd(p,m) = 1$
$S = \{\mathcal{P} \leqslant G \mid \mathcal{P} \text{ es } p\text{-subgrupo de Sylow}\} = \{\mathcal{P} \leqslant G \mid |\mathcal{P}| = p^k\}$
$S \neq \emptyset$ y $|S| = n_p$.
Consideramos la acción de G sobre S por conjugación

$$G \times S \to S \qquad {}^g\mathcal{P} := g\mathcal{P}g^{-1}$$

$(|g\mathcal{P}g^{-1}| = |\mathcal{P}| = p^k \Rightarrow g\mathcal{P}g^{-1} \in S)$
Elegimos $\mathcal{P}_1 \in S$ fijo pero arbitrario.

$$T = O(\mathcal{P}_1) = \{g\mathcal{P}_1 g^{-1} \mid g \in G\}$$

$Stab_G(\mathcal{P}_1) = N_G(\mathcal{P}_1)$.
Sabemos $|T| = [G : N_G(\mathcal{P}_1)]$.
Consideramos $\mathcal{P}_1 \leqslant N_G(\mathcal{P}_1) \leqslant G$.

$$m \underset{\mathcal{P}_1 \in S}{=} [G : \mathcal{P}_1] = [G : N_G(\mathcal{P}_1)][N_G(\mathcal{P}_1) : \mathcal{P}_1] = |T|[N_G(\mathcal{P}_1) : \mathcal{P}_1]$$

Por tanto $|T| \mid m$ y $mcd(p, |T|) = 1$.

(a) Sea H un p-subgrupo de G no trivial, entonces $|H| = p^r \quad 1 \leq r \leq k$.

Consideramos la acción anterior de H sobre T

$$H \times T \to T \qquad {}^h\mathcal{P} := h\mathcal{P}h^{-1}$$

$(\mathcal{P} \in T \Rightarrow \mathcal{P} = g\mathcal{P}_1 g^{-1} \Rightarrow h\mathcal{P}h^{-1} = hg\mathcal{P}_1(hg)^{-1} \Rightarrow h\mathcal{P}h^{-1} \in T)$

$$|T| = \sum_{\mathcal{P} \in T} |O(\mathcal{P})| = \sum_{\mathcal{P} \in T} [H : Stab_H(\mathcal{P})]$$

Es fácil ver que $Stab_H(\mathcal{P}) = H \cap N_G(\mathcal{P})$.

$$\begin{cases} H \cap N_G(\mathcal{P}) \leqslant N_G(\mathcal{P}) \ \ \mathcal{P} \text{ p-subgrupo de Sylow de } G \\ H \cap N_G(\mathcal{P}) \leqslant H \Rightarrow H \cap N_G(\mathcal{P}) \text{ es un p-subgrupo de } G \end{cases} \overset{\text{Lema}}{\Rightarrow}$$

$$\overset{\text{Lema}}{\Rightarrow} \begin{cases} H \cap N_G(\mathcal{P}) \leqslant \mathcal{P} \\ H \cap N_G(\mathcal{P}) \leqslant H \end{cases} \Rightarrow H \cap N_G(\mathcal{P}) \leqslant \mathcal{P} \cap H$$

y puesto que $\mathcal{P} \cap H \leqslant H \cap N_G(\mathcal{P})$ obviamente $\Rightarrow$

$$H \cap N_G(\mathcal{P}) = H \cap \mathcal{P}$$

$$\Rightarrow |T| = \sum_{\mathcal{P} \in T} [H : H \cap \mathcal{P}] \Rightarrow$$

$$\Rightarrow |T| \mid m \qquad [H : H \cap \mathcal{P}] \mid |H| = p^r \quad \text{y} \quad mcd(p,m) = 1$$

Entonces $\exists \mathcal{P} \in T$ tal que $[H : H \cap \mathcal{P}] = 1 \Rightarrow H = H \cap \mathcal{P}$ lo que demuestra (a).

(b) Sean $\mathcal{P}_1, \mathcal{P}_2$ dos p-subgrupos de Sylow de G.
Aplicamos (a) a $H = \mathcal{P}_2$ y entonces $\exists \mathcal{P} \in T = \{g\mathcal{P}_1 g^{-1} \mid g \in G\}$ tal que

$$\begin{cases} \mathcal{P}_2 \leqslant \mathcal{P} \\ |\mathcal{P}_2| = p^k = |\mathcal{P}| \end{cases} \Rightarrow \mathcal{P}_2 = \mathcal{P}$$

Por tanto $\exists g \in G$ tal que $\mathcal{P}_2 = g\mathcal{P}_1 g^{-1}$ que es (b).

(c) Por (b),

$$S = T$$

y entonces $n_p = |S| = |T|$ y por tanto $|n_p| \mid m$.
Tomamos $H = \mathcal{P}_1$ en (a) y entonces la igualdad

$$|T| = \sum_{\mathcal{P} \in T} [H : H \cap \mathcal{P}]$$

se traduce en

$$n_p = \sum_{\mathcal{P} \in T} [\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}]$$

Como anteriormente $\exists \mathcal{P} \in S$ tal que

$$[\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}] = 1 \Rightarrow \mathcal{P}_1 = \mathcal{P}_1 \cap \mathcal{P} \Rightarrow \mathcal{P} \leqslant \mathcal{P}_1$$

$$\begin{cases} \mathcal{P} \leqslant \mathcal{P}_1 \\ \text{ambos son de Sylow} \quad |\mathcal{P}| = p^k = |\mathcal{P}_1| \end{cases} \Rightarrow \mathcal{P} = \mathcal{P}_1$$

Entonces $\exists$ único $\mathcal{P} = \mathcal{P}_1 \in S$ tal que $[\mathcal{P}_1 : \mathcal{P} \cap \mathcal{P}_1] = 1$ y para cualquier $\mathcal{P} \in S, \mathcal{P} \neq \mathcal{P}_1$, necesariamente $[\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}] > 1$ y entonces divisible por el número p.

$$n_p = 1 + \sum_{\substack{\mathcal{P} \in S \\ \mathcal{P} \neq \mathcal{P}_1}} [\mathcal{P}_1 : \mathcal{P}_1 \cap \mathcal{P}] \Rightarrow n_p = 1 + pr \Rightarrow n_p \equiv 1 \bmod(p)$$

Corolario

En las hipótesis del segundo Teorema de Sylow.
Sea $\mathcal{P}$ un p-subgrupo de Sylow de G.

$$\mathcal{P} \trianglelefteq G \iff n_p = 1$$

Demostración

Como $g\mathcal{P}g^{-1}$ es p-subgrupo de Sylow de G entonces

$$n_p = 1 \iff g\mathcal{P}g^{-1} = \mathcal{P} \ \forall g \in G \iff \mathcal{P} \trianglelefteq G$$

Corolario

Sea G un grupo finito en el que todos sus subgrupos de Sylow son normales. Entonces G es el producto directo interno de sus subgrupos de Sylow.

Demostración

Usamos el resultado de un ejercicio. Sea G un grupo finito, $H_1, ..., H_k$ $(k \geq 2)$ subgrupos normales de G tal que $mcd(|H_i|, |H_j|) = 1$. Entonces $|H_1...H_k| = |H_1|...|H_k|$.

Supongamos $|G| = n = p_1^{t_1} p_2^{t_2} ... p_k^{t_k}$ su factorización en números primos. Para cada $1 \leq i \leq k$ sea $\mathcal{P}_i$ el único p_i-subgrupo de Sylow de G ($\mathcal{P} \trianglelefteq G \Rightarrow n_{p_i} = 1$).

1. $\mathcal{P} \trianglelefteq G \quad i = 1, ..., k.$

2. $|\mathcal{P}_i| = p_i^{t_i} \quad 1 \leq i \leq k.$

$$mcd(|\mathcal{P}_i|, |\mathcal{P}_j|) = 1 \quad \text{si } i \neq j$$

y entonces por el ejercicio anterior

$$|\mathcal{P}_1\mathcal{P}_2...\mathcal{P}_k| = p_1^{t_1} p_2^{t_2} ... p_k^{t_k} = |G| \Rightarrow \mathcal{P}_1\mathcal{P}_2...\mathcal{P}_k = G$$

3. $(\mathcal{P}_1...\mathcal{P}_{i-1}) \cap \mathcal{P}_i = 1 \quad \forall i = 2, ..., k.$
En efecto si $x \in (\mathcal{P}_1...\mathcal{P}_{i-1}) \cap \mathcal{P}_i \Rightarrow$
$$\begin{cases} \Rightarrow ord(x) \mid |\mathcal{P}_1...\mathcal{P}_{i-1}| = p_1^{t_1}...p_{i-1}^{t_{i-1}} \\ ord(x) \mid |\mathcal{P}_i| = p_i^{t_i} \end{cases} \Rightarrow ord(x) = 1 \Rightarrow x = 1.$$
Consecuentemente, G es el producto directo interno de $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_k$. En otros términos
$$G \equiv \mathcal{P}_1 \times \mathcal{P}_2 \times ... \times \mathcal{P}_k$$

Ejemplo

Si G es un grupo abeliano finito entonces para p primo divisor de $|G|, n_p = 1$ puesto que todo subgrupo de G es normal. Además si $\mathcal{P}$ es el único p-subgrupo de Sylow de G, esta es dada por

$$\mathcal{P} = \{x \in G \mid ord(x) = p^i \quad 0 \leq i \leq k\}$$

siendo p^k la máxima potencia de p que divide a G (Ejercicio).
$\mathcal{P}$ se llama la componente p-primaria de G.

6.2. Ejercicios

Relación 5: Ejercicio 20

Vídeo del 19/05/2021.

Relación 5: Ejercicio 21

Vídeo del 19/05/2021.

Relación 5: Ejercicio 23

Vídeo del 24/05/2021.

Relación 5: Ejercicio 26

Vídeo del 24/05/2021.

Relación 5: Ejercicio 25

Vídeo del 24/05/2021.

Relación 5: Ejercicio 30

Vídeo del 24/05/2021.

Relación 5: Ejercicio 32

Vídeo del 25/05/2021.

Relación 5: Ejercicios 35, 36 y 37

Vídeo del 25/05/2021.

Relación 5: Ejercicio 11

Vídeo del 25/05/2021.

Relación 5: Ejercicio 12

Vídeo del 26/05/2021.

Relación 3: Ejercicio 14

Vídeo del 26/05/2021.

Relación 5: Ejercicio 17

Vídeo del 26/05/2021.

Relación 5: Ejercicio 19

Vídeo del 26/05/2021.

7. Clasificación de grupos abelianos finitos

Usaremos dos resultados fundamentales:

(1) $C_n \times C_m \cong C_{nm} \iff mcd(n,m) = 1.$

(2) Si G es un grupo finito con $|G| = p_1^{n_1}...p_k^{n_k}$ y $n_{p_i} = 1 \ \forall i = 1,...,k$ entonces
$$G \cong \mathcal{P}_1 \times \mathcal{P}_2 \times ... \times \mathcal{P}_k$$
con $\mathcal{P}_i$ el único p_i-subgrupo de Sylow de G.

Proposición

Sea A un p-grupo abeliano con $|A| = p^n (n \geq 1)$. Entonces existen enteros $\beta_1 \geq \beta_2 \geq ... \geq \beta_t \geq 1$ tal que $\beta_1 + \beta_2 + ... + \beta_n = n$ y

$$A \cong C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times ... \times C_{p^{\beta_t}}$$

Además esta expresión es única, salvo el orden. Esto es, si:

$$A \cong C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times ... \times C_{p^{\alpha_s}}$$

donde $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_s \geq 1$ y $\alpha_1 + \alpha_2 + ... + \alpha_s = n$, entonces $s = t$ y $\alpha_i = \beta_i \ \forall i = 1,...,t$.

Definición

Un p-grupo abeliano finito E diremos que es un p-grupo abeliano elemental si $x^p = 1 \ \forall x \in E$.

Ejemplo

$$E = C_p \times C_p \times \overset{(n)}{\cdots} \times C_p \qquad n \geq 1$$

Lema

Sea E un p-grupo abeliano elemental. Entonces para cada $x \in E$ existe $M \leq E$ tal que E es el producto directo interno de M y $< x >$, es decir, $E \cong M\times < x >$.

Demostración

Si $x = 1$ tomando $M = E$ es claro que E es el producto directo interno de E y $< 1 >= \{1\}$. Supongamos $x \neq 1$ y entonces $ord(x) = p$.
Sea
$$\Sigma = \{H \leqslant E \mid x \notin H\}$$

$\Sigma \neq \emptyset$ (pues $\{1\} \in \Sigma$) y elegimos $M \in \Sigma$ de orden mayor.
Puesto que $x \notin M \Rightarrow M \lneq E \Rightarrow [E : M] > 1$.

Aseguramos que $[E : M] = p$ ($[E : M] \mid |E| = p^n \Rightarrow [E : M] = p^r \;\; r \geq 1$).

Supuesto ya visto que $[E : M] = p$ veamos que E es el producto directo interno de M y $< x >$.

1) Como E es abeliano, M y $< x >$ son subgrupos normales.

2) $M \cap < x >= \{1\}$

   Si $y \in M \cap < x > \Rightarrow \begin{cases} y \in M \\ y \in < x > \Rightarrow y = x^j \;\; 0 \leq j \leq p-1 \end{cases} \Rightarrow$
   $\Rightarrow < x^j > \leqslant M$.
   Como $x \notin M$, entonces $j = 0$, pues si $j \geq 1$ entonces $< x^j >=< x >$.
   Si $j = 0 \Rightarrow y = 1$.

3) $M :< x >= E$.

Aplicamos el 3º Teorema de isomorfia a $M \leqslant E$ y $< x > \leqslant E$, y obtenemos:

$$M < x > / < x > \cong M / M \cap < x > = M$$

$\Rightarrow |M < x > | = |M| \cdot | < x > |$.
Como $[E : M] = p \Rightarrow \frac{|E|}{|M|} = p \Rightarrow |M| = \frac{|E|}{p} = \frac{p^n}{p} = p^{n-1} \Rightarrow |M < x > | = p^{n-1}p = p^n = |E| \Rightarrow M < x >= E$.
Por tanto $E \cong M \times < x >$.

Veamos que $[E : M] = p$.
Supongamos que no fuera así, es decir que $[E : M] = p^i \;\; i \geq 2$.
Consideramos E/M que es también un p-grupo abeliano elemental

$$yM \in E/M \Rightarrow (yM)^p = y^p M = M$$

$$y \in E \Rightarrow y^p = 1$$

y entonces cualquier elemento distinto de M en E/M tiene orden p.
Elegimos $yM \in E/M \;\; yM \neq M \;\; \wedge \;\; yM \notin < xM >$.
$xM \in E/M, xM \neq M (x \notin M) \Rightarrow ord(xM) = p \Rightarrow < xM > \leq E/M$ y como $|E/M| = p^i \;\; i \geq 2 \Rightarrow | < xM > | = p \Rightarrow < xM > \lneq E/M$ y entonces $\exists yM$ en las condiciones anteriores.
Además también podemos asegurar que $xM \notin < yM >$ porque xM, yM tienen orden p.

Consideramos la proyección canónica:

$$\pi : E \to E/M \qquad \pi(a) = aM \;\; \forall a \in E$$

Sea $H = \pi^*(< yM >) = \{a \in E \mid \pi(a) \in < yM >\} = \{a \in E \mid aM \in < yM >\}$.

Como $xM \notin < yM > \Rightarrow x \notin H$.
Si $a \in M \Rightarrow aM = M \in < yM > \Rightarrow a \in H$, es decir, $M \leqslant H$.
Como $y \in H \ \ \wedge \ \ y \notin M$ entonces $M \lneq H$
$x \notin H \Rightarrow H \in \Sigma, M \lneq H$ en contra de la elección de M.

Definición

Sea $n \geq 1$. Una sucesión de enteros $\beta_1 \geq \beta_2 \geq ... \geq \beta_t \geq 1$ tal que $\beta_1 + \beta_2 + ... + \beta_t = n$ se llama una partición de n.

Ejemplo

Si $n = 5$, particiones:

$$\beta_1 = 5$$

$$\beta_1 = 4 \geq \beta_2 = 1$$

$$\beta_1 = 3 \geq \beta_2 = 2$$

$$\beta_1 = 3 \geq \beta_2 = 1 \geq \beta_3 = 1$$

$$\beta_1 = 2 \geq \beta_2 = 2 \geq \beta_3 = 1$$

$$\beta_1 = 2 \geq \beta_2 = 1 \geq \beta_3 = 1 \geq \beta_4 = 1$$

$$\beta_1 = 1 \geq \beta_2 = 1 \geq \beta_3 = 1 \geq \beta_4 = 1 \geq \beta_5 = 1$$

Demostración

Existencia (esquema) A abeliano y $|A| = p^n, n \geq 1$.
Hacemos inducción en n: Si $n = 1$, $|A| = p \Rightarrow A \cong C_p$.
Basta tomar $t = 1$ y $\beta_1 = 1$, y se tiene el resultado.
Sea $n > 1$ y el resultado cierto para todo p-grupo abeliano de orden menor que p^n.
Consideramos:

$$\varphi : A \rightarrow A \ \ \varphi(x) = x^p$$

Como A es abeliano entonces φ es un homomorfismo de grupos.
Sean

$$K = Ker(\varphi) = \{x \in A \mid x^p = 1\} \text{ y } H = Img(\varphi) = \{x^p \mid x \in A\}$$

Por el teorema de Cauchy, $\exists x \in A$ con $ord(x) = p$, es decir, $\exists x \in K, x \neq 1$. Por tanto, $K \neq 1$. Además se tiene:

- Por definición, K y ${}^{A}/_{H}$ son p-grupos abelianos finitos elementales.

$$(xH \in {}^{A}/_{H} \Rightarrow (xH)^p = x^pH \underset{x^p \in H}{=} H)$$

- Por el primer teorema de isomorfía.

$$A/K \cong H \Rightarrow [A:K] = |H|$$

- $|A/H| = \frac{|A|}{|H|} = \frac{|A|}{[A:K]} = |K| \Rightarrow [A:H] = |K| > 1 \Rightarrow h \lneq A$.

Entonces H es un p-grupo con $|H| = p^m$ siendo $m < n$.
Por hipótesis de inducción existen

$$\gamma_1 \geq \gamma_2 \geq ... \geq \gamma_r \geq 1 \text{ con } \gamma_1 + \gamma_2 + ... + \gamma_r = m$$

y

$$H \cong C_{p^{\gamma_1}} \times C_{p^{\gamma_2}} \times ... \times C_{p^{\gamma_r}}$$

Para cada $i = 1, ..., r$, sea $h_i \in H$ tal que $< h_i > \cong C_{p^{\gamma_i}}$. Notemos que

$$H \cong < h_1 > \times < h_2 > \times ... \times < h_r >$$

Puesto que $H = Img(\varphi) = \{x^p \mid x \in A\}$, para cada $i = 1, ..., r$, elegimos $g_i \in A$ tal que $\varphi(g_i) = g_i^p = h_i$.
Notemos que, puesto que $ord(h_i) = p^{\gamma_i} \Rightarrow ord(g_i) = p^{\gamma_i + 1}$.
Consideramos el siguiente subgrupo de A

$$H \leqslant A_0 := < g_1, g_2, ..., g_r > \leqslant A$$

Se verifica

(a) $A_0 \cong < g_1 > \times < g_2 > \times ... \times < g_r$.
$(|A_0| = \prod_{i=1}^r ord(g_i) = \prod_{i=1}^r p^{\gamma_i + 1} = p^{\sum_{i=1}^r \gamma_i + r} = p^{m+r})$

(b) $A_0/H \cong < g_1 H > \times < g_2 H > \times ... \times < g_r H >$.
A_0/H es un p-grupo abeliano elemental y $|A - 0/H = p^r$.

(c) $H \cap K \cong < k_1 > \times < k_2 > \times ... \times < k_r >$ donde

$$k_i = h_i^{p^{\gamma_i - 1}} \quad i = 1, ..., r$$

Además, $H \cap K$ es un p-grupo abeliano elemental de orden p^r.

Supuesto demostrado (a), (b) y (c), veamos el resultado de la existencia para el grupo A.

Caso 1. $K \leq H \Rightarrow H \cap K = K \underset{(c)}{=} |K| = p^r$.

Como $\begin{cases} [A:H] = |K| = p^r \\ \text{Por } (b) \ \ [A_0 : H] = p^r \end{cases} \Rightarrow [A:H] = [A_0 : H] \Rightarrow A = A_0$

Por (a):

$$A \cong < g_1 > \times < g_2 > \times ... \times < g_r > \cong C_{p^{\gamma_1 + 1}} \times C_{p^{\gamma_2 + 1}} \times ... \times C_{p^{\gamma_r + 1}}$$

Entonces hemos encontrado

$$\beta_1 = \gamma_1 + 1 \geq \beta_2 = \gamma_2 + 1 \geq ... \geq \beta_r = \gamma_r + 1$$

y $\beta_1 + ... + \beta_r = \gamma_1 + ... + \gamma_r + r = m + r = n$, pues $A = A_0 \Rightarrow |A| = p^n = |A_0| = p^{m+r} \Rightarrow n = m + r$.

Caso 2. K no es un subgrupo de H.
Elegimos $x \in K - H (\Rightarrow ord(x) = p)$.

$$\begin{cases} xH \in {}^{A}/_{H} \;\; xH \neq H \\ {}^{A}/_{H} \text{ es elemental} \end{cases} \Rightarrow ord(xH) = p$$

Aplicamos el lema anterior a ${}^{A}/_{H}$ y a $xH \in {}^{A}/_{H}$ y entonces $\exists {}^{M}/_{H} \leqslant {}^{A}/_{H}$ tal que

$${}^{A}/_{H} \cong {}^{M}/_{H} \times < xH >$$

Es fácil ver (ejercicio) que entonces

$$A \cong M \times < x >$$

$|A| = p^n$ y $| < x > | = ord(x) = p \Rightarrow |M| = p^{n-1}$.
Por hipótesis de inducción

$$\exists \beta_1 \geq \beta_2 \geq ... \geq \beta_t \geq 1$$

tal que

$$\beta_1 + \beta_2 + ... + \beta_t = n - 1$$

$$M \cong C_{p^{\beta_1}} \times ... \times C_{p^{\beta_t}}$$

Entonces tomando $\beta_{t+1} = 1$ se tiene una partición de n.

$$A \cong M \times < x > \cong C_{p^{\beta_1}} \times ... \times C_{p^{\beta_t}} \times C_{p^{\beta_{t+1}}}$$

y se tiene el resultado.

Teorema de estructura de grupos abelianos finitos

Sea A un grupo abeliano finito con $|A| = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$ la factorización en primos. Entonces

$$A \cong \prod_{i=1}^{k} (\prod_{j=1}^{t_i} C_{p_i^{n_{ij}}})$$

donde para cada $i = 1, ..., k$

$$n_{i1} \geq n_{i2} \geq ... \geq n_{it_i} \geq 1 \text{ y } n_{i1} + n_{i2} + ... + n_{it_i} = r_i$$

Además, esta descomposición es única (salvo el orden) y se llama la Descomposición Cíclica Primaria (DCP) del grupo A.
Al conjunto

$$\{p_i^{n_{ij}} \mid 1 \leq i \leq k, 1 \leq j \leq t_i\}$$

se les llama divisores elementales del grupo A.

Demostración

$$|A| = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$$

Al abeliano y entonces para cada $i = 1, ..., k$, hay un único p_i-subgrupo de Sylow $\mathcal{P}i$

$$|\mathcal{P}_i| = p_i^{r_i} \quad \forall 1, ..., k$$

Sabemos además que

$$A \cong \mathcal{P}_1 \times \mathcal{P}_2 \times ... \times \mathcal{P}_k \qquad (1)$$

Para cada $i = 1, ..., k$, $\mathcal{P}_i| = p_i^{r_i}$ es un p_i-subgrupo abeliano y entonces, por la proposición anterior, existen

$$n_{i1} \geq n_{i2} \geq ... \geq n_{it_i} \geq 1 \text{ tal que } n_{i1} + n_{i2} + ... + n_{it_i} = r_i$$

y $\mathcal{P}_i \cong C_{p_i}^{n_{i1}} \times C_{p_i}^{n_{i2}} \times ... \times C_{p_i}^{n_{it_i}} \qquad (2)$

Combinando (1) y (2) obtenemos la descomposición buscada.
La unicidad es consecuencia de la unicidad de la descomposición de cada $\mathcal{P}_i$.

Observación

Un grupo abeliano finito está totalmente determinado por sus divisores elementales.
Consecuentemente, dos grupos abelianos finito son isomorfos $\iff$ tiene los mismos divisores elementales.

Este hecho nos permite dar la lista de los distintos grupos no abelianos, no isomorfos entre sí, de un orden determinado, dando todas las listas de posibles divisores elementales.

Ejemplo

Determinar, salvo isomorfismo, todos los grupos abelianos de orden 360.

$$360 = 2^3 3^2 5$$

1) $\{2^3, 3^2, 5\} \to C_8 \times C_9 \times C_5$
2) $\{2^3, 3, 3, 5\} \to C_8 \times C_3 \times C_3 \times C_5$
3) $\{2^2, 2, 3^2, 5\} \to C_4 \times C_2 \times C_9 \times C_5$
4) $\{2^2, 2, 3, 3, 5\} \to C_4 \times C_2 \times C_3 \times C_3 \times C_5$
5) $\{2, 2, 2, 3^2, 5\} \to C_2 \times C_2 \times C_2 \times C_9 \times C_5$
6) $\{2, 2, 2, 3, 3, 5\} \to C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$

$$C_n \times C_m \cong C_{nm} \iff mcd(n, m) = 1$$

Teorema de descomposición cíclica de un grupo abeliano finito (DC)

Sea A un grupo abeliano finito. Entonces:

$$A \cong C_{d_1} \times C_{d_2} \times ... \times C_{d_t}$$

donde $d_1, d_2, ..., d_t$ son enteros positivos tal que

$$|A| = d_1 d_2 ... d_t \text{ y } d_i \mid d_j \text{ para cada } j \leq i$$

Además esta descomposición es única, esto es, si

$$A \cong C_{m_1} \times C_{m_2} \times ... \times C_{m_s}$$

con $|A| = m_1 m_2 ... m_s$ y $m_i \mid m_j$ para cada $j \leq i$, entonces $s = t$ y $d_i = m_i \ \ \forall i$.

A los $\{d_1, d_2, ..., d_t\}$ se les llama factores invariantes del grupo A.

Demostración

$$|A| = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$$
$$A \cong \prod_{i=1}^{k} (\prod_{j=1}^{t_i} C_{p_i}^{n_{ij}})$$

Para cada $i = 1, ..., k$

$$n_{i1} \geq n_{i2} \geq ... \geq n_{it_i} \qquad n_{i1} + n_{i2} + ... + n_{it_i} = r_i$$

Sea $t = \text{máx}\{t_1, t_2, ..., t_k\}$ y ponemos $n_{il} = 1$ para $t_i < l \leq t$.
Consideramos la siguiente matriz

$$\begin{pmatrix} p_1^{n_{11}} & p_2^{n_{21}} & ... & p_k^{n_{k1}} \\ p_1^{n_{12}} & p_2^{n_{22}} & ... & p_k^{n_{k2}} \\ \vdots & \vdots & ... & \vdots \\ p_1^{n_{1t}} & p_2^{n_{2t}} & ... & p_k^{n_{kt}} \end{pmatrix}$$

Sea

$$d_1 := p_1^{n_{11}} p_2^{n_{21}} ... p_k^{n_{k1}}$$
$$d_2 := p_1^{n_{12}} p_2^{n_{22}} ... p_k^{n_{k2}}$$
$$\vdots$$
$$d_t := p_1^{n_{1t}} p_2^{n_{2t}} ... p_k^{n_{kt}}$$

Es decir, cada d_i es el producto de la fila i-ésima.
Teniendo en cuenta que $n_{ij} \geq n_{ij+1} \ \ \forall i, \forall j$ entonces $d_i \mid d_j \ \ \forall j \leq i$.
Es claro que

$$C_{d_1} \cong C_{p^{n_{11}}} \times C_{p_2^{n_{21}}} \times ... \times C_{p_k^{n_{k1}}}$$
$$C_{d_2} \cong C_{p^{n_{12j}}} \times C_{p_2^{n_{22}}} \times ... \times C_{p_k^{n_{k2}}}$$
$$\vdots$$
$$C_{d_t} \cong C_{p^{n_{1t}}} \times C_{p_2^{n_{2t}}} \times ... \times C_{p_k^{n_{kt}}}$$

Entonces

$$A \cong C_{d_1} \times C_{d_2} \times ... \times C_{d_t}$$

Ejemplo

- Ejemplo anterior:

$$\{2, 2, 2, 3, 3, 5\} \to C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$$

Veamos cuál es su DC:

$$\begin{pmatrix} 2 & 3 & 5 \\ 2 & 3 & 1 \\ 2 & 1 & 1 \end{pmatrix} \begin{matrix} \to d_1 = 30 \\ \to d_2 = 6 \\ \to d_3 = 2 \end{matrix}$$

DC para los del tipo 6) es:

$$C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 \cong C_{30} \times C_6 \times C_2$$

- Otro caso:

$$\{2, 2, 2, 3^2, 5\} \to C_2 \times C_2 \times C_2 \times C_9 \times C_5$$

Veamos cuál es su DC:

$$\begin{pmatrix} 2 & 3^2 & 5 \\ 2 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix} \begin{matrix} \to d_1 = 90 \\ \to d_2 = 2 \\ \to d_3 = 2 \end{matrix}$$

DC para los del tipo 5) es:

$$C_2 \times C_2 \times C_2 \times C_9 \times C_5 \cong C_{90} \times C_2 \times C_2$$

- Y otro más:

$$\{2^2, 2, 3^2, 5\} \to C_4 \times C_2 \times C_9 \times C_5$$

Veamos cuál es su DC:

$$\begin{pmatrix} 2^2 & 3^2 & 5 \\ 2 & 1 & 1 \end{pmatrix} \begin{matrix} \to d_1 = 180 \\ \to d_2 = 2 \end{matrix}$$

DC para los del tipo 3) es:

$$C_4 \times C_2 \times C_9 \times C_5 \cong C_{180} \times C_2$$

Relación 6: Ejercicio 2

Vídeo del 02/06/2021.

Relación 6: Ejercicio 3

Vídeo del 02/06/2021.

Relación 6: Ejercicio 4

Vídeo del 02/06/2021.

Relación 6: Ejercicio 7

Vídeo del 02/06/2021.

8. Presentaciones de grupos. Productos semidirectos. Clasificación de grupos de orden bajo (≤ 5)

Definición

Sea G un grupo generado por $\{x_1, x_2, ..., x_n\}$. Cualquier ecuación que satisfagan los generadores se llama una relación del grupo G.

Por ejemplo, en D_n relaciones son:

$$r^n = 1 \qquad s^2 = 1 \qquad sr = r^{-1}s$$

también son relaciones en D_n

$$r^i = r^{n-i}s \qquad i \geq 1$$

En el grupo cíclico $C_n < x \mid x^n = 1 >$, una relación es

$$x^n = 1$$

también es una relación en C_n.

$$x^r = x^{\text{res}(r,n)}$$

Definición

Dar un grupo G (finitamente generado) por generadores y relaciones es dar un conjunto de generadores $S = \{x_1, x_2, ..., x_n\}$ de G y un conjunto de relaciones $\{R_1, R_2, ..., R_m\}$ (cada R_i es una ecuación en los generadores $x_1, ..., x_n$ y el 1) tal que cualquier otra relación de G entre los elementos de S (en particular la tabla de G) puede deducirse a partir de $\{R_1, ..., R_m\}$.

A estos generadores y relaciones lo llamaremos una presentación de G y escribiremos

$$G =< x_1, ..., x_n \mid R_1, ..., R_m >$$

Ejemplos

$$D_n =< r, s \mid r^n = 1 \;\; s^2 = 1 \;\; sr = rs >$$

$$C_n =< x \mid x^n = 1 >$$

$$K =< a, b \mid a^2 = 1 \;\; b^2 = 1 \;\; ab = ba >$$

Se verifica que todo grupo finitamente generado admite una presentación.

Teorema de Dyck

Sea G un grupo y son

$$G =< x_1, ..., x_n \mid R_1, ..., R_m >$$

una presentación de G.
Sea H un grupo y $a_1, a_2, ..., a_n \in H$ tal que las ecuaciones $R_1, ..., R_m$ son válidas en H al sustituir x_i por a_i $(i = 1, ..., n)$.

Entonces existe un único homomorfismo de grupos

$$f : G \to H$$

tal que $f(x_i) = a_i \ \ \forall i = 1, ..., n$.
Además, si $H =< a_1, a_2, ..., a_n >$, entonces f es un epimorfismo.

Ejemplo

$Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$ puede ser presentado como

$$Q_2 =< a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b >$$

En efecto, sea:

$$G =< a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b >$$

Consideramos $i, j \in Q_2$. Sabemos que:

$$i^4 = 1$$

$$j^2 = -1 = i^2$$

$$ji = -k = (-i)j = i^3 j = i^{-1} j$$

Entonces por el Teorema de Dick, $\exists !$ homomorfismo

$$f : G \to Q_2 \qquad \begin{cases} f(a) = i \\ f(b) = j \end{cases}$$

Además, puesto que $Q_2 =< i, j >$, es un epimorfismo. Por el primer teorema de isomorfía

$$Q/_{Ker(f)} \cong Q_2$$

Veamos que $Ker(f) = \{1\}$ y lo vamos observando que $|G| = 8$:

$$G =< a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b >$$

Sea $H =< a > \ \ |H| = ord(a) = 4$. Como $bab^{-1} = a^{-1}bb^{-1} = a^{-1} \in H \Rightarrow H \trianglelefteq G$.
$G/_H =< bH >$.
Como $(bH)^2 = b^2 H = a^2 H = H \Rightarrow ord(bH) = 2 \Rightarrow |G/_H| = 2$.

Por tanto, $|G| = |G/_H||H| = 2 \cdot 4 = 8$.

$$G \cong Q_2$$

Definición

Para cada $k \geq 1$ se define el k-ésimo grupo dicíclico como el grupo presentado por

$$Q_k =< a, b \mid a^{2k} = 1, b^2 = a^k, ba = a^{-1}b >$$

$k = 2$ Q_2 es los cuaternios.
$k = 1$ $Q_1 =< a, b \mid a^2 = 1, b^2 = a, ba = a^{-1}b >= C_4 =< b \mid b^4 = 1 >$,
$k \geq 2$ Q_k no es abeliano.

$$Q_k =< a, b \mid a^{2k} = 1, b^2 = a^k, ba = a^{-1}b >$$

$a^{2k} = 1$ es decir $ord(a) = 2k$ entonces $0 \leq i \leq 2k - 1$.
Como $b^2 = a^k \Rightarrow ord(b^2) = ord(a^k) = \frac{2k}{mcd(k,2k)} = \frac{2k}{k} = 2$.
Así que $ord(b^2) = 2 \Rightarrow ord(b) = 4$ y entonces $0 \leq j \leq 3, 0 \leq i \leq 2k-1$.

- Si $j = 2$, $a^i b^2 = a^i a^k = a^{i+k}, b^2 = a^k$.
- Si $j = 3$, $a^i b^3 = a^i b^2 b = a^i a^k b = a^{i+k} b$.

$$Q_k = \{a^i b^j \mid 0 \leq i \leq 2k - 1, 0 \leq j \leq 1\}$$

$$|Q_k| = 4k$$

$$a^i a^s = a^{\text{res}(i+s;2k)}$$

$$a^i (a^s b) = a^{\text{res}(i+s;2k)} b$$

$$(a^s b) a^i \underset{ba=a^{-1}b}{=} a^s a^{-1} b = a^{\text{res}(s-i;2k)} b$$

$$(a^s b)(a^i b) = a^s a^{-i} bb = a^s a^{-i} a^k = a^{s+k-i} = a^{\text{res}(s+k-1;2k)}$$

$k \geq 3$ $\exists N \trianglelefteq Q_k$ tal que ${}^{Q_k}/_{N} \cong D_k$ y entonces Q_k no es abeliano.

$$D_k =< r, s \mid r^n = 1, s^2 = 1, sr = r^{-1}s >$$

$$Q_k =< a, b \mid a^{2k} = 1, b^2 = a^k, ba = a^{-1}b >$$

$$r^{2k} = 1 \qquad s^2 = 1 = r^k \qquad sr = r^{-1}s$$

Teorema de Dyck

$$f : Q_k \to D_k \qquad \begin{cases} f(a) = r \\ f(b) = s \end{cases}$$

es un epimorfismo

$${}^{Q_k}/_{Kerf} \cong D_k$$

Clasificación de los grupos de orden ≤ 15

(1) Los de orden 2, 3, 5, 7, 11 y 13 son respectivamente isomorfos a $C_2, C_3, C_5, C_7, C_{11}$ y C_{13}.

(2) Como todo grupo de orden p^2 (p primo) es abeliano entonces sólo hay dos que son

$$C_{p^2} \quad \text{y} \quad C_p \times C_p$$

Consecuentemente:

- Orden 4 tenemos C_4 y $C_2 \times C_2$.
- Orden 9 tenemos C_9 y $C_3 \times C_3$.

(3) Grupos de orden 6, 10 y 14.

Proposición

Si p es un primo impar entonces todo grupo de orden $2p$ es isomorfo a C_{2p} ó D_p.

Demostración

Sea G tal que $|G| = 2p$.

$$n_p \mid 2 \text{ y } n_p \equiv 1 mod(p) \Rightarrow n_p = 1$$

Por tanto $\exists! \mathcal{P} \trianglelefteq G$ tal que $|\mathcal{P}| = p \Rightarrow \mathcal{P} \cong \mathcal{C}_p$.
Supongamos $\mathcal{P} =< a \mid a^p = 1 >$.
$n_2 \mid p$ y $n_2 \equiv 1 mod(2) \Rightarrow n_2 = 1$ ó $n_2 = p$.

Caso $n_2 = 1$ Puesto que $n_p = 1$, entonces si $Q \trianglelefteq G$ es el único 2-subgrupo de Sylow, $G \cong \mathcal{P} \times Q \cong C_p \times C_2 \cong C_{2p}$.

Caso $n_2 = p$ G no es abeliano.

$$\mathcal{P} =< a \mid a^p = 1 >$$

Como $[G : \mathcal{P}] = \frac{|G|}{|\mathcal{P}|} = \frac{2p}{p} = 2$ y entones hay únicamente dos clases laterales a derecha:

$$\{\mathcal{P}, \mathcal{P}_n\} \quad b \notin \mathcal{P}$$

Entonces

$$G = \mathcal{P} \cup \mathcal{P}b = \{1, a, ..., a^{p-1}, b, ab, ..., a^{p-1}b\}$$

Veamos que $ord(b) = 2$.

En efecto, $ord(b) \mid |G| = 2p \Rightarrow ord(b) = \begin{cases} \cancel{1} & b \neq 1 \\ 2 & \\ \cancel{p} & (< b >= \mathcal{P} \Rightarrow b \in \mathcal{P}) \\ \cancel{2p} & G \text{ no es abeliano} \end{cases}$

Veamos que $ba = a^{-1}b$. En efecto:

$$ord(ba) \mid |G| = 2p \Rightarrow ord(ba) = \begin{cases} \cancel{1} & (ba = 1 \Rightarrow b = a^{-1} \in \mathcal{P}) \\ 2 & \\ \cancel{p} & (< ba >= \mathcal{P} \Rightarrow ba \in \mathcal{P} \Rightarrow b \in \mathcal{P}) \\ \cancel{2p} & G \text{ no es abeliano} \end{cases}$$

$\Rightarrow ord(ba) = 2 \Rightarrow (ba)^2 = baba = 1 \Rightarrow ba = (ba)^{-1} =$
$= a^{-1}b^{-1} \underset{ord(b)=2}{=} a^{-1}b$

$$G =< a, b \mid a^p = 1, b^2 = 1, ba = a^{-1}b >\cong D_p$$

Grupos de orden 6: C_6 y D_3.
Grupos de orden 10: C_{10} y D_5.
Grupos de orden 14: C_{14} y D_7.

(4) Todo grupo de orden 15 es isomorfo a C_{15}

$$|G| = 15 = 3 \cdot 5$$

$n_3 \mid 5$ y $n_3 \equiv 1 \bmod(3) \Rightarrow n_3 = 1$.
$n_5 \mid 3$ y $n_5 \equiv 1 \bmod(5) \Rightarrow n_5 = 1$.
$\Rightarrow G \cong \mathcal{P} \times Q$.

$\mathcal{P}$ 3-subgrupo se Sylow (que es único).
Q 5-subgrupo de Sylow (que es único).

$$|\mathcal{P}| = 3 \Rightarrow \mathcal{P} \cong C_3$$

$|Q| = 5 \Rightarrow Q \cong C_5$

$$G \cong C_3 \times C_5 \cong C_{15}$$

(5) Grupos de orden 8.

Caso abeliano: $|G| = 8 = 2^3$.
Div. Elementales:

$$\{2^3\} \to C_8$$

$$\{2^2, 2\} \to C_4 \times C_2$$

$$\{2, 2, 2\} \to C_2 \times C_2 \times C_2$$

Caso no abeliano: $|G| = 8$ y G no abeliano
Como G no es abeliano los elementos no triviales tienen orden 2 ó 4.
Por otro lado, como G no es abeliano, no todos los elementos de G tienen orden 2 (Ejercicio de Relación 2).

Consecuentemente, $\exists a \in G$ tal que $ord(a) = 4$.
Sea

$$H =< a >= \{1, a, a^2, a^3\}$$

Como $[G : H] = \frac{|G|}{|H|} = \frac{8}{4} = 2 \Rightarrow H \trianglelefteq G$ y el número de clases laterales a derecha módulo H es exactamente 2:

$$\{H, Hb\} \quad b \notin H$$

Por tanto

$$G = H \cup Hb = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

Consideramos el elemento $b^2 \in G$

$$b^2 \in H \cup Hb \Rightarrow \begin{cases} b^2 \in H \\ b^2 \in Hb \Rightarrow b^2 = a^i b \;\; 0 \leq i \leq 3 \Rightarrow b = a^i \in H(!!!) \end{cases}$$

Así que $b^2 \in H = \{1, a, a^2, a^3\}$.
Si $b^2 = a \Rightarrow ord(b^2) = 4 \Rightarrow ord(b) = 8$.
$4 = ord(b^2) = \frac{ord(b)}{mcd(2, ord(b))} = \frac{ord(b)}{2}$.
$\Rightarrow G$ sería abeliano (!!!).
Por el mismo razonamiento, $b^2 \neq a^3$.
Así que $b^2 = 1$ o $b^2 = a^2$.

Caso $b^2 = 1$ Veamos que $ba = a^{-1}b = a^3b$.
Como $H \trianglelefteq G \Rightarrow bab^{-1} = bab \in H \Rightarrow b^2 = 1$.

$$bab = \begin{cases} \cancel{1} & (bab = 1 \Rightarrow ba = b \Rightarrow a = 1(!!!)) \\ \cancel{a} & (bab = a \Rightarrow ba = ab \Rightarrow G \text{ es abeliano } (!!!)) \\ \cancel{a^2} & \\ a^3 & \end{cases}$$

Si $bab = a^2 \Rightarrow (ba)^2 = baba = a^3 \Rightarrow ord((ba)^2) = ord(a^3) = 4 \Rightarrow ord((ba)) = 8$ en contra de G no es abeliano.
Luego $bab = a^3 \Rightarrow ba = a^3b$

$$G =< a, b \mid a^4 = 1, b^2 = 1, ba = a^3b >\cong D_4$$

Caso $b^2 = a^2$ Veamos que $ba = a^{-1}b = a^3b$.
Como $H \trianglelefteq G \Rightarrow bab^{-1} \in H$.

$$bab^{-1} = \begin{cases} \cancel{1} & (bab^{-1} = 1 \Rightarrow ba = b \Rightarrow a = 1(!!!)) \\ \cancel{a} & (bab^{-1} = a \Rightarrow ba = ab \Rightarrow G \text{ es abeliano } (!!!)) \\ \cancel{a^2} & \\ a^3 & \end{cases}$$

$bab^{-1} = a^2 \Rightarrow bab^{-1} = b^2 \Rightarrow ab^{-1} = b \Rightarrow a = b^2 \underset{a^2=b^2}{\Rightarrow} a = a^2 \Rightarrow a = 1(!!!)$
$bab^{-1} = a^3 \Rightarrow ba = a^3 b$

$$G =< a, b \mid a^4 = 1, a^2 = b^2, ba = a^{-1}b >\cong Q_2$$

(6) Grupos de orden 12

Caso abeliano: G abeliano y $|G| = 12 = 3 \cdot 2^2$.
Div. Elementales:

$$\{2^2, 3\} \rightarrow G \cong C_4 \times C_3 \cong C_{12}$$

$$\{2, 2, 3\} \rightarrow G \cong C_2 \times C_2 \times C_3 \cong C_6 \times C_2$$

Caso no abeliano: $|G| = 12 = 3 \cdot 2^2$
$n_3 \mid 4$ y $n_3 \equiv 1 mod(3) \Rightarrow n_3 = 1$ ó $n_3 = 4$.
Si $n_3 = 4$ (Rel 5) $G \cong A_4$.
Si $n_3 = 1$ Sea $\mathcal{P} \trianglelefteq G$ con $\mathcal{P} = 3$
$\mathcal{P} \cong C_3$ y $\mathcal{P} =< x \mid x^3 = 1 >$
($n_2 \mid 3$ y $n_3 \equiv 2(mod2) \Rightarrow \cancel{n_2 = 1}$ o $n_2 = 3$)
Veamos que en G hay un elemento de orden 6:
Consideramos $cl(x) = \{gxg^{-1} \mid g \in G\}$.
Puesto que $\mathcal{P} \trianglelefteq G$ entonces $cl(x) \leq \mathcal{P} = \{1, x, x^2\}$.
Además $1 \notin cl(x)$ (si $1 \in cl(x) \Rightarrow \exists g \in G$ tal que $x = gxg^{-1} \Rightarrow x = 1(!!!)$)
Entonces $cl(x) = \{x\}$ ó $cl(x) = \{x, x^2\}$.
Recordemos que

$$[G : c_G(x)] = |cl(x)|$$

donde $c_G(x) = \{g \in G \mid gx = xg\} \leqslant G$.
Entonces:

$$[G : c_G(x)] = 1 \text{ o } 2 \Rightarrow |c_G(x)| = 12 \text{ o } 6$$

En ambos casos, $2 \mid |c_G(x)|$ y, por el teorema de Cauchy, $\exists z \in c_G(x)$ tal que $ord(z) = 2$.
Sea $a := xz$ $\quad mcd(ord(x), ord(z)) = mcd(3, 2) = 1 \quad xz = zx$
$\overset{EjerRel2}{\Rightarrow} ord(a) = ord(x) \cdot ord(z) = 3 \cdot 2 = 6$.
Sea $K =< a >= \{1, a, a^2, a^3, a^4, a^5\}$

$$[G : K] = \frac{|G|}{|K|} = \frac{12}{6} = 2 \Rightarrow K \trianglelefteq G$$

Además hay únicamente dos clases laterales a derecha:

$$K, Kb \quad b \notin K$$

$G = K \cup Kb = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$
Veamos que $bab^{-1} = a^5$.
Como $\begin{cases} K \trianglelefteq G \Rightarrow bab^{-1} \in K \\ ord(bab^{-1}) = ord(a) = 6 \end{cases} \Rightarrow bab^{-1} = a$ o $bab^{-1} = a^5 \Rightarrow ba = ab(!!)$ o $ba = a^5b = a^{-1}b$
Consideramos $b^2 \in G = K \cup Kb \Rightarrow b^2 \in K$ ó $\cancel{b^2 \in Kb}$ pues $b \notin K$
Así que

$$b^2 \in K = \{1, \cancel{a}, \cancel{a^2}, a^3, \cancel{a^4}, \cancel{a^5}\}$$

Si $b^2 = a$ ó $a^5 \Rightarrow ord(b^2) = 6 \Rightarrow ord(b) = 12$ y G sería abeliano (!!!)
Si $b^2 = a^2 \Rightarrow bab^{-1} = a^{-1}$.
$(a^{-1})^2 = (bab^{-1})^2 = ba^2b^{-1} \underset{b^2=a^2}{=} bb^2b^{-1} = b^2 = a^2 \Rightarrow a^4 = 1$
en contradicción con que $ord(a) = 6$.
Si $b^2 = a^4$:
$(a^{-1})^4 = (bab^{-1})^4 = ba^4b^1 \underset{a^4=b^2}{=} bb^2b^{-1} = b^2 = a^4 \Rightarrow a^8 = 1$
en contradicción con que $ord(a) = 6$.
Entonces $b^2 = 1$ ó $b^2 = a_3$.
$b^1 = 1 \;\; G =< a, b \mid a^6 = 1, b^2 = 1, ba = a^{-1}b >= D_6$
$b^2 = a^3 \;\; G =< a, b \mid a^6 = 1, b^2 = a_3, ba = a^{-1}b >= Q_3$.

Relación 6: Ejercicio 9

Vídeo del 09/06/2021.

Relación 6: Ejercicio 10

Vídeo del 09/06/2021.