

Corolario: Sea G un grupo y sea $g \in G$, entonces:

1) $\langle g \rangle$ es infinito $\Leftrightarrow \{g^k\}$ son todos distintos entre sí.

2) $| \langle g \rangle | = m \Leftrightarrow m = \min \{ n > 0 : g^n = e \}$ y además $g^{m-n} = g^{-n} \Leftrightarrow m \mid n_2 - n_1$

En este caso $\langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\} \cong \mathbb{Z}_m$

Dem: Aplicar teo anterior al grupo $H = \langle g \rangle$

Def: Si G es grupo y $g \in G$, definimos el orden de g , y lo denotamos con $|g|$ o $l\langle g \rangle|$.

Resulta que $|g| = \begin{cases} \infty & \text{si } \exists n > 0 \text{ tal que } g^n = e. \\ \min \{ n > 0 : g^n = e \} & \text{caso contrario} \end{cases}$

Ejemplos: 1) En S_3 , $| \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} | = 2$, $| \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} | = 3$.

2) $|0| = \infty \quad \forall a \in \mathbb{Z}, a \neq 0$

3) En \mathbb{Z}_m , $|\bar{a}| = m \Leftrightarrow (a, m) = 1$

Determinar $|\bar{a}|$, $\forall \bar{a} \in \mathbb{Z}_m$ (en términos de (a, m))

Co-clases y congruencias

\mathbb{Z}_m es un grupo que se construye a partir de \mathbb{Z} así:

Tomemos subgrupo $H \subset \mathbb{Z}$ y definimos: ($H = \mathbb{Z}_m$)

1) $a \sim b \Leftrightarrow b - a \in H \quad (b - a = mu \cdot p \text{ para } m)$

2) definimos $\mathbb{Z}_m = \mathbb{Z}/n \leftarrow$ de 1

Aclararemos esto en general:

Def: Sea G grupo, $H \subset G$, definimos:

1) $g_1 \equiv g_2 \pmod{H}$ (\Leftrightarrow $g_2 - g_1 \in H$ $\Leftrightarrow g_1^{-1}g_2 \in H$)

2) $g_1 \equiv g_2 \pmod{H}$ (\Leftrightarrow $g_1^{-1}g_2 \in H \Leftrightarrow g_2^{-1}g_1 \in H$)

Y denotamos:

$$H^6 \quad a \quad 6/\mathbb{Z}_p$$

$$G/H \quad 0 \quad G/\mathbb{Z}_p$$

Ejercicio: Sea $G = S_3$, $H = \{\text{id}, \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 2 & 1 & 3 \\ \hline \end{array}\}$

Encuentrar $\sigma_1, \sigma_2 \in H$ tq $\sigma_1 \neq \sigma_2$ (σ_i)

Observa que si G es abeliano, $\sigma_1 = \sigma_2$

Clase 5 30/08

Definicións G

Resulta que σ_1, σ_2 Son relaciones de equivalencia (No nec. de congruencia)

Ejemplos: $\mathbb{N} \times \mathbb{N}$

Más obs: ①

$a \sigma_1 b \in H \Leftrightarrow \exists h \in H$ tq $ab^{-1} = h \Leftrightarrow \exists h \in H$ tq $a = hb \Leftrightarrow a \in hH$. $b = ha$.

$a \sigma_2 b \in H \Leftrightarrow \exists h \in H$ tq $b = ah \Leftrightarrow \exists h \in H$ tq $a = bh$

De estos dos casos se ve que $\overline{a} \underset{\text{en la relación anterior}}{\underset{\text{a dercha}}{\equiv}} H \overline{a}$

$\overline{a} \underset{\text{D.R.}}{\equiv} aH$

②

Es decir que los elementos de H^G son $\{Ha : a \in G\}$

$G/H \cong \{aH : a \in G\}$

③ Todos los clústeres de eg. tienen la misma cant. de elementos: $|H|$

Dem: $\overline{a} = Ha \xleftarrow{\psi} H$ sobre y 1-1
 $ha \xleftarrow{\psi} h$

Pruebo que $|\overline{a}| = |H|$

Idem $|\overline{a}^{-1}| = |H|$

④ En general, $H^G \neq G/H$, ver ejemplo en S_3 dentro, Sin embargo $|H^G| = |G/H|$

$H/G \xrightarrow{\Psi} G/H$ suryei Tomo $x \in G/H \Rightarrow \Psi(x^{-1}) = x \quad \therefore$ biye.

Recomiendo ver "laverade"

$\sigma_1, \sigma_2 \in H \Rightarrow \overline{\sigma_1} = \overline{\sigma_2} \Leftrightarrow \sigma_1^{-1} = \sigma_2^{-1}$

NOTA

$$\text{Dem: } g_1 \equiv g_2 \Rightarrow g_1^{-1} \equiv h g_2^{-1} \Rightarrow g_1^{-1} = (h g_2)^{-1} \Rightarrow g_1^{-1} \equiv g_2^{-1}$$

Una vez hecho la broma, φ es biyección pues $\varphi^{-1}(x^r) = \overline{x^{-r}}$

Def. La llamamos índice de H en G , γ lo devolvemos $[G:H]$ de numero. $|G/H| = |H^\gamma|$

Un conjunto de representantes de G/H es un conjunto $\{g_i \in G : i \in \mathbb{Z}\}$ + q $G/H = \{g_i H : i \in \mathbb{Z}\}$ sin repeticiones

es decir $g_i \neq g_j$ si $i \neq j$

Clausura $[S] = [G:H]$

ejemplo) En \mathbb{Z}_n , tomemos $\{0, 1, 2, \dots, n-1\}$ o un conjunto de representantes de \mathbb{Z}/\mathbb{Z}_n

$$2) \text{ En } H = \{I, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} \subset S_3$$

Representantes de G/H : Siendo $\bar{e}^r = \bar{e}^l = H$

$$S_3 = \left\{ \begin{array}{c|c|c|c|c|c|c} & \overset{\exists g}{\Delta} & & & & & \\ \hline 123 & 213 & 321 & 132 & 231 & 312 & \\ \hline - & 123 & 213 & 321 & 132 & & \\ \hline \overset{\exists g}{\Delta} & 213 & 123 & 231 & 312 & & \end{array} \right\}$$

$$\frac{-1}{S} = \sigma H$$

UN grupo rep. de G/H $\Rightarrow \{I_d, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$

Ej de c.c. $[G:H]=3$

$$|G| = |H| |G:H|$$

Tercero: Si $H \trianglelefteq G \Rightarrow |G| = |H| |G:H|$

$$\text{En particular } \Rightarrow |G| < \infty \Rightarrow [G:H] = \frac{|G|}{|H|}$$

Dem: Si $\{g_i\}_{i \in \mathbb{Z}}$ son rep. de $G/H \Rightarrow G = \bigcup_{i \in \mathbb{Z}} g_i H = \bigcup_{i \in \mathbb{Z}} g_i H$

Unión disjunta para $\{g_i\}$ con representante

$$\Rightarrow |G| = \sum_{i \in \mathbb{Z}} |g_i H| = |H| |G:H| = |H| \cdot |G:H|$$

Corolario (Teo. de Lagrange): Si $|G| < \infty$ y $H \trianglelefteq G \Rightarrow |H| \mid |G|$ En particular, si $g \in G$

$$\Rightarrow |g| \mid |G| \quad (\text{Usando en ej II})$$

Dem: de que $|H| \mid |G|$ es auto mágico por $|G| = |H| |G:H|$

de que $|g| \mid |G|$ sale de $|g| = \prod_{i=1}^k p_i^{e_i}$ > el rango anterior.

$$H \trianglelefteq G$$

Corolario: Si p es primo $\nexists p$ m tiene subgrupos propios ($\neq \{e\}, \mathbb{Z}_p$)

Además: Euler-Fermat: $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$$\text{O bien } (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

Dem: Por NP. p es primo, $|\mathbb{Z}_p| = p$ m es divisible por nadie salvo 1 y p

• Si $H \subset \mathbb{Z}_p$ resultado $|H| \geq 1 < p$.

Además: $\forall a \in \mathbb{Z}_p^\times$ $|a| = p-1 = \varphi(p)$

Sea $\bar{a} \in \mathbb{Z}_p^\times$ sabemos $|\bar{a}| \mid p-1 \Rightarrow p-1 = |\bar{a}| \cdot k$

$$\bar{a}^{|\bar{a}|} = 1, (\bar{a}^{|\bar{a}|})^k = 1$$

$$\begin{aligned} \bar{a}^{p-1} &= 1 \\ \bar{a}^{p-1} &= 1 \\ \Rightarrow a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

Teo: Si $K \triangleleft H \triangleleft G \Rightarrow [G:K] = [G:H] \cdot [H:K]$

$$\frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} \rightarrow \text{s: finitos, r.ido.}$$

Deron $\{g_i h_j\}_{i,j}$ representantes de H/K , $|\mathcal{I}| = [H:K]$

$$\otimes \vdash \{g_i h_j\}_{i,j} \text{ de } G/H, |\mathcal{J}| = [G:H]$$

Afirmamos que $\{g_i h_j : (i, j) \in \mathcal{I} \times \mathcal{J}\}$ son rep. de G/K

Hecho esto, ya verán más tarde $\Rightarrow |\mathcal{I} \times \mathcal{J}| = |\mathcal{I}| \cdot |\mathcal{J}|$

$$[G:K]$$

Demostremos la afirmación:

Debemos ver: $\begin{cases} (a) \text{ si } (i_1, j_1) \neq (i_2, j_2) \Rightarrow g_{j_1} h_{i_1} \neq g_{j_2} h_{i_2} (K) \\ (b) \forall g \in G, \exists (i, j) : g \equiv g_j h_i (H) \end{cases}$

b) Si $g \in G$, por $\otimes \exists j : g \equiv g_j (H) \Rightarrow g = g_j h_0 \xrightarrow{(1)} \exists i \text{ s.t. } h_0 \equiv_{\mathcal{H}} h_i (H)$

$$h_0 \in H$$

$$\Rightarrow h_0 = h_j u_0, u_0 \in K \Rightarrow g = g_j \cdot h_j \cdot u_0 \Rightarrow g \equiv_{\mathcal{H}} g_j h_j (K)$$

a) Sup $g_{j_1} h_{i_1} \equiv_{\mathcal{H}} g_{j_2} h_{i_2} (H) \Rightarrow \exists H \triangleleft K$

$$g_{j_1} h_{i_1} \stackrel{(1)}{=} g_{j_2} h_{i_2} H \Rightarrow g_{j_1} = g_{j_2} \underbrace{h_{i_2}^{-1} h_{i_1}}_{H} \Rightarrow g_{j_1} \equiv_{\mathcal{H}} g_{j_2} (H) \Rightarrow (i_1, j_1) = (i_2, j_2)$$

$$\text{NOTA: } \otimes \xrightarrow{(1)} j_1 = j_2 \Rightarrow h_{i_1} = h_{i_2} H \Rightarrow h_{i_1} \equiv_{\mathcal{H}} h_{i_2} (H)$$

$$\xrightarrow{(1)}$$

Ejercicio: Si $V = EV / F$, $\dim V = n$ y $S: W \rightarrow EV \otimes V$, dar una base de V/W . ¿ $\dim V/W$?

Proposición: Si $H, K \subset G$ y finitos $\Rightarrow |H|k| = \frac{|H||K|}{|H \cap K|}$

Dem: Relacionando con $\left\{ \begin{array}{l} \dim (W_1 + W_2) = \dim W_1 + \dim W_2 - \dim W_1 \cap W_2 \\ |A \cup B| = |A| + |B| - |A \cap B| \end{array} \right.$
 $n = [H : H \cap K]$ $\quad \textcircled{*}$

Sean h_1, \dots, h_n rep de $H/H \cap K \Rightarrow H = h_1(H \cap K) \cup h_2(H \cap K) \cup \dots \cup h_n(H \cap K)$

Unión disjunta. $n = \cancel{\# \text{ de } H} \quad \boxed{H = H \cap K}$

$$n = \frac{|H|}{|H \cap K|}$$

$\Rightarrow H/K = h_1K \cup h_2K \cup \dots \cup h_nK$. Con unión disj.

debemos ver $\textcircled{*} \Leftrightarrow$ lo disjunto.

$$=: \supseteq \quad \textcircled{v}$$

\subseteq Se ve $\textcircled{*}$: tom $h_i \in H \setminus K$, por \textcircled{v} $h = h_i \cup \dots \cup h_n \in H \cap K \Rightarrow h_i \cap h_j \cap K = \emptyset$ $\forall i \neq j$.

disj: Sup que hubiera $u \in h_i \cap h_j \cap K$. $\Rightarrow \exists u_1, u_2 \in K \ni h_i \cap u_1 = h_j \cap u_2 \Rightarrow h_i = h_j$ $\underbrace{u_1}_{\in K} \cup \underbrace{u_2}_{\in K}$

$$\Rightarrow h_i \equiv h_j (H \cap K) \Rightarrow i = j$$

$$(h_i^{-1} h_j = h_j h_i^{-1})$$

$$|H \cap K| = \sum_{i=1}^n |h_i \cap K| = n(K) = \frac{|H||K|}{|H \cap K|}$$

Cierre 6

01/09/23

Del teo de l'agrup: Si $|G| = p$ primo $\Rightarrow G \cong \mathbb{Z}_p$

Dem: Sea $g \in G, g \neq e \Rightarrow \langle g \rangle \neq \{e\} \Rightarrow \langle g \rangle = G \Rightarrow G$ cíclico $\Rightarrow G \cong \mathbb{Z}_p$

$$g^n \leftarrow h$$

$$2) \text{ Si } |G| = 4 \Rightarrow G \cong \begin{cases} \mathbb{Z}_4 & \text{if} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{else} \end{cases}$$

Def: Si G tiene un elemento de orden 4 $\Rightarrow G$ cíclico $\Rightarrow G \cong \mathbb{Z}_4$

Si no, todo $g \in G$, $g \neq e$ tiene $|g|=2$ ($(1g)(1g)$)

$G = \{e, g_1, g_2, g_3\}$ $|g_i| = 2 \Rightarrow g_i^2 = e \Rightarrow g_i, g_j \neq e$ si $i \neq j$

único

único

Ahora temporalmente supongamos que $g_i, g_j = \begin{cases} g_i & \Rightarrow g_i = e \\ g_j & \Rightarrow g_j = e \end{cases}$ obs.

Si $i \neq j$, $g_i g_j = g_{i+j}$, $i+j \neq i, j \Rightarrow$ abeliano ($g_i g_j = g_j g_i$) \Rightarrow

... y esto resulta $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Ejercicio: Si $\cup G$, todo $g \in G$ cumple $g^2 = e \Rightarrow G$ abel.

Ejercicio: Si $f: G_1 \rightarrow G_2$ es isomorfismo $\Rightarrow |f(x)| = 1 \forall x \in G_1$

$\therefore \mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$ pues \mathbb{Z}_4 tiene elementos de orden 4 y $\mathbb{Z}_2 \times \mathbb{Z}_2$ no

Subgrupos Normales

Def: Sea G grupo y $N \subset G$, decimos que N es normal y lo denotamos por $N \triangleleft G$

Si: $g, g^{-1} \in N, \forall n \in N, g \in G$

Obs: esa condición lo ves escribiendo $gN g^{-1} \subset N \quad \forall g \in G$ y resulta equivalente a

$gNg^{-1} = N \Leftrightarrow g \in G$

(1) \Rightarrow (2) Pues basta ver que si $n \in N \Rightarrow n \in gNg^{-1} \Rightarrow n = g \underbrace{(g^{-1}ng)}_{\in N \text{ gracias a (1)}} g^{-1} \in gNg^{-1}$

Sea $I: G \rightarrow \text{Aut}(G)$ definida así: $I_g(x) = g \cdot g^{-1}$. Resulta que I_g

es automorfismo