Clase 6: Teoremas de Sylow y Teorema chino del resto

Recuerdo: Si $|G| = p^n$, $n \geq 1$ $\Rightarrow |Z(G)| > 1$

§ 12 Fórmula de clases y p-grupos (continuación):

Corolario 2.2.15. — *Sea p un número primo y sea G un grupo finito.*

1. *Si $|G| = p^2$ entonces G es abeliano.*
2. *Si G es un p-grupo simple entonces $G \cong \mathbb{Z}/p\mathbb{Z}$.*

(Recuerdo: $G \neq \{e\}$ simple si $H \trianglelefteq G \Rightarrow H = \{e\}$ ó G)

Dem: (1) $|Z(G)| = p$ ó p^2. Si $x \in G$, $C_G(x) \overset{\text{def}}{=} \{g \in G \text{ tq } gx = xg\}$ contiene $Z(G)$ y $\{x\}$:

Si $x \notin Z(G) \Rightarrow |C_G(x)| \geq |Z(G)| + 1 \geq p+1 \Rightarrow |C_G(x)| = p^2$, ie, $C_G(x) = G$

ie, $x \in Z(G)$ $\cancel{\lightning}$ $\rightsquigarrow x \in Z(G)$ $\forall x \in G \iff G$ abeliano ✓

(2) $\{e\} \neq Z(G) \trianglelefteq G \underset{G \text{ simple}}{\Longrightarrow} G = Z(G)$, ie, G abeliano.

G p-grupo abeliano simple $\overset{G \text{ cíclico simple}}{\Longrightarrow} |G| = p \Longrightarrow G \cong \mathbb{Z}/p\mathbb{Z}$. ∎

(Sylow)

Obs: Sabemos que si $|G| = p \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$. Veremos más adelante que si $|G| = p^2 \Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z}$ ó $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

§ 13. Teoremas de Sylow

Durante esta sección, fijemos G un grupo finito. Además, si p es un número primo escribiremos:

$$|G| = p^\alpha m \quad \text{con} \quad p \nmid m \quad (\text{ie}, \ \alpha \text{ es maximal})$$

Definición 2.3.1 **(*p*-sub-grupo de Sylow).** — Un **p-sub-grupo de Sylow** de G es un sub-grupo $H \leq G$ de orden maximal $|H| = p^\alpha$.

ó "p-Sylow"

$\boxed{\text{Ejercicio}}$ Probar que el sub-grupo $T_n(\mathbb{F}_p)$ de matrices UNIPOTENTES, ie, de la forma

$$\begin{pmatrix} 1 & * & \cdots & * \\ & 1 & * & \vdots \\ & & \ddots & * \\ 0 & & & 1 \end{pmatrix}$$

es un p-subgrupo de Sylow de $GL_n(\mathbb{F}_p)$.
[Indicación: En otro Ejercicio se calculó $|GL_n(\mathbb{F}_p)|$.]

será útil hoy!

si $S \leq G$ p-subgrupo de Sylow y $g \in G$
$\Rightarrow gSg^{-1}$ es un p-subgrupo de Sylow (pues $S \cong gSg^{-1}$)

Lema 2.3.3. — *Si S es un p-sub-grupo de Sylow de G y $H \leq G$ es un sub-grupo arbitrario, entonces existe $g \in G$ tal que $gSg^{-1} \cap H$ es un p-sub-grupo de Sylow de H.*

<u>Dem</u>: $H \curvearrowright G/S$ por $h \cdot (gS) := (hg)S$

Estabilizador de $gS \in G/S$:

$$H_{gS} := \{ h \in H \text{ tq } hgS = gS \} = \{ h \in H \text{ tq } h \in gSg^{-1} \} = H \cap gSg^{-1}$$

<u>Obs</u>: $\mathrm{Card}(G/S) \overset{\text{Lagrange}}{=} |G| / |S| = p^{\alpha} m / p^{\alpha} = m$

↳ Como $p \nmid m = \mathrm{Card}(G/S)$, la fórmula de clases $\overset{m}{\overset{\shortparallel}{\mathrm{Card}(G/S)}} = \sum_{x \in R} [H : H_{xS}]$

$\Rightarrow \exists\, gS$ tq $p \nmid [H : H_{gS}]$

<u>Pero</u>: $H_{gS} = H \cap gSg^{-1} \leq \underbrace{gSg^{-1}}_{p\text{-Sylow}} \Rightarrow H_{gS}$ es p-grupo (ie, $|H_{gS}| = p^{\beta}$)

Como $p \nmid [H : H_{gS}] = \dfrac{|H|}{|H_{gS}|} \Rightarrow H_{gS}$ p-subgrupo de Sylow de H (ie, β es maximal) $\blacksquare$

Terminología: Sea $H \leq G$ subgrupo. El NORMALIZADOR de H en G es

$$N_G(H) := \{ g \in G \text{ tq } gHg^{-1} = H \}.$$

En part, $H \trianglelefteq G$ normal $\overset{\text{def}}{\iff} N_G(H) = G$. En gral, $H \trianglelefteq N_G(H)$.

Sea $X := \{ H \text{ subgrupo de } G \} \Rightarrow G \curvearrowright X$ mediante $g \cdot H := gHg^{-1}$

$\Rightarrow N_G(H)$ es el estabilizador de H resp. la acción anterior!

Teorema 2.3.5 (Sylow, 1872). — *Sea G un grupo y sea p un número primo tal que p divide $|G|$. Escribamos $|G| = p^\alpha m$ con $p \nmid m$. Entonces*

1. *G contiene un p-sub-grupo de Sylow.*
2. *Todo p-sub-grupo de G está contenido en algún p-sub-grupo de Sylow.*
3. *Todos los p-sub-grupos de Sylow son conjugados en G.*
4. *Sea n_p el número de p-sub-grupos de Sylow de G. Entonces $n_p \mid m$ y $n_p = 1 \mod p$.*

Dem: ① Sea $N = |G| \rightsquigarrow$ Cayley: $G \hookrightarrow S_N$ subgrupo.

$S_N \hookrightarrow GL_N(\mathbb{F}_p)$, $\sigma \mapsto u_\sigma$ con $u_\sigma(e_i) = e_{\sigma(i)}$ matriz de perm.

$\Rightarrow G \hookrightarrow GL_N(\mathbb{F}_p)$ y este último tiene un p-Sylow $\underset{\text{Lema}}{\Longrightarrow}$ G también, i.e, ① ✓✓

Dem (continuación): ② y ③: Sea $H \leq G$ p-grupo y $S \leq G$ p-Sylow

Lema $\Rightarrow \exists\, g \in G$ tq $gSg^{-1} \cap H$ es p-Sylow en H

$\underset{H \text{ p-grupo}}{\Longrightarrow} gSg^{-1} \cap H = H \Longrightarrow H \leq \underbrace{gSg^{-1}}_{\text{p-Sylow de } G}$ ✓

Si además H es p-Sylow de G: $|H| = p^{\alpha} = |gSg^{-1}| \underset{H \leq gSg^{-1}}{\Longrightarrow} H = gSg^{-1}$ ✓

④ $G \curvearrowright X = \{S \text{ p-Sylow de } G\}$, $g \cdot S := gSg^{-1}$ acción transitiva (por ③)

$\Rightarrow n_p = \operatorname{Card}(X)$ divide $|G| = p^{\alpha} m$.

Sea $S \in X$ fijo y consideremos $S \curvearrowright X$, $g \cdot \tilde{S} := g\tilde{S}g^{-1}$ $\forall g \in S$.

Hecho: $S \in X$ es el único punto fijo de $S \curvearrowright X$.

En efecto, si $\tilde{S} \in X^S$ fijo $\Longleftrightarrow g\tilde{S}g^{-1} = \tilde{S}$ $\forall g \in S$ $\overset{\text{def}}{\Longrightarrow} S \leq N_G(\tilde{S})$

Luego, S y $\tilde{S}$ son p-Sylow de $N_G(\tilde{S}) \overset{③}{\Longrightarrow} S$ y $\tilde{S}$ conjugados en $N_G(\tilde{S})$

ie, $\exists\, g \in N_G(\tilde{S})$ tq (i) $g\tilde{S}g^{-1} = S$ & (ii) $g\tilde{S}g^{-1} = \tilde{S}$ (def. de $N_G(\tilde{S})$!)

$\Rightarrow S = \tilde{S}$ ✓

$\rightsquigarrow X^S = \{S\}$ y luego $n_p = \operatorname{Card}(X) \equiv \operatorname{Card}(X^S) = 1 \pmod p$

$\Rightarrow n_p \equiv 1 \pmod p$ y $n_p \mid m$ ■

Corolario 2.3.6. — *Un p-sub-grupo de Sylow H de G es normal en G si y sólo si es el único p-sub-grupo de Sylow de G. En otras palabras, $H \trianglelefteq G$ si y sólo si $n_p = 1$.*

Ejemplos:

① La demostración de ④ muestra que $n_p = [G : N_G(S)]$, donde S es cualquier p-subgrupo de Sylow de G. (Ejercicio)

② Si $G = GL_n(\mathbb{F}_p)$, entonces todo p-subgrupo de Sylow de G está dado por matrices triang. superiores (en una base conveniente).

③ Sea p primo y consideremos S_p: $|S_p| = p! = p\cdot(p-1)\cdots 2\cdot 1$ y luego $H \leq S_p$ p-Sylow $\Rightarrow |H| = p$, i.e., $H = \langle (a_1, \dots, a_p) \rangle \cong \mathbb{Z}/p\mathbb{Z}$

Conteo: $a_1 \neq 1 \Rightarrow p-1$ elecciones para a_1 ✓ $\rightsquigarrow a_2 \neq 2$ y $a_2 \neq a_1 \Rightarrow p-2$ elecciones para a_2 $(\cdots) \Rightarrow \exists\ (p-1)!$ ciclos de largo p en S_p: $\sigma_1, \sigma_1^2, \dots, \sigma_1^{p-1}, \dots, \sigma_r, \sigma_r^2, \dots, \sigma_r^{p-1}$

⚠ $\langle \sigma_i \rangle = \langle \sigma_i^j \rangle$, $j \in \{1, \dots, p-1\}$ $\Rightarrow n_p = r$ (por definición!) $\Rightarrow (p-1)\, n_p = (p-1)!$

$\underset{\text{Sylow}}{\Longrightarrow} \underbrace{(p-2)!}_{n_p} \equiv 1 \pmod p$ ($\Rightarrow$ Teorema de Wilson: Si p primo, entonces $(p-1)! \equiv -1 \pmod p$)

Corolario 2.3.8. — *Sea G un grupo y sea p un número primo tal que p divide $|G|$. Escribamos $|G| = p^\alpha m$ con $p \nmid m$. Entonces, para todo $\beta \leq \alpha$ existe $H \leq G$ con $|H| = p^\beta$. En particular, si p divide $|G|$ entonces existe un elemento $g \in G$ con $\mathrm{ord}(g) = p$.* } Lema de Cauchy

Dem:

Sea $S \leq G$ p-Sylow (i.e, $|S| = p^\alpha$) y $g \in Z(S)^{\neq \{e\}}$ con $g \neq e$

$\Rightarrow \mathrm{ord}(g) = p^\gamma$ cierto $\gamma \in \mathbb{N}^{\geq 1}$ (Lagrange)

Astucia: $H := \langle g^{p^{\gamma-1}} \rangle \cong \mathbb{Z}/p\mathbb{Z}$

orden p

Como $g \in Z(S)$, $H \trianglelefteq S$ y $|S/H| = |S| / |H| = p^\alpha / p = p^{\alpha-1}$

Inducción en α: S/H posee subgrupos de ordenes $p, p^2, \ldots, p^{\alpha-2}$

Lagrange: Las preimágenes de dichos grupos por $S \xrightarrow{\pi} S/H$ tienen ordenes $p^2, p^3, \ldots, p^{\alpha-1}$ ■

Más ejemplos: Sea G grupo finito.

① Sup. $|G| = 42 = 2 \cdot 3 \cdot 7 \Rightarrow G$ NO es simple.

En efecto: Sylow implica $n_7 \equiv 1 \pmod 7$ y $n_7 \mid 2 \cdot 3 = 6 \Rightarrow n_7 = 1$

$\Rightarrow \exists!$ 7-subgrupo de Sylow S y $S \trianglelefteq G$.

② Sup. G simple $\Rightarrow |G|$ divide $n_p!$ para todo $p \mid |G|$.

En efecto: Vimos que $G \curvearrowright X = \{S \leq G \text{ p-Sylow}\}$, $g \cdot S = gSg^{-1}$ es transitiva

equivale a $\Phi : G \to \mathrm{Biy}(X) \cong S_{n_p}$ morfismo con $\ker(\Phi) \neq G$

G simple $\Rightarrow n_p > 1$ y además $\ker(\Phi) = \{e\}$ en este caso

$\Rightarrow G \hookrightarrow S_{n_p}$ inyectivo $\Rightarrow |G|$ divide $|S_{n_p}| = n_p!$ (Lagrange).

③ Sup. $|G| = 48 = 2^4 \cdot 3 \Rightarrow G$ NO es simple.

En efecto: Sylow implica $n_2 \equiv 1 \pmod 2$ y $n_2 \mid 3 \Rightarrow n_2 \in \{1, 3\}$.

Si G fuese simple, $n_3 = 3 \overset{②}{\Rightarrow} |G| = 48$ divide $3! = 6$ ↯

Ejemplo importante (Grupos abelianos finitos):

Sea $(G,+)$ un grupo abeliano finito ($\Rightarrow$ Todo subgrupo es normal !)

$\rightsquigarrow$ Sylow: Para todo p primo, $\exists!$ p-subgrupo de Sylow S (pues $S \trianglelefteq G$)

Consideremos el SUBGRUPO DE p-TORSIÓN de G dado por

$$T_p(G) := \{ g \in G \text{ tq } \exists n \in \mathbb{N}^{\geq 1} \text{ con } \underbrace{p^n g}_{\text{aditivo}} = 0 \}$$

$g + \cdots + g$ (p^n veces)

$\rightsquigarrow$ Subgrupo pues G abeliano !

Obs: Si $g \in S \Rightarrow ord(g) = p^n$ cierto $n \in \mathbb{N} \Rightarrow g \in T_p(G)$, ie, $S \leq T_p(G)$

⚠ Si $g \in T_p(G) \Rightarrow ord(g) = p^n$ cierto $n \in \mathbb{N} \xRightarrow{\text{Corolario anterior}} |T_p(G)| = p^\alpha$ cierto $\alpha \in \mathbb{N}$

$\Rightarrow S = T_p(G)$ pues $S \leq T_p(G)$ son p-grupos y S p-Sylow ✓

$\boxed{\text{Ejercicio}}$ $G = \mathbb{Z}/6\mathbb{Z}$, calcular $T_2(G)$ y $T_3(G)$.

§14 Teorema chino del resto


孫子算經卷上
唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋
度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

El siguiente resultado, enunciado por Sun Zi ($\approx 400-460$, China), es un resultado fundamental sobre grupos abelianos finitos.

Teorema 2.4.2 (Teorema chino del resto). — *Sea* $n \in \mathbb{N}^{\geq 1}$ *con* $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ *descomposición en números primos. Entonces,*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}.$$

<u>Dem</u> (Inducción en $r \in \mathbb{N}^{\geq 1}$): Basta probar que si $\operatorname{mcd}(d,e) = 1$ entonces $\mathbb{Z}/de\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$. Sea

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$$
$$x \longmapsto ([x]_d, [x]_e)$$

$$\Rightarrow \ker(f) = de\mathbb{Z} \overset{\text{Prop Univ.}}{\Longrightarrow} \exists!\, \hat{f} : \underbrace{\mathbb{Z}/de\mathbb{Z}}_{\text{cardinal}} \overset{\sim}{\hookrightarrow} \underbrace{\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}}_{\text{cardinal}}$$

cardinal $=$ de $=$ cardinal $\blacksquare$

En realidad, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$ es un isomorfismo de <u>anillos</u> $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$ grupos de unidades.