Álgebra II

Daniel Monjas Miguélez

13 de junio de 2021

Índice

23/02/2021

1. Tema 2. Grupos: Definición y ejemplos

1.1. Defincciones

Definición: Un grupo es un conjunto no vacío, $G \neq \emptyset$, junto con una operación interna,

$$\begin{aligned} \cdot : G \times G &\to G \\ (a, b) &\mapsto ab \end{aligned}$$

tal que se verifican las siguientes propiedades:

1. **Propiedad Asociativa:** $(ab)c = a(bc) \quad \forall a, b, c \in G$
2. **Existencia del Elemento Neutro:** $\exists 1 \in G$ tal que $a1 = a = 1a \ \forall a \in G$
3. **Existencia de inversos o elementos simétricos:** Para cada $a \in G$ existe $a^{-1} \in G$ tal que $aa^{-1} = 1 = a^{-1}a$

Si además se verifica,

- **Propiedad conmutativa:** $ab = ba \ \forall a, b \in G$

diremos que el grupo G es abeliano ó conmutativo.

Proposición 1: Sea G un grupo se tiene que,

(i) En G hay un único elemento neutro, que llamaremos la unidad o el uno de G.

(ii) Cada elemento de G tiene un único elemento inverso.

(iii) Para cada $a \in G$ se verifica $(a^{-1})^{-1} = a$.

(iv) Para cualesquiera $a, b \in G$, las ecuaciones

$$ax = b, \quad ya = b$$

donde x, y son las incógnitas, tiene solución y esta es única.

(v) Si $a \in G$ es un elemento tal que $a^2 = a$ entonces $a = 1$ (elemento neutro).

(vi) Sea $n \geq 1$, y $(a_1, a_2, \ldots, a_n) \in G^n$. Definimos el elemento $\prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n$, de forma inductiva como,

$$Si \;\; n = 1 \;\; \prod_{i=1}^{1} a_i = a_1$$

$$Si \;\; n > 1 \;\; \prod_{i=1}^{n} a_i := (\prod_{i=1}^{n-1}) a_n$$

(vii) $n \geq 1$ $(a_1, \ldots, a_n) \in G^n$

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

$$(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$$

(viii) Si $a_1 = a_2 = \ldots = a_n = a \in G \Rightarrow \prod_{i=1}^{n} a_i = a^n$, $n \geq 1$

(ix) Para todo $a \in G$ y todo $n \geq 1$ se verifica,

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

Definimos para cada $n \geq 1$ $a^{-n} := (a^n)^{-1} = (a^{-1})^n$, y para $n = 0$, $a^0 = 1$, donde 1 se refiere al elemento neutro.

(x) $\forall a \in G$, y $\forall r, s \in \mathbb{Z}$, se tiene que,

$$a^{r+s} = a^r a^s; \;\; (a^r)^s = a^{rs}$$

Proposición 2: **Propiedad Asociativa Generalizada.** Sea $n \geq 2$, entonces para cada m, con $1 \leq m < n$ se verifica,

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

Demostración: Si $n = 2$ entonces $m = 1$

$$\prod_{i=1}^{2} a_i = a_1 a_2 = (\prod_{i=1}^{1} a_i)(\prod_{i=2}^{2} a_i)$$

Supuesto cierto para n se demuestra para $n + 1$. Sea $1 \leq m < n + 1$,

Caso 1: $m = n$

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

Caso 2: $m < n$

$$\prod_{i=1}^{n+1} a_i := (\prod_{i=1}^{n} a_i)a_{n+1} = ((\prod_{i=1}^{m} a_i)(\prod_{i=m+1}^{n} a_i))a_{n+1} =$$
$$= (\prod_{i=1}^{m} a_i)[(\prod_{i=m+1}^{n} a_i)a_{n+1}] = (\prod_{i=1}^{m} a_i)(\prod_{i=m+1}^{n+1} a_i)$$

□

Demostraciones de las propiedades anteriores:

Dem. i: Supongamos que hay dos elementos neutros, $1, e \in G$, entonces se tendría,

$$1 = 1e = e$$

Dem. ii: Supongamos que $a \in G$ tiene dos inversos $a^{-1}, a' \in G$, entonces se tendría,

$$a' = a'1 = a'(aa^{-1}) = (a'a)a^{-1} = 1a^{-1} = a^{-1}$$

Dem. iii: Consecuencia de **(ii)**

Dem. iv: $x = a^{-1}b$ $y = ba^{-1}$, las soluciones se derivan de **(ii)**

Dem. v: Consecuencia de **(ii)**

Dem. vi: Trivial.

Dem. vii: Inducción en n. Si $n = 1$ es obvio. Supuesto cierto para n, se tiene,

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

, donde en la última igualdad se ha aplicado la hipótesis de inducción.

Dem. viii: Consecuencia directa de **(vii)**

Dem. ix:

Dem. x: $r, s \geq 1$ es **(viii)**

Cuando $r = 0$ ó $s = 0$ es obvio

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

$$a^r a^{-s},\ Caso\, r \geq s \Rightarrow r - s \geq 0$$
$$a^r a^{-s} = (a^{r-s}a^s)a^{-s} = a^{r-s}a^s a^{-s} = a^{r-s}$$
$$Caso\, r < s$$
$$a^r a^{-s} = a^r(a^{-1})^s = a^r(a^{-1})^r(a^{-1})^{s-r} =$$
$$= (a^{-1})^{s-r} = a^{-(s-r)} = a^{r-s}$$

Aánlogo para $a^{-r}a^{=}a^{-r+s}$. Sea $r \in \mathbb{Z}$, casos:

- $s \geq 1$ $(a^r)^s = a^r a^r \overbrace{\ldots}^{s-veces} a^r = a^{r+\overbrace{\ldots}^{s-veces}+r}$
- $s = 0$ $(a^r)^0 = 1 = a^{r0}$

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

□

24-02-2021

Proposición 2: Sea G un conjunto, $G \neq \emptyset$, y

$$\cdot : G \times G \to G$$
$$(a, b) \mapsto ab$$

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 demostra que $1a = a$ y $a^{-1}a = 1$

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

Por otro lado,

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

□

1.2. Ejemplos

$(A, +, \cdot)$ tal que $(A, +)$ es grupo abeliano y con respecto al producto, se verifica la propiedad asociativa ($(ab)c = a(bc)$ $\forall a, b, c \in A$) y la propiedad del elemento neutro ($\exists 1 \in A$ tal que $a1 = a = 1a$).

Además, se verifica la propiedad distributiva respecto a la suma: $a(b + c) = ab + ac$ $\forall a, b, c \in A$. $(A, +, \cdot)$ se dice conmutativo si se verifica que $ab = ba$ $\forall a, b \in A$.

Si A es un anillo,

- $(A, +)$ es un grupo abeliano
- $(A^*, \cdot)$ es un grupo (abeliano si A es un anillo conmutativo), donde $A^* = U(A) = \{u \in A |\ u\ es\ unidad\}$

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

Ejemplos:

- $\mathbb{Z} \to (\mathbb{Z}, +)$ es un grupo abeliano
  $\mathbb{Z}^x = \{-1, 1\}$ es un grupo abeliano con el producto.
- $\mathbb{Q} \to (\mathbb{Q}, +)$
  $\mathbb{Q}^x = \mathbb{Q} - \{0\}$
- $\mathbb{R} \to (\mathbb{R}, +)$
  $\mathbb{R}^x = \mathbb{R} - \{0\}$
- $\mathbb{C} \to (\mathbb{C}, +)$
  $\mathbb{C}^x = \mathbb{C} - \{0\}$

***Notación:** $\mathbb{C}^* = \mathbb{C}^x = \mathbb{C} - \{0\}$

$z = a + bi \neq 0 \Leftrightarrow a \neq 0$ *ó* $b \neq 0 \Leftrightarrow r = |z| = \sqrt{a^2 + b^2} \neq 0$ donde $a, b \in \mathbb{R}$

$z = r(cos\theta + isen\theta)$ (representación módulo-argumento de z), donde θ es el ángulo en radianes determinado por,

$$cos\theta = \frac{a}{\sqrt{a^2 + b^2}}\ ;\ sen\theta = \frac{b}{\sqrt{a^2 + b^2}}$$

y se denomina argumento.

Sean $z, z' \in \mathbb{C}$, con $z' = r'(cos\theta' + isen\theta')$ se verifica que,

$$zz' = rr'(cos(\theta + \theta') + isen(\theta + \theta'))$$

Demostración.

$$\begin{aligned} zz' &= rr'(cos\theta cos\theta' - sen\theta sen\theta' + i(cos\theta sen\theta' + sen\theta cos\theta')) \\ &= rr'(cos(\theta + \theta') + sen(\theta + \theta')) \end{aligned}$$

□

También se verifica que,

$$z^{-1} = \frac{1}{z} = \frac{1}{r}(cos\theta - isen\theta)$$

Para calcular la potencia n-ésima de un $z \in \mathbb{C}$ con $n \geq 1$ se tiene que,

$$z^n = r^n(cos(n\theta) + isen(n\theta))$$

Demostración. Se deduce directamente de la ecuación utilizada para el producto de dos complejos, sustituyendo z' por z y haciendo el producto n veces.

□

Ejemplo. Sea K un cuerpo, y $n \geq 2$.

$\mathcal{M}_n(K)$ es el anillo de matrices cuadradas de orden n con entradas en K. Este nos da lugar a dos grupos, $(\mathcal{M}_n(K), +)$, el cual es abeliano y,

$$GL_n(K) = \mathcal{M}_n(K)^x = \{B \in \mathcal{M}_n(K)/B\, es\, regular\} = \{B \in \mathcal{M}_n(K)/det(B) \neq 0\}$$

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

$\cdot$	1	x_1	$\ldots$	$\ldots$	x_r
1	1	x_1	$\ldots$	$\ldots$	x_r
x_1	x_1	x_1^2	x_1x_2	$\ldots$	x_1x_r
$\vdots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
x_r	x_r	x_rx_1	x_rx_2	$\ldots$	x_r^2

Ademaś, se verifica que, si $n \geq 2$, entonces

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{0, 1, \ldots, n-1\}$$

es un anillo conmutativo.

$(\mathbb{Z}_n, +)$ grupo abeliano y $\mathbb{Z}_n^x = \mathcal{U}(\mathbb{Z}_n) = \{r \in \mathbb{Z}_n / m.c.d(r, n) = 1\}$, donde $\mathbb{Z}_n^x$ es un grupo abeliano y $|\mathbb{Z}_n^x| = \varphi(n)$, donde φ es la función de Euler, y se define como

$$\varphi : \mathbb{N} - \{0\} \to \mathbb{N}$$
$$\varphi(n) = card\{r \in \mathbb{N} | 0 \leq r \leq n-1 \ y \ m.c.d(n, r) = 1\}$$

Luego si $p \in \mathbb{Z}$ es primo y $e \geq 1$, $\varphi(p^e) = p^{e-1}(p-1)$, entones $n = p_1^{e_1} \ldots p_k^{e_k}$ factoriza en primos. Es decir, $\varphi(n) = p_1^{e_1 - 1} \ldots p_k^{e_k - 1}(p_1 - 1) \ldots (p_k - 1)$. Luego finalmente, $m.c.d(n, m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$.

Sea $n \geq 2$ y sea $\mu_n := \{z \in \mathbb{C}^x / z^n = 1\}$, entonces μ_n con el producto es un grupo.

$$z, z' \in \mu_n, \ entonces \ (zz')^n = z^n z'^n = 1 \Rightarrow zz' \in \mu_n$$

el producto es una operación interna en μ_n de números complejos,

$$z \in \mu_n \Rightarrow \frac{1}{z} \in \mu_n, \ pues \ (\frac{1}{z})^n = \frac{1^n}{z^n} = \frac{1}{1} = 1$$

μ_n con el producto es un grupo abeliano y se llama el grupo de las raíces n-ésimas de la unidad $(x^n - 1)$

$$\mu_n = \{\xi_k = cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n} / 0 \leq k \leq n-1\}$$

,utilizando la fórmula módulo-argumento ya conocida y la fórmula módulo-argumento para la potencia n-ésima de un número complejo se obtiene,

$$\xi_k^n = cos2k\pi + isen2k\pi = 1 \Rightarrow \xi_k \in \mu_n$$

2-3-2021

$$\xi_k = cos(\frac{2k\pi}{n}) + isen(\frac{2k\pi}{n}) \in \mu_n$$
$$\xi_t = cos(\frac{2t\pi}{n}) + isen(\frac{2t\pi}{n}) \in \mu_n$$
$$k + t = n \cdot q + r \ 0 \leq r < n$$
$$r = resto(k + t; n)$$
$$\frac{2(k+t)\pi}{n} = \frac{2(nq+r)\pi}{n} = q2\pi + \frac{2r\pi}{n}$$
$$cos(\frac{2(k+t)\pi}{n}) = cos(\frac{2r\pi}{n}) \ ; \ sen(\frac{2(k+t)\pi}{n} = sen(\frac{2r\pi}{n})$$
$$\xi_k \cdot \xi_t = \xi_{resto(k+t;n)}$$

1.3. Grupos Simétricos

Sea $\mathcal{X}$ un conjunto con $\mathcal{X} \neq \emptyset$, definimos el grupo de permutaciones de $\mathcal{X}$ como,

$$S(\mathcal{X}) := \{\alpha : \mathcal{X} \to \mathcal{X} / \alpha \ es \ biyectiva\}$$

con operación (producto) dado por la composición de aplicaciones. El uno en $S(\mathcal{X})$ es $id_{\mathcal{X}} : \mathcal{X} \to X$, donde $id_{\mathcal{X}}(x) = x, \ \forall x$. Todo $\alpha \in S(\mathcal{X}), \ \exists \alpha^{-1} : \mathcal{X} \to \mathcal{X}$ tal que $\alpha\alpha^{-1} = id_{\mathcal{X}} = \alpha^{-1}\alpha$.

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

$$S_n = \{\alpha : \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\} / \alpha \ es \ biyectiva\}$$

con operación dada por la composición. S_n es un grupo finito, con $|S_n| = n!$.

Normal matricial de los elementos de S_n: $\alpha \in S_n$

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

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

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

Ejemplo: en S_5

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

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

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

$$id_{\mathcal{X}} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

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

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

Continuación ejemplo:

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

$$\alpha^{-1} = x \Leftrightarrow \alpha(x) = 1$$

Definición: Dados $\alpha, \beta \in S_n$ diremos que son disjuntos si los elementos (de $\mathcal{X}$) que mueve una de ellas quedan fijos por la otra. Es decir, si

a) Si $\alpha(x) \neq x \Rightarrow \beta(x) = x$

b) Si $\beta(x) \neq x \Rightarrow \alpha(x) = x$

Ejemplo S_6:

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

son disjuntas.

Proposición: Si $\alpha, \beta \in S_n$ son disjuntas entonces $\alpha\beta = \beta\alpha$ (composición de funciones)

Demostración: Hemos de ver que $\alpha\beta(x) = \beta\alpha(x) \ \forall x \in \mathcal{X}$

Caso 1: Sea $x \in \mathcal{X}$ tal que $\alpha(x) \neq x \xrightarrow{def} \beta(x) = x$ y entonces $\alpha\beta(x) = \alpha(x)$ $(\alpha(x) = y)$.

Si $\alpha(x) \neq x \Rightarrow \alpha(\alpha(x)) \neq \alpha(x) \xrightarrow{def} \beta(\alpha(x)) = \alpha(y)$

Caso 2: Sea $x \in \mathcal{X}$ tal que $\beta(x) \neq x$ entonces intercambiando los papeles de α y β en el caso anterior, pues llegamos a que $\beta\alpha(x) = \beta(x) = \alpha\beta(x)$

Caso 3: Sea $x \in \mathcal{X}$ tal que $\alpha(x) = x = \beta(x)$, entonces

$$\left.\begin{array}{l} \alpha\beta(x) = \alpha(x) = x \\ \beta\alpha(x) = \beta(x) = x \end{array}\right\} \Rightarrow \alpha\beta(x) = \beta\alpha(x)$$

□

Definición: Una permutación o un elemento $\alpha \in S_n$ diremos que es un ciclo si $\exists x_1, x_2, \ldots, x_r \in \mathcal{X}$ tal que

$$\begin{aligned} \alpha(x_1) &= x_2 \\ \alpha(x_2) &= x_3 \\ &\vdots \\ \alpha(x_{r-1}) &= x_r \\ \alpha(x_r) &= x_1 \end{aligned}$$

y $\alpha(x) = x \ \forall x \notin \{x_1, x_2, \ldots, x_r\}$. Diremos que α es un ciclo de longitud r o un r-ciclo y lo denotaremos por $\alpha(x_1 x_2 \ldots x_r)$

Proposición: El orden de un ciclo de longitud r es igual a r. Más generalmente, el orden de una permutación σ es igual al mínimo común multiplo de las longitudes de los ciclos disjuntos en los que se descompone σ

Ejemplo S_6:

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

$$\begin{aligned} x_1 &= 1 \\ x_2 &= 4 \\ x_3 &= 3 \\ x_4 &= 6 \\ x_6 &= 1 \end{aligned}$$

3-3-2021

Ejemplo: S_6

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

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

Es decir, que un r-ciclo tiene r expresiones

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

Definición: Sean $\alpha = (x_1 \dots x_r)$ y $\beta = (y_1 \dots y_s)$ dos ciclos en S_n. Entonces α y β son disjuntas $\Leftrightarrow \{x_1, \dots, x_r\} \cap \{y_1, \dots, y_s\} = \emptyset$

Ejemplo: S_4

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

$$x_1 = 1,\ x_2 = 3,\ x_3 = 2 \in \{1, 2, 3, 4\}$$
$$\alpha(x_1) = x_2,\ \alpha(x_2) = x_3,\ \alpha(x_3) = x_4$$
$$\alpha(x) = x\ \forall x \notin (1\ 2\ 3)$$

Teorema: Toda permutación de S_n, distinta de $id_{\mathcal{X}}$, se expresa de forma única (salvo el orden) como produto de ciclos disjuntos. Es decir, dado $\alpha \in S_n$, $\alpha \neq id_{\mathcal{X}}$, existen únicos ciclos $\alpha_1, \dots, \alpha_m \in S_n$ disjuntos dos dos tal que $\alpha = \alpha_1 \alpha_2 \dots \alpha_m$.

Demostración: (Existencia) $\alpha \in S_n$ $\alpha \neq id$ sea

$$s = |\{x \in \mathcal{X} / \alpha(x) \neq x\}| \geq 2$$

Como $\alpha \neq id_{\mathcal{X}}$ entonces $\exists x \in \mathcal{X}$ tal que $\alpha(x) \neq x$. Si $\alpha(x) = y$ e $y \neq x \Rightarrow \alpha(y) \neq \alpha(x) = y$. Hacemos inducción en s.

Primer caso $s = 2$, es decir, que existen únicamente dos elementos $x, y \in \mathcal{X}$ que son movidos por α ($\alpha(z) = z\ \forall z \neq x, y$). Entonces $\alpha(x) = y \wedge \alpha(y) = x$, es decir, $\alpha = (x\ y)$

Sea $s > 2$ y supongamos el resultado cierto para toda permutación que mueva menos de s elementos. Elegimos $x \in \mathcal{X}$ tal que $\alpha(x) \neq x$. Esta sucesión, $x, \alpha(x), \alpha^2(x), \alpha^3(x), \dots$ necesariamente es finita, es decir, $\exists k, k'$ con $k > k' \Rightarrow k - k' > 0$ y $k \neq k'$ tal que $\alpha^k(x) = \alpha^{k'}(x)$, es decir, $\alpha^{k-k'} = x$.

Sea r el menor número tal que $\alpha^r(x) = x$ ($r \geq 2$). Consideremos el siguiente ciclo $\alpha_1 := (x\ \alpha(x) \dots \alpha^{r-1}(x)) \in S_n$. Definimos $\alpha' \in S_n$ como sigue,

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

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

Caso $y \in \{x, \alpha(x), \dots, \alpha^{r-1}(x)\}$

$(\alpha_1\ \alpha')(y) = \alpha_1(y)$, entonces $y = \alpha^j(x)\ 0 \leq j \leq r-1$. Esto significa que $\alpha_1(x) = \alpha^{j+1}(x) = \alpha(\alpha^j(x)) = \alpha(y)$

Caso $y \notin \{x, \alpha(x), \ldots, \alpha^{r-1}\}$

α' mueve $s-r$ elementos $\Rightarrow s-r < s$, por hipótesis de inducción $\exists \alpha_2, \ldots, \alpha_m$ ciclos disjuntos dos a dos tal que $\alpha' = \alpha_2 \ldots \alpha_m$

$$\alpha = \alpha_1\alpha' = \alpha_1\alpha_2 \ldots \alpha_m$$

Unicidad:

$$\alpha = \alpha_1\alpha_2 \ldots \alpha_m\ \alpha_i \textit{ ciclos disjuntos}$$
$$\beta = \beta_1\beta_2 \ldots \beta_{m'}\ \beta_i \textit{ ciclos disjuntos}$$

$\Rightarrow)\ m = m'\ y\ \alpha_i = \beta_i\ \forall i = 1, \ldots, m$

$$\alpha_1 = (x\ \alpha_1(x)\ \alpha_1^2(x) \ldots) = (x\ \alpha(x)\ \alpha^2(x) \ldots)$$
$$\alpha_1(x) = \alpha(x)\ (\textit{pues } \alpha_1 \textit{ es disjunto con } \alpha_2, \alpha_3, \ldots, \alpha_m)$$

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 $\alpha = \beta_1\beta_2 \ldots \beta_{m'}$ es una expresión como producto de ciclos disjuntos.

Podemos suponer sin pérdida de generalidad que $j = 1$, es decir, $\beta_1(x) \neq x$ (que permutaciones disjuntas conmutan)

$$\beta_1 = (x\ \beta_1(x)\ \beta_1^2(x) \ldots) = (x\ \alpha(x)\ \alpha^2(x) \ldots)$$
$$\beta_1(x) = \alpha(x).\ \textit{Por tanto } \alpha_1 = \beta_1$$
$$\alpha = \alpha_1\alpha_2 \ldots \alpha_m$$
$$\alpha = \alpha_1\beta_2 \ldots \beta_m$$

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

$$\alpha_1 = \alpha_1\beta_2 \ldots \beta_{m'} \Rightarrow id_{\mathcal{X}} = \beta_2 \ldots \beta_{m'}\ (\textit{contradiccion})$$

Entonces $m' =!$. Supongamos $m > 1$ y cierto para $m-1$

$$\alpha_1\alpha_2 \ldots \alpha_m = \alpha_1\beta_2 \ldots \beta_{m'} \Rightarrow \alpha_2 \ldots \alpha_m = \beta_2 \ldots \beta_{m'} \xrightarrow{hip}$$
$$\xrightarrow{hip} \begin{cases} m-1 = m'-1 \Rightarrow m = m' \\ \alpha_i = \beta_i\ \forall i = 2, \ldots, m \end{cases}$$

□

Ejercicio 12 (Rel 1.): $\alpha \in S_7$/ Sean $\alpha_1, \alpha_2 \in S_7$

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

Describa $\alpha_1\alpha_2$, $\alpha_2\alpha_1$ y α_2^2 y expreselos como producto de ciclos disjuntos.

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

Ejercicio 13 (Rel 1.): S_9

$$P_1 = (1\ 3\ 2\ 8\ 5\ 9)(2\ 6\ 3) =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 8 & 4 & 9 & 2 & 7 & 5 & 1 \end{pmatrix} =$$
$$= (1\ 3\ 8\ 5\ 9)(2\ 6)$$

Ejercicio 19 (Rel 1.): Describir todos los ciclos de S_4 y expresar todos los elementos de S_4 como producto de ciclos disjuntos.

- Ciclos de longitud 2: $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$.
- Ciclos de longitud 3: $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3), (1\ 3\ 4), (1\ 4\ 3)$.
- Ciclos de longitud 4: $(1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$

Si nos fijamos en los ciclos anteriormente mencionados tenemos 20 ciclos disjuntos, que con la identidad hacen 21 de los elementos de S_4. Finalmente los tres elementos restantes se hacen con el producto de ciclos disjuntos de dos elementos $\alpha_1 = (1\ 2)(3\ 4)$, $\alpha_2 = (1\ 3)(2\ 4)$ y $\alpha_3 = (1\ 4)(2\ 3)$.

8-3-2021

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

1. $(x_1x_2 \dots x_r)^{-1} = (x_rx_{r-1} \dots x_2x_1)$
2. Para todo $\alpha \in S_n$

$$\alpha(x_1x_2 \dots x_r)\alpha^{-1} = (\alpha(x_1)\alpha(x_2) \dots \alpha(x_r))$$

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

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

Demostración: Se demostrará sólo 4.

Si $1 \leq k < r$ se verifica que $(x_1 \dots x_r)^k(x_1) = x_{k+1}$. Lo veremos por inducción sobre k.

Si $k = 1$ es claro $(x_1 \dots x_r)(x_1) = x_2$.

Sea $k > 1$

$$(x_1 \dots x_r)^k(x_1) = (x_1 \dots x_r)(x_1 \dots x_r)^{k-1}(x_1) =^{hip.} = (x_1 \dots x_r)x_k = x_{k+1}$$

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

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

Sea $2 \leq i \leq r$

$$\begin{gathered}(x_1 \dots x_r)^r(x_i) = (x_1 \dots x_r)^r(x_1 \dots x_r)^{i-1}(x_1) = \\ = (x_1 \dots x_r)^{i-1}(x_1 \dots x_r)^r(x_1) = (x_1 \dots x_r)^{i-1}(x_1) = x_i\end{gathered}$$

Si $x \notin \{x_1, \dots, x_r\}$ entonces $(x_1 \dots x_r)^r(x) = x$, luego queda demostrado que $(x_1 \dots x_r)^r = id$.

□

1.4. Los 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 las distancias) del plano $\mathbb{R}^2$ que globalmente dejan fijo a P_n.

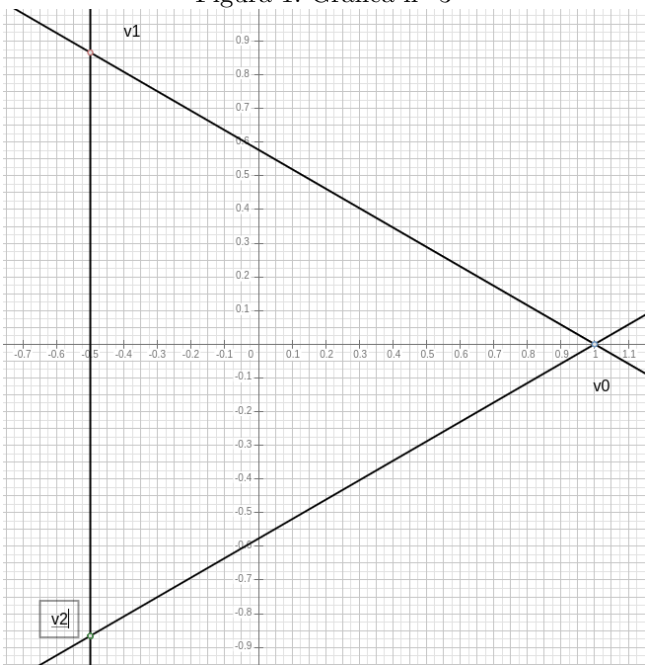
$$D_n = \{T : \mathbb{R}^2 \to \mathbb{R}^2 / T \, es \, isometria \, y \, T(P_n) = P_n\}$$

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 y suponemos está centrado de radio uno. Entonces los vértices de P_n son

$$v_0, v_1, \dots, v_{n-1} \quad donde \quad v_k = \left(cos\frac{2k\pi}{n}, sen\frac{2k\pi}{n} \right)$$

Figura 1: Gráfica n=3



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 de amplitud $\frac{2k\pi}{n}$.

$(R_0 = id)$

$$R_0 = id, R_1, R_2, \ldots, R_k$$

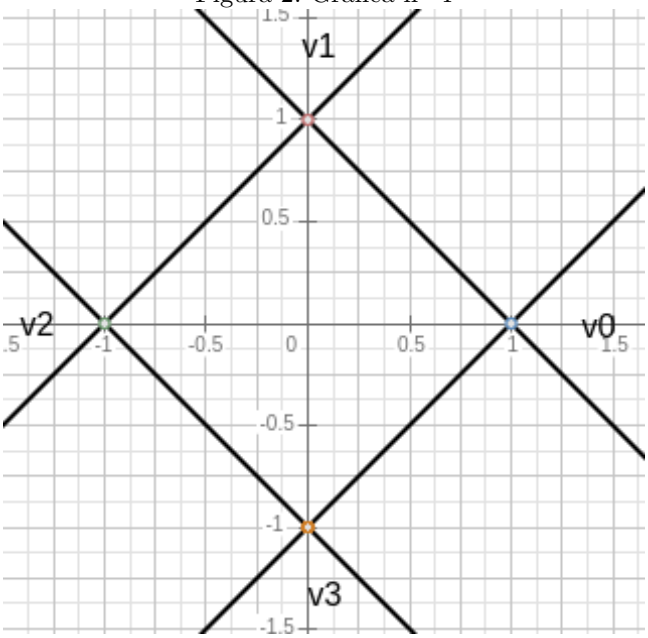
$$R_k : \mathbb{R}^2 \to \mathbb{R}^2 \qquad (x, y) \mapsto (x, y) \begin{pmatrix} cos\frac{2k\pi}{n} & sen\frac{2k\pi}{n} \\ -sen\frac{2k\pi}{n} & cos\frac{2k\pi}{n} \end{pmatrix}$$

Sean $S_0, S_1, \ldots, Sn-1$ 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.

Sea S_k la simetría respecto al eje S_k.

Figura 2: Gráfica n=4



$$0 \leq k \leq n-1, \quad S_0, S_1, \ldots, S_{n-1}$$

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

9-3-2021

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

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:
$$T|_{\{v_0,\ldots,v_{n-1}\}} : \{v_0, \ldots, v_{n-1}\} \longrightarrow \{v_0, \ldots, v_{n-1}\}$$
3. Si $T \in D_n$, entonces el origen es el único punto fijo.
4. Si $T \in D_n$, entonces T está completamente determinado por $T(v_0)$ y $T(v_1)$.
5. Siempre se cumple que $T(v_0)$ y $T(v_1)$ son vértices adyacentes.
6. Tenemos que
$$D_n = \{id = R_0, R_1, \ldots, R_{n-1}, S_0, \ldots, S_{n-1}\}$$

Demsotración:

(1) Todo movimiento del plano está totalmente determinado por la imagen de 3 puntos no alineados.

(2) Si $T \in D_n$ entonces,

$$T\big|_{\{v_0,\ldots,v_n\}} : \{v_0,\ldots,v_{n-1}\} \to \{v_0,\ldots,v_{n-1}\},$$

define un permutación de vértices.

- n par y v_i un vértie 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 $T(P_n) = P_n \quad \forall (p,q) \in P_n \times P_n$, entonces $d(p,q) \leq d(T(v_i),T(v_j)) = d(v_i,v_j) \Rightarrow T(v_i),\, T(v_j) \in \{v_0,\ldots,v_{n-1}\}$

- n impar y v_i un vértice de P_n y v_j, v_k los vértices del lado opuesto,

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

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

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

y $T\big|_{\{v_0,\ldots,v_n\}}$ es inyectiva (T preserva distancias) $\Rightarrow T\big|_{\{v_0,\ldots,v_{n-1}\}}$ es biyectiva, pues toda isometría es sobreyectiva.

(3) Si $T \in D_n$ entonces $T(0,0) = (0,0)$ $0 = (0,0)$, porque 0 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 $T(v_1)$. Poque 0, v_0, v_1 son tres puntos no alineados y $T(0) = 0$

Si $T, T' \in D_n$ tal que

$$\left.\begin{array}{l} T(v_0) = T'(v_0) \\ T(v_1) = T'(v_1) \end{array}\right\} \Rightarrow T = T'$$

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

(6) $D_n = \{R_0 \neq id, R_1, \ldots, R_{n-1}, S_0, \ldots, S_{n-1}\}$

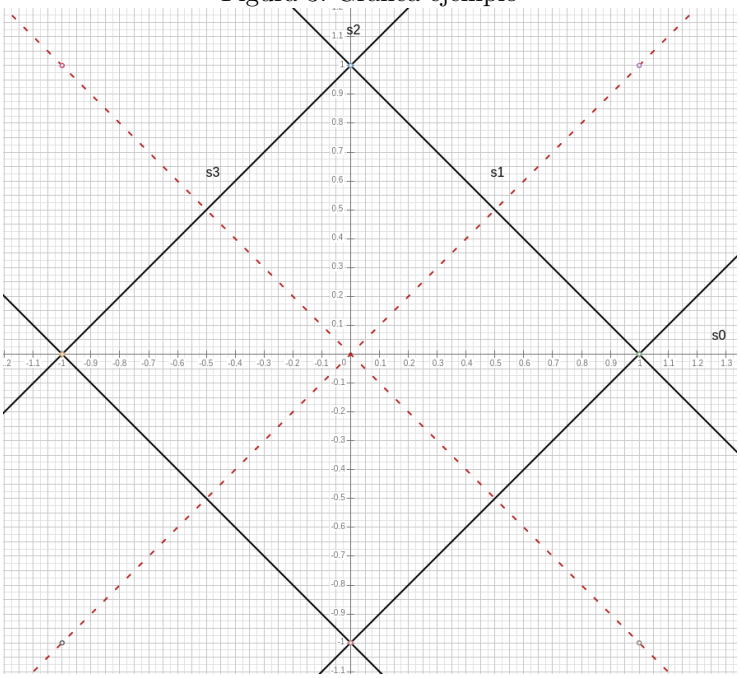
Sea $T \in D_n$ y supongamos $T(v_0) = v_k \quad 0 \leq k \leq n-1$.

- Si $T(v_1) = v_{k+1}$ (entendiendo v_0 si $k = n-1$) entonces $T = R_k$, 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 $S_k(v_1) = v_{k-1}$

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

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

Figura 3: Gráfica ejemplo



- $R_0 = id$
- $R_1 =$ giro de amplitud 90
- $R_2 =$ giro de amplitud 180
- $R_3 =$ giro de amplitud 270
- $S_0 =$ simetría respecto al eje s_0
- $S_1 =$ simetría respecto al eje s_1
- $S_2 =$ simetría respecto al eje s_2
- $S_3 =$ simetría respecto al eje s_3

- Entonces si $r = R_1$ y $s = S_0$ se tiene,

$$r^2 = R_2,\ r^3 = R_3,\ r^4 = id$$

$D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$ y $r^4 = 1 = s^2$.

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

$$\left.\begin{array}{c} sr(v_0) = v_3 = S_3(v_0) \\ sr(v_1) = v_2 = S_3(v_1) \end{array}\right\} \Rightarrow sr = S_3 = r^3s$$

$\cdot$	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

$$r^4 = 1 = s^2;\ sr = r^3s$$
$$sr^2 = srr = r^3sr = r^6s = r^2s$$

10-3-2021

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

- $r = R_1$, giro centrado en el origen de amplitud $\frac{2\pi}{n}$
- $s = S_0$, simetría respecto al eje $y = 0$

Entonces se verifica

$$\left\{\begin{array}{ll} R_k = r^k & 0 \leq k \leq n-1 \\ S_k = r^k s & 0 \leq k \leq n-1 \end{array}\right.$$

Además, $r^n = 1 = s^2$ y $sr = r^{n-1}s$. Es decir,

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

y se tiene que

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

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

$$sr^k = r^{n-k}s \tag{2}$$

y entonces podemos escribir la tabla del grupo D_n haciendo uso únicamente de las identidades (1) y (2).

Demostración: Veamos (2). Hacemos inducción sobre k.
Para $k = 1$ se tiene por (1). Supuesto cierto para k,

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

y se tiene (2).
Nótese que (2) es consecuencia de (1). Notemos además que otra forma de escribir (2) es como sigue

$$sr^k = r^{-k}s \tag{2'}$$

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

□

Describir la tabla D_n, es decir,

$$r^i r^j = r^{i+j} = r^{res(i+j;n)}$$
$$r^i r^j s = r^{i+j}s = r^{res(i+j;n)}s$$
$$r^i s r^j =^{(2')} r^i r^{-j}s = r^{i-j}s = r^{res(i-j;n)}s$$
$$r^i s r^j s =^{(2')} r^i r^{-j}ss =^{(1)} r^{i-j} = r^{res(i-j;n)}$$

Diremos que D_n está generado por r y s y escribiremos

$$D_n = \langle r, s / r^n = 1 = s^2;\ sr = r^{n-1}s \rangle$$

a las identidades

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

las llamaremos identidades fundamentales.

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

Puesto que $sr = r^{n-1}s$ y como $n \geq 3$ entonces $sr \neq rs$. Es decir, D_n no es un grupo abeliano para todo n.

□

1.5. Grupo de los cuaternios

El grupo de los cuaternios, que denotaremos $\mathcal{Q}_2$, es dado por

$$\mathcal{Q}_2 = \left\{ \begin{array}{c} 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, -1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ -i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, j = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, -j = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\ k = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, -k = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \end{array} \right\}$$

con operación dada por el producto de matrices.

$$\begin{gathered} (-1)^{-1} = -1 \\ i^{-1} = -i \Rightarrow (-i)^{-1} = i \\ k^{-1} = -k \Rightarrow (-k)^{-1} = k \\ j^{-1} = -j \Rightarrow (-j)^{-1} = j \end{gathered}$$

Proposición: Se verifica,

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) $ij = k$

Demostración: Se deja como ejercicio.

Ejercicio: Prescindiendo de la descripción de los elementos de $\mathcal{Q}_2$ como matrices, y utilizando únicamente las identidades anteriores, a), b), c), d), e), probar que $\mathcal{Q}_2$ se verifica que,

$$jk = i,\ ki = j,\ ji = -k,\ kj = -1,\ ik = -j$$

Se puede entonces escribir la tabla de $\mathcal{Q}_2$ prescindiendo de su descripción como matrices.

Veamos que $jk = i$. Por ejemplo sabemos que

$$\begin{gathered} ij = k \Rightarrow ijk = k^2 \Rightarrow ijk = -1 \Rightarrow i^2jk = -1i \Rightarrow \\ \Rightarrow -1jk = -1i \Rightarrow (-1)^2jk = (-1)^2i \Rightarrow jk = i \end{gathered}$$

Veamos que $ki = j$. Sabemos que

$$jk = i \Rightarrow jki = i^2 = -1 \Rightarrow j^2ki = j(-1) \Rightarrow (-1)ki = (-1)j \Rightarrow ki = j$$

Veamos que $ji = -k$. Sabemos que

$$ki = j \Rightarrow ki^2 = ji \Rightarrow k(-1) = ji \Rightarrow -k = ji$$

$\mathcal{Q}_2 = \{1, -1, i, -i, j, -j, k, -k\}$ verificando las identidades,

$$\begin{gathered} (-1)^2 = 1 \qquad i^2 = j^2 = k^2 = -1 \\ a(-1) = -a = (-1)a \qquad a = i, j, k \\ ij = k \end{gathered}$$

1.6. 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

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

y con producto definido como sigue:

$$(x, y)(x', y') = (xx', yy')$$

Es fácil ver que en efecto $G \times H$ es un grupo con la operación anterior, donde el 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

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

Definimos el grupo de Klein, que denotaremos por K, como el producto directo de μ_2 con μ_2, donde μ_2 es el grupo de las raíces cuadradas de la unidad.

$$\begin{gathered} K := \mu_2 \times \mu_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\} \\ \mu_2 = \{x \in \mathbb{C}^*/x^2 = 1\} = \{1, -1\} \\ |K| = 4 \end{gathered}$$

Ejercicio: Escribir la tabla.

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

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

- 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, $1_G : G \to G$ es un isomorfismo

2) $n \geq 2$, K cuerpo

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

es un homomorfismo (con el producto).

3) $\mathbb{R} \xrightarrow{f} \mathbb{R}^* \quad f(x) = e^x$ (con la suma $f(x+y) = f(x) \cdot f(y)$)

4) Para todo $n \geq 2$

$$p : \mathbb{Z} \to \mathbb{Z}_n$$
$$p(k) = res(k; n)$$

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

(I) $f(1) = 1$

(II) $f(a^{-1}) = f(a)^{-1} \qquad \forall a \in G$

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

(I) Si f y g son homomorfismos $\Rightarrow g \circ f$ es un homomorfismo.

(II) Si f y g son monomorfismos (respectivamente, epimorfismos, isomorfismos) $\Rightarrow g \circ f$ (respectivamente, epimorfismo, isomorfismo).

Demostración: Se deja como ejercicio.

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

$$f \text{ es isomorfismo} \Leftrightarrow \exists g : G' \to G \text{ tal que}$$
$$f \circ g = id_{G'} \text{ y } g \circ f = id_G$$

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

Dem: $\Leftarrow$) Obvio.

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

$$f \circ g = id_{G'} \quad y \quad g \circ f = id_G$$

Veremos que $g : G' \to G$ es un homomorfismo de grupos:

$$\forall x', y' \in G \qquad g(x'y') =^{?} g(x')g(y')$$
$$g(x'y') \in G \qquad g(x')g(y') \in G$$
$$f(g(x'y') = (f \circ g)(x'y') = x'y'$$
$$f(g(x')g(y')) = f(g(x'))f(g(y')) = (f \circ g)(x')(f \circ g)(y') = x'y'$$
$$f(g(x'y')) = f(g(x')g(y')) \Rightarrow^{f\ inyectiva} g(x'y') = g(x')g(y')$$

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 lo denotaremos por $G \cong G'$.

"Ser isomorfo" es una relación binaria en la clase de todos los grupos. Puesto qeu $1_G : G \to G$ es un isomorfismo $\Rightarrow G \cong G \quad \forall G$ (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

$$\left.\begin{array}{c} G \cong G' \\ G' \cong G'' \end{array}\right\} \quad \left.\begin{array}{c} \exists f : G \to G' \ isomorfismo \\ \exists g : G' \to G'' \ isomorfismo \end{array}\right\} \Rightarrow$$

$g \circ f : G \to G''$ es un isomorfismo $\Rightarrow G \cong G''$ (propiedad transitiva).

□

Uno de los objetivos de la teoría de grupos finitos es su clasificación. Es decir, obtener un listado de todos los grupos finitos no isomorfos entre sí.

15-3-2021

Teorema: Todos los grupos de orden 2 son isomorfos entre sí. Es decir, hay sólo una calse de equivalencia que la representaremos por el grupo $\mu_2 = \{1, -1\}$

Demostración: $G = \{1, a\}, \quad H = \{1, b\}$

Definimos,

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

f es un homomorfismo de grupos y entronces 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 $x = y = a$, entonces $xy = a^2 = 1$

·	1	a
1	1	a
a	a	1

$$(a^2 \neq a \, pues \, a^2 = a \Rightarrow a = 1)$$
$$\left.\begin{array}{c} f(xy) = f(a^2) = f(1) = 1 \\ f(x) \cdot f(y) = f(a) \cdot f(a) = b^2 = 1 \, (analogo \, al \, caso \, de \, a) \end{array}\right\} \Rightarrow f(a^2) = f(a) \cdot f(a)$$

Ejercicios:

- **Ejercicio 5) Rel 1:** No cumple la propiedad asociativa
- **Ejercicio 6) Rel 1:** $y, x \in G$, se tiene como hipótesis $x^2 = 1$, $y^2 = 1$.

$$(xy)^2 = xyxy = 1 \Rightarrow x^2yxy^2 = xy$$

lo que implica que G es un grupo abeliano.

- **Ejercicio 7) Rel 1:**
  - 1) $\Rightarrow$ 2) obvio $(xy)^2 = xyxy = xy^2x = x^2y^2$.
  - 2) $\Rightarrow$ 3)

$$(x^{-1}y^{-1})^2 = x^{-1}y^{-1}x^{-1}y^{-1} =^{(2)}$$
$$=^{(2)} x^{-1}x^{-1}y^{-1}y^{-1} \Rightarrow y^{-1}x^{-1} = (xy)^{-1} = x^{-1}y^{-1}$$

  - 3) $\Rightarrow$ 1) Puesto que

$$(xy)^{-1} = x^{-1}y^{-1} \Rightarrow xyx^{-1}y^{-1} = 1 \Rightarrow xy = yx$$

- **Ejercicio 9) Rel 1:** $G = \{f : \mathbb{R} \to \mathbb{R} / f(x) = ax + b,\ a,\ b \in \mathbb{R}\, a \neq 0\}$

$$\mathbb{R} \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R}$$
$$f(x) = ax + b, \quad g(x) = a'x + b \quad a, a' \neq 0$$
$$(g \circ f)(x) = g(ax + b) = a'(ax + b) + b' = a'ax + a'b + b' \quad a'a \neq 0$$
$$\Rightarrow g \circ f \in G$$

Propiedad Asociativo

$$1_R \in G \quad 1_R(x) = x = 1x + 0 \quad a = 1, \quad b = 0$$

Comprobar inversos: $f : \mathbb{R} \to \mathbb{R} \quad f(x) = ax + b$

$$f^{-1} : \mathbb{R} \to \mathbb{R} \quad es \quad f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$$
$$f \circ f^{-1}(x) = f(\frac{1}{a}x - \frac{b}{a}) = x$$

- **Ejercicio 10) Rel 1:** $GL_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_2) / ad = bc = 1 \right\}$

(1)

$$GL_2(\mathcal{M}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

$|GL_2(\mathbb{Z}_2)| = 6$

(2) $GL_2(\mathbb{Z}_2) = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$.

(3) Escribir la tabla de $GL_2(\mathbb{Z}_2)$, usando la representación de (2). Comprobar que

$$\left.\begin{array}{c} \alpha^3 = 1 = \beta^2 \\ \beta\alpha = \alpha^2\beta \end{array}\right\}$$

Entonces escribir la tabla sin necesidad de recurrir a su descripción como matrices.

- **16-3-2021**
- **Ejercicio 21) Rel 1:**

1)

$$1 \mapsto 1 \quad i \mapsto 2$$
$$-1 \mapsto 4 \quad -i \mapsto 3$$
$$\mu_4 = \{1, -1, i, -i\} \xrightarrow{x} \mathbb{Z}_5^x = \{1, 2, 3, 4\}$$

2) Otro isomorfismo

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

$g(1) = 1$ pues g ha de ser homomorfismo

$$g(-1) = 4 \quad g(i) = 3 \quad g(-i) = 2$$

Comprobar que $g : \mu_4 \to \mathbb{Z}_5^x$ es homomorfismo de grupos y isomorfismocon $g \neq f$.

- **Ejercicio 26) Rel 1:**

1) $\mathbb{R}^*$ no es isomorfo a $\mathbb{C}^*$.

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

Sea $f(i) = a \in \mathbb{R}^*$.

$$1 = f(1) = f(i^4) = f(i)^4 = a^4 \Rightarrow \cancel{a=1} \quad o \quad = -1$$

$a = 1$ no puede ser pues $i \neq 1$ y por tanto $f(i) \neq f(1) = 1$. Luego de aquí se deduce

$$f(i) = -1 \Rightarrow f(i) \cdot f(i) = (-1)(-1) = 1 = f(i^2) = f(-1)$$

luego se llega a contradicción con que f es inyectiva

2) $\mathbb{Z}$ y $\mathbb{Q}$ isomorfismo. Sea $g(1) = \frac{a}{b}$ entonces para $n \in \mathbb{Z}$ se tendrá que

$$n > 0 \quad g(n) = g(1 + \ldots + 1) = g(1) + \ldots + g(1) = n \cdot \frac{a}{b}$$
$$g(-n) = -g(n) = -n\frac{a}{b}, \qquad g(0) = 0$$

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

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

Lo cual es una contradicción.

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

$$Car(\mathbb{R}) = 0 = Car(\mathbb{Q}) = Car(\mathbb{C})$$
$$Car(\mathbb{Z}_p) = p \quad p \quad primo$$

Ejercicio 28) Rel 1: Supongamos que $\exists f : K^* \to K$ isomorfismo tal que

$$\begin{cases} f(xy) = f(x) + f(y) & \forall x, y \in K^* \\ f(1) = 0 \end{cases}$$
$$0 = f(1) = f((-1)(-1)) = f(-1) + f(-1)$$
$$\left.\begin{array}{c} 2 \cdot f(-1) = 0 \\ Si\, Car(K) \neq 2 \end{array}\right\} \Rightarrow f(-1) = 0$$
$$\Rightarrow f(-1) = f(1)$$

Lo cual es contradicción con que f sea inyectiva. Por otro lado supongamos que $Car(K) = 2$. Consideremos $f^{-1} : K \to K^*$ es también un isomorfismo

$$\begin{cases} f^{-1}(x+y) = f^{-1}(x) \cdot f^{-1}(y) & \forall x, y \in K \\ f^{-1}(0) = 1 \end{cases}$$

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

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

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

$$\begin{cases} a^2 = 1 \Rightarrow a\ es\ raiz\ de\ x^2 - 1,\ que\ son\ 1, -1 \\ Como\ Carac(K) = 2 \qquad 2 \cdot 1 = 1 + 1 = 0 \Rightarrow 1 = -1 \end{cases}$$

17-3-2021

2. Tema 3. Subgrupos. Generadores. Retículos

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

(1) Para cualesquiera $x, y \in H, \quad xy \in H$

(2) $1 \in H$

(3) $\forall x \in H, \quad x^{-1} \in H$

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

Ejemplos:

1) Para todo grupo G, el conjunto $\{1\}$ y G son subgrupos de G. A estos los llamaremos subgrupos impropios de G. El subgrupo $\{1\}$ se le llama subgrupo trivial de G. Los demás subgrupos, si los hay, se llaman subgrupos propios $\Rightarrow \{1\} \leq H \leq G \; con \; \{1\} \neq H \neq G$

2) $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$

3) $\forall n \geq 1 \quad \mu_n \leq \mathbb{C}^*$

4) Si $m, n \geq 1$ y $m \mid n \Rightarrow \mu_m \leq \mu_n$

Proposición: Sea G un grupo y $H \subset G$, $H \neq \emptyset$, entonces H es un subgrupo de G $\Leftrightarrow$ 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 consideramos $1 \in H$. Entonces, por hipótesis, $1 \cdot x^{-1} = x^{-1} \in H$. Se tiene así (3).

Sean $x, y \in H \Rightarrow xy^{-1} \in H \Rightarrow^{hip.} x(y^{-1})^{-1} = xy \in H$ y se tiene (1).

□

Proposición: Sea G un grupo finito y $H \subset G$, $H \neq \emptyset$. Entonces H es un subgrupo de G $\Leftrightarrow$ Para cualesquiera $x, y \in H$, $xy \in H$.

Demostración: $\Rightarrow$) Es obvio, por definición de subgrupo.

$\Leftarrow$) Por hipótesis verifica (1).

Sea $x \in H$. Consideramos $x, x^2, x^3, \ldots, x^n, \ldots$ todos son elementos de H, por hipótesis.

Puesto que G es finito, podemos asegurar que $\exists n, m, n \neq m$, tal que $x^n = x^m$. Sea $n > m$ y entonces $x^n \cdot x^{-m} = x^m \cdot x^{-m}$, es decir $x^{n-m} = 1$. Además, $n - m > 0$ y entonces $1 = x^{n-m} \in H$. Se tiene (2)

Si $x^{n-m} = 1 \Rightarrow x^{-1} = x^{n-m-1}$, pero $n - m > 0 \Rightarrow n - m - 1 \geq 0$ y así $x^{-1} = x^{n-m-1} \in H$ y se tiene (3).

□

Ejemplo:

1) Sea $n \geq 3$. En $D_n = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$. Además se verifican las identidades $r^2 = 1 = s^2$, $sr = r^{n-1}s$.

$$C = \{1, r, \ldots, r^{n-1}\} \leq D_n$$

pues $r^i r^j = r^{Res(i+j;n)} \in C$.

Para cada $0 \leq k \leq n-1$, $H_k = \{1, r^k s\} \leq D_n$

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

El conjunto $X = \{1, s, rs, \ldots, r^k s\}$ no es un subgrupo de D_n porque la operación no es interna en X

$$s(rs) = srs = r^{n-1}ss = r^{n-1}$$

2) En S_4, $K = \{id, \alpha_1 = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \alpha_2 = \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \alpha_3 = \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\}$

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	1	α_3	α_2
α_2	α_2	α_3	1	α_1
α_3	α_3	α_2	α_1	1

se llama el grupo de Klein de S_4.

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

(I) $H \leq G \Rightarrow f_*(H) \leq G' \qquad (f_*(H) := \{f(x)/x \in H\})$

(II) Si $H' \leq G' \Rightarrow f^*(H') \leq G \qquad (f^*(H') := \{x \in G : f(x) \in H'\} \subset G)$

(III) $Ker(f) = \{x \in G/f(x) = 1\} \leq G$
$Img(f) = \{f(x)/x \in G\} \leq G'$

(IV) f es monomorfismo $\Leftrightarrow Ker(f) = \{1\}$
f es epimorfismo $\Leftrightarrow Img(f) = G'$

Demostración:

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

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

Si $x, y \in H \Rightarrow xy^{-1} \in H$.

(ii) $H' \leq G'$ entonces $f^*(H') \subset G$ y, como $f(1) = 1 \in H' \Rightarrow 1 \in f^*(H')$, entonces $f^*(H') \neq \emptyset$

Sean $x, y \in f^*(H') \Rightarrow f(x), f(y) \in H' \Rightarrow f(x)f(y)^{-1} \in H' = f(xy)^{-1} \Rightarrow xy^{-1} \in f(H')$

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

(iv) Ejercicio

□

2.1. Grupos Alternados:

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

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

Todo ciclo se expresa como producto de transposiciones

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

Como consecuencia todo elemento de S_n se expresa como producto de transposiciones. Por ejemplo, podemos demostrar la identidad como $[id = (1\,2)(1\,2)]$. Dicha expresión no es única.

Teorema: Sea $n \geq 2$ y $\alpha \in S_n$. Supongamos que $\alpha = \tau_1 \tau_2 \dots \tau_s$, τ_i es una transposición $\forall i$.

$$\alpha = \tau_1' \tau_2' \dots \tau_r' \qquad \tau_j' \, transposicion \, \forall j$$

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

Demostración: Lo probamos primero para $\alpha = id$. Como $\alpha = (1\,2)(1\,2)$, entonces basta demostrar que si

$$id = \tau_1 \tau_2 \dots \tau_r \Rightarrow r \equiv 0 \mod (2)$$

, donde τ_i es una transposición $\forall i$. Hacemos inducción en r. El primer caso $r = 2$ y es claro que se verifica. Supongamos $r > 2$, y el resultado cierto para cualquier expresión id como producto de menos de r transposiciones.

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

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

Así $j < r$ y podemos considerar τ_{j+1}

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

Sustituyendo en la expresión de $id(x)$ obtenemos en el $1^{\underline{o}}$ caso que

$$id = \tau_1 \ldots \tau_{j-1}\tau_{j+2} \ldots \tau_r \Rightarrow r - 2 \equiv 0 \mod (2) \Rightarrow$$
$$\Rightarrow r \equiv 0 \mod (2)\ \textit{y quedaria demostrado}$$

En los casos $2^{\underline{o}}$, $3^{\underline{o}}$ y $4^{\underline{o}}$ obtenemos

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

donde la 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 $1^{\underline{a}}$. Es decir, en un número finito de pasos, llegamos a que

$$id = \tau'_1 \ldots \tau'_{r-2}$$

con τ'_i transposiciones $\forall i$. Por hipótesis de inducción, $r - 2 \equiv 0 \mod (2) \Rightarrow r \equiv 0 \mod (2)$

Sea $\alpha = \tau_1\tau_2 \ldots \tau_r \quad y \quad \alpha = \tau'_1\tau'_2 \ldots \tau'_s \qquad \tau_i, \tau'_j$ son transposiciones $\forall i \forall j$.

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

Entonces $r + s \equiv 0 \mod (2) \Leftrightarrow r \equiv s \mod (2)$

□

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

Ejemplo: $id \in S_n$ es permutación par. Cualquier transposición es impar.

$$(x_1x_2x_3) = (x_1x_2)(x_2x_3) \; es \; par$$

Como $(x_1x_2 \dots x_r) = (x_1x_2)(x_2x_3) \dots (x_{r-1}x_r)$.

$(x_1 \dots x_r)$ es par (respectivamente, impar) $\Leftrightarrow$ r es impar (respectivamente, par).

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

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

Se tiene $s : S_n \to \mu_2 = \{1, -1\}$ es un homomorfismo de grupos.

Demostración: Sea $\alpha, \beta \in S_n$

Sea $\alpha = \tau_1\tau_2 \dots \tau_r$ una expresión de α como producto de transposiciones, y $\beta = \tau'_1\tau'_2 \dots \tau'_s$ una expresión de β como producto de transposiciones.

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

$$\alpha\beta = \tau_1\tau_2 \dots \tau_r\tau'_1\tau'_2 \dots \tau'_s \Rightarrow s(\alpha\beta) = (-1)^{r+s}$$
$$s(\alpha\beta) = (-1)^{r+s} = (-1)^r(-1)^s = s(\alpha)s(\beta)$$

□

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

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

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

$$\begin{cases} S_3 = \{id, (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3)\} \\ A_3 = \{id, (1\,2\,3), (1\,3\,2)\} \end{cases}$$

n=4

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

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

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

22-3-2021

Demostración: Consideramos $z = (1\,2) \in S_n$ y sea

$$(1\,2)A_n = \{(1\,2)\alpha / \alpha \in A_n\}$$

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

$$\sigma = (1\,2)(1\,2)\sigma$$

pues sigma es impar $\Rightarrow (1\,2)\sigma \in A_n \Rightarrow (s((1\,2)\sigma)) = s(1\,2)s(\sigma) = (-1)(-1) = 1.$

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

$$\left.\begin{array}{c} A_n \cup (1\,2)A_n = S_n \\ A_n \cap (1\,2)A_n = \emptyset \end{array}\right\} \Rightarrow |S_n| = |A_n| + |(1\,2)A_n|$$

Por otro lado la aplicación

$$\lambda : A_n \to (1\,2)A_n$$
$$\lambda(\alpha) := (1\,2)\alpha$$

es biyectiva y entonces $|A_n| = |(1\,2)A_n|$. Tenemos que

$$|S_n| = |A_n| + |(1\,2)A_n| = 2|A_n| \Rightarrow |A_n| = \frac{|S_n|}{2}$$

□

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

$$Sub(G) = \{H \subseteq G / H \textit{ es un subgrupo de } G\}$$

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

$$\cap_{i \in I} H_i$$

es también un subgrupo de G.

Demostración: Ejercicio.

Corolario: $Sub(G)$ es un retículo.

Demostración: Sean $H_1,\ H_2 \in Sub(G)$

$$Inf\{H_1, H_2\} = H_1 \cap H_2$$

Si $K \subseteq H_1$ y $K \leq H_2 \Rightarrow K \leq H_1 \cap H_2$

- $Sup\{H_1, H_2\} = \cap_{k \in Sub(G),\ H_i \leq K\ i=1,2} K \in Sub(G)$

□

Notación: Denotaremos el supremo $Sup\{H_1, H_2\} = H_1 \vee H_2$. (La unión de subgrupos no es en general un subgrupo

$$G = D_3 = \left\langle\ r, s / r^3 = 1 = s^2,\ sr = r^2 s\ \right\rangle = \{1, r, r^2, s, rs, r^2 s\}$$

$H_1 = \{1, s\}, \qquad H_2 = \{1, rs\}$

$$H_1 \cup H_2 = \{1, s, rs\}$$

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

¿Quién es $H_1 \vee H_2$? $r, rs \in H_1 \vee H_2 \Rightarrow (rs)s = rs^2 = r \in H_1 \vee H_2$.

$$H_i \subseteq H_1 \vee H_2 \qquad i = 1, 2$$

Si $r \in H_1 \vee H_2,\ s \in H_1 \vee H_2 \Rightarrow G \leq H_1 \vee H_2 \Rightarrow H_1 \vee H_2 = G$.

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

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

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

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) $H_1 \vee H_2 = H_1 H_2$

23-3-2021

Demostración: $H_1, H_2 \in Sub(G)$ tal que $H_1 H_2 = H_2 H_1$

1) Sean $x, y \in H_1H_2 \Rightarrow$

$$x = h_1h_2, \quad y = h_1'h_2' \quad \textit{donde} \qquad \begin{matrix} h_1, h_1' \in H_1 \\ h_2, h_2' \in H_2 \end{matrix}$$

$xy^{-1} = h_1h_2(h_1'h_2')^{-1} = h_1h_2h_2'^{-1}h_1'^{-1}$

$$\left.\begin{matrix} h_2, h_2' \in H_2 \\ h_1'^{-1} \in H_1 \end{matrix} \quad \Rightarrow h_2, h_2'^{-1} \in H_2 \right\} \Rightarrow h_2h_2'^{-1}h_1'^{-1} \in H_2H_1 = H_2H_1$$
$$\Rightarrow \exists k_1 \in H_1,\ k_2 \in H_2 \quad \textit{tal que} \quad h_2h_2'^{-1}h_1'^{-1} = k_1k_2$$

Entonces

$$xy^{-1} = h_1k_1k_2 \in H_1H_2$$

, pues $h_1k_1 \in H_1$ y $k_2 \in H_2$. Por tanto H_1H_2 es un subgrupo de G.

2) $H_1 \leq H_1H_2$, $H_2 \leq H_1H_2$ $\left(\begin{matrix} h_1 = h_1 \cdot 1 \in H_1H_2 \\ h_2 = 1 \cdot h_2 \in H_1H_2 \end{matrix} \right)$

Si $K \in Sub(G)$ tal que $H_1 \leq K$ y $H_2 \leq K \Rightarrow H_1H_2 \leq K$. Por tanto $H_1 \vee H_2 = H_1H_2$

□

Si G es abeliano entonces $\forall H_1, H_2 \in Sub(G)$,

$$H_1 \vee H_2 = H_1H_2$$

Ejemplo: En S_4 sean

$$K = \{id, \alpha_1 = (1\,2)(3\,4), \alpha_2 = (1\,3)(2\,4), \alpha_3 = (1\,4)(2\,3)\} \leq S_4$$
$$H = \{id, (1\,2)\} \leq S_4$$
$$KH = \{id, \alpha_1 = (1\,2)(3\,4), \alpha_2 = (1\,3)(2\,4), \alpha_3 = (1\,4)(2\,3),$$
$$(1\,2), \alpha_1(1\,2) = (3\,4), \alpha_2(1\,2) = (1\,4\,2\,3), \alpha_3(1\,2) = (1\,3\,2\,4)\}$$
$$HK = \{id, \alpha_1, \alpha_2, \alpha_3, (1\,2), (1\,2)\alpha_1 = (3\,4), (1\,2)\alpha_2 = (1\,3\,2\,4), (1\,2)\alpha_3 = (1\,4\,2\,3)\}$$

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

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 a X. Lo denotaremos por $\langle X \rangle$, y es claro que

$$\langle X \rangle = \cap_{K \in Sub(G),\, X \subseteq K} K$$

Definición: Sea G un grupo y $X \subseteq G$, $X \neq \emptyset$. Una palabra en los elementos de X es una expresión de la forma

$$x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}$$

donde $k \geq 1$; $n_1, n_2, \dots, n_k \in \mathbb{Z}$ y $x_1, x_2, \dots, x_k \in X$. Diremos que dicha palabra es reducida si $x_i \neq x_{i+1}$.

Proposición: Sea G un grupo y X un subconjunto de G, $X \neq \emptyset$. Entonces

$$\langle X \rangle = \{x_1^{n_1} \dots x_k^{n_k} / x_i \in X,\ n_i \in \mathbb{Z},\ k \geq 1\}$$

Además, si G es finito, entonces

$$\langle X \rangle = \{x_1^{n_1} \dots x_k^{n_k} / x_i \in X,\ n_i \geq 0,\ k \geq 1\}$$

Demostración: $X \subseteq \{x_1^{n_1} \dots x_k^{n_k} / x_i \in X, n_i \in \mathbb{Z}, k \geq 1\}$ es claro y entonces dicho conjunto es no vacío. Sean x, y dos palabras en los elementos de X.

$$\exists x = x_1^{n_1} \dots x_k^{n_k} \quad y = y_1^{t_1} \dots y_s^{t_s}, \qquad \begin{matrix} x_i, y_i \in X \\ n_i, t_j \in \mathbb{Z} \\ s, k \geq 1 \end{matrix}$$
$$\Rightarrow xy^{-1} = x_1^{n_1} \dots x_k^{n_k} (y_1^{t_1} \dots y_s^{t_s})^{-1} =$$
$$= x_1^{n_1} \dots x_k^{n_k} y_s^{-t_s} \dots y_1^{-t_1}$$

que es claramente una palabra en elementos de X.

Se tiene que el conjunto de las palabras en un subgrupo de G es claramente el menor subgrupo de G que contiene a X.

Si G es finito entonces

$$\{x_1^{n_1} \dots x_k^{n_k} / x_i \in X,\ n_i \geq 0,\ k \geq 1\}$$

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

$$\langle X \rangle = \{x_1^{n_1} \dots x_k^{n_k} / x_i \in K,\ n_i \geq 0,\ k \geq 1\}$$

Definición: Sea G un grupo y $X \subseteq G$, $X \neq \emptyset$. Si $\langle X \rangle = G$, diremos que X es un conjunto de generadores del grupo G.

Un grupo G diremos que es finitamente generado si $\exists X \subseteq G$, $X \neq \emptyset$ y finito tal que $G = \langle X \rangle$. (Claramente todo grupo finito es finitamente generado).

Si $X = \{a\} \subseteq G$, al subgrupo generado por X, que denotaremos por $\langle a \rangle$, lo llamaremos el subgrupo cíclico generado por el elemento a.

$$\langle a\rangle = \{a^n / n \in \mathbb{Z}\}$$

y si G es finito, entonces

$$\langle a\rangle = \{a^n / n \geq 0\}$$

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

Ejemplo:

1) $D_n = \langle r, s\rangle \quad \forall n \geq 3$
$Q_2 = \langle i, j\rangle$

$$Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$$
$$(-1)^2 = 1 \qquad i^2 = j^2 = k^2 = -1$$
$$ij = k \qquad (-1)j = -a = a(-1) \qquad a = i, j, k$$

$n \geq 2 \qquad S_n = \langle (i\, j) / 1 \leq i < j \leq n\rangle$

2)

$$\mathbb{Z} = \langle 1\rangle = \langle -1\rangle \quad pues$$
$$\langle 1\rangle = \{n \cdot 1 / n \in \mathbb{Z}\} = \mathbb{Z}$$
$$\langle -1\rangle = \{n \cdot (-1) / n \in \mathbb{Z}\} = \mathbb{Z}$$

3)

$$\mathbb{Z} \times \mathbb{Z} \qquad (a, b) + (a', b') = (a + a', b + b')$$
$$\mathbb{Z} \times \mathbb{Z} = \langle (1, 0), (0, 1)\rangle$$
$$\{n_1(1, 0) + n_2(0, 1) / n_1, n_2 \in \mathbb{Z}\}$$

24-3-2021

Ejemplo:

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

$$\mu_n = \langle \xi_1\rangle$$
$$\xi_k \xi_r = \xi_{res(k+1;n)}$$

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

2) Ejercicio 4 (Rel 2.) $\mathbb{Z}_7^x = \{1,2,3,4,5,6\}$. Demostrar que es cíclico

$$\langle 2\rangle = \{2^n / n \geq 0\}$$
$$2^1 = 2 \quad \forall n \geq 4 \, si \, n = 3q + r \quad 0 \leq r < 2$$
$$2^2 = 4 \quad 2^n = 2^{3q} \cdot 2^r = 2^r$$
$$2^3 = 1 \quad \langle 2\rangle = \{1,2,4\} \leq \mathbb{Z}_7^x$$

$$\langle 3\rangle = \{3^n / n \geq 0\} = \{1,3,2,6,4,5\} = \mathbb{Z}_7^x$$
$$3^0 = 1 \qquad 3^3 = 6$$
$$3^1 = 3 \qquad 3^4 = 4$$
$$3^2 = 2 \qquad 3^5 = 5$$
$$\mathbb{Z}_7^x = \langle 5\rangle$$

3) $S_n = \langle (i\,j)/1 \leq i < j \leq n\rangle$. Se verifica que

$$S_n = \langle (1\,2), (1\,3), \ldots, (1\,n)\rangle$$

pues para todo $1 \leq i < j \leq n$ se tiene que

$$(i\,j) = (1\,i)(1\,j)(1\,i)$$
$$S_n = \langle (i\,j)/1 \leq i < j \leq n\rangle \subseteq \langle (1\,2), \ldots, (1\,n)\rangle \Rightarrow$$
$$S_n = \langle (1\,2), (1\,3), \ldots, (1\,n)\rangle$$

4) Ejercicio 5 (Rel 2) Demostrar que

$$S_n = \langle (1\,2), (2\,3), \ldots, (n-1\,n)\rangle$$

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

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

Entonces por inducción se demuestra que

$$\{(1\,2)(1\,3), \ldots, (1\,n)\} \subseteq \langle (1\,2), (2\,3), \ldots, (n-1 \quad n)\rangle$$

5) Ejercicio 6 (Rel 2) Demostrar que

$$S_n = \langle \sigma = (1\,2\ldots n), \tau = (1\,2)\rangle$$

Para todo $i \geq 1$

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

Por inducción, demostrar que

$$\{(1\,2), (2\,3), \ldots, (n-1 \quad n)\} \subseteq \langle \sigma, \tau \rangle$$

Proposición:

1) Sea G un grupo y sean X, Y subconjuntos de G. Entonces si

$$H = \langle X \rangle \quad y \quad K = \langle Y \rangle,$$
$$H \vee K = \langle X \cup Y \rangle$$

2) Sea $f : G \to G'$ un homomorfismo de grupos y sea X un subconjunto G. Entonces

$$f_*(\langle X \rangle) = \langle f_*(X) \rangle$$

En particular, la imagen directa de un subgrupo cíclico de G es un subgrupo cíclico de G'.

Demostración: Ejercicio.

Ejercicio: Sea $f : G \to G'$ es un homomorfismo de grupos y sea $X' \subseteq G'$. ¿Qué relación hay entre $\langle f^*(X') \rangle$ y $f^*(\langle X' \rangle)$?

Sea G un grupo y $H \leq G$ un subgrupo. ¿Quién es $\langle H \rangle$?

$$\langle H \rangle = H$$

Definición: Sea G un grupo y $H \leq G$ un subgrupo. Definimos en G dos realciones binarias como sigue
Dados $x, y \in G$

$$x \sim_I y \Leftrightarrow^{def} y^{-1}x \in H$$
$$x \sim_D y \Leftrightarrow^{def} xy^{-1} \in H$$

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 $\sim_D$.

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

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

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

Entonces se verifica
Proposición:

1) $x \in xH$ y $x \in Hx$

2) $xH = yH \Leftrightarrow y^{-1}x \in H$
   $Hx = Hy \Leftrightarrow xy^{-1} \in H$

3) $xH \neq yH \Leftrightarrow xH \cap yH = \emptyset$
   $Hx \neq Hy \Leftrightarrow Hx \cap Hy = \emptyset$

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, $\forall x \in G$.

6) Existe una biyección entre G/H y H/G

Demostración: (5) $\begin{array}{lll} t : H \to xH & t(h) = xh & es\ biyectiva \\ s : H \to Hx & s(h) = hx & es\ biyectiva \end{array}$

(6) Sea

$$\lambda : G/H \to H/G$$
$$\lambda(xH) := Hx^{-1}$$
$$xH = yH \Leftrightarrow y^{-1}x \in H \Leftrightarrow$$
$$\Leftrightarrow (y^{-1}x)^{-1} = x^{-1}y \in H \Leftrightarrow Hx^{-1} = Hy^{-1}$$

Luego λ es biyectiva.

□

Definición: Sea G un grupo finito y H un 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

$[G : H]$ = número de clases a izquierda módulo H
$[H : G]$ = número de clases a derecha módulo H

Teorema de Lagrange: Sea G un grupo finito y $H \leq G$ un subgrupo. Entonces

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

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

$$G/H = \{x_1H, x_2H, \ldots, x_rH\}$$

Por (4) de la proposición anterior

$$\left.\begin{array}{c} G = \cup_{i=1}^{r} x_iH \\ x_iH \cap x_jH = \emptyset \qquad \forall i \neq j \end{array}\right\} \Rightarrow |G| = \sum_{i=1}^{r} |x_iH| =$$

$$= \sum_{i=1}^{r} |H| = r|H| = [G : H]\,|H|$$

□

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

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

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

$$S_3/A_3 = \{idA_3 = A_3, (1\,2)A_3 = \{(1\,2), (1\,2)(1\,2\,3) = (2\,3), (1\,2)(1\,3\,2) = (1\,3)\}\}$$

$$A_3/S_3 = \{A_3id = A_3, A_3(1\,2) = \{(1\,2), (1\,2\,3)(1\,2) = (1\,3), (1\,3\,2)(1\,2) = (2\,3)\}\}$$

$$\forall \alpha \in S_3 \qquad \alpha A_3 = A_3\alpha$$

$$6 = |S_3| \qquad H = \{id, (2\,3)\} \leq S_3$$

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

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

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

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

Corolario: Sea G un grupo finito. Si H es un subgrupo de $G \Rightarrow |H|/|G|$ □

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

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 un orden finito. Es claro que $ord(1) = 1$ y de hecho $ord(a) = 1 \Leftrightarrow a = 1$.

Ejemplo:

1) En $\mathbb{Z}$ el único elemeto finito es el 0.

2) En μ_n, $\xi_1 = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$ tiene orden n ($ord(\xi_1) = n$).

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

4) Ejer 16 (Rel 2.) Listar los órdenes de los elementos de Q_2

$$Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$$
$$ord(1) = 1$$
$$ord(-1) = 2 \quad pues \quad (-1)^2 = 1$$
$$ord(i) = 4 = ord(-1) \quad i^2 = -1$$
$$ord(j) = 4 = ord(-j) \quad i^3 = (-1)i = -i$$
$$ord(k) = k = ord(-k) \quad i^4 = -ii = (-1)i^2 = (-1)(-1) = 1$$

Listar los órdenes de los elementos de D_4

$$D_4 = \langle r, s / r^4 = 1 s^2,\ sr = r^3 s \rangle =$$
$$= \{1, r, r^2, r^3, s, sr, s^2, s^3 r\}$$

6-4-2021

Ejercicio 15(Rel 2): $f : G \to G'$ es un isomorfismo$\Rightarrow ord(f(a)) = ord(a) \quad \forall a \in G$

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

(1) Si $ord(a) = n \Rightarrow \langle a \rangle = \{1, a, \dots, a^{n-1}\}$

(2) Si $ord(a) = \infty \Rightarrow \langle a \rangle \cong \mathbb{Z}$

Demostración: Sabemos que $\langle a \rangle = \{a^k / k \in \mathbb{Z}\}$

(1) $ord(a) = n > 0 \qquad \{1, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$

Dado $k \in \mathbb{Z}$, $\exists! q, r \in \mathbb{Z}$ tal que

$$k = nq + r \quad y \quad 0 \leq r < n$$
$$a^k = a^{nq} \cdot a^r = a^r \in \{1, a, \ldots, a^{n-1}\}$$
$$\langle a \rangle = \{1, a, \ldots, a^{n-1}\} \quad donde \quad a^r \cdot a^s = a^{res(r+s;n)}$$

En particular,

$$| \langle a \rangle | = ord(a)$$

(2) $ord(a) = \infty \quad \left(\nexists k \in \mathbb{Z},\ k \neq 0 \quad tal\ que \quad a^k = 1\right)$

Definimos

$$f : \mathbb{Z} \to \langle a \rangle = \{a^k / k \in \mathbb{Z}\}$$
$$f(k) := a^k$$
$$f(k + k') = a^{k+k'} = a^k \cdot a^{k'} = f(k) \cdot f(k')$$

f es homomorfismo de grupos, claramente epimorfismo

$$Ker(f) = \{k \in \mathbb{Z} / f(k) = 1\} = \{k \in \mathbb{Z} / a^k = 1\} = \{0\}$$

f es también monomorfismo $\Rightarrow$ f es isomorfismo.

□

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

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

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

Demostración:

$$H = \langle a \rangle \qquad |H| = n = |H'| \Rightarrow ord(a) = n = ord(b)$$
$$H' = \langle b \rangle$$
$$H = \{1, a, \ldots, a^{n-1}\} \qquad H \cong H'$$
$$H' = \{1, b, \ldots, b^{n-1}\}$$

□

Hay sólo una clase de isomorfismo de grupos cíclicos de orden n. Un representante es μ_n. De forma abstracta, representamos al cíclico de orden n por C_n y escribiremos

$$C_n = \langle a / a^n = 1 \rangle = \{1, a, \ldots, a^{n-1}\}$$
$$a^r \cdot a^s = a^{res(r+s;n)}$$

Teorema: Sea G un grupo con $ord(G) = p$, siendo p un número primo. Entonces $G \stackrel{\sim}{=} C_p$. Consecuentemente cualesquiera dos grupos de orden p son isomorfos.

Demostración: $|G| = p \quad p \geq 2$. Elegimos $a \in G, \quad a \neq 1$.

$$\left.\begin{array}{c} Entonces \quad ord(a) \mid |G| = p \\ a \neq 1 \Rightarrow ord(a) \neq 1 \\ p \quad primo \end{array}\right\} \Rightarrow ord(a) = p$$
$$\Rightarrow |\langle a \rangle| = p = |G| \Rightarrow \langle a \rangle = G$$

7-6-21

Sea $C_n = \langle x / x^n = 1 \rangle \qquad n \geq 2$

$$C_n = \{1, x, \ldots, x^{n-1}\} \qquad x^r x^s = x^{res(r+s;n)}$$

Proposición:

(1) $x^m = 1 \Leftrightarrow n \mid m$

(2) $ord(x^k) = \frac{n}{mcd(n,k)}$

(3) x^k es un generador de $C_n \Leftrightarrow mcd(n,k) = 1$

(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

$$m = nq + r \qquad 0 \leq r < n$$

$$\Rightarrow \left.\begin{array}{c} 1 = x^r \\ 0 \leq r < n \\ ord(x) = n \end{array}\right\} \Rightarrow r = 0 \Rightarrow m = nq$$

(2) $ord(x^k) = \frac{n}{mcd(n,k)}$¿? $\quad \begin{array}{c} d = mcd(n,k) \\ n = dn' \\ k = dk' \end{array}$

$$ord(x^k) = n' \qquad ?`?$$
$$(x^k)^{n'} = x^{kn'} = x^{dk'n'} = x^{nk'} = 1^{k'} = 1$$

Sea $m > 0$ tal que $(x^k)^m = x^{km} = 1 \Big\} \overset{(1)}{\Rightarrow} n \mid km$

$$\exists t \in \mathbb{Z} \, tal \, que \quad \left.\begin{array}{c} km = nt \\ dk'm = dn't \end{array}\right\} \Rightarrow k'm = n't$$
$$\Rightarrow \quad \left.\begin{array}{c} n' \mid k'm \\ mcd(n', k') = 1 \end{array}\right\} \Rightarrow n' \mid m$$

Recordatorio función de Euler:

$$\varphi(n) = card\{1 \leq k \leq n / mcd(n,k) = 1\}$$
$$\varphi(p^e) = p^{e-1}(p-1) \qquad p \, es \, primo$$
$$Si \, mcd(n,m) = 1 \Rightarrow \varphi(nm) = \varphi(n) \cdot \varphi(m)$$
$$n = p_1^{e_1} \dots p_k^{e_k} \Rightarrow \varphi(n) = p_1^{e_1 - 1} \dots p_k^{e_k - 1}(p_1 - 1) \dots (p_k - 1)$$

Fin recordatorio función de Euler

El orden del producto de dos elementos no tiene que ser igual que el producto de los órdenes

Ejercicio 17 (Relación 2): G un grupo, $a, b \in G$ tal que son de orden finito y

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

Entonces

(1) $\langle a \rangle \cap \langle b \rangle = \{1\}$

(2) $ord(ab) = ord(a) \cdot ord(b)$

Resolución:

(1) $x \in \langle a \rangle \cap \langle b \rangle \Rightarrow \left\{ \begin{array}{c} x \in \langle a \rangle \\ \wedge \\ x \in \langle b \rangle \end{array} \right.$

$$\Rightarrow \left\{ \begin{array}{c} ord(x) \mid ord(\langle a \rangle) = ord(a) \\ \wedge \\ ord(x) \mid ord(\langle b \rangle) = ord(b) \end{array} \right. \left\{ \begin{array}{c} \overset{mcd(ord(a), ord(b)) = 1}{\Rightarrow} ord(x) = 1 \Rightarrow x = 1 \\ \end{array} \right.$$

(2) $ord(a) = n \quad ord(b) = m \quad ord(ab) = nm$¿?

$$(ab)^{nm} \overset{ab=ba}{=} a^{nm}b^{nm} = 1 \cdot 1 = 1$$
$$(ab)^k = 1 = a^k b^k \Rightarrow a^k = (b^k)^{-1} \in \langle a \rangle \cap \langle b \rangle = \{1\} \Rightarrow$$
$$\Rightarrow a^k = 1 = b^k \Rightarrow \left.\begin{matrix} n \mid k \\ m \mid k \end{matrix}\right\} \Rightarrow nm = mcm(n,m) \mid k$$

Ejemplo:

$G = \mathbb{Z}_8^x = \{1, 3, 5, 7\}$

$$a = 3 \qquad ord(a) = 2 \qquad mcd(ord(a), ord(b)) = 2 \neq 1$$
$$b = 5 \qquad ord(b) = 2$$
$$ab = 7 \qquad ord(7) = 2 \neq ord(a) \cdot ord(b)$$

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 descomponen).

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

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

$$\alpha(x) \neq x \overset{\alpha \text{ y } \beta \text{ disjuntas}}{\Rightarrow} \beta(x) = x \Rightarrow \beta^k(x) = x$$

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

$$(\alpha\beta)^m \overset{\alpha\beta=\beta\alpha}{=} \alpha^m\beta^m = id \cdot id = id$$

Sea k tal que $1 = (\alpha\beta)^k \overset{\alpha\beta=\beta\alpha}{=} \alpha^k\beta^k$, como α^k y β^k son disjuntas, entonces $\alpha^k = id = \beta^k$. Pues si $\alpha^k \neq id$, sea x tal que $\alpha^k(x) \neq x \Rightarrow \beta^k(x) = x$

$$(\alpha^k\beta^k)(x) = \alpha^k(x) \neq x \downarrow \alpha^k\beta^k = id$$
$$\left.\begin{matrix} \alpha^k = id \Rightarrow r \mid k \\ \beta^k = id \Rightarrow s \mid k \end{matrix}\right\} \Rightarrow m = mcm(r,s) \mid k$$

Ejercicio 18 (Relación 2): $\sigma = (1\,8\,10\,4)(2\,8)(5\,1\,4\,8) \in S_{15}$

La expresión de σ en ciclo disjuntos es $\sigma = (2\,10\,4)(5\,8)$

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

Ejercicio 20 (Relación 2): 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.

Resolución:

$$G = \langle a, b\rangle \overset{ab=ba}{=} \{a^r b^s / r, s \in \mathbb{Z}\} \overset{ord(a)=ord(b)=2}{=}$$
$$\overset{ord(a)=ord(b)=2}{=} \{a^r b^s / 0 \leq r \leq 1,\ 0 \leq s \leq 1\} = \{1, a, b, ab\}$$

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

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

Grupos de Klein

$$K = \langle a, b / a^2 = 1 = b^2; ab = ba\rangle$$

Ejercicio 23 (Relación 2):

(1) Si G es un grupo de orden 4, entonces $G \cong C_4$ ó $G \cong K$ (grupo de Klein).

(2) Si G es un grupo de orden 6, entonces $G \cong C_6$ ó $G \cong D_3$.

Resolución:

(1) $G \qquad |G| = 4.$

$$Si \quad a \in G \quad a \neq 1 \Rightarrow \left.\begin{array}{c} ord(a) \mid 4 \\ a = 1 \end{array}\right\} \Rightarrow ord(a) = 2 \text{ ó } 4$$

Caso 1: $\exists a \in G$ tal que $ord(a) = 4$ entonces

$$\langle a\rangle = G \Rightarrow G \cong C_4$$

Caso 2: No existen en G elementos de orden 4, entonces todos los elementos de G ($\neq 1$) tienen orden 2, luego G es abeliano (**Ejercicio 6 (Relacion 1)**).

Elegimos $a, b \in G$, $a \neq b$ distintos de 1

$$\left.\begin{array}{c} H = \langle a, b \rangle \\ a^2 = 1 = b^2 \\ ab = ba \end{array}\right\} \Rightarrow H = K \quad el\ grupo\ de\ Klein\ y\ |H| = 4 \Rightarrow H = G$$

(2) $G, \quad |G| = 6, \quad a \in G, \quad a \neq 1, \quad ord(a) = 2, 3\ ó\ 6$

Caso 1: G es abeliano. No todos los elementos de G ($\neq 1$) tienen orden 2 porque si así fuera, elegimos $a, b \in G$, $a \neq b\ (\neq 1)$ y $H = \langle a, b \rangle \leq G$

$$H \cong K \quad pues \quad a^2 = 1 = b^2 \quad y \quad ab = ba \quad (G\ abeliano)$$
$$\Rightarrow |H| = 4 \mid |G| = 6 \downarrow$$

Así, $\exists a \in G$ tal que $ord(a) = 6$ ó $ord(a) = 3$. Si $ord(a) = 6 \Rightarrow \langle a \rangle = 6$ y $G \cong C_6$. Supongamos que $a \in G$ con $ord(a) = 3$. Sea $H = \langle a \rangle = \{1, a, a^2\} \leq G$

$$[G : H] = \frac{|G|}{|H|} = \frac{6}{3} = 2$$
$$H/G = \{H, Hb\} \qquad b \in G \quad tal\ que \quad b \notin H$$
$$G = H \cup Hb = \{1, a, a^2, b, ab, a^2b\}$$
$$b^2 \in G \Rightarrow b^2 \in H\ ó\ b^2 \in Hb$$

Si $b^2 \in Hb \Rightarrow b^2 = a^i b \quad 0 \leq i \leq 2 \Rightarrow b = a^i \quad 0 \leq i \leq 2$, es decir, $b \in H\ \downarrow$.

Por tanto $b^2 \in H = \{1, a, a^2\}$

$$Si\ b^2 = a \Rightarrow ord(b^2) = ord(a) = 3 \Rightarrow$$
$$\Rightarrow ord(b) = 3 \Rightarrow b = b^4 = (b^2)^2 = a^2 \Rightarrow b \in H \downarrow$$

De la misma forma, $b^2 \neq a^2$. Consecuentemente $b^2 =!$, es decir, $ord(b) = 2$

$$a, b \in G \qquad ab = ba\ (G\ es\ abeliano)$$
$$mcd(ord(a), ord(b)) = mcd(3, 2) = 1 \Rightarrow$$
$$\Rightarrow ord(ab) = ord(a)ord(b) = 6$$
$$ab \in G \quad ord(ab) = 6 \Rightarrow \langle ab \rangle = G \Rightarrow G \cong C_6$$

Caso 2: G no es abeliano

$$a \in G,\ a \neq 1 \Rightarrow ord(a) = 2, 3\ ó\ \not{6}\ (G\ no\ es\ abeliano)$$

Como G no es abeliano, existe $a \in G$ tal que $ord(a) = 3$

$$H = \langle a \rangle = \{1, a, a^2\} \leq G$$
$$[G : H] = 2 \; y \; H/G = \{H, Hb\} \quad b \in G, \; b \notin H$$
$$G = H \cup Hb = \{1, a, a^2, b, ab, a^2b\}$$

Razonando como anteriormente, $ord(b) = 2$

$$(D_3 = \langle r, s / r^3 = 1 = s^2, \; sr = r^2 s \rangle = \{1, r, r^2, s, rs, r^2, s\})$$

$$ba = a^2b \quad ??$$
$$ab \in G = H \cup Hb \Rightarrow ba \in H \; \acute{o} \; ba \in Hb$$

Si $ba \in H = \{1, a, a^2\}$ entonces $ba = a^i, \quad 0 \leq i \leq 2 \Rightarrow$

$$\Rightarrow b = a^{i-1} \qquad 0 \leq i \leq 2 \Rightarrow b \in H \; \downarrow$$

Por tanto $ba \in Hb = \{b, ab, a^2b\}$

$$Si \; ba = b \Rightarrow a = 1 \; \downarrow$$
$$Si \; ba = ab, \; como \; G = \langle a, b \rangle, \; G \; seria \; abeliano \; \downarrow$$

Por tanto $ba = a^2b$

$$G = \langle a, b / a^3 = 1 = b^2, \; ba = a^2b \rangle \cong D_3$$

$S_3 \cong D_3$

Descripción de $Sub(G)$, para G algunos grupos de orden finito. Empezamos con los grupos cíclicos finitos.

Teorema: $C_n = \langle x / x^n = 1 \rangle = \{1, x, \ldots, x^{n-1}\} \quad n \geq 2$

(1) Para cada divisor positivo d de n, $\langle x^{\frac{n}{d}} \rangle \leq C_n$ tiene orden d. Por tanto $\langle x^{\frac{n}{d}} \rangle = C_d$

(2) Sea $H \leq C_n$, $H \neq \{1\}$ y sea $s = min\{r \geq 1 / x^r \in H\}$. Entonces s es un divisor de n y $H = \langle a^s \rangle$

(3) Denotemos por $Div(n) = \{d \geq 1 / d \mid n\}$. Entonces la aplicación

$$Div(n) \longrightarrow Sub(C_n)$$
$$d \longmapsto \langle x^{\frac{n}{d}} \rangle$$

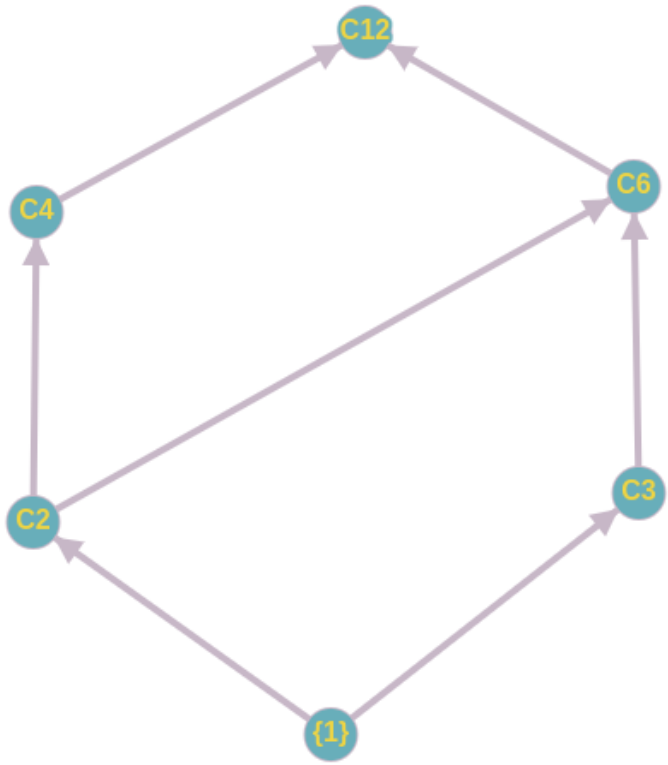
es biyectiva.

(4) Sean $d_1, d_2 \in Div(n)$

$$d_1 \mid d_2 \Leftrightarrow \left\langle x^{\frac{n}{d_1}} \right\rangle \leq \left\langle x^{\frac{n}{d_2}} \right\rangle$$

$$n = 12 \qquad C_{12} = \langle x/x^{12} \rangle \qquad Div(12) = \{1, 2, 3, 4, 6, 12\}$$
$$Sub(C_{12}) = \{\langle x^{12} \rangle = \{1\},\ \langle x^6 \rangle = C_2,\ \langle x^4 \rangle = C_3,$$
$$\langle x^3 \rangle = C_4,\ \langle x^2 \rangle = C_6,\ \langle x \rangle = C_{12}\}$$

Figura 4: Grafo un poco deforme



$H, K \in Sub(G)$ si $H \leq K$ y $\nexists H' \in Sub(G)$ con $H \leq H' \leq K$

$$H \longrightarrow K \longrightarrow L$$

12-4-21

Demostración:

(1) $d \mid n, \quad d \geq 1, \quad \left\langle x^{\frac{n}{d}} \right\rangle$

Puesto que $(x^{\frac{n}{d}}) = \frac{n}{mcd(n,\frac{n}{d})} = \frac{n}{mcd(n,s)} = \frac{n}{s} = d$

$\frac{n}{d} = s \Rightarrow n = sd$

Entonces $|\left\langle x^{\frac{n}{d}} \right\rangle| = d$, es decir, $\left\langle x^{\frac{n}{d}} \right\rangle = C_d$

(2) $H \leq C_n, \quad H \neq \{1\}, \quad s = min\{r \geq 1 / x^r \in H\}$

Debemos comprobar que $s \mid n$ y $\langle a^s \rangle = H$.

Puesto que $s \in \{r \geq 1 / x^r \in H\} \Rightarrow x^s \in H \Rightarrow \langle x^s \rangle \leq H$

Sea $x^m \in H$, dividimos m entre s, $m = sq + t \quad 0 \leq t < s$

$$x^m = x^{sq} \cdot x^t \Rightarrow x^t = x^m \cdot (x^{sq})^{-1} \Rightarrow$$
$$\left.\begin{array}{c} x^t \in H \\ 0 \leq t < s \\ s \; es \; el \; minimo \; de \; A \end{array}\right\} \Rightarrow t = 0$$

Entonces $m = sq$ con lo que

$$x^m = x^{sq} \in \langle x^s \rangle \Rightarrow H \leq \langle x^s \rangle$$

Por tanto $\langle x^s \rangle = H$. Puesto que $x^n = 1 \in H$, entonces $s \mid n$ por el mismo razonamiento anterior.

$$H = \langle x^s \rangle \quad s \mid n \Rightarrow n = sd \Rightarrow s = \frac{n}{d}$$
$$H = \left\langle x^{\frac{n}{d}} \right\rangle$$

Los apartados (3) y (4) se dejan como ejercicios.

Ejercicio 28 (Relación 2): p un primo y $n \geq 1$

$$C_{p^n} = \left\langle x / x^{p^n} = 1 \right\rangle$$
$$Div(p^n) = \{p^k / 0 \leq k \leq n\} \quad p^k$$
$$\updownarrow \qquad\qquad\qquad\qquad \downarrow$$
$$Sup(C_{p^n}) \qquad\qquad \left\langle x^{\frac{p^n}{p^k}} \right\rangle = \left\langle x^{p^{n-k}} \right\rangle$$
$$Sub(C_{p^n}) = \{\left\langle x^{p^{n-k}} \right\rangle = C_{p^k} / 0 \leq k \leq n\}$$
$$C_{p^n} \to C_{p^{n-1}} \to C_{p^{n-2}} \to \ldots \to C_p \to \{1\}$$

Ejercicio 27 (Relación 2): Describir $Sub(S_3)$ y $Sub(D_4)$

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

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

- De orden 1 es $\{1\}$
- De orden 6 es S_3
- De orden 2: todo grupo de orden 2 es cíclico generado por un elemento, luego hay tres subgrupo de orden 2

$$C_2 = \langle(1\,2)\rangle = \{id, (12)\}, \quad C_2' = \langle(1\,3)\rangle = \{id, (13)\}, \quad C_2'' = \langle(2\,3)\rangle = \{id, (23)\}$$

- De orden 3: todo grupo de orden 3 es cíclico:

$$C_3 = \langle(1\,2\,3)\rangle = \{id, (1\,2\,3), (1\,2\,3)^2 = (1\,3\,2)\} =$$
$$= \langle(1\,3\,2)\rangle = \{id, (1\,3\,2), (1\,3\,2)^2 = (1\,2\,3)\}$$

$Sub(D_4)$:

$$D_4 = \langle r, s | r^4 = 1 = s^2 \quad sr = r^3 s\rangle = \{1,\, r,\, r^2,\, r^3,\, s,\, rs,\, r^2 s,\, r^3 s\}$$

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

- Orden $1 \to \{1\}$
- Orden $8 \to D_4$
- Orden $2 \to$ Generador por elementos de orden 2 de D_4

$$C_2 = \langle r^2\rangle = \{1,\, r^2\} \qquad C_2''' = \langle rs\rangle = \{1,\, rs\}$$
$$C_2' = \langle s\rangle = \{1,\, s\} \qquad C_2^{iv} = \langle r^3 s\rangle = \{1,\, r^3 s\}$$
$$C_2'' = \langle r^2 s\rangle = \{1,\, r^2 s\}$$

- 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 los elementos de orde 4 en D_4, que son r y r^3.

$$C_4 = \langle r\rangle = \{1,\, r,\, r^2,\, r^3\} = \langle r^3\rangle$$

Para buscar los subgrupos en D_4 que sean tipo Klein, tenemos que buscar dos elementos de orden 2 que conmuten entre si

$$r^2,\ s,\ rs,\ r^2s,\ r^3s$$

$$r^2,\ s\ tienen\ orden\ 2 \qquad (sr^i = r^{-i}s,\ en\ el\ grupo\ diedrico)$$

$$sr^2 = r^2s \qquad K = \{1,\ r^2,\ s,\ r^2s\} \leq D_4$$

$$r^2,\ rs\ tienen\ orden\ 2$$

$$\left.\begin{array}{c} r^2(rs) = r^{3s} \\ rsr^2 = rr^2s = r^3s \end{array}\right\} \Rightarrow r^2(rs) = (rs)r^2$$

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

13-4-21

Proposición: Sea $C_n = \langle x / x^n = 1 \rangle$

(1) $\langle x^m \rangle = \left\langle x^{mcd(m,n)} \right\rangle$

(2) $\langle x^{m_1},\ x^{m_2}, \ldots, x^{m_k} \rangle = \left\langle x^{mcd(m_1,m_2,\ldots,m_k,n)} \right\rangle$

Demostración:

(1) Sea $d = mcd(m,n)$. Tendremos que $n = ds$. Sabemos que existe un único subrgrupo cíclico de orden s que es

$$\left\langle x^{\frac{n}{s}} \right\rangle = \left\langle x^d \right\rangle$$

$$|\ \langle x^m \rangle\ | = ord(x^m) = \frac{n}{mcd(n,m)} = \frac{n}{d} = s$$

Por tanto $\langle x^m \rangle = \left\langle x^d \right\rangle$

(2) $N = \langle x^{m_1},\ x^{m_2}, \ldots,\ x^{m_k} \rangle \leq C_n$. Sea $d = mcd(m_1,\ m_2, \ldots,\ m_k, n)$. Puesto que $d \mid m_i \Rightarrow x^{m_i} \in \left\langle x^d \right\rangle \quad \forall i = 1, \ldots, k$, por tanto $N \leq \left\langle x^d \right\rangle$.

Por el teorema de Bezout, $\exists t_1,\ t_2, \ldots,\ t_n,\ t \in \mathbb{Z}$, tal que

$$d = m_1t_1 + m_2t_2 + \ldots + m_kt_k + nt$$

, entonces

$$x^d = x^{m_1t_1} \cdot x^{m_2t_2} \ldots x^{m_kt_k} \in N$$

con lo que $\left\langle x^d \right\rangle \leq N$

3. Tema 4. Grupos Cocientes. Teoremas de Isomorfías.

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

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

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

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 $N = \langle r \rangle = \{1, r, r^2, r^3\}$

$$D_4 = \langle r, s / r^4 = 1 = s^2,\ sr = r^3 s \rangle$$

$$[D_4 : N] = \frac{|D_4|}{|N|} = \frac{8}{4} = 2$$

$$D_4/N = \{N, sN\} \quad N/D_4 = \{N, Ns\}$$

$$sN = \{s, sr, sr^2, sr^3\} = \{s, r^3 s, r^2 s, rs\} = Ns$$

Por tanto $N \trianglelefteq D_4$

Sea $N = \langle s \rangle = \{1, s\} \leq D_4$, no es normal en D_4

$$rN = \{r, rs\} \neq N_r = \{r, sr\} = \{r, r^3 s\}$$

Teorema: Sea G un grupo y $N \leq G$, son equivalentes los siguientes enunciados:

(1) N es un subgrupo normal en G.

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

(3) $aNa^{-1} \leq N \quad \forall a \in G$

Es decir, N es un subgrupo normal de G si y sólo si coincide con todos sus conjugados ó, si y sólo si contiene a todos sus conjutados.

Para $N \leq G$ y $a \in G$, el subgrupo

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

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

Demostración: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) Lo hace en clase. 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, $xa^{-1} = ana^{-1} \in aNa^{-1} \leq N \Rightarrow \exists n' \in N$ tal que $xa^{-1} = n'$, luego $x = n'a \in Na$.

Tenemos pues que $aN \leq Na$.

Sea $y \in Na \Rightarrow \exists m \in N$ tal que $y = mc$. Entonces $a^{-1}y = a^{-1}ma \in a'Na \leq N \Rightarrow \exists m' \in N$ tal que $a^{-1}y \in m' \Rightarrow y = am' \in aN$.

Por tanto, $Na \leq aN$

□

Ejemplo:

(1) Sea $f : G \to G'$ un homomorfismo de grupos.

$$Ker(f) = \{x \in G / f(x) = 1\}$$

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 $aKer(f)a^{-1} \leq Ker(f) \quad \forall a \in G$, 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 $\alpha \in S_4$

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

por ser α biyectiva.

Análogamente, por el mismo razonamiento,

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

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

Proposición: Sea G un grupo y $X \subseteq G$ un subconjunto de G no vacío. Sea $N = \langle X \rangle$

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

Demostración: $\Leftarrow$) Obvio

$\Rightarrow$) Sea $a \in G$ y sea

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

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

$$aNa^{-1} = (\varphi_{a_*})(N) = (\varphi_{a_*})(\langle X \rangle) =$$
$$= \langle (\varphi_{a_*})(X) \rangle = \left\langle aXa^{-1} \in N \right\rangle \leq N$$

Por tanto $N \trianglelefteq G$

□

Ejemplo: $\forall n \geq 2 \quad A_n \trianglelefteq S_n$. Para ello, utilizamos que A_n está generado por

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

Sea $\alpha \in S_n$ y $(x_1,\, x_2,\, x_3) \in X$, entonces $\alpha(x_1,\, x_2,\, x_3)\alpha^{-1} = (\alpha(x_1)\alpha(x_2)\alpha(x_3)) \in X \subseteq A_n$.

Por tanto, $A_n \trianglelefteq S_n$

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

14-4-21

Ejercicio 3 (Relación 3): Sea G un grupo finito y $H \leq G$ tal que $[G : H] = 2 \Rightarrow H \trianglelefteq G$.

Resolución: $[G : H] = 2 \Rightarrow$

$$G/H = \{H, aH\} \quad a \notin H$$
$$H/G = \{H, Ha\}$$

Como $\begin{matrix} G = H \cup aH \\ G = H \cup Ha \end{matrix}$ y ambas uniones son disjuntas $\Rightarrow$

$$H = H \quad y \quad aH = Ha$$

Entonces $H \trianglelefteq G$.

□

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

$$D_n = \langle r, s / r^n = 1 = s^2, \quad sr = r^{n-1}s \rangle$$

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

Ejercicio 4 (Relación 3): Describid el retículo de subgrupos de A_4.

$$A_4 = \{id,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3),\ (1\,2\,3),\ (1\,3\,1),$$
$$(1\,2\,4),\ (1\,4\,2),\ (1\,3\,4),\ (1\,4\,3),\ (2\,3\,4),\ (2\,4\,3)\}$$
$$|A_n| = \frac{n!}{2} \qquad |A_4| = 12$$

tendrá posiblemente subgrupos de orden 1, 2, 3, 4, 6 ó 12.

$$orden\ 2:\ \{(1\,2)(3\,4)\},\ \{(1\,3)(2\,4)\},\ \{(1\,4)(2\,3)\}$$
$$orden\ 3:\ \{(1\,2\,4),\ (1\,4\,2)\}, \{(1\,3\,4),\ (1\,4\,3)\}, \{(2\,3\,4),\ (2\,4\,3)\}$$
$$orden\ 4:\ no\ hay\ subgrupos\ isomorfos\ a\ C_4\ pero\ hay\ subgrupos\ de\ tipo\ Klein$$
$$K = \{id,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\} \trianglelefteq A_4$$
$$orden\ 6:\ no\ tiene\ subgrupos\ de\ orden\ 6$$

Supongamos que $\exists N \leq A_4$ 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

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

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

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

Sea $\beta = (1\,2)(2\,4) \in A_4$, 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 $|N| = 7 \downarrow$.

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

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

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

$$\alpha(1\,2)(3\,4)\alpha^{-1} = \alpha(1\,2)\alpha^{-1}\alpha(3\,4)\alpha^{-1} = (2\,3)(1\,4) = (1\,4)(2\,3) \notin C_2$$
$$\alpha C_2 \alpha^{-1} \not\leq C_2 \Rightarrow C_2 \not\trianglelefteq A_4$$
$$\left.\begin{array}{c} C_2 \leq K \\ K\ es\ abeliano \end{array}\right\} entonces\ C_2 \trianglelefteq K$$

3.1. Grupo Cociente

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

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

Definimos en G/N la siguiente operación binaria

$$G/N \times G/N \longrightarrow G/N$$
$$(aN,\, bN) \longmapsto (aN)(bN) := abN$$

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

$$\left.\begin{array}{c} aN = a_1N \\ bN = b_1N \end{array}\right\} \overset{?}{\Rightarrow} abN = a_1b_1N$$
$$aN = a_1N \Leftrightarrow a_1^{-1}a \in N \Leftrightarrow \exists n \in N \; tal \; que \; a_1^{-1}a = n \Rightarrow a = a_1n$$
$$bN = b_1N \Leftrightarrow \exists m \in N \; tal \; que \; b = b_1m$$

Entonces $ab = a_1nb_1m$. Como $nb_1 \in Nb_1 \overset{N \trianglelefteq G}{=} b_1N \Rightarrow \exists n' \in N \; tal \; que \; nb_1 = b_1n'$

Entonces $ab = a_1nb_1m = a_1b_1n'm \overset{n'm \in N}{\Rightarrow} (a_1b_1)^{-1}(ab) \in N \Rightarrow abN = a_1b_1N$.

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 grupo cociente de G por N.

Se tiene un epimorfismo de grupo

$$p : G \longrightarrow G/N \qquad p(a) := aN$$

que llamaremos la proyección canónica.

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

(1) Existe un único homomorfismo

$$\overline{f} : G/N \to G'$$

tal que $\overline{f} \cdot p = f$ (p proyección canónica).

(2) $\overline{f}$ es epimorfismo $\Leftrightarrow$ f es epimorfismo.

(3) $\overline{f}$ es monomorfismo $\Leftrightarrow$ $N = Ker(f)$

$\overline{f}$ se llama el homomorfismo inducido por f en el grupo cociente G/N

Demostración: $f : G \to G'$, $N \trianglelefteq G$ tal que $N \leq Ker(f) \quad G/N = \{aN/a \in G\}$

(1) Definimos

$$\overline{f} : G/N \to G' \quad por \quad \overline{f}(aN) := f(a)$$

Veamos que $\overline{f}$ está bien definido. Si

$$\left.\begin{array}{l} aN = bN \Leftrightarrow b^{-1}a \in N \overset{N \leq Ker(f)}{\Rightarrow} b^{-1}a \in Ker(f) \\ \Rightarrow \quad f(b^{-1}a) = 1 = f(b)^{-1}f(a) \end{array}\right\} \Rightarrow f(a) = f(b)$$

Es fácil ver que $\overline{f}$ es un homomorfismo así como que $\overline{f} \circ p = f$. Supongamos que $g : G/N \to G'$ es un homomorfismo tal que $g \circ p = f$. Sea $aN \in G/N$, entonces $g(aN) = g(p(a)) = (g \circ p)(a) = f(a) = \overline{f}(aN)$

(2) Puesto que $Im(\overline{f}) = Im(f)$

$$\left.\begin{array}{l} \overline{f} : G/N \to G' \\ \overline{f}(aN) = f(a) \end{array}\right\}$$

entonces $\overline{f}$ es epimorfismo $\Leftrightarrow Im\overline{f} = G' \Leftrightarrow Imf = G' \Leftrightarrow f$ es epimorfismo.

(3) $\overline{f}$ es monomorfismo $\Leftrightarrow N = Ker(f)$

$\Rightarrow$) Tenemos que ver que $Ker(f) \leq N$. Sea $a \in Ker(f) \Rightarrow f(a) = 1$. Como $\overline{f}(aN) = f(a) = 1 \Rightarrow aN \in Ker(\overline{f}) \overset{\overline{f}\ monomorfismo}{=} \{N\} \Rightarrow aN = N \Rightarrow a \in N$

$\Leftarrow$) Si $N = Ker(f)$ $\overline{f} : G/N \to G'$. Sea $aN \in G/N$ tal que $\overline{f}(aN) = f(a) = 1$, entonces $a \in Ker(f) = N \Rightarrow aN = N$

Así pues $Ker\overline{f} = \{N\}$ y $\overline{f}$ es monomorfismo.

□

Corolario: ($1^{\underline{o}}$ Teorema de Isomorfía)
Sea $f : G \to G'$ un homomorfismo de grupos. Entonces f induce en isomorfismo

$$G/Ker(f) \overset{\sim}{=} Imf \qquad aKer(\overline{f}) \mapsto f(a)$$

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

$$\left.\begin{array}{c} \overline{f} : G/Ker(f) \to Imf \qquad \overline{f}(a\,Ker(f)) = f(a) \\ \overline{f}\ es\ epimorfismo\ por\ (2) \\ Como\ N = Ker(f),\ \overline{f}\ es\ monomorfismo\ por\ (3) \end{array}\right\} \overline{f}\ es\ isomorfismo$$

□

Ejercicio 12 (Relación 3): G y H finitos y $mcd(|G|, |H|) = 1$. Probar que si $f : G \to H$ es un homomorfismo, entonces $f(a) = 1 \quad \forall a \in G$.

Resolución:

$$G/Ker(f) \cong Img(f) \qquad |G/Ker(f)| = |Img(f)| \Rightarrow |G| = |Ker(f)||Imf|$$

$$\left.\begin{array}{c} En\ particular\ |Imf|\ es\ un\ divisor\ de\ |G| \\ Imf \leq H \Rightarrow |Imf|\ es\ un\ divisor\ de\ |H| \end{array}\right\} = mdc(|G|, |H|) = 1$$

$$|Imf| = 1 \Rightarrow Imf = \{1\} \Rightarrow f(a) = 1 \forall a \in G$$

Corolario: Si $f : G \to G'$ es un homomorfismo y G y G' son finitos, entonces $|G| = |Imf||Nucf|$

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

(1) Si $H \in Sub(G)$ tal que $N \leq H$ entonces $N \trianglelefteq H$ y $H/N \in Sub(G/N)$.

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

(3) Sea $L \in Sub(G/N)$. Entonces $\exists! H \in Sub(G)$ tal que $N \trianglelefteq H$ y $L = H/N$

Demostración:

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

(2) $\Leftarrow$) Es obvio

$\Rightarrow$) $H_1,\ H_2 \leq G$ tal que $N \trianglelefteq H_i \quad i = 1, 2$ tal que $H_1/N = H_2/N$.

Sea $a \in H_1 \Rightarrow aN \in H_1/N = H_2/N \Rightarrow \exists t \in H_2$ tal que $aN = tN \Leftrightarrow\ t^{-1}a \in\ N \leq\ H_2$

$$\left.\begin{array}{c} t^{-1}a \in H_2 \\ t \in H_2 \end{array}\right\} a = t(t^{-1}a) \in H_2$$

Tenemos que $H_1 \leq H_2$. De la misma forma obtenemos que $H_2 \leq H_1 \Rightarrow\ H_2 =\ H_1$

(3) $L \leq G/N$. Consideramos la proyección canónica $p : G \to G/N \quad p(a) = aN$. $L \leq G/N$ entonces $p^*(L) \leq G$. Sea

$$H = p^*(L) = \{a \in G/p(a) \in L\} = \{a \in G/aN \in L\} \leq G$$

Sea $a \in N \Rightarrow p(a) = aN = N \overset{L \leq G/N}{\in} L \Rightarrow a \in H$. Por tanto $N \leq H$. Veamos que $L = H/N$. Es claro que $H/N \leq L$. Recíprocamente, si $aN \in\ L \Rightarrow a \in H \Rightarrow aN \in H$, es decir, $L \leq H/N$. La unicidad es consecuencia de (2).

Teorema (2^{o} Teorema de Isomorfía o Teorema del Doble Cociente): Sea G un grupo y $N \trianglelefteq G$ y sea $H \in Sub(G)$ tal que $N \leq H$. Entonces,

$$H/N \trianglelefteq G/N \Leftrightarrow H \trianglelefteq G$$

Además en tal caso

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

19-4-21

Demsotración: $N \trianglelefteq G$ y $H \leq G$ con $N \trianglelefteq H \Leftrightarrow H \trianglelefteq G$ y tenemos que ver que $H/N \trianglelefteq G/N$.

Sea $aN \in H/N$ y $xN \in G/N$, es decir, $a \in H$

$$(xN)(aN)(xN)^{-1} = (xax^{-1})N \in H/N$$

Como $\left.\begin{array}{l} a \in H \\ x \in G \\ H \trianglelefteq G \end{array}\right\} \Rightarrow xHx^{-1} \leq H$, y por tanto $xax^{-1} \in H$

Es decir, $(xN)(H/N)^{-1} \leq H/N, \quad \forall xN \in G/N\big\} \Rightarrow H/N \trianglelefteq G/N$

$\Rightarrow$) Suponemos ahora que $H/N \trianglelefteq G/N$

$$G \xrightarrow{p} G/N \xrightarrow{q} (G/N)(H/N)$$
$$Sea \quad f = q \circ p : G \longrightarrow (G/N)/(H/N)$$

, y p y q proyecciones canónicas, con $f(a) = (aN)H/N$, entonces f es un epimorfismo por ser composición de epimorfismos.

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

Veamos que $H = Ker(f)$ por doble inclusión.

Es claro que $H \leq Ker(f)$.

Sea $a \in Ker(f)$ entonces $aN \in H/N \Rightarrow \exists b \in H$ tal que $aN = bN \Rightarrow$

$$\Rightarrow \left.\begin{array}{c} b^{-1}a \in N \leq H \\ b \in H \end{array}\right\} \Rightarrow a = b(b^{-1}a) \in H$$

, por tanto $Ker(f) \leq H$. Consecuentemente, $H = Ker(f) \Rightarrow H \trianglelefteq G$. Además, aplicando el primer teorema de isomorfía a f,

$$G/Ker(f) \cong Im(f)$$

,es decir,

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

pues f es epimorfismo.

□

Teorema:(3 Teorema de Isomorfía)
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 $K/(K \cap N) \cong KN/N$

Demostración:
(1) Para demostrar que $KN \leq G$ 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 $N \leq KN$ ($x \in N$, $x = 1x \in KN$) y $N \trianglelefteq G$, entonces $N \trianglelefteq KN$.

Veamos (2) y (3). Consideramos los siguientes homomorfismos.

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

y sea

$$g = p \circ i : K \longrightarrow G/N$$
$$g(a) = aN \qquad \forall a \in K$$
$$Ker(g) = \{a \in K / g(a) = N\} = \{a \in K / aN = N\} = \{a \in K / a \in N\} = K \cap N$$

y entonces $K \cap N \trianglelefteq K$ y tenemos (2).

Además por el primer teorema de isomorfía aplicado a g,

$$K/K \cap N \cong Im(g)$$
$$Im(g) = \{g(a)/a \in K\} = \{aN/a \in K\} \overset{?}{=} KN/N$$

Puesto que $K \leq N$, es claro que $Im(g) \leq KN/N$. 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

$$xN = (ab)/N = (aN)(bN) \overset{b \in N}{=} (aN)N = aN \in Im(g), \; pues \; a \in K$$
$$K/K \cap N \cong KN/N \Rightarrow$$
$$\Rightarrow Im(g) = \{g(a)/a \in K\} = \{aN/a \in K\} = KN/N$$

Ejercicio 14 (Relación 3): G grupo, $N \trianglelefteq G$ tal que N y G/N son abelianos y $H \leq G$. Demostrar que existe $K \trianglelefteq H$ tal que K y H/K son abelianos.

$$G, \quad H, \, N \in Sub(G), \; N \trianglelefteq G$$
$$N \cap H \trianglelefteq H \quad y \quad NH/N \cong H/N \cap H \; (3\,T\,isomorfia)$$

Tomamos $K = N \cap H \trianglelefteq H$, como $K \leq N$ y N es abeliano $\Rightarrow K$ abeliano. Por otro lado $H/K = H/N \cap H \cong HN/N \leq G/H$. Como G/N es abeliano $\Rightarrow$ HN/N es abeliano $\Rightarrow H/K$ es abeliano.

□

Ejercicio 15 (Relación 3): G un grupo finito, K, $N \in Sub(G)$ con $N \trianglelefteq G$. Suponemos que $|K|$ y $[G : N]$ son primos relativos. Demostrad que $K \leq N$.

Resolución: Sabemos que

$$K/K \cap N \cong KN/N \ (3\,T\,isomorfia)$$

entonces $[K : NK] = [KN : N] = r$. Como

$$KN/N \leq G/N \Rightarrow r = |KN/N| \mid |G/N| = [G : N]$$

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 que

$$|K/K \cap N| = 1 \Rightarrow K = K \cap N$$

con lo que $K \leq N$, lo que queríamos demostrar.
20-4-21

Definición: Sea G un grupo. Se define el centro de G como

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

$Z(G) \trianglelefteq G$ (Ejercicio 6, Relación 3).
G es abeliano $\Leftrightarrow Z(G) = G$

Ejercicio 8 (Relación 3): 2) Demostrar que $Z(A_3) = A_3$ y que $Z(A_n) = \{id\} \quad \forall n \geq 4$

$$A_3 = \{id, (1\,2\,3), (1\,3\,2)\} = \langle (1\,2\,3) \rangle \quad es \quad abeliano$$

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 $\exists i \in \{1, 2 \ldots, n\}$ tal que $\sigma(i) = j$ siendo $j \neq i$. Elegimos $k, l \in \{1, 2, \ldots, n\}$ tal que $k \neq l$ y $\{k, l\} \cap \{i, j\} = \emptyset$ (podemos elegirlos porque $n \geq 4$).

Sea $\alpha = (j\,k\,l) \in A_n$

$$\left.\begin{array}{l} \sigma\alpha(i) = \sigma(i) = j \\ \alpha\sigma(i) = \alpha(j) = k \end{array}\right\} \Rightarrow \sigma\alpha(i) \neq \alpha\sigma(i) \Rightarrow \sigma\alpha \neq \alpha\sigma \Rightarrow \sigma \notin Z(A_n)$$

Consecuentemente $Z(A_n) = \{id\}$

1) $Z(S_2) = S_2 \quad y \quad Z(S_n) = \{id\}$ para $n \geq 3$

Ejercicio 9 (Relación 3): Demostrar que $Z(D_n) = \{1,\, r^m\}$ si $n = 2m$, y $Z(D_n) = \{1\}$ si $m = 2m + 1$

a) $n = 2m \quad D_n = \langle r, s / r^n = 1 = s^2, \quad sr = r^{-1}s \rangle = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$
Observamos primero que $r^k s \notin Z(D_n) \quad \forall k = 0, \ldots, n-1$

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

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

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

¿Cuándo $r^k \in Z(D_n)$?
Obviamente $r^k r^j = r^j r^k \quad \forall j = 0, \ldots, n-1$, por tanto decir que $r^k \in Z(D_n)$, es decir

$$r^k(r^j s) = (r^j s)r^k \quad \forall j = 0, \ldots, n-1$$

$$r^{k+j}s = r^j r^{-k} s = r^{j-k}s \Leftrightarrow r^{k+j} = r^{j-k} \quad \forall j \Leftrightarrow r^k = r^{-k} \Leftrightarrow$$

$$\Leftrightarrow (r^k)^2 = 1 \Rightarrow ord(r^k) = 2$$

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

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

$$como \quad n = 2m \Rightarrow 2m = 2mcd(2m,k) \Rightarrow m = mcd(2m,k) \Rightarrow k = m$$

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

Ejercicios 16-20: Se refieren al grupo de automorfismos de un grupo.

Definición: Sea G un grupo. Un automorfismo de G es un isomorfismo

$$f : G \longrightarrow G$$

$$Aut(G) = \{f : G \longrightarrow G / f\ es\ automorfismo\}$$

$Aut(G)$ con la composición es un grupo.

Ejercicio 18 (Relacion 3): Sea $n \geq 2$ y $C_n = \langle x / x^n = 1 \rangle = \{1, x, \ldots, x^{n-1}\}$.
Sea G un grupo arbitrario. Demostrar que

(1) Si $\theta : C_n \longrightarrow G$ es un homomorfismo de grupos con $\theta(x) = g \quad (g \in G)$, entonces

$$ord(g) \mid n \quad y \quad \theta \in (x^k) = g^k \quad \forall k = 0, \ldots, n-1$$

Puesto que θ es un homomorfismo,

$$\theta(1) = 1 = \theta(x^n) = \theta(x)^n = g^n$$

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 que lo denota por

$$\theta_g : C_n \longrightarrow G \quad tal\ que \quad \theta_g(x) = g$$

Definimos $\theta_g : C_n \longrightarrow G$ por $\theta_g(x^k) := g^k \quad k = 0, \ldots, n-1$. Veamos que θ_g es un homomorfismo.

x^k, $x^r \in C_n$ hemos de ver que $\theta_g(x^k \cdot x^r) = \theta_g(x^k) \cdot \theta_g(x^r)$

$$\theta_g(x^k \cdot x^r) = \theta(x^{res(k+r;n)}) = g^{res(k+r;n)} = g^s = g^{res(s;t)}$$
$$res(k+r;n) = s$$

Sea $ord(g) = t$

$$\theta_g(x^k) \cdot \theta_g(x^r) = g^k \cdot g^r = g^{res(k+r;t)}$$
$$s = tq + h \quad h = res(s;t) \quad 0 \leq h \leq t-1$$
$$s = res(k+r;n) \quad entonces \quad k + r = nq' + s \quad 0 \leq s \leq n-1$$
$$\Rightarrow res(k+r;t) = h = res(s;t)$$

Entonces $\theta_g(x^k x^r) = \theta_g(x^k) \cdot \theta_g(x^r)$. La unicidad es consecuencia de (1).

(3) Sea $g \in G$ tal que $ord(g) \mid n$. Demostrar que

$$\theta_g : C_n \longrightarrow G \quad es\ monomorfismo \Leftrightarrow ord(g) = n$$
$$Como \quad \theta_g : C_n \longrightarrow G \quad \theta_g(x^k) = g^k \quad \forall k$$

$\Rightarrow$) Supongamos que θ_g es monomorfismo $\Rightarrow Ker(\theta_g) = \{1\}$.

Sea $t = ord(g)$ entonces $g^t = 1$. Entonces

$$1 = g^t = \theta_g(x^t) \Rightarrow x^t \in Ker(\theta_g) = \{1\} \Rightarrow x^t = 1 \overset{ord(x)=n}{\Rightarrow} n \mid t$$

como $t \mid n \Rightarrow n = t$

21-4-21

$\Leftarrow$) $ord(g) = n, \quad \theta_g : C_n \longrightarrow G, \quad \theta_g(x^k) = g^k$

Sea $x^k \in Ker(\theta_g) \Rightarrow \theta_g(x^k) = g^k = 1 \overset{ord(g)=n}{\Rightarrow} n \mid k$

(4) Demostrar que existe un isomorfismo

$$\mathcal{U}(\mathbb{Z}_n) \cong Aut(C_n)$$

dado por $r \longmapsto f_r : C_n \longrightarrow C_n, \quad f_r(x) = x^r$

En particular $Aut(C_n)$ es abeliano y tiene $\varphi(n)$ elementos (φ función de Euler)

$$\mathcal{U}(\mathbb{Z}_n) = \{r/1 \leq r \leq n-1 \quad y \quad mcd(n,r) = 1\}$$

Entonces para $r \in \mathcal{U}(\mathbb{Z}_n)$, x^r es un generador de C_n, pues $ord(x^r) = \frac{n}{mcd(n,r)} = n$.
Por (2) y (3) $f_r : C_n \longrightarrow C_n \quad f_r(x) = x^r$ ($f_r(x^k) = x^{kr}$), es un monomorfismo.

Como $Im(f_r) = \langle f_r(x) \rangle = \langle x^r \rangle = C_n$, entonces f_r es también epimorfismo, y por lo tanto es un isomorfismo.

Tenemos pues una aplicación

$$\begin{gathered} f : \mathcal{U}(\mathbb{Z}_n) \longrightarrow Aut(C_n) \\ r \longmapsto f_r \end{gathered}$$

f es un homomorfismo de grupos

$$\begin{gathered} f(rs) = f_{rs} : C_n \longrightarrow C_n \qquad f(r) \circ f(s) = f_r \circ f_s : C_n \longrightarrow C_n \\ f_r \circ f_s(x) = f_r(x) = x^{rs} = x^{res(r \cdot s;n)} = f_{res(r \cdot s;n)}(x) = f(rs) \end{gathered}$$

Por (1) y (2) es fácil ver que f es un isomorfismo.

Ejercicio 19 (Relación 3): Describir $Aut(C_8)$ y demostrar que es isomorfo al grupo de Klein.

$$\begin{gathered} Aut(C_8) \cong \mathcal{U}(\mathbb{Z}_8) = \{1,3,5,7\} \\ Aut(C_8) = \{f_1, f_3, f_5, f_7\} \\ f_k : C_5 \longrightarrow C_8 \quad f_k(x) = x^k \quad k = 1,3,5,7 \end{gathered}$$

Para $k = 1$, $f_1 = id$, f_3, f_5, f_7 tienen orden 2

$$(f_3^2)(x) = f_3(f_3(x)) = f_3(x^3) = (x^3)^3 = x^9 = x \Rightarrow f_3^2 = id \Rightarrow ord(f_3) = 2 = ord(f_5) = ord(f_7)$$

Ejercicio 20 (Relación 3): $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong$ al grupo de Klein. Trabajamos con el grupo de Klein de forma abstracta.

$$\begin{gathered} K = \{1, a_1, a_2, a_3\} \quad a_i^2 = 1 \quad i = 0,1,2,3 \\ a_i a_j = a_k \quad con \quad k \neq i, j \neq 1 \\ Aut(K) \cong S_3 \end{gathered}$$

Sea $\alpha \in S_3 \longrightarrow \begin{array}{c} f_\alpha : K \longrightarrow K \\ f_\alpha(1) = 1 \\ f_\alpha(a_i) = a_{\alpha(i)} \end{array}$ biyectiva.

f_α es un homomorfismo y entonces un autormorfismo.

$$S_3 \to Aut(K)$$
$$\alpha \longmapsto f_\alpha$$

f es un isomorfismo.

3.2. Producto Directo de Grupos:

Definición: Sea $G_1, G_2, \ldots, G_n$ $(n \geq 2)$ grupos. Definimos su producto directo como el grupo cuyos elementos son los del producto cartesiano

$$\prod_{i=1}^{n} G_i = G_1 \times \ldots \times G_n = \{(x_1, x_2, \ldots, x_n)/x_i \in G_i \quad \forall i = 1, 2, \ldots, n\}$$

y con operación definida como sigue

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$$

Es fácil ver que en efecto $\prod_{i=1}^{n} G_i$ es un grupo con uno la n-tupla $(1, 1, \ldots, 1)$ (donde cada uno es el de su correspondiente G_i), y donde

$$(x_1, \ldots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$$

Se tiene para cada $k = 1, \ldots, n$ homomorfismo

$$P_k : \prod_{i=1}^{n} G_i \longrightarrow G_k \qquad P_k(x_1, \ldots, x_n) = x_k$$

que se llama proyección k-ésima. También se tiene un homomorfismo

$$j_k : G_k \longrightarrow \prod_{i=1}^{n} G_i \qquad j_k(x_k) = (1, \ldots, x_k, \ldots, 1)$$

que se llama proyección k-ésima.

Es claro que las proyecciones son epimorfismos y las inyecciones son monomorfismos. Además se verifica

- $G_k = Im(P_k) \qquad \forall k = 1, \ldots, n$
- $Im(j_k) \trianglelefteq \prod_{i=1}^{n} G_i \qquad \forall k = 1, \ldots, n$
  Así, G_k es isomorfo a un subgrupo normal del producto directo.
- Sea dado $H_k \in Sub(G_k)$ para cada $k = 1, \ldots, n$, entonces $\prod k = 1^n H_k$ es un subgrupo de $\prod_{k=1}^{n} G_k$

Proposición: Sean $G_1, G_2, \ldots, G_n$ grupos finitos, entonces

(1) $\prod_{i=1}^{n} G_i$ es también finito y

$$|\prod_{i=1}^{n} G_i| = \prod_{i=1}^{n} |G_i|$$

(2) Sea $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} G_i$, entonces

$$ord((x_1, x_2, \ldots, x_n)) = mcm(ord(x_1), ord(x_2), \ldots, ord(x_n))$$

Supongamos que $mcd(|G_i|, |G_j|) = 1 \quad \forall i \neq j$

(3) Si cada G_i es cíclico entonces $\prod_{i=1}^{n} G_i$ es cíclico.

(4) Si $L \leq \prod_{i=1}^{n} G_i$ entonces existe $H_1 \leq G_1, H_2 \leq G_2, \ldots, H_n \leq G_n$ tal que

$$L = \prod_{i=1}^{n} H_i$$

Demostración: (2) $(x_1, x_2, \ldots, x_k) \in \prod_{i=1}^{k} G_i$ y sea $t_i = ord(x_i), i = 1, \ldots, n$.
Sea $t = mcm(t_1, t_2, \ldots, t_n)$

$$(x_1, x_2, \ldots, x_n)^t = (x_1^t, x_2^t, \ldots, x_n^t) \underset{t_i \mid t \quad \forall i}{\overset{ord(x_i) = t_i}{=}} (1, 1, \ldots, 1)$$

Supongamos $m \geq 1$ tal que

$$\left.\begin{array}{c}(x_1, x_2, \ldots, x_n)^m = (1, 1, \ldots, 1) \\ (x_1^m, x_2^m, \ldots, x_n^m)\end{array}\right\} \Rightarrow x_i^m = 1 \quad \forall i = 1, \ldots, n$$

como $ord(x_i) = t_i \Rightarrow t_i \mid m \quad \forall i = 1, \ldots, n$ y como $t = mcm(t_1, \ldots, t_n) \Rightarrow t \mid m$
Luego $ord(x_1, x_2, \ldots, x_n) = mcm(ord(x_1), \ldots, ord(x_n))$

(3) $mcd(|G_i|, |G_j|) = 1 \quad \forall i \neq j$. Supongamos que $G_i = \langle a_i \rangle \quad i = 1, \ldots, n$, y consideramos el elemento $a = (a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i$
Por (2)

$$\begin{aligned} ord(a) &= mcm(ord(a_1), \ldots, ord(a_n)) = \\ &= mcm(|G_1|, \ldots, |G_n|) = |G_1||G_2| \ldots |G_n| \end{aligned}$$

Entonces $\langle a \rangle = \prod_{i=1}^{n} G_i$ y entonces es cíclico.

(4) $mcd(|G_i|, |G_j|) = 1 \quad \forall i \neq j$. Hacemos inducción en n.
Caso $n = 2$. $L \leq G_1 \times G_2$, queremos buscar $H_1 \leq G_1$ y $H_2 \leq G_2$ tal que $L = H_1 \times H_2$. Consideramos

$$\begin{aligned} p_1 : G_1 \times G_2 &\longrightarrow, \qquad (x_1, x_2) \longmapsto x_1 \\ p_2 : G_1 \times G_2 &\longrightarrow, \qquad (x_1, x_2) \longmapsto x_2 \end{aligned}$$

Sea $H_1 = (P_1)_*(L) \leq G_1 \qquad H_2 = (P_2)_*(L) \leq G_2$.

Si $(x_1, x_2) \in L \Rightarrow \left\{ \begin{array}{l} P_1(x_1, x_2) = x_1 \in (P_1)_*(L) = H_1 \\ P_2(x_1, x_2) = x_2 \in (P_2)_*(L) = H_2 \end{array} \right\} \Rightarrow (x_1, x_2) \in H_1 \times H_2$

Por tanto, $L \leq H_1 \times H_2$

Recíprocamente, $r = |G_1|, \quad s = |G_2| \quad mcd(r, s) = 1$, 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 $(x_1, y_2) \in L$

$$(x_1, y_2) \in L \Rightarrow (x_1, y_2)^{bs} \in L$$

$$(x_1, y_2)^{bs} = (x_1^{bs}, y_2^{bs}) = (x_1^{bs}, 1) = (x_1^{1-ar}, 1) = (x_1^1 \cdot x_1^{-ar}, 1) = (x_1, 1)$$

$$y_2 \in G_2 \Rightarrow ord(y_2) \mid |G_2| = s \qquad x_1 \in G_i \Rightarrow ord(x_1) \mid |G_1| = r$$

Así si $x_1 \in H_1$ entonces $(x_1, 1) \in L$. Análogamente, si $x_2 \in H_2 \Rightarrow (1, x_2) \in L$.

Sea $(x_1, x_2) \in H_1 \times H_2 \Rightarrow x_1 \in H_1 \quad y \quad x_2 \in H_2$

$$\Rightarrow (x_1, 1), (1, x_2) \in L \Rightarrow (x_1, 1)(1, x_2) = (x_1, x_2) \in L$$

Así $L = H_1 \times H_2$.

Sea n¿2, y el resultado cierto para n-1. Sea

$$L \leq \prod_{i=1}^{n} G_i = \prod_{i=1}^{n-1} G_i \times G_n$$

como $mcd(|\prod_{i=1}^{n} G_i|, |G_n|) = 1$, por el caso $n = 2$

$$\exists K \leq \prod_{i=1}^{n} G_i \quad y \quad \exists H_n \leq G_n \quad tal\ que \quad L = K \times H_n$$

Por hipótesis de inducción si $K \leq \prod_{i=1}^{n-1} G_i, \quad \exists H_1 \leq G_i, \quad i = 1, \ldots, n-1$ tal que

$$K = \prod_{i=1}^{n-1} H_i$$

, combinando, obtenemos que $L = H_1 \times \ldots \times H_n$.

Corolario: Sean $n, m \geq 1$

$$C_n \times C_m \cong C_{nm} \Leftrightarrow mcd(n, m) = 1$$

Supongamos un grupo G y $H_1, H_2, \ldots, H_n \in Sub(G)$. Consideramos $H_1 \times H_2 \times \ldots \times H_n$. Tenemos una aplicación

$$\phi : H_1 \times H_2 \times \ldots \times H_n \longrightarrow G$$
$$\phi(x_1, x_2, \ldots, x_n) := x_1 x_2 \ldots x_n \in G$$

Se verifica

Proposición:

$$\phi \, es \, un \, isomorfismo \Leftrightarrow \left\{ \begin{array}{c} (a)\, H_i \trianglelefteq G \quad \forall i = 1, \ldots, n \\ (b)\, H_1 H_2 \ldots H_n = G \\ (c)\, (H_1 \ldots H_{i-1}) \cap H_i = \{1\} \quad \forall i = 2, \ldots, n \end{array} \right.$$

$$\left(n = 2 \quad \phi \, es \, isomorfismo \Leftrightarrow \left\{ \begin{array}{c} (a)\, H_1 \trianglelefteq G \quad H_2 \trianglelefteq G \\ (b)\, H_1 H_2 = G \\ (c)\, (H_1) \cap H_2 = \{1\} \end{array} \right. \right)$$

En estas condiciones se dice que el grupo es producto interno de los subgrupos $H_1, H_2, \ldots, H_n$.

Demostración: $\Rightarrow$) $\phi : H_1 \times \ldots \times H_n \longrightarrow G \qquad \phi(x_1 \ldots x_n) = x_1 \ldots x_n$ es isomorfismo. En particular es epimorfismo y entonces

$$Im(\phi) = H_1 H_2 \ldots H_n = G \quad y \, se \, tiene \, (b)$$

Ejercicio: Sea $f : G \longrightarrow G'$ un homomorfismo d grupo y $N \trianglelefteq G$. Demostrad que $f_*(N) \trianglelefteq Im(f)$.

Entonces como para cada $k = 1, \ldots, n$

$$Im(j_k) \trianglelefteq \prod_{i=1}^{n} H_i \Rightarrow \phi_*(Im(j_k)) = H_k \trianglelefteq Im(\phi) = G$$

$j_k : H_k \longrightarrow \prod_{i=1}^{n} H_i$ la k-ésima inyección canónica. Por tanto se tiene (a).

26-4-21

Veamos (c). Sea $x \in (H_1 \ldots H_{i-1}) \cap H_i \quad 2 \leq i \leq n-1$.
Como $x \in H_1 H_2 \ldots H_{i-1}$, existirán $h_1 \in H_1, \ldots, h_{i-1} \in H_{i-1}$ tal que $x = h_1 \ldots h_{i-1}$.
Entonces $x = \phi((h_1, h_2, \ldots, h_{i-1}, 1, \ldots, 1))$

Como $x \in H_i$, podemos considerar el elemento

$$(1, 1, \ldots, 1, x, 1, \ldots, 1) \in H_1 \times H_2 \times \ldots \times H_n \quad y$$
$$\phi((1, 1, \ldots, 1, x, 1, \ldots, 1)) = x$$

Entonces como ϕ es monomorfismo, tendremos que

$$(h_1, h_2, \ldots, h_{i-1}, 1, \ldots, 1) = (1, 1, \ldots, 1, \overbrace{x}^{i-esima \, posicion}, 1 \ldots, 1)$$
$$\Rightarrow h_i = 1 \quad \forall i \quad y \quad x = 1$$

Tenemos entonces que $(H_1 \dots H_{i-1}) \cap H_i = \{1\} \quad 2 \leq i \leq n$

$\Leftarrow$) Supongamos que se verifican (a), (b) y (c). Queremos demostrar que

$$\phi : H_1 \times \ldots \times H_n \longrightarrow G \qquad \phi(h_1, h_2, \ldots, h_n) = h_1 h_2 \ldots h_n$$

es isomorfismo.

Primero veamos que $\forall i \neq j$, los elementos de H_i conmutan con los elementos de H_j.

Supongamos que $i < j$ y sea $h_i \in H_i$, $h_j \in H_j$. Consideramos el elementos $a = h_i h_j h_i^{-1} h_j^{-1}$

Como $H_i \trianglelefteq G$ entonces $\left.\begin{array}{c} h_j h_i^{-1} h_j^{-1} \in H_i \\ h_i \in H_i \end{array}\right\} \Rightarrow a \in H_i$

Como $H_j \trianglelefteq G$ entonces $\left.\begin{array}{c} h_i h_j h_i^{-1} \in H_j \\ h_j^{-1} \in H_j \end{array}\right\} \Rightarrow a \in H_j$

Por tanto $a \in H_i \cap H_j$. Si $i < j \Rightarrow H_i \leq H_1 H_2 \dots H_{j-1}\} \Rightarrow a \in H_1 H_2 \dots H_{j-1} \cap H_j$

(Ejercicio: Sean $H, K \in Sub(G)$ $\begin{array}{c} H \subseteq HK \\ K \subseteq HK \end{array}$)

Entonces utilizando (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

$$\begin{array}{c} \phi((h_1, h_2, \ldots, h_n)(k_1, k_2, \ldots, k_n)) = \phi((h_1 k_1, h_2 k_2, \ldots, h_n k_n)) = \\ = h_1 k_1 h_2 k_2 \ldots h_n k_n = h_1 h_2 k_1 k_2 h_3 k_3 \ldots h_n k_n = h_1 h_2 h_3 k_1 k_2 k_3 \ldots h_n k_n = \\ = h_1 h_2 \ldots h_n k_1 k_2 \ldots k_n = \phi((h_1, h_2, \ldots, h_n)) \cdot \phi((k_1, k_2, \ldots, k_n)) \end{array}$$

Por definición de ϕ

$$Im(\phi) = H_1 H_2 \ldots H_n \overset{(b)}{=} G \Rightarrow \phi \quad es\, epimorfismo$$

Sea $(h_1, h_2, \ldots, h_n) \in Ker(\phi) \Rightarrow \phi((h_1, \ldots, h_n)) \Rightarrow 1$, es decir,

$$h_1 h_2 \ldots h_n = 1 \Rightarrow h_1 h_2 \ldots h_{n-1} = h_n^{-1} \in (H_1 \ldots H_{n-1}) \cap H_n$$

que por (c) $\Rightarrow h_n = 1$ y $h_1 h_2 \ldots h_{n-1} = 1 \Rightarrow h_1 h_2 \ldots h_{n-2} = h_{n-1}^{-1} \in (H_1 \ldots H_{n-2}) \cap H_{n-1}$, que por (c) $\Rightarrow h_{n-1} = 1$ y $h_1 h_2 \ldots h_{n-2} = 1$.

En definitiva, en un número finito de pasos, llegamos a que

$$h_1 = h_2 = \ldots = h_n = 1, \quad es\, decir, \quad (h_1, h_2, \ldots, h_n) = (1, 1, \ldots, 1)$$

y ϕ es monomorfismo.

Ejercicios 21-32: Ejercicios de producto directo.

Ejercicio 21 (Relación 3): S_3, C_{p^n} (con p primo) y $\mathbb{Z}$ no son producto directo internos de subgrupos propios

$$S_3 \overset{subgrupos\ propios}{\longrightarrow} A_3 \trianglelefteq S_3,\ \langle(1\,2)\rangle \not\trianglelefteq S_3,\ \langle(1\,3)\rangle \not\trianglelefteq S_3,\ \langle(2\,3)\rangle \not\trianglelefteq S_3$$

Luego no existe subgrupos tal que $S_3 = K \cdot G$ con $K, G \in Sub(S_3)$ y $K \trianglelefteq S_3$ y $G \trianglelefteq S_3$.

$C_p \leq C_{p^2} \leq \ldots \leq C_{p^{n-1}}$ $\quad (H \leq K \Rightarrow HK = K)$. Nunca dará C_{p^n}, pues usaríamos un subgrupo impropio.

$\mathbb{Z} \longrightarrow$ si $\{0\} \neq H \leq \mathbb{Z}$, entonces $\exists n > 1$ tal que $H = n\mathbb{Z}$. En efecto sea $n = min\{x > 0 / x \in H\} \neq \emptyset$. Como $H \leq \mathbb{Z}$, $n > 1$ (pues si $n = 1$, entonces $H = \mathbb{Z}$).
Veamos que $H = n\mathbb{Z}$. Puesto que $n \in H \Rightarrow n\mathbb{Z} \leq H$.

Recíprocamente, sea $x \in H$, dividimos x entre n,

$$\left.\begin{array}{c} x = nq + r \qquad 0 \leq r < n \\ r = x - nq \in H \\ 0 \leq r < n \end{array}\right\} \Rightarrow r = 0$$

con lo que $x = nq \in n\mathbb{Z}$

$$n\mathbb{Z},\ m\mathbb{Z} \quad n\mathbb{Z} + m\mathbb{Z} = mcd(n,m)\mathbb{Z}$$
$$n\mathbb{Z} + m\mathbb{Z} = mcm(n,m)\mathbb{Z}$$

27-4-21

4. Tema 5. Grupos Resolubles (Solubles)

Definición: Sea G un grupo. Una cadena de subgrupos de G en la forma

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

la llamaremos serie normal de G.

Cada H_i se llama término i-ésimo de la serie, con $i = 0, \ldots, n$.
Cada H_i/H_{i-1} se llama factor i-ésimo de la serie, con $i = 1, \ldots, n$
La serie se dice propia si $H_{i-1} \subsetneq H_i \quad \forall i = 1, \ldots, n$ (es decir, todas las inclusiones son propias). En tal caso, diremos que la serie tiene longitud n.

Dadas dos series,

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G \tag{1}$$
$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_{m-1} \trianglelefteq K_m = G \tag{2}$$

, diremos que la serie (2) es un refinamiento de la serie (1) si se verifica

(i) $n \leq m$

(ii) Para cada $j \in \{0, \ldots, n\}$ existe un $r \in \{0, \ldots, m\}$ tal que $H_j = K_r$ (es decir, todos los grupos de la serie (1) aparecen en la serie (2))

Si $n < m$, 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

$$\{id\} \trianglelefteq A_4 \trianglelefteq S_4$$
$$\{id\} \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4 \qquad K = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$
$$\{id\} \trianglelefteq C_2 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4 \qquad C_2 = \langle (1\,2)(3\,4) \rangle = \{id, (1\,2)(3\,4)\}$$

La tercera es un refinamiento propio de la primera y de la segunda.
La segunda es un refinamiento propio de la primera.
La primera tiene longitud 2, la segunda tiene longitud 3 y la tercera tiene longitud 4.

Notemos: que en una serie normal de un grupo G

$$\{1\} \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

H_{i-1} es normal en H_i, pero no tiene porque 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

$$\{0\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = \mathbb{Z}$$

Si $n = 1$, $\{0\} = H_0 \trianglelefteq H_1 = \mathbb{Z}$, consideramos $K = m\mathbb{Z}$, $m \geq 2$, entonces

$$\{0\} = H_0 \trianglelefteq K \trianglelefteq H_1 = \mathbb{Z}$$

es un refinamiento propio de la serie.

Si $n > 1$ entonces $H_1 \lneq \mathbb{Z}$, $H_1 \neq \{0\}$ entonces $H_1 = m\mathbb{Z}$ para $m \geq 2$
Consideramos $K = 2m\mathbb{Z}$, entonces

$$\{0\} = H_0 \lneq K \lneq H_1 \lneq H_2 \lneq \ldots \lneq H_n = \mathbb{Z}$$

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 o, 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 $\Leftrightarrow$ G es finito de orden número primo.

Demostración: $\Leftarrow$) $|G| = p$, p primo $\Rightarrow G \cong C_p = \langle x / x^p = 1 \rangle$.
Si $H \leq G \Rightarrow |H| \mid |G| = p \Rightarrow \left\{ \begin{array}{l} |H| = 1 \Rightarrow H = \{1\} \\ |H| = p \Rightarrow H = G \end{array} \right.$

$\Rightarrow$) 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 $\langle x \rangle$

$$\left. \begin{array}{c} \{1\} \neq \langle x \rangle \trianglelefteq G \\ G \quad simple \end{array} \right\} \Rightarrow G = \langle x \rangle$$

Supongamos $ord(x) = \infty$, en ese caso $G \cong \mathbb{Z}$, que no es simple. Por tanto, necesariamente $ord(x)$ es finito.

Supongamos $ord(x) = m$. Como $G = \langle x \rangle$ entonces

$$|G| = |\langle x \rangle| = ord(x) = m$$

y así G es un grupo finito.
Sea $n \in \mathbb{Z}$, $n \mid m$ $(n > 0)$ y consideramos el elemtnos $x^n \in \langle x \rangle = G$ y el subgrupo $\langle x^n \rangle$

$$\left. \begin{array}{c} \langle x^n \rangle \trianglelefteq G \\ G \quad es\ simple \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} \langle x^n \rangle = \{1\} \\ \langle x^n \rangle = G = \langle x \rangle \end{array} \right.$$

En el primer caso $ord(x^n) = 1 = \frac{m}{mcd(n,m)} = \frac{m}{n} \} \Rightarrow n = m$

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

$$\{1\} \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

una serie normal de G. Dicha serie es de composición $\Leftrightarrow H_i/H_{i-1}$ es simple $\forall i = 1, \ldots, n$

Demostración: $\Rightarrow$) Suponemos que la serie (1) es de composición. En particular es una serie propia y entonces $H_{i-1} \lneq H_i \quad \forall i = 1, \ldots, n \Rightarrow H_i/H_{i-1}$ es no trivial $\forall i = 1, \ldots, n$.

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 si $\exists i \in \{1, \ldots, n\}$ tal que H_i/H_{i-1} no es simple, estaríamos diciendo, que $\exists K \leq G$ tal que

$$H_{i-1} \lneq K \lneq H_i \qquad (H_{i-1}/H_{i-1} \neq K/H_{i-1} \lneq H_i/H_{i-1})$$

Pero entonces la serie

$$\{1\} = H_0 \lneq \ldots \lneq H_{n-1} \lneq K \lneq H_i \lneq \ldots \lneq H_n = G$$

es un refinamiento propio de la serie (1), en contradicción con que (1) es de composición.

28-4-21

$\Leftarrow$) $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G \qquad (1)$
Suponemos que H_i/H_{i-1} son simples $\forall i = 1, \ldots, n$

$$\forall i \quad H_i/H_{i-1} \neq 1 \Rightarrow H_{i-1} \trianglelefteq H_i \quad \forall i = 1, \ldots, n, \quad \textit{por ser simple}$$

Luego la series es normal propia.

Supongamos que

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_m = G \qquad (2)$$

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 $l \in \{0, \ldots, m\}$ tal que $K_l \neq H_i \quad \forall i \in \{0, 1, \ldots, n\}$.

Sea $t \in \{0, \ldots, m\}$ el mayor subíndice tal que K_t no aparece en (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, $\exists r \in \{0, \ldots, n\}$, tal que $K_{t+1} = H_r$. Entonces tenemos la siguiente situación

$$H_{r-1} \lneq K_t \lneq K_{t+1} = H_r \Rightarrow K_t/H_{r-1} \neq 1 \trianglelefteq H_r/H_{r-1}$$

en contra de la simplicidad de H_r/H_{r-1}. Consecuentemente, la serie (1) no admite refinamientos propios.

□

Ejemplo: $G = S_4 \qquad 1 \trianglelefteq A_4 \trianglelefteq S_4$

Sus factores son $A_4/1 = A_4$ y S_4/A_4, donde el primero no es simple, luego 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, $K/1 = K$, donde el últimono es simple, luego la serie no es de composición.

$$1 \trianglelefteq C_2 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4 \qquad C_2 = \langle (1\,2)(3\,4) \rangle = \{id, (1\,2)(3\,4)\}$$

$$\begin{aligned} |S_4/A_4| = 2 &\Rightarrow S_4/A_4 \cong C_2, \quad \textit{y entonces simple} \\ |A_4/K| = 3 &\Rightarrow A_4/K \cong C_3, \quad \textit{y entonces simple} \\ |K/C_2| = 2 &\Rightarrow K/C_2 \cong C_2, \quad \textit{y entonces simple} \\ |H/1| = H &\Rightarrow \cong C_2, \quad \textit{y entonces simple.} \end{aligned}$$

Consecuentement la serie es un serie de composición.

Teorema: Todo grupo finito tiene al menos 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 $1 \trianglelefteq G$ es un serie de composición de G.

Supongamos $|G| > 2$ y el resultado cierto para todo grupo de orden menor que $|G|$. Sea

$$\Delta = \{K \in Sub(G)/K \trianglelefteq G\}$$

$\Delta \neq \emptyset$. Δ es un conjunto finito, pues G lo es. Elegimos $K \in \Delta$ tal que $|K|$ sea el mayor de los órdenes de los elementos de Δ. Se tiene que G/K es un grupo simple.

En efecto, como $K \trianglelefteq G$, 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, $H \trianglelefteq G$, $H \in \Delta$ y $|K| < |H|$ pues $K \trianglelefteq H \downarrow$. Por la elección de K.

$$\begin{aligned} Si \quad H \neq K \Rightarrow H = G \Rightarrow L = G/K \\ Si \quad H = K \Rightarrow L = \{1\} \end{aligned}$$

es decir, G/K es simple.

Como $K \trianglelefteq G \Rightarrow |K| < |G|$ y por hipótesis de inducción, K tiene una serie de composición

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_r = K$$

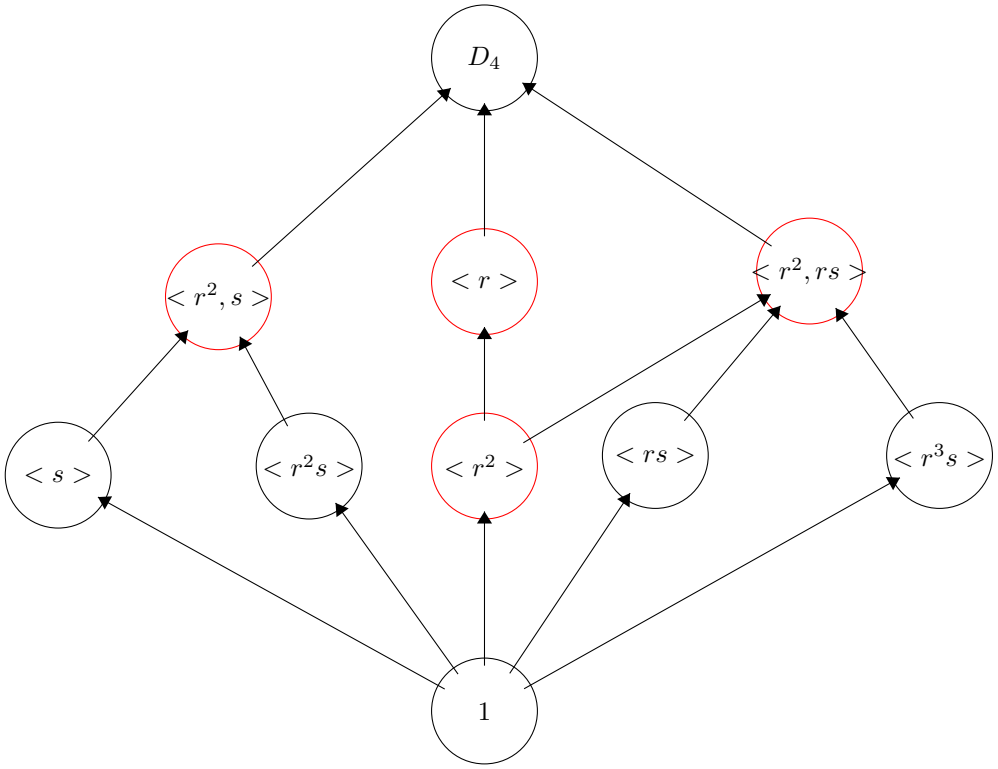
Entonces es claro que

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_r = K \trianglelefteq K_{r+1} = G$$

es una serie de composición de G.

□

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



(Los rodeados de rojo son subgrupos normales).

Subgrupos normales son

$$\langle r^2, s\rangle \quad \langle r\rangle \quad y \quad \langle r^2, rs\rangle$$

pues son de índice dos en D_4

$$Z(D_4) = \{1, r^2\} = \langle r^2\rangle$$

y entonces $\langle r^2\rangle \trianglelefteq D_4$. El resto de subgrupos de orden 2 de D_4 no son normales en D_4.

$$\langle s\rangle = \{1, s\} \qquad r \in D_4$$
$$rsr^{-1} = rsr^3 = rr^{-3}s = r^{-2}s = r^2s \notin \langle s\rangle$$

Por tanto

$$r\langle s\rangle r^{-1} \not\leq \langle s\rangle \Rightarrow \langle s\rangle \not\trianglelefteq D_4$$

De igual forma para los otros tres.

1. $1 \subsetneq \langle s\rangle \subsetneq \langle r^2, s\rangle \subsetneq D_4$
2. $1 \subsetneq \langle r^2\rangle \subsetneq \langle r^2, s\rangle \subsetneq D_4$
3. $1 \subsetneq \langle r^2 s\rangle \subsetneq \langle r^2, s\rangle \subsetneq D_4$
4. $1 \subsetneq \langle r^2\rangle \subsetneq \langle r\rangle \subsetneq D_4$
5. $1 \subsetneq \langle r^2\rangle \subsetneq \langle r^2, rs\rangle \subsetneq D_4$
6. $1 \subsetneq \langle rs\rangle \subsetneq \langle r^2, rs\rangle \subsetneq D_4$
7. $1 \subsetneq \langle r^3 s\rangle \subsetneq \langle r^2, rs\rangle \subsetneq D_4$

Son 7 seeries de composición distintas de D_4, las cuales comparten longitud y factores, salvo isomorfismo.

Factores de la primera serie son:

$$D_4/\langle r^2, s\rangle \cong C_2, \quad \langle r^2, s\rangle / \langle s\rangle \cong C_2, \quad \langle s\rangle /1 = \langle s\rangle \cong C_2$$

De forma análoga se observa que los factores del resto de las series son también, salvo isomorfismo, C_2, C_2, C_2.

Definición: Sea G un grupo y

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G \qquad 1 = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_m = G$$

dos series normales de G. Diremos que son equivalentes ó isomorfismo si

(i) $n = m$

(ii) $\exists \sigma \in S_n$ tal que $H_i/H_{i-1} \cong K_{\sigma(i)}/K_{\sigma(i)-1} \qquad \forall i = 1, \ldots, n$

4.1. Teorema de Jordan-Holder. Teorema de Refinamiento de Shreier.

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 (Teoreama 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 (del T$^{\underline{a}}$ de Jordan-Holder):
Sea

$$1 = G_0 \subsetneq G_1 \subsetneq \ldots \subsetneq G_n = G$$

una serie de composición de G.

a) Sea

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_r = G$$

una serie normal de G. Por el T$^{\underline{a}}$ 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

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_r = G \tag{1}$$

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 T$^{\underline{a}}$ 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) $G = S_2$

$1 \subsetneq S_2$ es un serie de composición de S_2. Entonces

$$l(S_2) = 1 \qquad fact(S_2) = \{C_2\}$$

2) S_3

$1 \subsetneq A_3 \subsetneq S_3$ es una serie de composición de S_3 pues

$$\left.\begin{array}{c} S_3/A_3 \cong C_2 \\ A_3/1 = A_3 \cong C_3 \end{array}\right\} simples$$

Entonces $l(S_3) = 2$ y $fact(S_3) = \{C_2, C_3\}$

3) $S_4 \qquad 1 \trianglelefteq C_2 \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$ serie de composición de S_4.

$$l(S_4) = 4 \quad y \quad fact(S_4) = \{C_2, C_3, C_2, C_2\} =$$
$$= \{S_4/A_4 \cong C_2,\ A_4/K \cong C_3, K/C_2 \cong C_2,\ C_2/1 = C_2\}$$

4) $G = D_3 = \{1, r, r^2, s, rs, r^2s\}$

$$1 \trianglelefteq \langle r \rangle \trianglelefteq D_3$$

serie de composición de D_3

$$l(D_3) = 2 \qquad fact(D_3) = \{D_3/\langle r \rangle \cong C_2, \langle r \rangle \cong C_3\}$$

5) $G = D_4$

$1 \trianglelefteq \langle s \rangle \trianglelefteq \langle r^2, s \rangle \trianglelefteq D_4$ es una serie de composición.

$$l(D_4) = 3 \quad y \quad fact(D_4) = \{D_4/\langle r^2, s \rangle \cong C_2, \langle r^2, s \rangle / \langle s \rangle \cong C_2, \langle s \rangle \cong C_2\}$$

6) Ejercicio 12 (Relación 4): Hallar las series de composición de D_6.

$$l(D_6) = 3$$
$$D_6 = \langle r, s / r^6 = 1 = s^2, \quad sr = r^{-1}s \rangle =$$
$$= \{1, r, r^2, r^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, r^5s\}$$

$|D_6| = 12$, sus subgrupos propios de orden 2, 3, 4 ó 6.

Orden 2: $\langle r^3 \rangle, \langle s \rangle, \langle rs \rangle, \langle r^2s \rangle, \langle r^3s \rangle, \langle r^4s \rangle, \langle r^5s \rangle$

$$\langle r^3 \rangle = \{1, r^3\} = Z(D_6) \trianglelefteq D_6$$

Los demás no son normales en D_6.

Orden 4: Cíclicos no hay porque en D_6 no hay elementos de orden 4. De tipo Klein (parejas de elementos de orden 2 que conmutan entre sí).

$$K_1 = \langle r^3, s \rangle = \{1, r^3, s, r^3s\} = \langle r^3, r^3s \rangle = \langle s, r^3s \rangle$$
$$K_2 = \langle r^3, rs \rangle = \{1, r^3, rs, r^4s\} = \langle r^3, r^4s \rangle = \langle rs, r^4s \rangle$$
$$K_3 = \langle r^3, r^2s \rangle = \{1, r^3, r^2s, r^5s\} = \langle r^3, r^5s \rangle = \langle r^2s, r^5s \rangle$$

Ninguno normal en D_6

$$rK_1r^{-1} \not\trianglelefteq K_1 \qquad rsr^{-1} = r^2s \notin K_1$$

Orden 6: Cíclicos $\rightarrow$ hay dos elementos de orden 6 en D_6, que son r y r^5

$$\langle r \rangle = \{1, r, r^2, r^3, r^4, r^5\} = \langle r^5 \rangle$$

Isomorfos a D_3. Buscamos parejas $a, b \begin{cases} a^3 = 1 \\ b^2 = 1 \\ ba = a^2 b \end{cases}$, con $a \in \{r^2, r^4\}$

$$H_1 = \langle r^2, s \rangle = \{1, r^2, r^4, s, r^2 s, r^4 s\}$$
$$H_2 = \langle r^2, rs \rangle = \{1, r^2, r^4, rs, r^3 s, r^5 s\}$$

Todos los subgrupos de D_6 de orden 6 son normales porque tienen índice 2. Las series de composición son

$$\begin{array}{l} 1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_6 \\ 1 \trianglelefteq \langle r^3 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_6 \\ 1 \trianglelefteq \langle r^2 \rangle \trianglelefteq H_1 \trianglelefteq D_6 \\ 1 \trianglelefteq \langle r^2 \rangle \trianglelefteq H_2 \trianglelefteq D_6 \end{array} \Rightarrow \left\{ \begin{array}{l} C_2, C_2, C_3 \\ C_2, C_3, C_2 \\ C_2, C_2, C_3 \\ C_2, C_2, C_3 \end{array} \right\} \Rightarrow factores$$

$l(D_6) = 3$.

4-5-21

Proposición: Sea G un grupo finito y N un subgrupo normal propio de G.

$$l(G) = l(N) + l(G/N)$$
$$fact(G) = fact(N) \cup fact(G/N)$$

Demostración: Como N es un subgrupo normal propio de G entonces la serie

$$1 \lneq N \lneq G$$

es una serie normal propia de G.

Por el T$^{\underline{a}}$ de Jordan-Holder se puede refinar hasta una serie de composición de G. Sea

$$1 = K_0 \lneq K_1 \lneq \ldots \lneq K_r = N \lneq K_{r+1} \lneq \ldots \lneq K_n = G$$

dicho refinamiento, entonces

$1 = K_0 \lneq K_1 \lneq \ldots \lneq K_r = N$ es serie de composición de N y

$1 = K_r/N \lneq K_{r+1}/N \lneq \ldots \lneq K_n/N = G/N$ 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.

Corolario: Para cada $n \geq 5$, la longitud de S_n es 2, y los factores de S_n son

$$fact(S_n) = \{A_n, C_2\}$$

Demostración: Por el teorema de Abel, la serie

$$1 \trianglelefteq A_n \trianglelefteq S_n$$

es una serie de composición de S_n pues sus factores son

$$S_n/A_n \cong C_2 \quad y \quad A_n/1 \cong A_n$$

y por tanto simples. Entonces

$$l(S_n) = 2 \qquad fact(S_n) = \{A_n, C_2\}$$

□

Lema: Sea $n \geq 3$ y $x_1, x_2 \in \{1, 2, \ldots, n\}$ con $x_1 \neq x_2$. Entonces se verifica que

$$A_n = \langle (x_1\ x_2\ k)/k \neq x_1, x_2 \rangle$$

Demostración: Sabemos que A_n está generado por todos los ciclos de longitud 3. Sea

$$H = \langle (x_1\ x_2\ k)/k \neq x_1, x_2 \rangle$$

Demostremos 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

$$(x_1\ x_2\ k)^{-1} = (x_1\ k\ x_2) \in H \qquad (x_1\ k\ x_2) = (k\ x_2\ x_1) \in H$$

Sea $(i\ j\ k)$ un 3-ciclo,

Caso 1 : $\{x_1, x_2\} \subseteq \{i, j, k\} \Rightarrow$ por la observación anterior, $(i\ j\ k) \in H$

Caso 2 : $x_1 \in \{i, j, k\}$ y $x_2 \notin \{i, j, k\}$

a) Si $i = x_1$ entonces

$$\alpha = (x_1\ j\ k) = (x_1\ x_2\ k)^{-1}(x_1\ x_2\ j)(x_1\ x_2\ k) \in H$$

b) Si $j = x_1$ entonces

$$\alpha = (i\ x_1\ k) = (x_1\ k\ i) \in H$$

por el caso anterior (a).

c) Si $k = x_1$ entonces

$$\alpha = (i\ j\ x_1) = (x_1\ i\ j) \in H$$

por el caso (a)

Caso 3 : $x_1 \notin \{i,j,k\} \quad \wedge \quad x_2 \in \{i,j,k\}$. Se procede de forma análoga al caso 2 y se concluye entonces $\alpha \in H$.

Caso 4 $x_1 \notin \{i,j,k\} \quad \wedge \quad x_2 \notin \{i,j,k\}$

$$\alpha = (i\ j\ k) = (x_1\ x_2\ i)(x_2\ j\ k)(x_1\ x_2\ i)^{-1} \in H$$

Por tanto H contiene todos los 3-ciclos y entonces $H = A_n$.

□

Demostración (Teorema de Abel): $n \geq 5$ y sea $N \trianglelefteq A_n$ con $N \neq 1$. Vamos a demostrar que $N = A_n$. Como $N \neq 1$, elegimos en N aquella permutación $\alpha \in N$, $\alpha \neq id$ y que mueve el menor número de elementos de $\{1, 2, \ldots, n\}$.

Veamos que α es un 3-ciclo, es decir, mueve exactamente 3 elementos. Supongamos que α no es 3-ciclo, es decir, que mueve más de 3 elemetos ($N \leq A_n$, luego tienen que ser transposiciones pares).

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 $x_5 \in \{1, 2, \ldots, n\}$ tal que $x_5 \neq x_i \quad i = 1, 2, 3, 4$ (que podemos hacerlo pues $n \geq 5$) y consideramos $\beta = (x_3\ x_4\ x_5) \in A_n$

Entonces $\beta^{-1} N \beta \leq N$ 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.

$$\sigma = (x_3\ x_5\ x_4)(x_1\ x_2)(x_3\ x_4)(x_3\ x_4\ x_5)(x_1\ x_2)(x_3\ x_4) = (x_3\ x_4\ x_5)$$

Caso 2 α mueve 5 o más elementos. Elegimos $x_1, x_2, x_3, x_4, x_5 \in \{1, \ldots, n\}$, 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 el caso anterior

$$\sigma = \beta^{-1}\alpha^{-1}\beta\alpha \in N$$

Veamos que σ mueve menos elementos que α, o σ deja fijos más elementos que α.

En efecto, si $j \in \{1, \ldots, n\}$ tal que $\alpha(j) = j$ entonces $j \neq x_i \quad \forall i = 1, \ldots, 5$ 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 $k \neq x_i \quad i = 1, 2, 3$ y consideremos $\gamma = (x_1\ x_2)(x_3\ k) \in A_n$. Entonces $\gamma N \gamma^{-1} \leq N$ por ser $N \trianglelefteq A_4$ y entonces

$$\gamma\alpha^{-1}\gamma^{-1} \in N$$

Es fácil ver que

$$\gamma\alpha^{-1}\gamma^{-1} = (x_1\ x_2\ k)$$

Entonces, $\{(x_1\ x_2\ k)/\ k \neq x_1, x_2\} \subseteq N$ y aplicando el lema anterior

$$A_n = \langle (x_1\ x_2\ k)/\ k \neq x_1, x_2 \rangle \leq N \Rightarrow A_n = N$$

□

4.2. Grupos Resolubles

Definición: Un grupo G se dice resoluble si tiene una serie normal

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$$

tal que H_i/H_{i-1} es abeliano $\forall i = 1, \ldots, n$.
Es claro que si G es un grupo abeliano entonces G es resoluble, pues la serie

$$1 = H_0 \trianglelefteq H_1 = G$$

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, sean

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$$

serie normal de G con G_i/G_{i-1} abeliano $\forall i = 1, \ldots, n$.

Como G es finito, podemos aplicar el T$^{\underline{a}}$ de Jordan-Holder, la serie anterior puede refinarse a una serie de composición de G.

Sea $1 = H_0 \trianglelefteq\!\!\!\!\cdot\ H_1 \trianglelefteq\!\!\!\!\cdot\ \ldots \trianglelefteq\!\!\!\!\cdot\ H_m = G$ serie de composición de G que refina a la anterior.

Veamos que H_r/H_{r-1} es abeliano $\forall r = 1, \ldots, m$. Elegimos un r, y existirá un $i \in \{1, \ldots, n\}$ tal que $H_r \leq G_i$ (usando que la serie de composición es un refinamiento.

Caso 1 $H_{r-1} = G_{i-1}$ entonces

$$H_r/H_{r-1} = H_r/G_{i-1} \leq G_i/G_{i-1}$$

que es abeliano $\Rightarrow H_r/H_{r-1}$ también es abeliano.

Caso 2 $H_{r-1} \neq G_{i-1}$ entonces

$$G_{i-1} \trianglelefteq H_{r-1} \trianglelefteq\!\!\!\!\cdot\ H_r \leq G_i$$

Entonces

$$H_r/H_{r-1} \overset{2\,T.\,isomorfia}{\cong} \frac{H_r/G_{i-1}}{H_{r-1}/G_{i-1}}$$

es abeliano porque H_r/G_{i-1}, H_{r-1}/G_{i-1} son sugrupos 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, $\forall r = 1, \ldots, m$.

□

Corolario: S_n es resoluble $\Leftrightarrow n \leq 4$.

Demostración: $\Rightarrow$) Si $n \leq 4 \Rightarrow n = 2, 3\ o\ 4$

$$\left.\begin{array}{c} fact(S_2) = \{C_2\} \\ fact(S_3) = \{C_2, C_3\} \\ fact(S_4) = \{C_2, C_2, C_2, C_3\} \end{array}\right\} \Rightarrow \textit{son resolubles por el t. anterior}$$

$\Rightarrow$) 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 $H \leq G$, 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 dos siguiente resultados

(a) Sea $N, N', H \leq G$ con $N \trianglelefteq N' \Rightarrow N \cap H \trianglelefteq N' \cap H$

(b) $H, H', N \leq G$ con $\left.\begin{array}{c} H \trianglelefteq H' \\ N \trianglelefteq G \end{array}\right\} \Rightarrow NH \trianglelefteq NH'$

1) Sea $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$, serie normal de G con G_i/G_{i-1} abeliano, $i = 1, \ldots, n$.

Sea $H \leq G$. Por (a), obtenemos una serie normal

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \ldots \trianglelefteq G_n \cap H = G \cap H = H$$

de H.

Sea $i \in \{1, \ldots, n\}$, aplicamos el 3^{o} Teorema de isomorfía a G_i y a los subgrupos

$$K = G_i \cap H \leq G_i \qquad N = G_{i-1} \trianglelefteq G_i$$

Entonces $K/(N \cap K) \cong KN/N$, es decir,

$$(G_i \cap H)/(G_{i-1} \cap G_i \cap H) \cong G_{i-1}(G_i \cap H)/G_{i-1}$$
$$(G_i \cap H)/(G_{i-1} \cap H) = (G_i \cap H)/(G_{i-1} \cap G_i \cap H)$$

Puesto que $G_{i-1}(G_i \cap H)/G_{i-1} \leq G_i/G_{i-1}$ y entonces abeliano.

Consecuentemente H tiene una serie normal con factores abelianos. Es decir, H es resoluble.

2) $N \trianglelefteq G$, G resoluble. Sea

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$$

serie normal de G con G_i/G_{i-1} abeliano, $i = 1, \ldots, n$.

Por (b), $G_{i-1}N \trianglelefteq G_iN \quad \forall i = 1, \ldots, n$. Además, N es normal en todo G_iN pues N es normal en G y entonces, tomando cociente

$$1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \ldots \trianglelefteq G_nN/N = GN/N$$

es una serie normal de G/N. Sus factores $\forall i = 1, \ldots, n$

$$\frac{G_iN/N}{G_{i-1}N/N} \cong G_iN/G_{i-1}N$$

Aplicamos el tercer teorema de isomorfías a

$$\begin{gathered} K = G_i \leq G_iN \\ N = G_{i-1}N \leq G_iN \\ G_i/(G_{i-1}N) \cap G_i \cong G_i(G_{i-1}N)/G_{i-1}N = G_iN/G_{i-1}N \\ G_i/(G_{i-1}N) \cap G_i \overset{2\,T.\,Isomorfia}{\cong} \frac{G_i/G_{i-1}}{((G_{i-1}N) \cap G_i)/G_i} \end{gathered}$$

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 $1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = N$ serie normal de N tal que N_i/N_{i-1} abeliano $\forall i = 1, \ldots, r$.

Sea

$$1 = N/N \trianglelefteq H_1/N \trianglelefteq \ldots \trianglelefteq H_s/N = G/N$$

serie normal de G/N tal que $\frac{H_j/N}{H_{j-1}/N} \cong H_j/H_{j-1}$ es abeliano $\forall j = 1, \ldots, s$.

Entonces es inmediato que

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = N \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_s = G$$

es una serie cuyos factores son abelianos. Por tanto G es resoluble.

□

Corolario: Para todo $n \geq 3$, el grupo diédrico D_n es resoluble.

Demostración: $D_n = \langle r, s / r^n = 1 = s^2, \quad sr = r^{-1}s \rangle$.
Consideramos $N = \langle r \rangle \cong C_n$. $N \trianglelefteq D_n$ pues $[D_n : N] = 2$.

$$\left.\begin{array}{c} N \text{ es abeliano y entonces resoluble} \\ D_n/N \cong C_2 \quad \text{abeliano y entonces resoluble} \end{array}\right\} \Rightarrow D_n \quad \text{es resoluble}$$

Definición: Sea G un grupo, y sean $x, y \in G$. 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

$$[G, G] := \langle [x, y] / \, x, y \in G \rangle$$

Proposición: Sea G un grupo. Entonces

(i) $[G, G] \trianglelefteq G$

(ii) $[G, G] = 1 \Leftrightarrow G$ es abeliano

(iii) $G/[G, G]$ es un grupo abeliano.

(iv) Si $N \trianglelefteq G$, entonces G/N es abeliano $\Leftrightarrow [G, G] \leq N$

Al cociente $G/[G, G]$ se le llama el abelianizado de G.

Demostración:

(i) Puesto que $\{[x, y] / x, y \in G\}$ generan $[G, G]$, para ver que $[G, G] \trianglelefteq G$, basta demostrar que $a[x, y]a^{-1} \in [G, G] \quad \forall a \in G$. Esto último es claro porque

$$a[x, y]a^{-1} = [axa^{-1}, aya^{-1}] \in [G, G]$$

(ii) Es inmediato

(iii) Sean $x[G, G]$, $y[G, G] \in G/[G, G]$. Por ser $[G, G] \trianglelefteq G$ se tiene que

$$(x[G, G])(y[G, G]) = (xy)[G, G]$$
$$(y[G, G])(x[G, G]) = (yx)[G, G]$$

(Aclaración)

$$(x[G, G])(y[G, G]) = (xy)[G, G] \Leftrightarrow x[G, G]y[G, G] = (xy)[G, G] \Leftrightarrow$$
$$\Leftrightarrow (xy)^{-1}x[G, G]y[G, G] = [G, G] \Leftrightarrow y^{-1}[G, G]y[G, G] = [G, G] \Leftrightarrow$$
$$\Leftrightarrow y^{-1}[G, G]y = [G, G] \Leftrightarrow [G, G] \trianglelefteq G$$

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.

(iv) $N \trianglelefteq G$

$$G/N \quad es\ abeliano \Leftrightarrow (xN)(yN) = (yN)(xN) \quad \forall x, y \in G$$
$$\Leftrightarrow (yx)^{-1}(xy) = x^{-1}y^{-1}xy = [x^{-1}, y^{-1}] \in N \quad \forall x, y \in G$$
$$\Leftrightarrow \{[x, y] / \ x, y \in G\} \subseteq N \Leftrightarrow [G, G] \leq N$$

□

Ejercicio 3 (Relación 4): Demostrar que $\forall n \geq 3$, $[S_n, S_n] = A_n$.

$$A_n \trianglelefteq S_n \quad y \quad S_n/A_n \quad es\ abeliano \Rightarrow [S_n, S_n] \leq A_n$$

Para la otra inclusión basta ver que todo 3-ciclo pertenece a $[S_n, S_n]$ porque A_n está generado por los 3-ciclos

$$(i\ j\ k) = [(i\ j), (i\ k)] \in [S_n, S_n]$$

Así $A_n \leq [S_n, S_n]$.

Definición: Sea G un grupo. Para cada $n \geq 0$ definimos el n-ésimo subgrupo derivado de G, denotado por $G^{(n)}$, por recurrencia, como sigue

$$G^{(0)} := G \qquad G^{(n+1)} := [G^{(n)}, G^{(n)}] \qquad \forall n \geq 0$$

Notemos que tenemos la siguiente serie

$$\ldots \trianglelefteq G^{(n+1)} \trianglelefteq G^{(n)} \trianglelefteq \ldots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G = G^{(0)}$$

que en general no tiene porque ser finita. Sus factores son

$$G^{(n)}/G^{(n+1)} = G^{(n)}/[G^{(n)}, G^{(n)}] \quad abeliano \quad \forall n \geq 0$$

Esta serie se conoce por la serie derivada de G.

Teorema: Sea G un grupo. G resoluble $\Leftrightarrow \exists n$ tal que $G^{(n)} = 1$.

Demostración: $\Leftarrow$) Inmediato
$\Rightarrow$) Supongamos G resoluble y sea

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$$

serie normal de G con H_i/H_{i-1} abeliano $\forall i = 1, \ldots, n$.

Veamos que para todo $i \geq 1$, $G^{(i)} \leq H_{n-1}$, por inducción en i. Sea $i = 1$, puesto que

$$H_n/H_{n-1} = G/H_{n-1} \quad es\ abeliano \Rightarrow [G, G] = G^{(1)} \leq H_{n-1}$$

y se tiene el resultado para $i = 1$.

Supuesto cierto para i, vease para $i+1$ ($G^{(i)} \leq H_{n-1}$), veámoslo para $i+1$. Puesto que H_{n-i}/H_{n-i-1} es abeliano $\Rightarrow$

$$\Rightarrow [H_{n-i}, H_{n-i}] \leq H_{n-(i+1)}$$
$$G^{(i)} \leq H_{n-i} \Rightarrow [G^{(i)}, G^{(i)}] = G^{(i+1)} \leq [H_{n-i}, H_{n-i}] \leq H_{n-(i+1)}$$

tenemos que $G^{(i+1)} \leq H_{n-(i+1)}$.
Tomando $i = n$, $G^{(n)} \leq H_{n-n} = H_0 = 1 \Rightarrow G^{(n)} = 1$

□

10-5-21

Ejercicio 2 (Relación 4):
$N \trianglelefteq G \quad G/N$ abeliano $\Leftrightarrow [G, G] \leq N$

$$K = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \trianglelefteq A_4$$
$$A_4/K \cong C_3 \quad \textit{y entonces abeliano} \Rightarrow [A_4, A_4] \leq K$$

Por otro lado se verifica

$$(1\,2)(3\,4) = [(1\,3\,2), (1\,3)(2\,4)] \in [A_4, A_4]$$
$$(1\,3)(2\,4) = [(1\,2\,3), (1\,2)(3\,4)] \in [A_4, A_4]$$
$$(1\,4)(2\,3) = [(1\,2\,4), (1\,2)(3\,4)] \in [A_4, A_4]$$

Es decir, $K \leq [A_4, A_4]$, entonces $\Rightarrow K = [A_4, A_4]$

$[D_4, D_4] = \langle r^2 \rangle = \{1, r^2\}$
$[Q_2, Q_2] = \langle -1 \rangle = \{1, -1\}$

Ejercicio 4 (Relación 4): $\forall n \geq 3$, A_n es el único subgrupo de S_n de orden $\frac{n!}{2}$. Sea $H \leq S_n$ tal que $|H| = \frac{n!}{2}$, entonces

$$[S_n : H] = 2 \Rightarrow H \trianglelefteq S_n$$

$S_n/H \cong C_2$ y por tanto abeliano

$$\Rightarrow [S_n, S_n] = A_n \leq H$$

y como $|A_n| = \frac{n!}{2} = |H| \Rightarrow A_n = H$

Ejercicio 6 (Relación 4): Sea G un grupo abeliano. Demostrar G tiene una serie de composición $\Leftrightarrow G$ finito.

Resolución: $\Leftarrow$) Si G es finito se verifica sea o no abeliano.

$\Rightarrow$) Sea

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$$

una serie de composición de G. Por tanto

$$G_i/G_{i-1} \quad son\ simples \quad \forall i = 1, \ldots, n$$

Como G es abeliano G_i es abeliano $\forall i$, por ser abeliano. Entonces G_i/G_{i-1}, es abeliano $\forall i = 1, \ldots, n$.

Entonces G_i/G_{i-1} abeliano y simple $\Rightarrow$ G_i/G_{i-1} cíclico de orden primo $\forall i = 1, \ldots, n$. En particular G_i/G_{i-1} es finito $\forall i = 1, \ldots, n$.

Ejercicio: Si G es un grupo y $N \trianglelefteq G$ tal que N y G/N son finitos entonces G es finito

$$\left.\begin{array}{c} G_1/G_0 = G_1 \quad es\ finito \\ G_2/G_1 \quad es\ finito \end{array}\right\} \Rightarrow G_2 \quad es\ finito$$

$$\left.\begin{array}{c} G_2 \quad finito \\ G_3/G_2 \quad finito \end{array}\right\} \Rightarrow G_3 \quad es\ finito$$

Razonando de esta forma, en un número finito de pasos llegamos a que $G_n = G$ es finito.

Ejercicio 11 (Relación 4): Series de composición S_n, $n \geq 5$.
Por el Tª de Abel, sabemos que

$$1 \trianglelefteq A_n \trianglelefteq S_n$$

es una serie de composición de S_n

$$l(S_n) = 2 \qquad fact(S_n) = \{A_n, C_2\}$$

Sea $1 \trianglelefteq N \trianglelefteq S_n$ otra serie de composición de S_n

$$N/1 = N = A_n \quad o \quad N/1 = C_2$$

Supongamos que $N/1 \cong C_2 \Rightarrow N = \langle\alpha\rangle = \{1, \alpha\}$ $\alpha \in S_n$ con orden 2. Entonces

$$\alpha = (x_1\ y_1)(x_2\ y_2)\ldots(x_k\ y_k)$$

donde $\{x_i, y_i\} \cap \{x_j, y_j\} = \emptyset$ si $i \neq j$.
Si $k = 1$, es decir, $\alpha = (x_1\ y_1)$. Consideramos $\beta = (x_1\ z)$ siendo $z \neq x_1, y_1$

$$\beta\alpha\beta^{-1} = (x_1\ z)(x_1\ y_1)(x_1\ z) = (z\ y_1) \notin N = \{1, \alpha\}$$

Por tanto $\beta N \beta^{-1} \not\leq N$ en contradicción con que N es normal.

Para $k \geq 2$

$$\alpha = (x_1\ y_1)(x_2\ y_2)\ldots(x_k\ y_k)$$

consideramos $\gamma = (x_1\ x_2)$

$$\gamma\alpha\gamma^{-1} = (x_1\ x_2)\alpha(x_1\ x_2) = (x_2\ y_1)(x_1\ y_2)(x_3\ y_3)\dots(x_k\ y_k) \neq \alpha$$

Entonces $\gamma\alpha\gamma^{-1} \notin N$ en contradicción $N \trianglelefteq S_4 \quad (N/1 \neq C_2)$.
S_n, $n \geq 5$ tiene una única serie de composición

$$1 \trianglelefteq A_n \trianglelefteq S_n$$

Ejercicio 15 (Relación 4): G resoluble con una serie de composición $\Rightarrow G$ es finito. Por ser G resoluble, existe una serie

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

tal que G_i/G_{i-1} abeliano $\forall i = 1, \dots, n$.

Como G tiene series de composición, podemos aplicar el primer apartado de Tª de Jordan-Holder, y entonces la serie anterior tiene un refinamiento

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$$

que es una serie de composición.

Se verifica, por ser G_i/G_{i-1} abeliano $\forall i = 1, \dots, n$, que H_j/H_{j-1} es abeliano $\forall j = 1, \dots, m$. H_j/H_{j-1} es abeliano y simple $\Rightarrow$ cíclico de orden primo, en particular finito

$$H_j/H_{j-1} \quad finito \quad \forall j = 1, \dots, m$$

Razonando como en el ejercicio 6 que G es finito.

11-5-21

5. Tema 6: G-conjuntos y p-grupos.

Definición: Sea G un grupo y $X \neq \emptyset$. Una acción de G sobre X (por la izquierda) es una aplicación

$$G \times X \longrightarrow X \qquad (g, x) \longmapsto gx$$

que verifica las dos siguientes propiedades

1) $1x = x \quad \forall x \in X$

2) $(gh)x = g(hx) \quad \forall g, h \in G \quad y \quad \forall x \in X$

Al elemento gx 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. A G se le suele llamar dominio de operadores, y a la aplicación anterior (acción) $G \times X \longrightarrow X$ se la llama aplicación G-estructura de X.

Trabajaremos siempre con acciones por la izquierda (la definición anterior también se puede hacer por la derecha). Para cada $g \in G$, podemos definir la siguiente aplicación

$$\phi(g) : X \longrightarrow X \qquad \phi(g)(x) := gx$$

La condición (1) nos dice que $\phi(1) = id_X : X \longrightarrow X$.
La condición (2) nos dice que, dados, $g, h \in G$.

$$\phi(gh) = \phi(g) \circ \phi(h)$$

En particular

$$\phi(gg^{-1}) = id_X = \phi(g) \circ \phi(g^{-1})$$
$$\phi(g^{-1}g) = id_X = \phi(g^{-1}) \circ \phi(g)$$

Es decir, $\phi(g) : X \longrightarrow X$ es biyectiva con

$$\phi(g)^{-1} = \phi(g^{-1})$$

Entonces tenemos definido un homomorfismo de grupo

$$\phi : G \longrightarrow S(X)$$
$$g \longmapsto \phi(g) := X \longrightarrow X$$
$$\phi(g)(x) = gx$$

donde $S(X)$ es el grupo de permutaciones del conjunto X. Este homomorfismo lo llamaremos representación de G con permutaciones asociada a la acción.
Recíprocamente: Sea G un grupo y X un conjunto no vacío. Supongamos dado un homomorfismo

$$f : G \longrightarrow S(X)$$

Entonces podemos definir una acción de G sobre X como sigue:

$$G \times X \longrightarrow X \qquad (g, x) \longmapsto gx := f(g)(x)$$

La condición 1) se deduce de que $f(1) = id_X$.
La condición 2) se deduce de que f es un homomorfismo, es decir, $f(gh) = f(g) \circ f(h)$. Además, es fácil ver que la representación de G asociada a esta acción es el homomorfismo f.

Definición: Una acción de G sobre un conjunto X diremos que es fiel si el núcleo de $\phi : G \longrightarrow S(X)$ es trivial (monomorfismo)

$$Ker(\phi) = \{g \in G / \ \phi(g) = id_X\} = \{g \in X / \ \phi(g)(x) = x \quad \forall x \in X\} =$$
$$= \{g \in G / \ gx = x \quad \forall x \in X\}$$

Ejemplos:

1) Dado G un grupo y $X \neq \emptyset$. La aplicación

$$G \times X \longrightarrow X \qquad (g, x) \longmapsto gx := x$$

es una acción de G sobre X que llamaremos la acción trivial de G sobre X. La representación asociada en el homomorfismo trivial

$$\begin{aligned} \phi : G &\longrightarrow S(X) \\ g &\longmapsto id_X \end{aligned}$$

Además, $Ker(\phi) = G$.

2) Supongamos X un G-conjunto y $H \leq G$ un subgrupo de G. Entonces X también es un H-conjunto con acción dada por $H \times X \longrightarrow X$, definida como la de $G \times X \longrightarrow X$ restringiéndose a los elementos de H.

Esta acción se llama la acción por restricción. Si $\phi : G \longrightarrow S(X)$ 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 $X = \{1, 2, \ldots, n\}$

$$S_n \times X \longrightarrow X \qquad (\sigma, i) \longmapsto \sigma_i := \sigma(i)$$

esta aplicación es una acción de S_n sobre X cuya representación asociada

$$id_{S_n} = \phi : S_n \longrightarrow S(X) = S_n$$

Por tanto se trata de una acción fiel.

4) $G = D_4 = \langle r, s / r^4 = 1 = s^2 \quad sr = r^{-1}s \rangle$ y $X = \{1, 2, 3, 4\}$. Sea

$$\begin{aligned} \phi : D_4 &\longrightarrow S(X) = S_4 \\ \phi(r^i) &= (1\,2\,3\,4)^i \qquad 0 \leq i \leq 3 \\ \phi(r^i s) &= (1\,2\,3\,4)^i (2\,4) \qquad 0 \leq i \leq 3 \end{aligned}$$

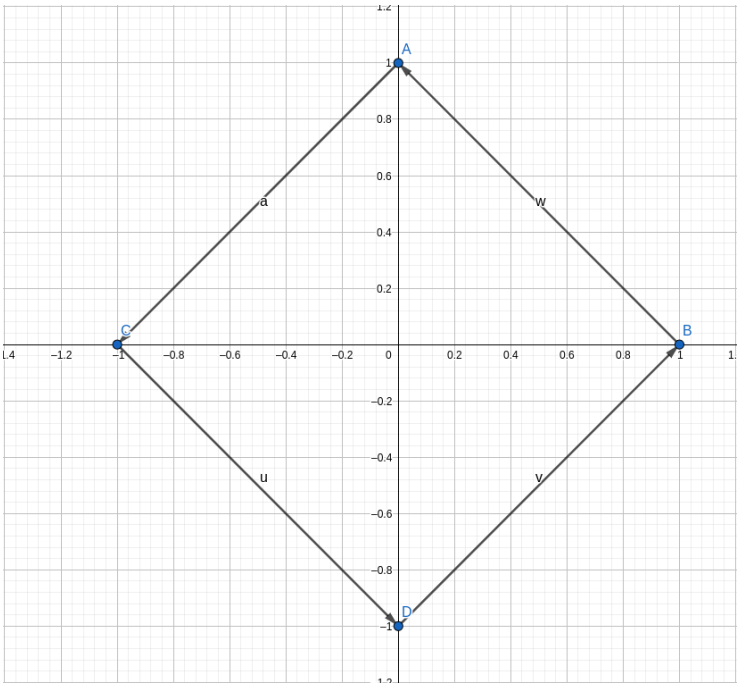
ϕ es un homomorfismo de grupos (ejercicio).

Tenemos entonces una acción

$$\begin{aligned} D_4 \times \{1, 2, 3, 4\} &\longrightarrow \{1, 2, 3, 4\} \\ g_j := \phi(g)(j) \qquad \forall g \in D_4, &\quad j \in \{1, 2, 3, 4\} \end{aligned}$$

g_j es precisamente el resultado de aplicar al vértice j el movimiento que corresponde a g.

$r_j = \phi(r)(j) = (1\,2\,3\,4)(j)$



5) $G = S_n$ X cualquier conjunto, con $X \neq \emptyset$. Consideremos $X^n = X \times \overbrace{\ldots}^{n-veces} \times X$. Definimos una acción de S_n sobre X^n como sigue

$$S_n \times X^n \longrightarrow X^n$$
$$(\sigma(x_1, x_2, \ldots, x_n)) \longmapsto \sigma_{(x_1,x_2,\ldots,x_n)} := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)})$$

Veamos la propiedad 2). Sean $\sigma, \tau \in S_n$

$$\sigma\tau_{(x_1,x_2,\ldots,x_n)} \stackrel{?}{=} \sigma(\tau_{(x_1,x_2,\ldots,x_n)})$$
$$\sigma\tau_{(x_1,x_2,\ldots,x_n)} = (x_{(\sigma\tau)^{-1}(1)}, x_{(\sigma\tau)^{-1}(2)}, \ldots, x_{(\sigma\tau)^{-1}(n)}) =$$
$$= (x_{\tau^{-1}\sigma^{-1}(1)}, x_{\tau^{-1}\sigma^{-1}(2)}, \ldots, x_{\tau^{-1}\sigma^{-1}(n)})$$
$$\sigma_{(\tau_{(x_1,x_2,\ldots,x_n)})} = \sigma_{(x_{\tau^{-1}(1)}, x_{\tau^{-1}(2)}, \ldots, x_{\tau^{-1}(n)})} =$$
$$= \sigma_{(y_1,\ldots,y_n)} \qquad y_j = x_{\tau^{-1}(j)} \quad j = 1, \ldots, n$$
$$= (y_{\sigma^{-1}(1)}, y_{\sigma^{-1}(2)}, \ldots, y_{\sigma^{-1}(n)}) =$$
$$= (x_{\tau^{-1}(\sigma^{-1}(1))}, x_{\tau^{-1}(\sigma^{-1}(2))}, \ldots, x_{\tau^{-1}(\sigma^{-1}(n))}) =$$
$$= (x_{\tau^{-1}\sigma^{-1}(1)}, x_{\tau^{-1}\sigma^{-1}(2)}, \ldots, x_{\tau^{-1}\sigma^{-1}(n)}$$
$$\Rightarrow \sigma\tau_{(x_1,x_2,\ldots,x_n)} = \sigma_{(\tau_{(x_1,x_2,\ldots,x_n)})}$$

Nótese, la aplicación

$$S_n \times X^n \longrightarrow X^n$$
$$(\sigma(x_1, \ldots, x_n)) \longmapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

en general, no es acción (por ejemplo, compruébese para $n = 3$.

12-5-21

6) Sea G un grupo y $X = G$, entonces podemos definir una acción de G sobre G llamada, la acción por traslación y que está definida como sigue

$$G \times G \longrightarrow G \qquad (g, h) \longmapsto g_h := gh$$

Si $\phi : G \longrightarrow S(G)$ es la representación asociada

$$Ker(\phi) = \{g \in G / \phi(g) = id_G\} = \{g \in G / \phi(g)(h) = h \quad \forall h \in G\} =$$
$$= \{g \in G / g_h = h \quad \forall h \in G\} = \{g \in G / gh = h \quad \forall h \in G\} = \{1\}$$

Es decir, esta acción es fiel.

Si G finito y $|G| = n$, entonces $S(G) \cong S_n$ y como

$$\phi : G \longrightarrow S(G) \cong S_n$$

es un monomorfismo, aplicando el primer teorema de isomorfía, deducimos que $G \cong Im(\phi)$.

Teorema de Cayley: Todo grupo finito es isomorfo a un subgrupo de permutaciones.

7) Sea G un grupo y $H \leq G$ subgrupo. Entonces

$$G \times G/H \longrightarrow G/H$$
$$(g, xH) \longmapsto g_{(xH)} := gxH$$

es una acción. También

$$G \times H/G \longrightarrow H/G$$
$$(g, Hx) \longmapsto g_{(Hx)} := Hxg^{-1}$$

es una acción.

8) Sea G un grupo y consideramos $X = G$. Entonces la aplicación

$$G \times G \longrightarrow G \qquad (g, h) \longmapsto g_h := ghg^{-1}$$

es una acción, que llamaremos la acción por conjugación de G sobre si mismo

$$\begin{aligned} \phi : G &\longrightarrow S(G) \\ g \longmapsto \phi(g) : G &\longrightarrow G \\ \phi(g)(h) &= g_h = ghg^{-1} \end{aligned}$$

Es decir, $\phi(g) = \varphi_g$ es el automorfismo interno por el elemento $g \in G$

$$\begin{aligned} Img(\phi) = Int(G) \leq Aut(G) \\ Ker(\phi) = \{g \in G / \varphi_g = id_G\} = \{g \in G / \varphi_g(h) = h \quad \forall x \in G\} = \\ = \{g \in G / ghg^{-1} = h \quad \forall h \in G\} = \{g \in G / gh = hg \forall h \in G\} = Z(G) \end{aligned}$$

9) Sea G un grupo y considremos el conjunto $X = Sub(G)$

$$\begin{aligned} G \times Sub(G) &\longrightarrow Sub(G) \\ (g, H) &\longmapsto g_H = gHg^{-1} \end{aligned}$$

es una acción.

Sea G un grupo y X un $G - conjunto$ y sea

$$G \times X \longrightarrow X \qquad (g, x) \longmapsto g_x$$

la acción.

Podemos definir en X la siguiente relación binaria, denotada por $\sim$. Dados $x, y \in X$

$$x \sim y \overset{def}{\Leftrightarrow} \exists g \in G \quad tal\ que \quad y = g_x$$

Esta relación binaria es una relación de equivalencia. En efecto

- Simétrica. Supongamos que $x \sim y \Rightarrow$

$$\exists g \in G \quad tal\ que \quad y = g_x$$

$$y = g_x \Rightarrow g_{(y)}^{-1} = g^{-1}(g_x) \overset{2)}{=} (g^{-1}g)_x \overset{1)}{=} 1_x \overset{1)}{=} x \Rightarrow y \sim x$$

De la misma forma se demuestra la propiedad relfexiva y transitiva.

Definición: Para cada $x \in X$, definimos la órbita de x, que denotaremos por $\mathcal{O}(x)$, como la clase de equivalencia de x por la relación de equivalencia anterior. Entonces

$$\begin{aligned} \mathcal{O}(x) = \{y \in X / x \sim y\} = \\ = \{y \in X / y = g_x \quad para \quad g \in G\} = \{g_x / g \in G\} \end{aligned}$$

Tenemos que

1) $\mathcal{O}(x) = \mathcal{O}(y) \Leftrightarrow x \sim y \Leftrightarrow \exists g \in G \quad tal\ que \quad y = g_x$

2) $\mathcal{O}(x) \neq \mathcal{O}(y) \Leftrightarrow \mathcal{O}(x) \cap \mathcal{O}(y) = \emptyset$

3) El conjunto de todos las órbitas, es decir, $X/\sim$, es una partición de X

$$X = \cup_{x \in X} \mathcal{O}(x) \qquad union\ finita$$

Una acción diremos que es transitiva si tiene una única órbita (si $X/\sim$ es unitario). Es decir,

$$\mathcal{O}(x) = \mathcal{O}(y) \quad \forall x, y \in X$$

o, en otros términos, si

$$\forall x, y \in X \quad \exists g \in G \quad tal\ que \quad y = g_x$$

Definición: Sea G un grupo y X un $G - conjunto$. Para cada $x \in X$ definimos el estabilizador de x en G como

$$Stab_G(x) := \{g \in G / g_x = x\}$$

Se verifica que $Stab_G(x)$ es un subgrupo de G, también llamado grupo de isotropía de x en G.

Proposición: Sea G un grupo y X un $G-conjunto$. Sean $x, y \in X$, entonces

$$\mathcal{O}(x) = \mathcal{O}(y) \Leftrightarrow Stab_G(x),\ Stab_G(y) \quad son\ subgrupos\ conjugados\ de\ G.$$

($H, K \leq G$, H y K se dicen conjugados si $\exists g \in G$ tal que $y = g_x$).

Demostración: Suponemos que $\mathcal{O}(x) = \mathcal{O}(y) \Rightarrow x \sim y \Rightarrow \exists g \in G$ tal que $y = g_x$. 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 $gStab_G(x)g^{-1} \leq Stab_G(y)$. Por el mismo razonamiento y puesto que $x = g_y^{-1}$, tendremos que

$$g^{-1}Stab_G(y)g \leq Stab_G(x) \Rightarrow Stab_G(y) \leq gStab_G(x)g^{-1}$$

Consecuentemente

$$gStab_G(x)g^{-1} = Stab_G(y)$$

□

Teorema: Sea G un grupo finito y X un $G-conjunto$. Entonces para cada $x \in X$, $\mathcal{O}(x)$ es también finito, teniéndose que

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

En particular $|\mathcal{O}(x)|$ es un divisor de $|G|$.

Demostración:

$$G/Stab_G(x) = \{gStab_G(x)/g \in G\} \xrightarrow{\lambda} \mathcal{O}(x) = \{g_x/g \in G\}$$

Definimos $\lambda(gStab_G(x)) := g_x$

$$gStab_G(x) = hStab_G(x) \Leftrightarrow h^{-1}g \in Stab_G(x)$$
$$\Leftrightarrow (h^{-1}g)_x = x \Leftrightarrow g_x = h_x$$

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 $\mathcal{O}(x)$ es finito y $|\mathcal{O}(x)| = [G : Stab_G(x)]$

□

Ejercicio 1 (Relación 6): $X = \{1, 2, 3, 4\}$

$$S_4 \times X \longrightarrow X \qquad \sigma_i := \sigma(i)$$

(2)$A_4 \times X \longrightarrow X \qquad \sigma_i := \sigma(i)$
Calcula $\mathcal{O}(2)$ y $Stab_{A_4}(2)$

$$\mathcal{O}(2) = \{\sigma_2/\sigma \in A_4\} = \{\sigma(2)/\sigma \in A_4\} = \{1, 2, 3, 4\}$$
$$[A_4 : Stab_{A_4}(2)] = |\mathcal{O}(2)| = 4 \Rightarrow |Stab_{A_4}(2)| = 3$$
$$Stab_{A_4}(2) = \{\sigma \in A_4/\sigma_2 = 2\} = \{\sigma \in A_4/\sigma(2) = 2\} =$$
$$= \langle(1\ 3\ 4)\rangle = \{id, (1\ 3\ 4), (1\ 4\ 3)\}$$

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

$$K \times X \longrightarrow X \qquad \sigma_i := \sigma(i)$$
$$\mathcal{O}(2) = \{\sigma_2/\sigma \in K\} = \{\sigma(2)/\sigma \in K\} = \{2, 1, 4, 3\} = X$$
$$[K : Stab_K(2)] = |\mathcal{O}(2)| = 4 \Rightarrow Stab_K(2) = \{id\}$$

Definición: Sea G un grupo y X un $G-conjunto$. Un elemento de X diremos que es un elemento fijo por la acción si $g_x = x \quad \forall g \in G$.
El conjunto de los elementos fijos lo denotaremos por $Fix(X)$

$$Fix(X) = \{x \in X/g_x = x \quad \forall g \in G\}$$

Notemos que

$$x \in Fix(X) \Leftrightarrow \mathcal{O}(x) = \{x\} \Leftrightarrow Stab_G(x) = G$$

Sea G un grupo finito y X un $G-conjunto$ finito. El conjunto $X/\sim$ también es finito. Supongamos

$$X/\sim = \{\mathcal{O}(x_1), \mathcal{O}(x_2), \ldots, \mathcal{O}(x_r)\}$$

Sabemos que es una partición de $X = \cup_{i=1}^{r} \mathcal{O}(x_i)$ unión disjunto $\Rightarrow$

$$|X| = \sum_{i=1}^{r} |\mathcal{O}(x_i)| = |Fix(X)| + \sum_{x_i \notin Fix(X)} |\mathcal{O}(x_i)| =$$
$$= |Fix(X)| + \sum_{x_i \notin Fix(X)} [G : Stab_G(x_i)]$$

Ejemplo:

1) Sea G un grupo cualquiera, y consideramos la acción de G sobre sí misma por traslación

$$G \times G \longrightarrow G \qquad g_h := gh$$

Sea $h \in G$

$$\mathcal{O}(h) = \{g_h / g \in G\} = \{gh / g \in G\} = G$$

Por tanto $\forall h, h' \in G$, si tiene que $\mathcal{O}(h) = \mathcal{O}(h')$, es decir, esta acción es transitiva

$$Stab_G(h) = \{g \in G / g_h = h\} = \{g \in G / gh = h\} = \{1\}$$
$$Fix(G) = \{h \in G / g_h = h \quad \forall g \in G\} = \{h \in G / gh = h \quad \forall g \in G\} = \emptyset$$

2) Sea G un grupo y consideramos la acción de G sobre sí mismo por conjugación

$$G \times G \longrightarrow G \qquad g_h := ghg^{-1}$$
$$h \in G \qquad \mathcal{O}(h) = \{g_h / g \in G\} = \{ghg^{-1} / g \in G\}$$

se llama la clase de conjugación del elemento h en G y se denota por $cl(h)$

$$Stab_G(h) = \{g \in G / g_h = h\} = \{g \in G / ghg^{-1} = h\} = \{g \in G / gh = hg\} \leq G$$

se llama el centralizador de h en G y se denota por $C_G(h)$

$$Fix(G) = \{h \in G / g_h = h \quad \forall g \in G\} = \{h \in G / ghg^{-1} = h \quad \forall g \in G\} =$$
$$= \{h \in G / gh = hg \quad \forall g \in G\} = Z(G)$$

Supongamos que G es un grupo finito

$$G/N = \{cl(h_1), cl(h_2), \ldots, cl(h_r)\}$$

Ejercicio 9 (Relación 6): Describir explícitamente las clases de conjugación de D_4

$$D_4 = \langle r, s / r^4 = 1 = s^2 \quad sr = r^{-1}s \rangle = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

- $cl(1) = \{1\}$
- $cl(r) = \{r, r^3\} = cl(r^3)$
- $cl(r^2) = \{r^2\}$
- $cl(s) = \{s, r^2s\} = cl(r^2s\}$
- $cl(rs) = \{rs, r^3s\} = cl(r^3s)$

¿Quiénes son los centralizadores de los elementos de D_4? $x \in D_4$

$$[D_4 : C_G(x)] = |cl(x)|$$

17-5-21

Ejercicio 7 (Relación 6): Demostrar que si G es finito contiene un elemento x que tiene exactamente 2 conjugados, entonces G admite un subgrupo normal propio.

Resolución: $x \in G$ tal que $|cl(x)| = 2$. En particular $x \neq 1$.
Consideramos $C_G(x)$ $(= Stab_G(x))$. Sabemos que

$$[G : N] = |cl(x)| = 2 \Rightarrow N \trianglelefteq G$$

Por otro lado, como $x \in N = \{g \in G / gx = xg\} \Rightarrow N \neq 1$. Por tanto, N es un grupo normal propio de G. Sea G un grupo, y consideramos la acción

$$G \times Sub(G) \longrightarrow Sub(G) \qquad g_H := gHg^{-1}$$

Para $H \in Sub(G)$

$$O(H) = \{g_H / g \in G\} = \{gHg^{-1} / g \in G\}$$
$$Stab_G(H) = \{g \in G / g_H = H\} = \{g \in G / gHg^{-1} = H\} =$$
$$= \{g \in G / gH = Hg\} = N_G(H) \longrightarrow Ejercicio\,33\,(Relacion\,3)$$

- $N \trianglelefteq N_G(H)$
- Si $K \leq G$ tal que $H \trianglelefteq K \Rightarrow N_G(H) \leq K$

$$Fix(Sub(G)) = \{H \leq G / g_H = H \quad \forall g \in G\} = \{H \leq G / gHg^{-1} = H \quad \forall g \in G\} =$$
$$= \{H \leq G / H \quad es\ un\ subgrupo\ normal\ de\ G\}$$

Si G es finito $\Rightarrow O(H)$ es finito, esto es, el número de conjugados de H es finito. Como

$$|O(H)| = [G : N_G(H)]$$

entonces $|O(H)|$ es un divisor de $|G|$

5.1. p-grupos (p número primo)

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 $n \geq 1$, $C_{p^n} = \langle x / x^{p^n} = 1 \rangle$ es un p-grupo. Porque si $a \in C_{p^n} \Rightarrow ord(a) \mid |C_{p^n}| = p^n \Rightarrow ord(a) = p^k \quad 0 \leq k \leq n$

2) Para cada $n \geq 2$, el producto directo

$$C_p \times C_p \times \overbrace{\ldots}^{n-veces} \times C_p$$

es un p-grupo.

Si $(x_1, \ldots, x_n) \in G$

$$ord((x_1, \ldots, x_n)) = mcm(ord(x_1), \ldots, ord(x_n))$$
$$ord((x_1, \ldots, x_n)) = p^k \quad 0 \leq k \leq 1$$

Así todo elemento de G tiene de 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 $\exists H = \langle x \rangle \leq G$ tal que $|H| = p$).

Demostración: Sea $|G| = n$ y $p \mid n$ con p número primo. Sea X definido como sigue

$$X := \{(x_1, x_2, \ldots, x_p) \in G^p / x_1 x_2 \ldots x_p = 1\}$$

Como $|G| = n \Rightarrow |X| = n^{p-1}$.
Consideramos el ciclo $\sigma = (1\,2\,\ldots\,p) \in S_p$ y $H = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$.

Definimos una acción de H sobre X como sigue

$$\sigma_{(x_1,\ldots,x_p)} := (x_1, \ldots, x_p)$$
$$1 \leq j \leq p-1 \quad \sigma^j_{(x_1,\ldots,x_p)} := (x_{j+1}, \ldots, x_p, x_1, \ldots, x_j)$$

Ejercicio: Demostrar que es una acción. Sea $(x_1, \ldots, x_p) \in X$

$$O((x_1, \ldots, x_p)) = \{\sigma^j_{(x_1,x_2,\ldots,x_p)} / 0 \leq j \leq p-1\} =$$
$$= \{(x_1, x_2, \ldots, x_p), (x_2, \ldots, x_p, x_1), \ldots, (x_p, \ldots, x_{p-1})\}$$

$|O((x_1, \ldots, x_p))|$ divide a $|H| = p \Rightarrow |O(x_1, \ldots, x_p))| = 1$ *o* p.

Los elementos con $|O(x_1,\ldots,x_p)|=1$ son precisamente $(x_1,\ldots,x_p)\in Fix(X)$

$$(x_1,\ldots,x_p)\in Fix(X)\Leftrightarrow x_1=x_2=\ldots=x_p$$

Puesto que $(1,1,\ldots,1)\in Fix(X)$ entonces $Fix(X)\neq\emptyset$.

Sabemos también

$$|X|=|Fix(X)|+\sum_{(x_1,\ldots,x_p)\notin Fix(X)}|O((x_1,\ldots,x_p))|$$

Si $(x_1,\ldots,x_p)\notin Fix(X)\Rightarrow|O((x_1,\ldots,x_p))|=p$.
Sea $r=|Fix(X)|$ y $s=$n$^{\underline{o}}$ de elementos $\notin Fix(X)$

$$\left.\begin{array}{c} n^{p-1}=|X|=r+ps\Rightarrow r=n^{p-1}-ps \\ p\mid n \end{array}\right\}\Rightarrow p\mid r\Rightarrow r\geq 2$$

Decir que $r\geq 2$ significa que $\exists(x,x,\ldots,x)\in Fix(X)$ y

$$(x,x,\ldots,x)\neq(1,1,\ldots,1)$$

Entonces como $(x,x,\ldots,x)\in X$, por definición de X, $x\ldots x=x^p=1\quad x\neq 1$. Concluimos pues $\exists x\in X$ tal que $ord(x)=p$

□

Corolario: Sea G un grupo finito no trivial.

$$G\ es\ un\ p-grupo\Leftrightarrow|G|=p^n\quad para\ algun\quad n\geq 1$$

Demostración: $\Leftarrow$) Ejemplo 3.
$\Rightarrow$) Sea $|G|=m\quad(m\geq 1)$
Sea q 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 $ord(x)=p^k\quad k\geq 1$.
Consecuentemente

$$q=p^k\Rightarrow k=1\quad y\quad p=q$$

Si el único divisor primo de m es $p\Rightarrow m=p^n$ para algún $n\geq 1$.

18-5-21

Teorema de Burnside: Sea G un p-grupo finito. Entonces $|Z(G)|\geq p$. En particular, $Z(G)$ no es trivial.

Demostración: Como G es un p-grupo, supongamos

$$|G|=p^n,\quad n\geq 1$$

Si G es abeliano $\Rightarrow Z(G)=G$ y se tendrá 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,

$$|cl(h)| \mid |G| = p^n, \quad entonces \quad |cl(h)| = p^k \quad k > 0$$

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 cual $|Z(G)| = p$ ó $|Z(G)| = p^2$.

Supongamos que $|Z(G)| = p$ entonces $\exists a \in G$ tal que $a \notin Z(G)$.

$$C_G(a) \leq G \qquad C_G(a) = \{g \in G / \ ag = ga\}$$

Es claro que

$$Z(G) \leq C_G(a) \Rightarrow |C_G(a)| = p^2 \Rightarrow C_G(a) = G \Rightarrow a \in Z(G) \downarrow$$

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 $|G| = p^n \quad n \geq 1$.
Hacemos inducción en n.
Si $n = 1$, entonces $|G| = p \Rightarrow G \cong C_p$ y por tanto resoluble, pues todo grupo abeliano es resoluble.

Sea $n > 1$ y el resultado cierto para todo p-grupo de orden estrictamente menor que p^n. Si G es abeliano $\Rightarrow G$ es resoluble y lo tendríamos.
Supongamos G no abeliano

$$1 \lneq Z(G) \lneq G \Rightarrow |Z(G)| = p^k \qquad 1 \leq k < n$$

Por hipótesis de inducción, $Z(G)$ es resoluble. Por otro lado

$$|G/Z(G)| = p^{n-k} \qquad 1 \leq n - k < n$$

y entonces, por hipótesis de inducción $G/Z(G)$ es resoluble

$$\left.\begin{array}{c} Z(G) \trianglelefteq G \quad resoluble \\ G/Z(G) \quad resoluble \end{array}\right\} \Rightarrow G \quad resoluble$$

Definición: Sea G un grupo finito y p un número primo. Un subgrupo H de G que sea p-grupo, lo llamaremos p-subgrupo de G.

Observación: El teorema de Cauchy nos dice que para cada primo p de $|G|$ existe un $H \leq G$, $|H| = p$ y entonces un p-subgrupo.

1º 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 $H \leq G$ 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, $j < i$. Veamos para $i > 1$, $|G| = n$ y $p^i \mid n$ buscamos

$$H \leq G \quad tal\ que \quad |H| = p^i$$

Hacemos inducción sobre $|G|$. 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 estrictamente menor que n, y divisible por p^i.

Caso 1: $\exists K \leq G$ tal que $p \not| [G : K]$.

Como

$$\left.\begin{array}{c} |G| = [G : K]\,|K| \\ p^i \mid |G| \\ p \not| [G : K] \end{array}\right\} \Rightarrow p^i \mid |K|$$

$$\left.\begin{array}{c} p^i \mid |K| \\ K \leq G \Rightarrow |K| < |G| \end{array}\right\} \overset{hip.induccion}{\Rightarrow} \exists H \leq K \quad tal\ que \quad |H| = p^i$$

Claramente $H \leq G$ y se tiene el resultado.

Caso 2: Para todo $K \leq G$, $p \mid [G : K]$

Por la fórmula de las clases

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

$$p \mid |G| \quad y \quad p \mid \sum [G : C_G(h)] \Rightarrow p \mid |Z(G)|$$

Aplicamos el teorema a $Z(G)$ y entonces $\exists N \leq Z(G)$ tal que $|N| = p$. Como $N \leq Z(G) \Rightarrow N \trianglelefteq G$.

$$x \in N \Rightarrow a \cdot x = x \cdot a \quad \forall a \in G \Rightarrow axa^{-1} = x \quad \forall a \in G$$
$$\Rightarrow aNa^{-1} = N \quad \forall a \in G \Rightarrow N \trianglelefteq G$$

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 potencia de p, $\exists L \leq G/N$ tal que $|L| = p^{i-1}$

$$L = H/N \qquad N \trianglelefteq H \trianglelefteq G$$
$$|H/N| = p^{i-1} \Rightarrow |H| = |H/N| \cdot |N| = p^{i-1} \cdot p = p^i$$

□

Definición: Sea G un grupo finito, y p un número primo divisor de $|G|$. Sea p^k la máxima potencia de p que divide a $|G|$ (es decir, $|G| = p^k m$, $p \not| m$). 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 primo divisor de $|G|$.

Ejemplos:

1) $n \geq 2 \quad y \quad C_n = \langle x / x^n = 1 \rangle$.

   Sea $n = p_1^{t_1} p_2^{t_2} \cdot p_k^{t_k}$ la factorización de n en primos.

   Para cada $1 \leq i \leq k$, los p_i-grupos de Sylow tienen orden $p_i^{t_i}$. Sólo hay uno que

$$C_{p_i^{t_i}}) \langle x^{s_i} \rangle \qquad s_i = p_1^{t_1} p_2^{t_2} \cdot p_{i-1}^{t_{i-1}} p_{i+1}^{t_{i+1}} \ldots p_k^{t_k}$$

2) $G = A_4, \quad |A_4| = 12 = 3 \cdot 2^2$.

   Los 3-subgrupos de Sylow de A_4 tienen orden 3 y entonces cíclicos de orden 3.

$$\mathcal{P}_1 = \langle (1\,2\,3) \rangle \qquad \mathcal{P}_2 = \langle (1\,2\,4) \rangle$$
$$\mathcal{P}_3 = \langle (1\,3\,4) \rangle \qquad \mathcal{P}_4 = \langle (2\,3\,4) \rangle$$

   Los 2-subgrupos de Sylow de A_4 tienen orden 4 y sólo tienen 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

$$|G| = p^k m \qquad mcd(m, p) = 1$$

   Entonces $|\mathcal{P}| = p^k$ y por tanto $[G : \mathcal{P}] = m$

$$\Rightarrow mcd(|\mathcal{P}|, [G : \mathcal{P}]) = 1$$

19-5-21

Lema: Sea G un grupo finito y p un número primo divisro de $|G|$ y P un p-subgrupo de Sylow de G.

Sea $H \leq G$ un p-subgrupo de G tal que $H \leq N_G(P)$, entonces $H \leq P$.

Demostración:

$\left.\begin{array}{l} P \trianglelefteq N_G(P) \\ H \leq N_G(P) \end{array}\right.$ Aplicamos el tercer teorema de isomorfía y entonces

$$H/(H \cap P) \cong (HP)/P$$

con lo que $[H : H \cap P] = [HP : P] = r$

$$r \mid |H| \overset{H\ es\ un\ p-grupo}{\Rightarrow} r = p^t \quad t \geq 0$$

Consideramos $P \leq HP \leq G \Rightarrow [G : P] = [G : HP]\,[HP : P] = [G : HP] \cdot r$

$$\left.\begin{array}{c} \Rightarrow r \mid [G : P] \\ Como\ P\ es\ un\ p - subgrupo\ de\ Sylow\ mcd([G : P], |P|) = 1 \end{array}\right\} \Rightarrow mcd(r, p) = 1$$

$$\left.\begin{array}{l} mcd(r, p) = 1 \\ r = p^t \quad t \geq 0 \end{array}\right\} \Rightarrow t = 0 \quad y \quad r = 1$$

Tenemos que $1 = [H : H \cap P] \Rightarrow H = H \cap P \Rightarrow H \leq P$.

□

2º Teorema de Sylow: Sea G un grupo finito y p un número primo divisor de $|G|$. Supongamos

$$|G| = p^k m \quad con \quad mcd(p, m) = 1$$

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 P_1, P_2, son dos p-subgrupos de Sylow de G entonces $\exists g \in G$ tal que $P_2 = gP_2g^{-1}$).

(c) Si $n_p :=$ número de p-subgrupo de Sylow de G, se tiene que

$$n_p \mid m \quad y \quad n_p \equiv 1 \mod p$$

Demostración:

$$S = \{P \leq G/P \quad es\ p - subgrupo\ de\ Sylow\} = \{P \leq G/|P| = p^k\}$$
$$S = \emptyset \quad y \quad |S| = n_p$$

Consideramos la acción de G sobre S por conjugación

$$G \times S \longrightarrow S \qquad g_p := gPg^{-1}$$
$$(|gPg^{-1}| = |P| = p^k \Rightarrow gPg^{-1} \in S)$$

Elegimos $P_1 \in S$ fijo pero arbitrario

$$O(P_1) = \{gP_1g^{-1}/g \in G\} \qquad Stab_G(P_1) = N_G(P_1)$$

Sabemos $|T| = [G : N_G(P_1)]$.
Consideramos

$$P_1 \leq N_G(P_1) \leq G \Rightarrow [G : P_1] = m = [G : N_G(P_1)]\,[N_G(P_1) : P_1] = |T|\,[N_G(P_1) : P_1]$$

Por tanto $|T| \mid m \quad y \quad mcd(p, |T|) = 1$

(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

$$H \times T \longrightarrow T \qquad h_p := hPh^{-1}$$
$$(P \in T \Rightarrow P = gP_1g^{-1} \Rightarrow hPh^{-1} = hgP_1(hg)^{-1} \Rightarrow hPh^{-1} \in T)$$
$$|T| = \sum_{p \in T} |\mathcal{O}(P)| = \sum_{p \in T} [H : Stab_H(P)]$$

Es fácil ver que $Stab_H(P) = H \cap N_G(P)$

$$\left.\begin{array}{c} H \cap N_G(P) \leq N_G(P) \quad P\ p - subgrupo\ de\ Sylow\ de\ G \\ H \cap N_G(P) \leq H \Rightarrow H \cap N_G(P) \quad es\ un\ p - subgrupo\ de\ G \end{array}\right\} \Rightarrow$$
$$\Rightarrow \left.\begin{array}{c} H \cap N_G(P) \leq P \\ H \cap N_G(P) \leq H \end{array}\right\} \Rightarrow H \cap N_G(P) \leq P \cap H$$

y puesto que $P \cap H \leq H \cap N_G(P)$ obviamente $\Rightarrow H \cap N_G(P) = H \cap P$

$$|T| = \sum_{P \in T} [H : H \cap P]$$
$$|T| \mid m \quad [H : H \cap P] \mid |H| = p^r \quad y \quad mcd(p, m) = 1$$

Entonces $\exists P \in T$ tal que $[H : H \cap P] = 1 \Rightarrow H = H \cap P \Rightarrow H \leq P$ lo que demuestra (a).

(b) Sean P_1, P_2, dos p-subgrupos de Sylow de G. Aplicamos (a) a $H = P_2$ y entonces $\exists P \in T = \{gP_1g^{-1}/g \in G\}$ tal que

$$\left.\begin{array}{c} P_2 \leq P \\ |P_2| = p^k = |P| \end{array}\right\} \Rightarrow P_2 = P$$

Por tanto $\exists g \in G$ tal que $P_2 = gP_1g^{-1}$ que es (b).

(c) Por (b), $S = T$, y entonces $n_p = |S| = |T|$ y por tanto $n_p \mid m$. Tomamos $H = P_1$ en (a) y entonces la igualdad

$$|T| = \sum_{P \in T} [H : H \cap P]$$

se traduce en

$$n_p = \sum_{P \in S} [P_1 : P_1 \cap P]$$

Como anteriormente $\exists P \in S$ tal que

$$[P_1 : P_1 \cap P] = 1 \Rightarrow P_1 = P_1 \cap P \Rightarrow P \leq P_1$$

como ambos son de Sylow $|P| = p^k = |P_1| \Rightarrow P = P_1$.

Entonces existe un único $P = P_1 \in S$ tal que

$$[P_1 : P \cap P_1] = 1$$

y para cualquier $P \in S$, $P \neq P_1$, necesariamente $[P_1 : P_1 \cap P] > 1$ y entonces divisible por el número p.

$$n_p = 1 + \sum_{\substack{P \in S \\ P \neq P_1}} [P_1 : P_1 \cap P] \Rightarrow n_p = 1 + pr \Rightarrow n_p = 1 \mod p$$

□

Corolario: En las hipótesis del 2º Teorema de Sylow. Sea P un p-subgrupo de Sylow de G

$$P \trianglelefteq G \Leftrightarrow n_p = 1$$

Demostración: Como gPg^{-1} es p-subgrupo de Sylow de G entonces

$$n_p = 1 \Leftrightarrow gPg^{-1} = P \qquad \forall g \in G \Leftrightarrow P \trianglelefteq G$$

Corolario: Sea G un grupo finito en el que todo sus subgrupos de Sylow son normales. Entonces G es el producto directo interno de sus subgrupos de Sylow.

Demostración. Ejercicio: Sea G un grupo finito, $H_1, \ldots, H_k \quad k \geq 2$, subgrupos normales de G tal que $mcd(|H_i|, |H_j|) = 1$. Entonces

$$|H_1 \ldots H_k| = |H_1| \ldots |H_k|$$

Supongamos que $|G| = p_1^{t_1} p_2^{t_2} \ldots p_k^{t_k}$ su factorización en número primos. Para cada $1 \leq i \leq k$ sea P_i el único p_i-subgrupo de Sylow de G. ($P_i \trianglelefteq G \Rightarrow n_{p_i} = 1$)

1. $P_i \trianglelefteq G \qquad i = 1, \ldots, k$

2. $|P_i| = p_i^{t_i} \qquad 1 \leq i \leq k$

$$mcd(|P_i|, |P_j|) = 1 \quad si \quad i \neq j$$

y entonces por el ejercicio anterior

$$|P_1 P_2 \ldots P_k| = p_1^{t_1} p_2^{t_2} \ldots p_k^{t_k} = |G| \Rightarrow P_1 P_2 \ldots P_k = G$$

3. $(P_1 \ldots P_{i-1}) \cap P_i = 1 \qquad \forall i = 2, \ldots, k.$

En efecto si

$$\left.\begin{array}{c} x \in (P_1 \ldots P_{i-1}) \cap P_i \Rightarrow ord(x) \mid (P_1 \ldots P_{i-1}) = p_1^{t_1} \ldots p_{i-1}^{t_{i-1}} \\ ord(x) \mid |P_i| = p_i^{t_i} \end{array}\right\} \Rightarrow ord(x) = 1 \Rightarrow x = 1$$

Consecuentemente, G es el producto directo interno de $P_1, P_2, \ldots, P_k$. En otros términos

$$G \cong P_1 \times P_2 \times \ldots \times P_k$$

Ejemplo: Si G es un grupo abeliano finito, entonces para p primo divisor de $|G|$, $np = 1$, puesto que todo subgrupo de G es normal.

Además si P es el único p-subgrupo de Sylow de G, este es dado por

$$P = \{x \in G / ord(x) = p^i \quad 0 \leq i \leq k\}$$

siendo p^k la máxima potencia de p que divide a $|G|$ (Ejercicio). P se llama la componente p-primaria de G.

Ejercicio 5 (Relación 5): Hallar todos los subgrupos de Sylow de S_3 y S_4

$$|S_3| = 6 = 2 \cdot 3$$

Los 2-subgrupos de Sylow de S_3 tienen orden 2, y entonces son

$$\langle (1\,2) \rangle, \quad \langle (1\,3) \rangle, \quad \langle (2\,3) \rangle$$

Los 3-subgrupos de Sylow de S_3 tienen orden 3 y sólo hay 1

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

$S_4 \qquad |S_4| = 24 = 3 \cdot 2^3$

Los 3-subgrupos de Sylow de S_4 tienen orden 3 y entonces son

$$P_1 = \langle (1\,2\,3) \rangle, \quad P_2 = \langle (1\,2\,4) \rangle, \quad P_3 = \langle (1\,3\,4) \rangle, \quad P_4 = \langle (2\,3\,4) \rangle$$

Los 2-subgrupos de Sylow de S_4 tienen orden

$$2^3 = 8 \qquad n_2 = n \text{ de subgrupos de Sylow de } G$$

Por el 2º Teorema de Sylow

$$n_2 \mid 3 \quad y \quad n_2 \equiv 1 \mod 2 \Rightarrow n_2 = 1 \ o \ n_2 = 3$$

Si $n_2 = 1$ entonces $\exists! P \leq S_4$ con $|P| = 8$. Sea $(ij) \in S_4$ cualquier trasposición y $H = \langle (i\,j) \rangle$.

Como $|H| = 2$ es un 2-subgrupo de S_4 entonces por (a) del 2º Teorema de Sylow, $H \leq P$. Con lo que $(i\,j) \in P \quad \forall (i\,j) \in S_4 \Rightarrow S_4 \leq P$, pues las trasposiciones generan $S_4 \downarrow$.

Por tanto $n_2 = 3$. Sean Q_1, Q_2, Q_3 los 2-subgrupos de Sylow de S_4

$$|Q_i| = 8 \qquad i = 1, 2, 3$$

Por tanto $i = 1, 2, 3$

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

En efecto puesto que $|K| = 4 = 2^2$, K es un 2-subgrupo de S_4 y entonces por (a) del 2º Teorema de Sylow

$$\exists i \quad tal\ que \quad K \leq Q_i$$

Supongamos $i = 1$, es decir, $K \leq Q_1$. Por (b) del 2º Teorema de Sylow $\exists \sigma, \gamma \in S_4$ tal que

$$Q_2 = \sigma Q_1 \sigma^{-1}, \qquad Q_3 = \gamma Q_1 \gamma^{-1}$$

Sabemos que $K \trianglelefteq S_4$

$$K \leq Q_1 \overset{K \trianglelefteq S_4}{\Rightarrow} \begin{array}{l} K = \sigma K \sigma^{-1} \leq \sigma Q_1 \sigma^{-1} = Q_2 \\ K = \gamma K \gamma^{-1} \leq \gamma Q_1 \gamma^{-1} = Q_3 \end{array}$$

Tenemos pues determinado cuatro elementos en cada Q_i. Para buscar los otros cuatro, razonamos como sigue. Sea $\tau \in S_4$ una trasposición. Aplicamos el 3º Teorema de isomorfía

$$\left.\begin{array}{c} K \trianglelefteq S_4 \\ H = \langle \tau \rangle \leq S_4 \end{array}\right\} \Rightarrow H/(K \cap H) \cong (KH)/K$$

Como

$$\begin{array}{c} K \cap H = \{id\} \\ H = \{id, \tau\} \end{array} \quad , \quad entonces \quad H \cong (KH)/K$$

$$|(KH)/K| = |H| \Rightarrow |KH| = |K||H| = 4 \cdot 2 = 8$$

Por tanto, multiplicamos K por $\langle \tau \rangle$ y obtenemos los 2-subgrupos de Sylow

$$\begin{aligned} Q_1 = K\langle (1\,2) \rangle = \{&id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), \\ &, (1\,2), (3\,4), (1\,3\,2\,4), (1\,4\,2\,3)\} \\ Q_2 = K\langle (1\,3) \rangle = \{&id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), \\ &, (1\,3), (2\,4), (1\,2\,3\,4), (1\,4\,3\,2)\} \\ Q_3 = K\langle (1\,4) \rangle = \{&id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), \\ &, (1\,4), (2\,3), (1\,2\,4\,3), (1\,3\,4\,2)\} \end{aligned}$$

Ejercicio 21 (Relación 5): Demostrar que D_4 es isomorfo a los 2-subgrupos de Sylow de S_4.
Pista: Considerar la representación asociada a la acción de D_4 sobre los vértices del cuadrado

$$D_4 = \langle r, s / r^4 = 1 = s^2, \quad sr = r^{-1}s \rangle$$

$$\phi : D_4 \longrightarrow S_4 \qquad \begin{array}{c} \phi(r^i) = (1\,2\,3\,4)^i \qquad 0 \leq i \leq 3 \\ \phi(r^i s) = (1\,2\,3\,4)^i (2\,4) \qquad 0 \leq i \leq 3 \end{array}$$

ϕ es un monomorfismo

$$D_4 / Ker(\phi) \cong Img(\phi)$$

Como $Ker(\phi) = 1$, $D_4 \cong Img(\phi) \Rightarrow |D_4| = |Img(\phi)|$. $Img(\phi)$ es un 2-subgrupo de Sylow de S_4 (concretamente, $Img(\phi) = Q_2$)

$$D_4 \cong Q_2 \quad y\, entonces\, como \qquad \begin{array}{c} Q_2 \cong Q_1 \\ Q_2 \cong Q_3 \end{array}$$

Se concluye el ejercicio.

24-5-21

Ejercicio 23 (Relación 5): G con $|G| = 12$ y con $n_3 > 1$. Demostrar que $G \cong A_4$.

$|G| = 12 = 3 \cdot 2^2$

Sea $\mathcal{P}$ un 3-subgrupo de Sylow de G, $|\mathcal{P}| = 3$, y $\mathcal{P}$ es un subgrupo no normal en G (pues $n_3 > 1$).

Se considera $G/\mathcal{P} = \{x\mathcal{P} / x \in G\}$ conjunto, y se considera la acción por traslación

$$G \times G/\mathcal{P} \longrightarrow G/\mathcal{P} \qquad g_{(x\mathcal{P})} = (gx)\mathcal{P}$$

Consideramos la representación asociada

$$\phi : G \longrightarrow S(G/\mathcal{P}) \quad homomorfismo$$

$$g \longmapsto \begin{array}{c} \phi(g) \\ \phi(g)(x\mathcal{P}) = g_{x\mathcal{P}} = (gx)\mathcal{P} \end{array}$$

$$Ker(\phi) = \{g \in G / \phi(g) = id_{G/\mathcal{P}}\} = \{g \in G / \phi(g)(x\mathcal{P}) = x\mathcal{P} \quad \forall x \in G\} =$$
$$= \{g \in G / g_{x\mathcal{P}} = x\mathcal{P} \quad \forall x \in G\} = \{g \in G / (gx)\mathcal{P} = x\mathcal{P} \quad \forall x \in G\}$$

Veamos $Ker(\phi) \leq \mathcal{P}$. Sea $g \in Ker(\phi) \Rightarrow (gx)\mathcal{P} = x\mathcal{P} \quad \forall x \in G$. En particular, considerando $x = 1$, será

$$g\mathcal{P} = \mathcal{P} \Rightarrow g \in \mathcal{P}$$

Por tanto

$$\left.\begin{array}{c} Ker(\phi) \leq \mathcal{P} \\ |\mathcal{P}| = 3 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} Ker(\phi) = \{1\} \\ Ker(\phi) = \mathcal{P} \end{array}\right.$$

Como $Ker(\phi) \trianglelefteq G$ y $\mathcal{P} \not\trianglelefteq G \Rightarrow Ker(\phi) \neq \mathcal{P}$. Entonces $Ker(\phi) = \{1\}$

$$\phi : G \longrightarrow S(G/\mathcal{P}) \quad es\, monomorfismo \Rightarrow G \cong Img(\phi)$$
$$|G/X| = [G : \mathcal{P}] = \frac{|G|}{|\mathcal{P}|} = \frac{12}{3} = 4 \Rightarrow S(G/\mathcal{P}) \cong S_4$$

$Img(\phi)$ es isomorfo a un subgrupo de S_4 de orden 12 y entonces $Img(\phi) \cong A_4$. Considerando ambos isomorfismos obtenemos

$$G \cong A_4$$

Ejercicio 26 (Relación 5):

1) Demostrar que no existen grupos simples de orden 28.

2) Demostrar que todo grupo de orden 28 es resoluble.

Resolución: G con $|G| = 28 = 7 \cdot 2^2$

$$n_7 \mid 4 \quad y \quad n_7 \equiv 1 \mod 7 \Rightarrow n_7 = 1$$

Si $n_7 = 1 \Rightarrow \exists \mathcal{P} \trianglelefteq G$ tal que $|\mathcal{P}| = 7$. En particular G no es simple.

2) $$\left.\begin{array}{c} \mathcal{P} \trianglelefteq G \quad y \quad |\mathcal{P}| = 7 \Rightarrow \mathcal{P} \quad es\, resoluble \\ |G/\mathcal{P}| = 4 \Rightarrow G/\mathcal{P} \quad es\, un\, 2-grupo \Rightarrow G/\mathcal{P} \quad resoluble \end{array}\right\} \Rightarrow G \quad resoluble$$

Ejercicio 25 (Relación 5):

1) Demostrar que todo grupo de orden 12 admite un subgrupo normal de orden 3 o un subgrupo normal de orden 4. En particular, no es simple.

2) Demostrar que todo grupo de orden 12 es resoluble.

Resolución: G con $|G| = 12 = 3 \cdot 2^2$

$$n_3 \mid 4 \quad y \quad n_3 \equiv 1 \mod 3 \Rightarrow n_3 = 1 \quad o \quad n_3 = 4$$

Si $n_3 = 1 \quad \exists! \mathcal{P} \trianglelefteq G$ tal que $|\mathcal{P}| = 3$ estaría hecho.
Si $n_3 = 4$ veamos que $n_2 = 1$.
Sean $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4$ los 3-subgrupos de Sylow de G

$$\mathcal{P}_\rangle \neq \mathcal{P}_j \quad \forall i \neq j \qquad |\mathcal{P}_i| = 3 \quad \forall i = 1, 2, 3, 4$$

Se tiene además que $\mathcal{P}_i \cap \mathcal{P}_j = \{1\} \quad \forall i \neq j$ porque

$$\left.\begin{array}{c} \mathcal{P}_i \cap \mathcal{P}_j \leq \mathcal{P}_i \\ |\mathcal{P}_i| = 3 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} \mathcal{P}_i \cap \mathcal{P}_j = \{1\} \\ \mathcal{P}_i \cap \mathcal{P}_j = \mathcal{P}_i \Rightarrow \mathcal{P}_j \leq \mathcal{P}_i \Rightarrow \mathcal{P}_j = \mathcal{P}_i \downarrow \end{array}\right.$$

Luego $\mathcal{P}_i \cap \mathcal{P}_j = \{1\}$. Todos los elementos de cada $\mathcal{P}_i$ no triviales tienen orden 3, para cada $i = 1, 2, 3, 4$.

Consideramos el conjunto

$$\cup_{i=1}^{4}\mathcal{P}_i - \{1\}$$

dicho conjunto tiene exactamente 8 elementos, todos ellos de orden 3. De hecho en dicho conjunto están todos los elementos del grupo G de orden 3.

Nos quedan entonces $12-8=4$ elementos de G cuyo orden es 3. Como ha de existir un 2-grupo de Sylow $Q \trianglelefteq G$ y entonces

$$\exists Q \leq G \quad con \quad |Q| = 4$$

Combinando ambos hechos $\exists! Q \trianglelefteq G$ con $|Q|=4$, es decir, $n_2 = 1$.

2) $|G| = 12 \Rightarrow G$ resoluble.

Por (1) $\exists \mathcal{P} \trianglelefteq G$ con $|\mathcal{P}| = 3$ ó $\exists Q \trianglelefteq G$ con $|Q| = 4$.

En el primer caso

$$\left.\begin{array}{c} \mathcal{P} \trianglelefteq G \quad |\mathcal{P}| = 3 \Rightarrow \mathcal{P} \quad resoluble \\ |G/\mathcal{P}| = 4 \Rightarrow G/\mathcal{P} \quad es\ un\ 2-grupo \Rightarrow G/\mathcal{P} \quad resoluble \end{array}\right\} \Rightarrow G \quad resoluble$$

En el segundo caso

$$\left.\begin{array}{c} Q \trianglelefteq G \quad con \quad |Q| = 4 \Rightarrow Q \quad resoluble \\ |G/Q| = 3 \Rightarrow G/Q \quad resoluble \end{array}\right\} \Rightarrow G \quad resoluble$$

Ejercicio 30 (Relación 5): Demostrar que todo grupo de orden 24 es resoluble. Sea G con

$$|G| = 24 = 8 \cdot 3 = 2^3 \cdot 3$$
$$n_3 \mid 8 \quad y \quad n_3 \equiv 1 \mod 3 \Rightarrow n_3 = 1 \quad o \quad n_3 = 4$$

Si $n_3 = 1 \Rightarrow \exists! \mathcal{P} \trianglelefteq G$ con $|\mathcal{P}| = 3$ y por tanto resoluble.

Como $|G/\mathcal{P}| = 8 = 2^3 \Rightarrow$ es un 2-grupo, luego es resoluble $\Rightarrow$ concluimos pues que G es resoluble.

Si $n_3 = 4$. Sean $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4$ los 3-subgrupos de Sylow

$$|\mathcal{P}_i| = 3 \qquad \forall i = 1,2,3,4$$
$$\mathcal{P}_i \cap \mathcal{P}_j = \{1\} \qquad \forall i \neq j$$

Sea $X = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4\}$ y

$$G \times X \longrightarrow X \qquad g_{\mathcal{P}_i} = g\mathcal{P}_i g^{-1} \quad \forall i = 1,2,3,4$$

La representación asociada es un homomorfismo

$$\phi : G \longrightarrow S(X) \cong S_4$$
$$Ker(\phi) = \{g/\phi(g) = Id_X\} = \{g \in G/\phi(g)(\mathcal{P}_i) = \mathcal{P}_i \quad \forall i = 1,2,3,4\} =$$
$$= \{g \in G/g\mathcal{P}_i g^{-1} = \mathcal{P}_i \quad \forall i = 1,2,3,4\}$$

Como $\mathcal{P}_i$ no es normal en G ($n_3 = 4 > 1$) entonces

$$\left.\begin{array}{c} Ker(\phi) \lneq G \\ |G| = 24 \end{array}\right\} \Rightarrow |Ker(\phi)| \in \{1, 2, 3, 4, 6, 8, 12\}$$

$\Rightarrow Ker(\phi)$ es resoluble.

$$G/Ker(\phi) \cong Img(\phi) \leq S_4$$

S_4 resoluble $\Rightarrow Img(\phi)$ es resoluble (pues todo subgrupo de un grupo resolubles es resoluble).

25-5-21

Ejercicio 32 (Relación 5): Si G es un grupo de orden 30 entonces $n_3 = 1$ ó $n_5 = 1$. Concluir que G es resoluble.

$$|G| = 30 = 2 \cdot 3 \cdot 5$$
$$n_3 \mid 10 \quad y \quad n_3 \equiv 1 \mod 3 \Rightarrow n_3 = 1 \quad o \quad n_3 = 10$$
$$n_5 \mid 6 \quad y \quad n_5 \equiv 1 \mod 5 \Rightarrow n_5 = 1 \quad o \quad n_5 = 6$$

Supongamos que $n_3 > 1$ y $n_5 > 1$.

Si $n_3 > 1 \Rightarrow n_3 = 10$. Sean $\{\mathcal{P}_i\}_{i=1,\ldots,10}$ los 3-subgrupos de Sylow. Como $|\mathcal{P}_i| = 3 \quad \forall i$, entonces $\mathcal{P}_i \cap \mathcal{P}_j = \{1\} \quad \forall i \neq j$.

Por tanto en $\cup_{i=1}^{10} \mathcal{P}_i - \{1\}$ hay 20 elementos de orden 3.

Si $n_5 > 1 \Rightarrow n_5 = 6$. Sea $\{\mathcal{Q}_j\}_{j=1,\ldots,5}$ los 5-subgrupos de Sylow. Como $|\mathcal{Q}_i| = 5 \quad \forall i$, entonces $\mathcal{Q}_j \cap \mathcal{Q}_r = \{1\} \quad \forall j \neq r$.

Por tanto, en $\cup_{j=1}^{6} \mathcal{Q}_j - \{1\}$ hay 24 elementos de orden 5. Entonces

$$|G| \geq 20 + 24 = 44 \downarrow$$

$n_3 = 1 \quad o \quad n_5 = 1$. Si $n_3 = 1 \Rightarrow \exists! \mathcal{P} \trianglelefteq G$ con $|\mathcal{P}| = 3$ (resoluble)

$$|G/\mathcal{P}| = 10 \quad (resoluble) \Rightarrow G \quad resoluble$$

Si $n_5 = 1 \Rightarrow \exists! \mathcal{Q} \trianglelefteq G$ con $|\mathcal{Q}| = 5$ (resoluble)

$$|G/\mathcal{Q}| = 6 \quad (resoluble) \Rightarrow G \quad (resoluble)$$

Ejercicios 35, 36 y 37 (Relación 5):

(a) Demostrar que todo grupo de orden $p \cdot q$, con p y q primos distintos, es resoluble

$$|G| = pq \quad supongamos \quad p > q$$

Sabemos que

$$n_p \mid q \quad y \quad n_p \equiv 1 \mod p \Rightarrow n_p = 1$$

Si $n_p = q$ entonces $q \equiv 1 \mod p$, es decir,

$$q = 1 + kp \quad \textit{en contradiccion con que} \quad p > q$$

Por tanto $n_p = 1$ y con ello se deduce que G es resoluble.

(b) Si $|G| = p^2 q$ con p y q primos distintos G es resoluble.

Caso 1: $p > q$ entonces razonando como en (a) $n_p = 1$ y G es resoluble.

Caso 2: $p < q$

$$n_q \mid p^2 \quad y \quad n_q \equiv 1 \mod q$$

$n_q \neq p$ pues $p < q$. Luego $n_q = 1 \quad o \quad n_q = p^2$.
Si $n_q = 1 \Rightarrow \exists! \mathcal{Q} \trianglelefteq G \quad |\mathcal{Q}| = q$ y por lo tanto resoluble. Como $|G/\mathcal{Q}| = p^2$ (resoluble por ser un p-grupo) $\Rightarrow G$ es resoluble.

Si $n_q = p^2$, sea $\{\mathcal{P}_i\}_{i=1,\ldots,p^2}$ los q-subgrupos de Sylow de G.

$$|\mathcal{P}_i| = q \quad \forall i \quad y \textit{ entonces} \quad \mathcal{P}_i \cap \mathcal{P}_j = \{1\}$$

Entonces en $\cup_{i=1}^{p^2} \mathcal{P}_i - \{1\}$ hay $p^2(q-1)$ elementos de orden q. Como $|G| = p^2 q$, nos quedan

$$p^2 q - p^2(q-1) = p^2$$

en el grupo de G, que son los que forman el único p-subgrupo de Sylow de G.
Así $n_p = 1 \Rightarrow G$ es resoluble.

(c) Demostrar que si $|G| = p_1 p_2 p_3$, p_1, p_2, p_3 primos distintos tales que $p_3 > p_1 p_2$, en ese caso G es resoluble

$$n_{p_3} \mid p_1 p_2 \quad y \quad n_{p_3} \equiv 1 \mod p_3$$

Veamos que necesariamente $n_{p_3} = 1$.

$$\begin{aligned} Si \quad n_{p_3} = p_1 \Rightarrow p_1 \equiv 1 \mod p_3 \Rightarrow p_1 = 1 + kp_3 \\ \Rightarrow p_1 p_2 = p_2 + kp_3 p_2 \Rightarrow p_1 p_2 > p_3 \downarrow \end{aligned}$$

De la misma forma se demuestra $n_{p_3} \neq p_2$.

$$\begin{aligned} &Si \quad n_{p_3} = p_1 p_2 \Rightarrow p_1 p_2 \equiv 1 \mod p_3 \Rightarrow p_1 p_2 = 1 + tp_3 \Rightarrow p_1 p_2 > p_3 \downarrow \\ &Si \quad n_{p_3} = 1 \Rightarrow \exists! \mathcal{Q} \trianglelefteq G \quad tal\ que \quad |\mathcal{Q}| = p_3 \quad como \quad |G/\mathcal{Q}| = p_1 p_2 \Rightarrow \\ &\overset{(a)}{\Rightarrow} |G/\mathcal{Q}| \quad resoluble \Rightarrow G \quad resoluble \end{aligned}$$

Ejercicio 4 (Relación 5): Sea G un p-grupo y X un G-conjunto finito. Demostrar que $|X| = |Fix(X)| \mod p$

Supongamos que $X/\sim = \{O(x_1), \ldots, O(x_n)\}$

$$|X| = |Fix(X)| + \sum_{x_i \notin Fix(X)} |O(x_i)| = |Fix(X)| + \sum_{x_i \notin Fix(X)} [G : Stab_G(x_i)]$$

$$x_i \notin Fix(X) \Leftrightarrow |O(x_i)| > 1 \Leftrightarrow [G : Stab_G(x_i)] > 1$$

$$[G : Stab_G(x_i)] \mid |G| = p^k \quad k \geq 1 \Rightarrow [G : Stab_G(x_i)] = p^r \quad 0 < r \leq k$$

Por tanto, $p \mid \sum_{x_i \notin Fix(X)} [G : Stab_G(x_i)]$

$$|X| = |Fix(X)| + ps \quad s \in \mathbb{N} \Rightarrow |X| = |Fix(X)| \mod p$$

Ejercicio 11 (Relación 5): Un subgrupo $G \leq S_n$ se dice transitivo si la acción de G sobre $X = \{1, 2, \ldots, n\}$ es transitiva.

$$S_n \times \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$$
$$\sigma_i := \sigma(i)$$

$G \leq S_n$, podemos considerar la acción de G sobre X por restricción de la anterior

$$G \times X \longrightarrow X \qquad \sigma_i := \sigma(i) \qquad \begin{matrix} \forall \sigma \in G \\ \forall i \in X \end{matrix}$$

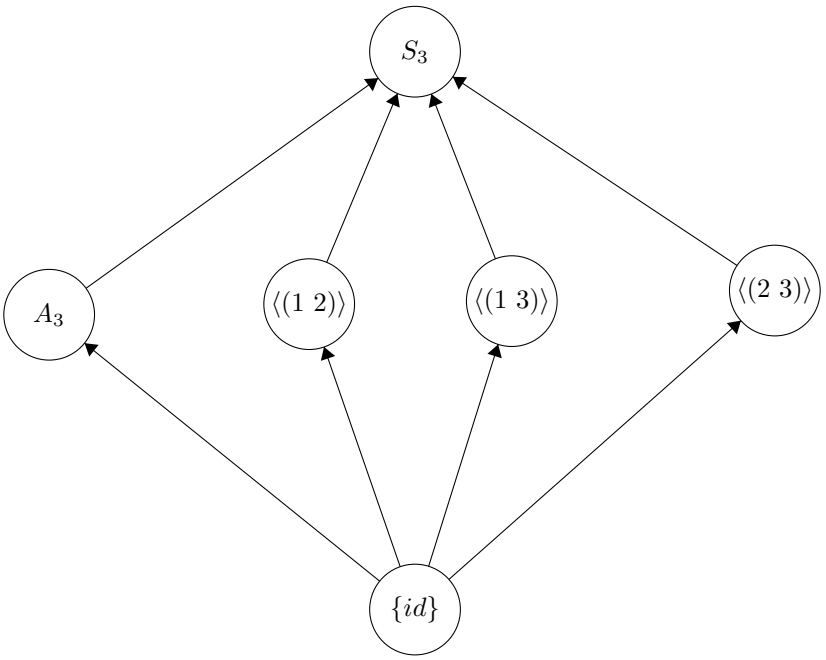
Decir que dicha acción es transitiva es decir que tiene una única órbita. En otros términos

$$O(i) = O(j) = X \qquad \forall i, j \in X$$
$$O(i) = \{\sigma_i / \sigma \in G\} = \{\sigma(i) / \sigma \in G\}$$

Entonces, decir que G es transitiva es equivalente a decir que

"*para cualesquiera* $\quad i, j \in X = \{1, 2, \ldots, n\}, \quad \exists \sigma \in G \quad$ *tal que* $\quad \sigma(i) = j$"

Encontrar los subgrupos transitivos de S_3 y S_4.



$S_3 \leq S_3$ transitivo claramente.
$A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$ también transitivo.

$$O(1) = \{\sigma_1/\sigma \in A_3\} = \{\sigma(1)/\sigma \in A_3\} = \{1,2,3\} = O(2) = O(3)$$
$$\langle(1\ 2)\rangle = \{id, (1\ 2)\} \quad no\ es\ transitiva$$
$$O(1) = \{\sigma(1)/\sigma \in \langle(1\ 2)\rangle\} = \{1,2\} = O(2)$$
$$O(3) = \{\sigma(3)/\sigma \in \langle(1\ 2)\rangle\} = \{3\}$$

De la misma forma se ve que $\langle(1\ 2)\rangle$, $\langle(2\ 3)\rangle$ tampoco son transitivas.

26-5-21

Ejercicio 12 (Relación 5): Sea G un grupo finito y $H \leq G$ subgrupo tal que $[G : H] = p$ siendo p el menor primo que divide al orden de G. Demuestre que $H \trianglelefteq G$.

1) $G/H = \{xH/x \in G\}$

$$G \times G/H \longrightarrow G/H \qquad g_{(xH)} := (gx)H$$
$$\rho : G \longrightarrow S(G/H) \quad la\ representacion\ asociada.$$

Veamos que $Ker(\rho) \leq H$

$$Ker(\rho) = \{g \in G/\rho(g) := id_{G/H}\} = \{g \in G/\rho(g)(xH) = xH \quad \forall x \in G\} =$$
$$= \{g \in G/(gx)H = xH \quad \forall x \in G\}$$

Si $g \in Ker(\rho) \Rightarrow (gx)H = xH \quad \forall x.$

En particular, para $x = 1$

$$gH = H \Rightarrow g \in H$$

2) Probar $[G : Ker(\rho)] \mid p!$

Por el 1º Teorema de isomorfía tenemos que

$$\left.\begin{array}{c} G/Ker(\rho) \cong Img(\rho) \qquad [G : Ker(\rho)] = |Img(\rho)| \\ Img(\rho) \leq S(G/H) \cong S_p \\ |G/H| = [G : H] = p \end{array}\right\} \Rightarrow |Img(\rho)| \mid p!$$

Consecuentemente $[G : Ker(\rho)] \mid p!$

3) $Ker(\rho) \leq H$

Probar que $[H : Ker(\rho)] \mid (p-1)!$. Consideramos

$$Ker(\rho) \leq H \leq G \Rightarrow [G : Ker(\rho)] = [G : H]\,[H : Ker(\rho)]$$

Como $[G : Ker(\rho)] \mid p!$ por 2)$\Rightarrow$

$$\begin{array}{c} \Rightarrow p! = [G : Ker(\rho)]\,k \qquad k \in \mathcal{Z} \Rightarrow \\ \Rightarrow p! = p \cdot [H : Ker(\rho)] \cdot k \Rightarrow (p-1)! = [H : Ker(\rho)]\,k \Rightarrow \\ \Rightarrow [H : Ker(\rho)] \mid (p-1)! \end{array}$$

4) Concluid que $[H : Ker(\rho)] = 1$

Si no fuera 1, elegimos un primo q tal que $q \mid [H : Ker(\rho)]$

$$[H : Ker(\rho)] \mid |H| \Rightarrow q \mid |H| \Rightarrow q \mid |G|$$

Como, por el apartado 3)

$$[H : Ker(\rho)] \mid (p-1)!$$

por transitividad

$$\left.\begin{array}{c} [H : Ker(\rho)] \mid (p-1)! \\ q \mid [H : Ker(\rho)] \end{array}\right\} \Rightarrow q \mid (p-1)!$$

$\Rightarrow \begin{array}{c} q < p \\ q \mid |G| \end{array}$ con que p es el menor primo que divide a $|G|$.

$H \trianglelefteq G$ pues el núcleo es siempre normal en el dominio de ρ.

Ejercicio 14 (Relación 3): Sea G un p-grupo y $H \trianglelefteq G$ tal que $|H| = p$. Demostrar que $H \leq Z(G)$.

Resolución: $|G| = p^n \qquad n \geq 1$

$$H \trianglelefteq G \quad y \quad |H| = p$$

Como $H \trianglelefteq G \Rightarrow gHg^{-1} = H \quad \forall g \in G$.
Entonces podemos considerar la acción por conjugación de G sobre H

$$G \times H \longrightarrow H \qquad g_h := ghg^{-1}$$

Entonces

$$|H| = |Fix(H)| + \sum_{h \notin Fix(H)} [G : Stab_G(h)]$$

$$h \notin Fix(H) \Rightarrow \left.\begin{array}{c} [G : Stab_G(h)] > 1 \\ [G : Stab_G(h)] \mid G = p^n \end{array}\right\} \Rightarrow [G : Stab_G(h)] = p^r \qquad r \geq 1$$

Consecuentemente $p \mid \sum_{h \notin Fix(H)} [G : Stab_G(h)]$, y como $|H| = p$, entonces

$$p \mid |Fix(H)|$$
$$h \in Fix(H) \Leftrightarrow O(h) = \{h\} \Leftrightarrow \{ghg^{-1}/g \in G\} = \{h\} \Leftrightarrow$$
$$\Leftrightarrow ghg^{-1} = h \quad \forall g \in G \Leftrightarrow gh = hg \quad \forall g \in G \Leftrightarrow h \in Z(G)$$

Por tanto $Fix(H) = H \cap Z(G)$

$$\left.\begin{array}{c} p \mid |H \cap Z(G)| \\ H \cap Z(G) \leq H \Rightarrow |H \cap Z(G)| \mid |H| = p \end{array}\right\} \Rightarrow |H \cap Z(G)| = p = |H| \Rightarrow H \cap Z(G) = H$$

En particular, $H \leq Z(G)$

Ejercicio 17 (Relación 5): Sea G un p-grupo con $|G| = p^n$. Demostrad que para cada k, $0 \leq k \leq n$, existe $H \trianglelefteq G$ tal que $|H| = p^k$

$$|G| = p^n \qquad n \geq 1$$

Hacemos inducción en n.
Si $n = 1$ entonces $|G| = p$

$$Para \quad k = 0 \quad tenemos \quad H = \{1\} \trianglelefteq G$$
$$Para \quad k = 1 \quad tenemos \quad H = G \trianglelefteq G$$

y se tiene el resultado.

Supuesto cierto para n, veamoslo para $n + 1$

$$|G| = p^{n+1}$$

Por el Teorema de Burnside $|Z(G)| \geq p$, y entonces $|Z(G)| = p^s \quad 1 \leq s \leq n+1$.
Por el Teorema de Cauchy $\exists N \leq Z(G)$ con $|N| = p$

$$\left.\begin{array}{c} N \leq G \\ N \trianglelefteq Z(G) \end{array}\right\} N \trianglelefteq G$$

Consideramos G/N

$$|G/N| = \frac{|G|}{|N|} = \frac{p^{n+1}}{p} = p^n$$

Entonces, por hipótesis de inducción, para cada $0 \leq k \leq n$, $\exists L \trianglelefteq G/N$ tal que

$$|L| = p^k$$
$$L \trianglelefteq G/N \Rightarrow L = H/N \quad con \quad N \trianglelefteq H \trianglelefteq G$$
$$p^k = |L| = \frac{|H|}{|N|} \Rightarrow |H| = p^{k+1}$$

Si $0 \leq k \leq n \Rightarrow 1 \leq k+1 \leq n+1$.
Para $k = 0$, tenemos $H = \{1\} \trianglelefteq G$ y $|H| = p^0 = 1$.

Ejercicio 19 (Relación 5): Sea G un p-grupo de orden p^n $(n \geq 1)$. Demostrar que

$$l(G) = n \quad y \quad fact(G) = \{\overbrace{C_p, \ldots, C_p}^{n}\}$$

Resolución:

$$|G| = p^n \Rightarrow \exists H_{n-1} \trianglelefteq G \quad tal\ que \quad |H_{n-1}| = p^{n-1}$$
$$|H_{n-1}| = p^{n-1} \Rightarrow \exists H_{n-2} \trianglelefteq H_{n-1} \quad tal\ que \quad |H_{n-2}| = p^{n-2}$$
$$\vdots$$
$$|H_2| = p^2 \Rightarrow \exists H_1 \trianglelefteq H_2 \quad tal\ que \quad |H_1| = p$$

Obtenemos entonces una serie normal propio

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_{n-2} \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

sus factores $|H_i/H_{i-1}| = |H_i|/|H_{i-1}| = p^i/p^{i-1} = p \qquad \forall i = 1, \ldots, n$

$$\Rightarrow H_i/H_{i-1} \cong C_p \quad es\ simple \quad \forall i = 1, \ldots, n$$

Por tanto la serie anterior es una serie de composición. Entonces

$$l(G) = n \quad y \quad fact(G) = \{\overbrace{C_p, \ldots, C_p}^{n}\}$$

6. Tema 7: Clasificación de grupos abelianos finitos.

Usaremos dos resultados fundamentales

(1) $C_n \times C_m \cong C_{nm} \Leftrightarrow mcd(n,m) = 1$

(2) Si G es un grupo finito con $|G| = p_1^{n_1} \dots p_k^{n_k}$ y $n_{p_i} = 1 \quad \forall i = 1, \dots, k$ entonces

$$G \cong P_1 \times P_2 \times \ldots \times P_k$$

Proposición: Sea G un p-grupo abeliano con $|A| = p^n \quad (n \geq 1)$. Entonces existen enteros $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1$ tal que

$$\beta_1 + \beta_2 + \ldots + \beta_t = n \quad y \quad A \cong C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \ldots \times C_{p^{\beta_t}}$$

Además esta expresión única (salvo en orden). Esto es, si

$$A \cong C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \ldots \times C_{p^{\alpha_s}}$$

donde $\alpha_1 \geq \alpha_2 \geq \ldots \geq s \geq 1$ y $\alpha_1 + \alpha_2 + \ldots + \alpha_s = n$, entonces

$$s = t \quad y \quad \alpha_i = \beta_i \qquad \forall i = 1, \dots, t$$

Demostración: Existencia (esquema).
A abeliano y $|A| = p^n \quad n \geq 1$.
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 estrictamente menor que p^n. Consideramos

$$\varphi : A \longrightarrow A \qquad \varphi(x) = x^p$$

Como A es abeliano, entonces φ es un homomorfismo de grupos. Sean

$$K = Ker(\varphi) = \{x \in A / x^p = 1\} \quad y \quad H = Img(\varphi) = \{x^p / x \in A\}$$

Por el teorema de Cauchy, $\exists x \in A$ con $ord(x) = p$, es decir, $\exists x \in L$, $x \neq 1$. Por tanto, $K \neq 1$.
Además se tiene

- Por definición K y A/H son p-grupos abelianos finitos elementales.

$$(xH \in A/H \Rightarrow (xH)^p = x^p H \overset{x^p \in H}{=} H)$$

- Por el 1º teorema de isomorfía

$$A/K \cong H \Rightarrow [A : K] = |H|$$

- $|A/H| = \frac{|A|}{|H|} = \frac{|A|}{[A:K]} = |K| \Rightarrow$

$$[A : H] = |K| > 1 \Rightarrow H < A$$

Entonces H es un p-grupo con $|H| = p^m$ siendo $m < n$. Por hipótesis de inducción existen

$$\gamma_1 \geq \gamma_2 \geq \ldots \geq \gamma_r \geq 1 \quad con \quad \gamma_1 + \gamma_2 + \ldots + \gamma_r = m$$

y

$$H \cong C_{p^{\gamma_1}} \times C_{p^{\gamma_2}} \times \ldots \times C_{p^{\gamma_r}}$$

Para cada $i = 1, 2, \ldots, r$ sean $h_i \in H$ tal que

$$\langle h_i \rangle \cong C_{p^{\gamma_i}}$$

Notemos que $H \cong \langle h_1 \rangle \times \langle h_2 \rangle \times \ldots \times \langle h_r \rangle$. Puesto que

$$H = Img(\varphi) = \{x^p / x \in A\} \quad para\, cada \quad i = 1, \ldots, r$$

elegimos $g_i \in A$ tal que $\varphi(g_i) = g_i^p = h_i$.
Notemos que, puesto que $ord(h_i) = p^{\gamma_i} \Rightarrow$

$$\Rightarrow ord(g_i) = p^{\gamma_i + 1}$$

Consideramos el siguiente subgrupo de A

$$A_0 := \langle g_1, g_2, \ldots, g_r \rangle \leq A$$

Se verifica

(a) $A_0 \cong \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle$

$$(\Rightarrow |A_0| = \prod_{i=1}^{r} ord(g_i) = \prod_{i=1}^{r} p^{\gamma_i + 1} = p^{\sum_{i=1}^{r} \gamma_i + r} = p^{m+r}$$

(b) $A_0/H \cong \langle g_1 H \rangle \times \langle g_2 H \rangle \times \ldots \times \langle g_r H \rangle$.

A_0/H es un p-grupo abeliano elemental y $|A_0/H| = p^r$

(c)

$$H \cap K \cong \langle K_1 \rangle \times \langle K_2 \rangle \times \ldots \times \langle K_r \rangle \quad donde$$
$$K_i = h_i^{p^{\gamma_i - 1}} \quad i = 1, \ldots, r$$

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: $K \leq H \Rightarrow H \cap K = K \overset{(c)}{\Rightarrow} |K| = p^r$

$$\left.\begin{array}{cc} Como & [A:H] = |K| = p^r \\ Por\ (b) & [A_0:H] = p^r \end{array}\right\} \Rightarrow [A:H] = [A_0:H] \Rightarrow A = A_0$$

Por (a)

$$A \cong \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \langle g_r \rangle \cong C_{p^{\gamma_1+1}} \times C_{p^{\gamma_2+1}} \times \ldots \times C_{p^{\gamma_r+1}}$$

Entonces hemos encontrado

$$\beta_1 = \gamma_1 + 1 \geq \beta_2 = \gamma_2 + 1 \geq \ldots \geq \beta_r = \gamma_r + 1$$

y

$$\beta_1 + \beta_2 + \ldots + \beta_r = \gamma_1 + \ldots + \gamma_r + r = m + r = n$$

pues $A = A_0 \Rightarrow \left.\begin{array}{c} |A| = p^n \\ |A_0| = p^{m+r} \end{array}\right\} \Rightarrow n = m + r$

Caso 2: K no es un subgrupo de H.

Elegimos $x \in K - H$ ($\Rightarrow ord(x) = p$)

$$\left.\begin{array}{cc} xH \in A/H & xH \neq H \\ A/H & es\ elemental \end{array}\right\} \Rightarrow ord(xH) = p$$

Aplicamos el lema siguiente a A/H y a $xH \in A/H$ entonces

$$\exists \mathcal{M}/H \leq A/H \quad tal\ que \quad A/H \cong \mathcal{M}/H \times \langle xH \rangle$$

Es fácil ver que entonces

$$A \cong \mathcal{M} \times \langle x \rangle$$
$$|A| = p^n \quad y \quad |\langle x \rangle| = ord(x) = p \Rightarrow |\mathcal{M}| = p^{n-1}$$

Por hipótesis de inducción

$$\exists \beta_1 \geq \beta_2 \geq \ldots \beta_t \geq 1 \quad tal\ que$$
$$\beta_1 + \beta_2 + \ldots + \beta_t = n - 1$$
$$\mathcal{M} \cong C_{p^{\beta_1}} \times \ldots \times C_{p^{\beta_t}}$$

Entonces tomando $\beta_{t+1} = 1$ se tiene un partición de n

$$A \cong \mathcal{M} \times \langle x \rangle \cong C_{p^{\beta_1}} \times \ldots \times C_{p^{\beta_t}} \times C_{p^{\beta_{t+1}}}$$

y se tiene el resultado

□

Definición: Un p-grupo abeliano finito E, diremos que es un p-grupo abeliano elemental si

$$x^p = 1 \qquad \forall x \in E$$

Ejemplo:

$$E = \overbrace{C_p \times C_p \times \ldots \times C_p}^{n} \qquad n \geq 1$$

Lema: Sea E un p-grupo abeliano elemental finito. Entonces para cada $x \in E$ existe $\mathcal{M} \leq E$ tal que E es el producto interno de $\mathcal{M}$ y $\langle x \rangle$.

Demostración: Si $x = 1$ tomando $\mathcal{M} = E$ es claro que E es el producto interno de E y $\langle 1 \rangle = \{1\}$. Supongamos que $x \neq 1$ y entonces $ord(x) = p$.

Sea

$$\Sigma = \{H \leq E / x \notin H\}$$

$\Sigma \neq \emptyset$ (pues $\{1\} \in \Sigma$) y elegimos $\mathcal{M} \in \Sigma$ el elemento de orden mayor. Puesto que $x \notin \mathcal{M} \Rightarrow \mathcal{M} < E \Rightarrow [E : \mathcal{M}] > 1$.

Aseguramos que $[E : \mathcal{M}] = p$ veamos que E es el producto directo interno de $\mathcal{M}$ y $\langle x \rangle$

1) Como E es abeliano, $\mathcal{M}$ y $\langle x \rangle$ son subgrupos normales

2) $\mathcal{M} \cap \langle x \rangle = \{1\}$

$$Si \quad y \in \mathcal{M} \cap \langle x \rangle \Rightarrow \begin{cases} y \in \mathcal{M} \\ \wedge \\ y \in \langle x \rangle \Rightarrow y = x^j \quad 0 \leq j \leq p-1 \end{cases}$$

$\Rightarrow \langle x^j \rangle \leq \mathcal{M}$.

Como $x \notin \mathcal{M}$, entonces $j = 0$, pues si $j \geq 1 \quad \langle x^j \rangle = \langle x \rangle$. Si $j = 0 \Rightarrow y = 1$

3) $\mathcal{M} \cdot \langle x \rangle = E$.

Aplicamos el 3^{o} teorema de isomorfía a $\mathcal{M} \leq E$ y $\langle x \rangle \leq E$, y obtenemos

$$\mathcal{M} \cdot \langle x \rangle \,/\, \langle x \rangle \cong \mathcal{M}/(\mathcal{M} \cap \langle x \rangle) \Rightarrow |\mathcal{M} \cdot \langle x \rangle| = |\mathcal{M}| \cdot |\langle x \rangle|$$

Como

$$[E : \mathcal{M}] = p \Rightarrow \frac{|E|}{|\mathcal{M}|} = p \Rightarrow |\mathcal{M}| = \frac{|E|}{p} = \frac{p^n}{p} = p^{n-1} \Rightarrow$$
$$\Rightarrow |\mathcal{M} \cdot \langle x \rangle| = p^{n-1}p = p^n = |E| \Rightarrow \mathcal{M} \cdot \langle x \rangle = E$$

Por tanto $E \cong \mathcal{M} \times \langle x \rangle$

Veamos que $[E : \mathcal{M}] = p$ $\qquad \begin{matrix} ME \\ x \in \mathcal{M} \end{matrix}$

Supongamos que no fuera así, es decir, que

$$[E : \mathcal{M}] = p^i \qquad i \geq 2$$

Consideramos $E/\mathcal{M}$ que es también un p-grupo abeliano elemental

$$y\mathcal{M} \in E/\mathcal{M} \Rightarrow (y\mathcal{M})^p = y^p\mathcal{M} = \mathcal{M}$$
$$y \in E \Rightarrow y^p = 1$$

y entonces cualquier elemento distinto de $\mathcal{M}$ en $E/\mathcal{M}$ tiene orden p. Elegimos
$y\mathcal{M} \in E/\mathcal{M} \quad y\mathcal{M} \neq \mathcal{M} \quad \wedge \quad y\mathcal{M} \notin \langle x\mathcal{M}\rangle$

$$x\mathcal{M} \in E/\mathcal{M}, \quad x\mathcal{M} \neq \mathcal{M}\ (x \notin \mathcal{M}) \Rightarrow ord(x\mathcal{M}) = p$$
$$\Rightarrow \begin{array}{c} \langle x\mathcal{M}\rangle \leq E/\mathcal{M} \\ |\langle x\mathcal{M}\rangle| = p \end{array} \qquad y\ como \quad |E/\mathcal{M}| = p^i \quad i \geq 2$$
$$\Rightarrow \langle x\mathcal{M}\rangle \leq E/\mathcal{M} \quad y\ entonces \quad \exists y\mathcal{M} \quad en\ las\ condiciones\ anteriores$$

Además también podemos asegurar que $x\mathcal{M} \notin \langle y\mathcal{M}\rangle$ porque $x\mathcal{M}, y\mathcal{M}$ tienen orden p.

Consideramos la proyección canónica

$$\pi : E \longrightarrow E/\mathcal{M} \qquad \pi(a) = a\mathcal{M} \qquad \forall a \in E$$

Sea $H = \pi^*(\langle y\mathcal{M}\rangle) = \{a \in E/\pi(a) \in \langle y\mathcal{M}\rangle\} = \{a \in E/a\mathcal{M} \in \langle y\mathcal{M}\rangle\}$.

Como $x\mathcal{M} \notin \langle y\mathcal{M}\rangle \Rightarrow x \notin H$.

Si $a \in \mathcal{M} \Rightarrow a\mathcal{M} = \mathcal{M} \in \langle y\mathcal{M}\rangle \Rightarrow a \in H$, es decir, $\mathcal{M} \leq H$.

Como $y \in H \quad \wedge \quad y \notin \mathcal{M}$ entonces $\mathcal{M} < H$

$$x \notin H \Rightarrow \begin{array}{c} H \in \Sigma \\ \mathcal{M} < H \end{array} \qquad en\ contra\ de\ la\ eleccion\ de \quad \mathcal{M}$$

31-5-21

Definición: Sea $n \geq 1$. Una sucesión de enteros

$$\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1 \quad tal\ que \quad \beta_1 + \beta_2 + \ldots + \beta_t = n$$

se llama partición de n.

Ejemplo: Si $n = 5$. Particiones de 5.

$$
\begin{aligned}
5 \\
4 \geq 1 \\
3 \geq 2 \\
3 \geq 1 \geq 1 \\
2 \geq 2 \geq 1 \\
2 \geq 1 \geq 1 \geq 1 \\
1 \geq 1 \geq 1 \geq 1 \geq 1 \geq 1
\end{aligned}
$$

1-6-21

Teorema (Teorema de estructura de grupos abelianos finitos):
Sea A un grupo abeliano finito, con $|A| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, la factorización en primos. Entonces

$$A \cong \prod_{i=1}^{k} \left(\prod_{j=1}^{t_i} C_{p_i}^{n_{ij}} \right)$$

donde para cada $i = 1, \ldots, k$

$$n_{i1} \geq n_{i2} \geq \ldots \geq n_{it_i} \geq 1 \qquad y \qquad n_{i1} + n_{i2} + \cdots + n_{it_i} = r_i$$

Además esta descomposición es única (salvo el orden), y se llama la descomposición cíclica primaria (DCP) del grupo A.
A los

$$\{p_i^{n_{ij}} / 1 \leq i \leq k,\ 1 \leq j \leq t_i\}$$

se les llama divisores elementales del grupo A.

Demostración: $|A| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$
A abeliano y entonces para cada $i = 1, \ldots, k$, hay un único p_i-subgrupo de Sylow de $\mathcal{P}_i$

$$|\mathcal{P}_i| = p_i^{r_i}$$

Sabemos además que

$$A \cong \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_k \tag{1}$$

Para cada $i = 1, \ldots, k$

$$|\mathcal{P}_i| = p_i^{r_i} \quad es\ un\ p_i - grupo\ abeliano$$

entones, por la proposición anterior, existen

$$n_{i1} \geq n_{i2} \geq \ldots \geq n_{it_i} \geq 1 \quad tal\ que \quad n_{i1} + n_{i2} + \ldots + n_{it_i} = r_i$$

y

$$\mathcal{P}_i \cong C_{p_i^{n_{i1}}} \times C_{p_i^{n_{i2}}} \times \cdots \times C_{p_i^{n_{iti}}} \tag{2}$$

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 finitos son isomorfos si y solo si tienen los mismos divisores elementales.

Este hecho nos permite dar la lista de los distintos grupos abelianos, no isomorfos entre sí, de un orden determinado. ¿Cómo?

Dando todas las listas de posibles divisores elementales.

Ejemplo: Determinar, salvo isomorfismo, todos los grupos abelianos de orden 360.

Lista de divisores elementales

(1) $\{2^3, 3^2, 5\} \Rightarrow A = C_8 \times C_9 \times C_5$

(2) $\{2^3, 3, 3, 5\} \Rightarrow A = C_8 \times C_3 \times C_3 \times C_5$

(3) $\{2^2, 2, 3^2, 5\} \Rightarrow A = C_4 \times C_2 \times C_9 \times C_5$

(4) $\{2^2, 2, 3, 3, 5\} \Rightarrow A = C_4 \times C_2 \times C_3 \times C_3 \times C_5$

(5) $\{2, 2, 2, 3^2, 5\} \Rightarrow A = C_2 \times C_2 \times C_2 \times C_9 \times C_5$

(6) $\{2, 2, 2, 3, 3, 5\} \Rightarrow A = C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$

Teorema de descomposición cíclica de un grupo abeliano (DC): Sea A un grupo abeliano finito. Entonces

$$A \cong C_{d_1} \times C_{d_2} \times \ldots \times C_{d_t}$$

donde $d_1, d_2, \ldots, d_t$ son enteros positivos tal que

$$|A| = d_1 d_2 \cdots d_t \quad y \quad d_i \mid d_j \quad para\ cada \quad j \leq i$$

Además esta descomposición es única, esto es, si

$$A \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_s}$$

con $|A| = m_1 m_2 \cdots m_s$ y $m_i \mid m_j$ para cada $j \leq i$, entonces $s = t$ y $d_i = m_i \quad \forall i$. A los $\{d_1, d_2, \ldots, d_t\}$ se les llama factores invariantes del grupo A.

Demostración: $|A| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

$$A \cong \prod_{i=1}^{k} \left(\prod_{j=1}^{t_i} C_{p_i^{n_{ij}}} \right)$$

Para cada $i = 1, \ldots, k$

$$n_{i1} \geq n_{i2} \geq \ldots \geq n_{iti} \qquad n_{i1} + n_{i2} + \ldots + n_{iti} = r_i$$

Sea $t = max\{t_1, t_2, \ldots, t_k\}$ y ponemos $n_{il} = 0$ para $t_i < l < t$. Consideramos las siguiente matriz

$$\begin{pmatrix} p_1^{n_{11}} & p_2^{n_{21}} & \cdots & p_k^{n_{k1}} \\ p_1^{n_{12}} & p_2^{n_{22}} & \cdots & p_k^{n_{k2}} \\ \vdots & \vdots & \ddots & \vdots \\ p_1^{n_{1t}} & p_2^{n_{2t}} & \cdots & p_k^{n_{kt}} \end{pmatrix}$$

Sea

$$\begin{aligned} d_1 &= p_1^{n_{11}} p_2^{n_{21}} \cdots p_k^{n_{k1}} \\ d_2 &= p_1^{n_{12}} p_2^{n_{22}} \cdots p_k^{n_{k2}} \\ &\vdots \\ d_t &= p_1^{n_{1t}} p_2^{n_{2t}} \cdots p_k^{n_{kt}} \end{aligned}$$

es decir, cada d_i es el producto de los elementos de la fila i-ésima. Teniendo en cuenta que $n_{ij} \geq n_{ij+1} \quad \forall i \, \forall j$, entonces $d_i \mid d_j \quad \forall j \leq i$.

Es claro que

$$\begin{aligned} C_{d_1} &\cong C_{p_1^{n_{11}}} \times C_{p_2^{n_{21}}} \times \cdots \times C_{p_k^{n_{k1}}} \\ C_{d_2} &\cong C_{p_1^{n_{12}}} \times C_{p_2^{n_{22}}} \times \cdots \times C_{p_k^{n_{k2}}} \\ &\vdots \\ C_{d_t} &\cong C_{p_1^{n_{1k}}} \times C_{p_2^{n_{2k}}} \times \cdots \times C_{p_k^{n_{kt}}} \end{aligned}$$

Entonces

$$A \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$$

DC de A.

Volviendo al ejemplo de los subgrupos de orden 360, veamos cúal es la descomposición cíclica de 6.

$$\begin{pmatrix} 2 & 3 & 5 \\ 2 & 3 & 1 \\ 2 & 1 & 1 \end{pmatrix} \quad d_1 = 30, \quad d_2 = 6, \quad d_3 = 2$$

$$\Rightarrow C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 \cong C_{30} \times C_6 \times C_2$$

2-6-21

Ejemplo 5: $\{2, 2, 2, 3^2, 5\}$

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

$$d_1 = 2 \cdot 9 \cdot 5 = 90 \qquad d_2 = 2 \qquad d_3 = 2$$

La descomposición cíclica de los de tipo 5 es

$$C_{90} \times C_2 \times C_2$$

Ejemplo 4: $\{2^2, 2, 3, 3, 5\}$

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

$$d_1 = 2^2 \cdot 3 \cdot 5 = 60 \qquad d_2 = 2 \cdot 3 = 6$$

La descomposición de los de tipo 4 es

$$C_{60} \times C_6$$

Ejemplo 3: $\{2^2, 2, 3^2, 5\}$

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

$$d_1 = 2^2 \cdot 3^2 \cdot 5 = 180 \qquad d_2 = 2$$

La descomposición de los de tipo 3 es

$$C_{180} \times C_2$$

Ejemplo 2: $\{2^3, 3, 3, 5\}$

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

$$d_1 = 2^3 \cdot 3 \cdot 5 = 120 \qquad d_2 = 3$$

La descomposición de los de tipo 2 es

$$C_{120} \times C_3$$

Ejemplo 1: $\{2^3, 3^2, 5\}$

$$\begin{pmatrix} 2^3 & 3^2 & 5 \end{pmatrix} \to d_1 = 360$$

La descomposición de los de tipo 1 es

$$C_{360}$$

Ejercicio 2 (Relación 6): $G_1 \leq \mathcal{U}(\mathbb{Z}_{65})$

$$|G_1| = 16 = 2^4$$

Los grupos abelianos de orden 16 son

$$\{2^4\} \longrightarrow C_{16}$$
$$\{2^3, 2\} \longrightarrow C_8 \times C_2$$
$$\{2^2, 2^2\} \longrightarrow C_4 \times C_4$$
$$\{2^2, 2, 2\} \longrightarrow C_4 \times C_2 \times C_2$$
$$\{2, 2, 2, 2\} \longrightarrow C_2 \times C_2 \times C_2 \times C_2$$

Orden de los elementos de G_1

$$8^2 = 64$$
$$8^3 = 64 \cdot 8 = 512 = 57 \quad \text{mód } 65$$
$$8^4 = 57 \cdot 8 = 456 = 1 \quad \text{mód } 65$$
$$\Rightarrow ord(8) = 4$$

Elementos de orden 2:$14, 51, 64$
Elementos de orden 4, el resto.
En G_1 hay 3 elementos de orden 2 y 12 elementos de orden 4.

$$C_4 \times C_4 = \langle x/x^4 = 1\rangle \times \langle y/y^4 = 1\rangle$$

$(1,1)$	$orden\ 1$	$(1,y)$	$orden\ 4$
$(x,1)$	$orden\ 4$	(x,y)	$orden\ 4$
$(x^2,1)$	$orden\ 2$	(x^2,y)	$orden\ 4$
$(x^3,1)$	$orden\ 4$	(x^3,y)	$orden\ 4$
$(1,y^2)$	$orden\ 2$	$(1,y^3)$	$orden\ 4$
(x,y^2)	$orden\ 4$	(x,y^3)	$orden\ 4$
(x^2,y^2)	$orden\ 2$	(x^2,y^3)	$orden\ 4$
(x^3,y^2)	$orden\ 4$	(x^3,y^3)	$orden\ 4$

Entonces $G_1 \cong C_4 \times C_4$. En

$$C_4 \times C_2 \times C_2 = \langle x/x^4 = 1\rangle \times \langle y/y^2 = 1\rangle \times \langle z/z^2 = 1\rangle$$
$$ord(a,b,c) = mcm(ord(a), ord(b), ord(c))$$

Hay 8 elementos de orden 4 y 7 elementos de orden 2.

Ejercicio 3 (Relación 6): Calcular la DCP y DC de los grupos abeliano

$$A = C_{24} \times C_{40} \times C_{35} \cong C_{35} \times C_{40} \times C_{24}$$
$$B = C_{50} \times C_{56} \times C_{12}$$

Veamos si son isomorfos. Utilizamos $C_n \times C_m \cong C_{nm}$ si $mcd(n,m) = 1$

$$A = C_{24} \times C_{40} \times C_{35} \cong C_8 \times C_3 \times C_8 \times C_5 \times C_7 \times C_5 \cong$$
$$\cong C_8 \times C_8 \times C_3 \times C_5 \times C_5 \times C_7 \quad DCP$$

Divisores elementales de A

$$\{2^3, 2^3, 3, 5, 5, 7\}$$
$$\begin{pmatrix} 2^3 & 3 & 5 & 7 \\ 2^3 & 1 & 5 & 1 \end{pmatrix}$$
$$d_1 = 2^3 \cdot 3 \cdot 5 \cdot 7 = 840 \qquad d_2 = 40$$
$$A \cong C_{840} \times C_{40} \qquad DC$$
$$B = C_{50} \times C_{56} \times C_{12} \cong C_{25} \times C_2 \times C_8 \times C_7 \times C_3 \times C_4 \cong$$
$$\cong C_8 \times C_4 \times C_2 \times C_3 \times C_{25} \times C_7 \quad DCP$$

Divisores elementales de B son

$$\{2^3, 2^2, 2, 3, 5^2, 7\}$$
$$\begin{pmatrix} 2^3 & 3 & 5^2 & 7 \\ 2^2 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 \end{pmatrix}$$
$$d_1 = 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 4200 \qquad d_2 = 4 \qquad d_3 = 2$$
$$A \cong C_{4200} \times C_4 \times C_2 \quad DC$$

Ejercicio 7 (Relación 6): A grupo abeliano $p||A|$ y $|A| = p^r m \quad mcd(m,p) = 1$, $\exists!$ p-subgrupo de Sylow que es

$$\mathcal{P} = \{x \in A / ord(x) = p^i \quad 0 \leq i \leq r\}$$

y se llama la componente p-primaria de A.
DCP y DC de los grupos abelianos no isomorfos de orden 13916

$$13916 = 2^2 \cdot 7^2 \cdot 71$$

Partición	DCP	DC
$2^2, 7^2, 71$	$C_4 \times C_{49} \times C_{71}$	C_{13196}
$2^2, 7, 7, 71$	$C_4 \times C_7 \times C_7 \times C_{71}$	$C_{1988} \times C_7$
$2, 2, 7^2, 71$	$C_2 \times C_2 \times C_{49} \times C_{71}$	$C_{69588} \times C_2$
$2, 2, 7, 7, 71$	$C_2 \times C_2 \times C_7 \times C_7 \times C_{71}$	$C_{999} \times C_{14}$

La componente 2-primaria

$$P_2 = \{(a,b,c) \in C_4 \times C_{49} \times C_{71} / ord(a,b,c) = 2^i \quad 0 \leq i \leq 2\} = \{(a,1,1)/a \in C_4\}$$

Ejercicio 4 (Relación 6): Sea A un grupo abeliano de orden n.
Si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ es la descomposición en factores primos. Demostrad

$$l(G) = e_1 + e_2 + \ldots + e_r$$
$$fact(G) = \{C_{p_1}, \overset{(e_1)}{\ldots}, C_{p_1}, C_{p_2}, \overset{(e_2)}{\ldots}, C_{p_2}, \ldots, C_{p_r}, \overset{(e_r)}{\ldots}, C_{p_r}\}$$

Sea $\mathcal{P}_i$ el único p_i-subgrupo de Sylow de A, con $i = 1, \ldots, r$.
Sabemos que

$$A \cong \mathcal{P}_1 \times \mathcal{P}_2 \times \ldots \times \mathcal{P}_r$$

Entonces

$$l(A) = \sum_{i=1}^{r} l(\mathcal{P}_i)$$
$$fact(A) = \cup_{i=1}^{r} fact(\mathcal{P}_i)$$

Como $|\mathcal{P}_i| = p_i^{e_i} \overset{Relacion\ 5}{\Rightarrow} l(\mathcal{P}_i) = e_i \quad fact(\mathcal{P}_i) = \{C_{p_i}, \overset{(e_i)}{\ldots}, C_{p_i}\}$

Ejercicio 5 (Relación 6): Sea $n \geq 3$ y D_n el grupo diédrico.
Sea $n = p_1^{e_1} \cdots p_r^{e_r}$ la descomposición en primos. Demostrad

$$l(D_n) = e_1 + \ldots + e_r + 1$$
$$fact(D_n) = \{C_{p_1}, \overset{(e_1)}{\ldots}, C_{p_1}, \ldots, C_{p_r}, \overset{(e_r)}{\ldots}, C_{p_r}, C_2\}$$
$$D_n = \left\langle r, s / r^n = s^2 = 1, \quad sr = r^{-1}s \right\rangle$$

Sea $N = \langle r \rangle \trianglelefteq D_n$ entonces

$$l(D_n) = l(N) + l(D_n/N)$$
$$fact(D_n) = fact(N) \cup fact(D_n/N)$$
$$N = \langle r \rangle \cong C_n \quad y \quad D_n/N \cong C_2$$

Haciendo uso del ejercicio anterior se obtiene el resultado.

7-6-21

7. Tema 8: Presentaciones de grupos. Clasificación de los grupos de orden menor o igual que 15

Definición: Sea G un grupo abeliano generado por $\{x_1, x_2, \ldots, x_n\}$. Cualquier ecuación que satisfagan los generadores se llama una relación del grupo

G.

Por ejemplo, en D_n relaciones son

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

también son relaciones en D_n

$$r^i = r^{n-i}s \quad i \geq 1$$

En el grupo cíclico $C_n = \langle x/x^n = 1\rangle$, una relación es

$$x^n = 1$$

también es una relación en C_n

$$x^r = x^{res(r;n)}$$

Definición: Dar un grupo G (finitamente generado) por generadores y relaciones es dar un conjunto de generadores $S = \{x_1, x_2, \ldots, x_n\}$ de G y un conjunto de relaciones $\{R_1, R_2, \ldots, R_m\}$ (cada R_i es una ecuación en los generadores $x_1, \ldots, x_n$ 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 $\{R_1, \ldots, R_m\}$.

A estos genradores y relaciones los llamaremos una representación de G y escribiremos

$$G = \langle x_1, \ldots, x_n/R_1, \ldots, R_m\rangle$$

Ejemplos:

$$D_n = \left\langle r, s/r^n = 1,\ s^2 = 1,\ sr = r^{-1}s\right\rangle$$
$$C_n = \langle x/x^n = 1\rangle$$
$$K = \left\langle a, b/a^2 = 1,\ b^2 = 1,\ ab = ba\right\rangle$$

Se verifica que todo grupo finitamente generado admite una presentación.

Teorema de Dyck: Sea G un grupo y

$$G = \langle x_1, \ldots, x_n/R_1, \ldots, R_m\rangle$$

una representación de G.
Sea H un grupo y $a_1, a_2, \ldots, a_n \in H$ tal que las ecuaciones $R_1, R_2, \ldots, R_m$ son válidas en H al sustituir x_i por a_i $(i = 1, \ldots, n)$
Entonces existe un único homomorfismo de grupos

$$f : G \longrightarrow H$$

tal que

$$f(x_i) = a_i \quad \forall i = 1, \ldots, n$$

Además si $H = \langle a_1, a_2, \ldots, a_n \rangle$, entonces f es epimorfismo.

Ejemplo: $\mathcal{Q}_2 = \{1, -1, i, -i, j, -j, k, -k\}$ puede ser representado como sigue

$$\mathcal{Q}_2 = \langle a, b / a^4 = 1,\ b^2 = a^2,\ ba = a^{-1}b \rangle$$

En efecto sea

$$G = \langle a, b / a^4 = 1,\ b^2 = a^2,\ ba = a^{-1}b \rangle$$

Consideramos $i, j \in \mathcal{Q}_2$. Sabemos que

$$i^4 = 1 \qquad j^2 = -1 = i^2 \qquad ji = -k = (-i)j = i^3 j = i^{-1} j$$

Entonces por el teorema de Dyck existe un único homomorfismo

$$f : G \longrightarrow \mathcal{Q}_2 \qquad \begin{array}{l} f(a) = i \\ f(b) = j \end{array}$$

Además, puesto que $\mathcal{Q}_2 = \langle i, j \rangle$, es un epimorfismo.
Por el primer teorema de isomorfía

$$G/Ker(f) \cong Img(f) = \mathcal{Q}_2$$

Veamos que $Ker(f) = \{1\}$ y lo vemos observando que $|G| = 8$.

Sea $H = \langle a \rangle \quad |H| = 4 = ord(a)$
Como $bab^{-1} = a^{-1}bb^{-1} = a^{-1} \in H \Rightarrow H \trianglelefteq G$

$$G/H = \langle bH \rangle$$

Como $(bH)^2 = b^2H = a^2H = H \Rightarrow ord(bH) = 2 \Rightarrow |G/H| = 2$. Por tanto $|G| = |G/H| \cdot |H| = 4 \cdot 2 = 8$.

$$|G/Ker(f)| = |\mathcal{Q}_2| = 8 \Rightarrow |Ker(f)| = 1 \Rightarrow Ker(f) = \{1\}$$

Definición: Para cada $k \geq 1$ se define el k-ésimo grupo dicíclico como el grupo presentado por

$$\mathcal{Q}_k = \langle a, b / a^{2k} = 1,\ b^2 = a^k,\ ba = a^{-1}b \rangle$$

$k = 2$ $\mathcal{Q}_2$ es el grupo de los cuaternios.

$k = 1$

$$\begin{gathered} \mathcal{Q}_1 = \langle a, b / a^2 = 1,\ b^2 = a,\ ba = a^{-1}b \rangle \\ = \langle b \rangle = C_4 \\ Q_k = \langle a, b / a^{2k} = 1,\ b^2 = a^k,\ ba = a^{-1}b \rangle \\ a^i b^j \in \mathbb{Z} \end{gathered}$$

$a^{2k} = 1$, es decir, $ord(a) = 2k$ entones $0 \leq i \leq 2k-1$.

$$b^2 = a^k \Rightarrow ord(b^2) = ord(a^k) = \frac{2k}{mcd(k, 2k)} = 2$$

Así que $ord(b^2) = 2 \Rightarrow ord(b) = 4$ y entonces $0 \leq j \leq 3$.

$$Si \quad j = 2 \qquad \begin{matrix} a^i b^2 = a^i a^k = a^{i+k} \\ b^2 = a^k \end{matrix}$$

$$Si \quad j = 3 \quad a^i b^3 = a^i b^2 b = a^{i+k} b$$

$$\mathcal{Q}_k = \{a^i b^j / 0 \leq i \leq 2k-1,\ 0 \leq j \leq 1\}$$

$$|\mathcal{Q}_k| = 4k \quad elementos$$

$$a^i \cdot a^s = a^{res(i+s;2k)}$$

$$a^i(a^s b) = a^{res(i+s;2k)} b$$

$$(a^s b)a^i \overset{ba=a^{-1}b}{=} a^s a^{-i} b = a^{res(s-i;2k)} b$$

$$(a^s b)(a^i b) = a^s a^{-1} b^2 = a^s a^{-i} a^k = a^{res(s-i+k;2k)}$$

$$k \geq 3 \quad \exists N \trianglelefteq \mathcal{Q}_k \quad tal\ que \quad \mathcal{Q}_k / N \cong D_k$$

y entonces $\mathcal{Q}_k$ no es abeliano.

$$D_k = \langle r, s / r^k = 1,\ s^2 = 1,\ sr = r^{-1}s \rangle$$

$$r^2 k = 1 \quad s^2 = 1 = r^k \quad sr = r^{-1}s$$

, luego verifican las relaciones de $\mathcal{Q}_k$, y por el teorema de Dyck

$$\exists f : \mathcal{Q}_k \longrightarrow D_k \qquad \begin{matrix} f(a) = r \\ f(b) = s \end{matrix}$$

es un epimorfismo

$$\mathcal{Q}_k / Ker(f) \cong D_k$$

8-6-21

7.1. Clasificación de los grupos de orden menor o igual que 15.

(1) Los grupos 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 son

$$C_{p^2} \quad y \quad C_p \times C_p$$

Consecuentemente,

- De orden 4 tenemos C_4 y $C_2 \times C_2 = K$
- De 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 $|G| = 2p$

$$n_p \mid 2 \quad y \quad n_p \equiv 1 \mod p \Rightarrow n_p = 1$$

Por tanto existe un único $\mathcal{P} \trianglelefteq G$ tal que $|\mathcal{P}| = p \Rightarrow$

$$\mathcal{P} \cong C_p$$

Caso $n_2 = p$**:** G no es abeliano

$$\mathcal{P} = \langle a / a^p = 1 \rangle$$

Como $[G : \mathcal{P}] = \frac{|G|}{|\mathcal{P}|} = \frac{2p}{p} = 2$ y entonces hay únicamente dos clases laterales a derecha:

$$\mathcal{P}, \quad \mathcal{P}b \quad b \notin \mathcal{P}$$

En particular

$$G = \mathcal{P} \cup \mathcal{P}b = \{1, a, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b\}$$

Veamos que $ord(b) = 2$. En efecto, $ord(b) \mid |G| = 2p$

$$\Rightarrow ord(b) = \begin{cases} \cancel{1} & b \neq 1 \\ & 2 \\ \cancel{p} & (\langle b \rangle = \mathcal{P} \Rightarrow b \in \mathcal{P}) \\ \cancel{2p} & G \text{ no es abeliano sino } G = \langle b / b^{2p} = 1 \rangle \end{cases}$$

Veamos que $ba = a^{-1}b$. En efecto

$$ord(ba) \mid |G| = 2p \Rightarrow$$

$$ord(ba) = \begin{cases} \cancel{1} & (ba = 1 \Rightarrow b = a^{-1} \in \mathcal{P}) \\ & 2 \\ \cancel{p} & (\langle ba \rangle = \mathcal{P} \Rightarrow ba \in \mathcal{P} \Rightarrow b \in \mathcal{P}) \\ \cancel{2p} & \Rightarrow G \text{ no es abeliano} \end{cases}$$

$$\Rightarrow ord(ba) = 2 \Rightarrow (ba)^2 = baba = 1 \Rightarrow ba = (ba)^{-1} = a^{-1}b^{-1} \overset{ord(b)=2}{=} a^{-1}b$$

$$G = \langle a, b / a^p = 1,\ b^2 = 1,\ ba = a^{-1}b \rangle \cong D_p$$

□

- Grupos de orden $6 \Rightarrow C_6$ y D_3
- Gurpos de orden $10 \Rightarrow C_{10}$ y D_5
- Grupos de orden $14 \Rightarrow C_{14}$ y D_7

(4) Todo grupo de orden 15 es isomorfo a C_{15}

$$\begin{gathered} |G| = 15 = 3 \cdot 5 \\ n_3 \mid 5 \quad y \quad n_3 \equiv 1 \mod 3 \Rightarrow n_3 = 1 \\ n_5 \mid 3 \quad y \quad n_5 \equiv 1 \mod 5 \Rightarrow n_5 = 1 \\ \Rightarrow G \cong \mathcal{P} \times \mathcal{Q} \end{gathered}$$

$\mathcal{P}$ es un 3-subgrupo de Sylow (único).

$\mathcal{Q}$ es un 5-subgrupo de Sylow (único).

$$\left.\begin{array}{l} |\mathcal{P}| = 3 \Rightarrow \mathcal{P} \cong C_3 \\ |\mathcal{Q}| = 5 \Rightarrow \mathcal{Q} \cong C_5 \end{array}\right\} \Rightarrow G \cong C_3 \times C_5 \cong C_{15}$$

(5) Grupos de orden 8.

Caso abeliano: $|G| = 8 = 2^3$. Fijándonos en los divisores elementales,

$$\begin{gathered} \{2^3\} \longrightarrow C_8 \\ \{2^2, 2\} \longrightarrow C_4 \times C_2 \\ \{2, 2, 2\} \longrightarrow C_2 \times C_2 \times C_2 \end{gathered}$$

Caso no abeliano:

$$|G| = 8 \quad y \quad G \, no \, abeliano$$

Como G no es abeliano los elementos no triviales tienen orden 2 ó orden 4. Por otro lado, como G no es abeliano, no todos los elementos de G tienen orden 2.

Consecuentemente, $\exists a \in G$ tal que $ord(a) = 4$. Sea

$$H = \langle a \rangle = \{1, a, a^2, a^3\}$$

Como $[G : H] = \frac{|G|}{|H|} = \frac{8}{4} = 2 \Rightarrow H \trianglelefteq G$, y como 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 elementos $b^2 \in G$

$$b^2 \in H \cup Hb \Rightarrow \begin{cases} b^2 \notin H \\ b^2 \in Hb \Rightarrow b^2 = a^i b \quad a \leq i \leq 3 \Rightarrow b = a^i \in H \downarrow \end{cases}$$

Así que $b^2 \in H = \{1, a, a^2, a^3\}$.

$$Si \quad b^2 = a \Rightarrow ord(b^2) = 4 \Rightarrow ord(b) = 8$$

$$4 = ord(b^2) = \frac{ord(b)}{mcd(ord(b), 2)} = \frac{ord(b)}{2} \Rightarrow ord(b) = 8$$

$$\Rightarrow G \, es \, abeliano \downarrow$$

Por el mismo razonamiento $b^2 \neq a^3$.
Así que $b^2 = 1$ ó $b^2 = a^2$.

Caso $b^2 = 1$**:** Veamos que $ba = a^{-1}b = a^3 b$.
Como $H \trianglelefteq G \Rightarrow bab^{-1} \overset{b^2=1}{=} bab \in H \Rightarrow$

$$\Rightarrow bab = \begin{cases} \not{1} \quad (bab = 1 \Rightarrow ba = b \Rightarrow a = 1 \downarrow) \\ \not{a} \quad (bab = a \Rightarrow ba = ab \Rightarrow G \, es \, abeliano \downarrow) \\ \not{a^2} \quad (bab = a^2 \Rightarrow baba = a^3 \Rightarrow ord((ba)^2) = ord(a^3) = 4 \Rightarrow ord(ba) = 8 \downarrow) \\ a^3 \end{cases}$$

Luego $bab = a^3 \Rightarrow ba = a^3 b$

$$G = \langle a, b / a^4 = 1, \, b^2 = 1, \, ba = a^3 b \rangle \cong D_4$$

Caso $b^2 = a^2$**:** Veamos que $ba = a^{-1}b = a^3 b$.

Como $H \trianglelefteq G \Rightarrow bab^{-1} \in H \Rightarrow$

$$\Rightarrow bab^{-1} = \begin{cases} \not{1} (bab^{-1} = 1 \Rightarrow ba = b \Rightarrow a = 1 \downarrow) \\ \not{a} (bab^{-1} = a \Rightarrow ba = ab \Rightarrow G \, abeliano = \\ \not{a^2} (bab^{1-} = a^2 \Rightarrow bab^{1-} = b^2 \Rightarrow ab^{-1} = b \Rightarrow a = b^2 \Rightarrow a = a^2 \Rightarrow a = 1 \downarrow \\ a^3 \end{cases}$$

$$bab^{-1} = a^3 \Rightarrow ba = a^3 b \Rightarrow G = \langle a, b / a^4 = 1, \, a^2 = b^2, \, ba = a^{-1} b \rangle \cong \mathcal{Q}_2$$

9-6-21

7.1.1. Grupos de orden 12:

Caso abeliano: G abeliano y $|G| = 12 = 3 \cdot 2^2$. Sus divisores elementales son

$$\{2^2, 3\} \longrightarrow C_4 \times C_3 \cong C_{12}$$

$$\{2, 2, 3\} \longrightarrow C_2 \times C_2 \times C_3 \cong C_6 \times C_2$$

Caso no abeliano: $|G| = 12 = 3 \cdot 2^2$

$$n_3 \mid 4 \quad y \quad n_3 \equiv \quad \text{mód } 3 \Rightarrow n_3 = 1 \quad o \quad n_3 = 4$$

- Si $n_3 = 4$ (Rel 5) $G \cong A_4$
- Si $n_3 = 1$, sea $\mathcal{P} \trianglelefteq G$ con $|P| = 3$

$$\mathcal{P} \cong C_3 \quad y \quad \mathcal{P} = \langle x / x^3 = 1 \rangle$$
$$(n_2 \mid 3 \quad y \quad n_2 \equiv 1 \mod 3 \Rightarrow \cancel{n_2 = 1} \quad o \quad n_2 = 3)$$

Pues si $n_2 = 1 \Rightarrow$

$$G \cong \mathcal{P} \times \mathcal{Q} \quad abeliano$$

Veamos que en G hay un elemento de orden 6. Consideramos

$$cl(x) = \{gxg^{-1} / g \in G\}$$

Puesto que $\mathcal{P} \trianglelefteq G$ entonces $cl(x) \subseteq \mathcal{P} = \{1, x, x^2\}$. Además $1 \notin cl(x)$

$$(Si \quad 1 \in cl(x) \Rightarrow \exists g \in G \quad tal\ que \quad gxg^{-1} = 1 \Rightarrow x = 1 \downarrow)$$

Entonces $cl(x) = \{x\}$ ó $cl(x) = \{x, x^2\}$. Recordemos que

$$[G : C_G(x)] = |cl(x)|$$

donde $C_G(x) = \{g \in G / gxg^{-1} = x\} \leq G$. Entonces

$$[G : C_G(x)] = 1 \quad o \quad [G : C_G(x)] = 2 \Rightarrow |C_G(x)| = 12 \quad o \quad 6$$

En ambos casos, $2 \mid |C_G(x)|$ y, por el teorema de Cauchy

$$\exists z \in C_G(x) \quad tal\ que \quad ord(z) = 2$$

Sea $a = xz \quad mcd(ord(x), ord(z)) \overset{xz \equiv zx}{=} mcd(3, 2) = 1 \Rightarrow$

$$\overset{Relacion\ 2}{=} ord(a) = ord(x) \cdot ord(z) = 3 \cdot 2 = 6$$

Sea $K = \langle a \rangle = \{1, a, a^2, a^3, a^4, a^5\}$

$$[G : K] = \frac{|G|}{|K|} = \frac{12}{6} = 2 \Rightarrow K \trianglelefteq G$$

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

$$\left.\begin{array}{c} K \trianglelefteq G \Rightarrow bab^{-1} \in K \\ ord(bab^{-1}) = ord(a) = 6 \end{array}\right\} \Rightarrow bab^{-1} = a \quad o \quad bab^{-1} = a^5$$

Si $bab^{-1} = a \Rightarrow ba = ab \downarrow$ pues G no es abeliano.

$$\Rightarrow bab^{-1} = a^5 \Rightarrow ba = a^5 b \Rightarrow ba = a^{-1}b$$

Consideramos el elemento $b^2 \in G = K \cup Kb$

$$\Rightarrow b^2 \in K \quad o \quad \cancel{b^2 \in Kb} \quad pues \quad b \notin K$$

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 $b^2 = a^5 \Rightarrow ord(b^2) = 6 \Rightarrow ord(b) = 12$ y sería abeliano $\downarrow$.
Si $b^2 = a^2$

$$bab^{-1} = a^{-1}$$

$$(a^{-1})^2 = (bab^{-1})^2 = ba^2b^{-1} \overset{b^2 = a^2}{=} bb^2b^{-1} = b^2 = a^2 \Rightarrow a^4 = 1$$

, en contradicción con que $ord(a) = 6$.

Si $b^2 = a^4$

$$(a^{-1})^4 = (bab^{-1})^4 = ba^4b^{-1} \overset{a^4 = b^2}{=} bb^2b^{-1} = b^2 = a^4 \Rightarrow a^8 = 1$$

, en contradicción con que $ord(a) = 6$. Entonces $b^2 = 1$ ó $b^2 = a^3$

- $b^2 = 1$

$$G = \langle a, b / a^6 = 1,\ b^2 = 1,\ ba = a^{-1}b \rangle = D_6$$

- $b^2 = a^3$

$$G = \langle a, b / a^6 = 1,\ b^2 = a^3,\ ba = a^{-1}b \rangle = Q_3$$

Ejercicio 9 (Relación 6): Demostrar que

$$A_4 \cong \langle a, b / a^2 = 1,\ b^3 = 1,\ (ab)^3 = 1 \rangle$$

procediendo como sigue

(1) Sea $G = \langle a, b / a^2 = 1,\ b^3 = 1,\ (ab)^3 = 1 \rangle$.

Demostrar que existe un epimorfismo $G \longrightarrow A_4$.

Sea $\sigma = (1\,2)(3\,4) \in A_4$
$\tau = (1\,2\,3) \in A_4$

$$\sigma^2 = 1,\ \tau^3 = 1$$

$$\sigma\tau = (1\,2)(3\,4)(1\,2\,3) = (2\,4\,3) \Rightarrow (\sigma\tau)^3 = 1$$

Por el teorema de Dyck existe un único homomorfismo $f : G \longrightarrow A_4$ tal que

$$f(a) = \sigma \quad y \quad f(b) = \tau$$

Es fácil ver que $A_4 = \langle \sigma, \tau \rangle$ y entonces f es un epimorfismo

$$G/Ker(f) \cong A_4 \Rightarrow |G/Ker(f)| = 12 \Rightarrow |G| \geq 12$$

Notemos que $ord(a) = 2$ y $ord(b) = 3$.

(2) Demostrar que los elementos a, $bab^2 \in G$ tienen orden 2 y conmutan entre sí, generando entonces un subgrupo de G, $N = \langle a, bab^2 \rangle$ tipo Klein. Demostrar que N es un subgrupo normal de G.

$$G/N = \langle bN \rangle \quad (bN)^3 = b^3 N \overset{b^3=1}{=} N$$
$$\Rightarrow ord(bN) = 3 \quad (b \notin N \Rightarrow G/N = 1 \Rightarrow G = N \Rightarrow |G| = 4 \downarrow)$$
$$(bab^2)^2 = bab^2bab^2 = ba^2b = bb^2 = b^3 = 1 \Rightarrow ord(bab^2) = 2$$

Para ver que $a(bab^2) = (bab^2)a$, veremos que ambos son iguales a b^2ab

$$1 = (ab)^3 = ababab \Rightarrow abab = (ab)^{-1} \Rightarrow abab = b^{-1}a^{-1} = b^2a$$
$$a(bab^2) = abab^2 = ababb = b^2ab$$
$$(bab^2)a = babba = bab^2a = baabab = b^2ab$$
$$N = \langle a, bab^2 \rangle = \{1, a, bab^2, b^2ab\}$$

Veamos ahora que N es normal. Como $G = \langle a, b \rangle$, basta con ver que

$$aNa^{-1} \leq N \quad y \quad bNb^{-1} \leq N$$

y como $N = \langle a, bab^2 \rangle$, basta con ver que

$$bab^{-1} \in N \quad b(bab^2)b^{-1} \in N$$
$$aaa^{-1} \quad y \quad a(bab^2)a^{-1} \, (conmutan)$$
$$b(bab^2)b^{-1} = b^2ab \in N \quad pues \quad (abab^2) = b^2ab \in N$$

y entonces $N \trianglelefteq G$. Entonces $|G| = 12$ y $G/Ker(f) \cong A_4 \Rightarrow$

$$Ker(f) = \{1\} \quad y \quad f \, es \, un \, isomorfismo$$

Ejercicio 10 (Relación 6): Demostrar que

$$S_4 \cong \langle a, b / a^2 = 1, b^3 = 1, (ab)^4 = 1 \rangle$$

(1) $G = \langle a, b / a^2 = 1, b^3 = 1, (ab)^4 = 1 \rangle$

Sea $\sigma = (1\,2)$, $\tau = (2\,3\,4)$ $\qquad \sigma^2 = id, \ \tau^3 = id$
$$\sigma\tau = (1\,2)(2\,3\,4) = (1\,2\,3\,4)$$
$$(\sigma\tau)^4 = id$$

Además, $S_4 = \langle \sigma, \tau \rangle$. Entonces por el teorema de Dyck existe un epimorfismo

$$f : G \longrightarrow S_4 \qquad \begin{matrix} f(a) = \sigma \\ f(b) = \tau \end{matrix}$$
$$G/Ker(f) \cong S_4 \quad |G| \geq 24$$
$$ord(a) = 2 \quad ord(b) = 3$$

(2) $(ab)^2$, $(ba)^2$ son de orden 2 y conmutan entre sí

$$\left.\begin{array}{c}((ab)^2)^2=(ab)^4=1\\ f(ab)=f(a)f(b)=\sigma\tau=(1\,2\,3\,4)\\ f(ab)^2=(1\,2\,3\,4)^2=(1\,3)(2\,4)\neq id\end{array}\right\}\Rightarrow (ab)^2\neq 1$$

Por tanto, $ord((ab)^2)=2$

$$(ba)^2=baba\overset{a^2=1}{=}aababa=a(ab)^2a^{-1}\Rightarrow ord((ba)^2)=ord((ab)^2)=2$$
$$(ab)^2(ba)^2=(ba)^2(ab)^2=bab^2ab$$
$$N=\left\langle (ab)^2,(ba)^2\right\rangle=\{1,(ab)^2,(ba)^2,bab^2ab\}$$

Veamos que $N\trianglelefteq G$ y para ello basta ver que

$$aNa^{-1}\leq N\quad y\quad bNb^{-1}\leq N$$
$$a(ab)^2a^{-1}=a(ab)^2a=aababa=baba=(ba)^2\in N$$
$$b(ab)^2b^{-1}=bababb^2=baba=(ba)^2\in N$$
$$a(ba)^2a^{-1}=ababaa=abab=(ab)^2\in N$$
$$b(ba)^2b^{-1}=bbabab^2=b^2abab^2=(ab)^2(ba)^2\in N$$

(3) $G/N=\langle aN,bN\rangle$. Demostrar que existe un epimorfismo

$$D_3\longrightarrow G/N$$
$$D_3=\left\langle r,s/r^3=1,\ s^2=1,\ sr=r^{-1}s\right\rangle$$
$$(bN)^3=b^3N=N\qquad (aN)^2=a^2N=N$$
$$(aN)(bN)=abN\Rightarrow[(aN)(bN)]\cong(ab)^2N=N\Rightarrow$$
$$\Rightarrow aNbNaNbN=N\Rightarrow aNbN=(aNbN)^{-1}=(bN)^{-1}\cdot(aN)^{-1}=(bN)^{-1}\cdot(aN)$$

Por el teorema de Dyck, existe un único

$$h:D_3\longrightarrow G/N\qquad \begin{array}{l}h(r)=bN\\ h(s)=aN\end{array}$$

epimorfismo

$$D_3/Ker(h)\cong G/N\Rightarrow |G/N|\leq 6$$
$$|G|=|G/N||N|\leq 6\cdot 4=24\quad G/Ker(f)\cong S_4\quad entonces\quad |G|=24$$

y $Ker(f)=\{1\}$, y por tanto f es un isomorfismo.