2|10|24

Corolario: $[G:S]=p \Rightarrow S \trianglelefteq G$ (G p-grupo finito)

Demostración:

$S \subsetneq N_G(S) \Rightarrow N_G(S) = G \Leftrightarrow S \trianglelefteq G$

$\square$

Proposición: $|G| = p^n$, $n \in \mathbb{N}_0$. Entonces:

i) $\forall\ 0 \leq i \leq n$, G posee subgrupos de orden p^i

ii) Si $0 \leq i \leq n-1$ y $S \leq G$ con $|S| = p^i \Rightarrow \exists$ subgrupo T de orden p^{i+1} tal que $S \trianglelefteq T$

Recordar:

1) $G \times X \longrightarrow X$, $|X| = |X^G| + \sum_{i \in I} [G:G_i]$, $G_i \subsetneq G$

2) $H \trianglelefteq G$, $\{\text{subgrupos } U \text{ de } G/H\} \longleftrightarrow \{\text{subgrupos } W \text{ de } G,\ H \leq W\}$

correspondencia

Demostración:

i) Inducción sobre n:

Si $n=0$ no hay nada que probar

Supongamos $n \geq 1$ y que el enunciado vale para grupos de orden p^m, $0 \leq m < n$

- Caso G abeliano ($G = Z(G)$):

Por Teorema de Cauchy ($n>0$) $p \mid |G| \Rightarrow \exists x \in G$ tq $|x| = p$

$\langle x \rangle \trianglelefteq G$, $\left| G/\langle x \rangle \right| = p^{n-1}$

Por HI $G/\langle x \rangle$ posee subgrupo $\tilde{S}$ de orden p^j $\forall j = 0, \dots, n-1$

Entonces, por el Teorema de Correspondencia (donde f sería la proyección al cociente), $\tilde{S} = S/\langle x \rangle$, $\langle x \rangle \leq S \leq G$

$$|\tilde{S}| = p^j = \frac{|S|}{\underbrace{|x|}_{=p}} \Rightarrow |S| = p^{j+1}$$

Si $i=1$ tomamos $\langle x \rangle$, si $i = j+1$ tomamos S y así obtenemos i) para este caso de G abeliano.

Caso G no abeliano ($Z(G) \subsetneq G$):

$|Z(G)| = p^m \qquad 0 < m < n \qquad (|G| = p^n)$

↳ por ser p-grupo

Por HI $G/Z(G)$ contiene un subgrupo $\tilde{S}$ de orden p^k, para cada $0 \leq k \leq n-m$ tal que $|\tilde{S}| = p^k$

Por otro lado $Z(G)$ contiene subgrupos de orden p^i para cada $0 \leq i \leq m$

Estos son subgrupos de G

- Si $n \geq i \geq m+1$ sea $\tilde{S} \leq G/Z(G)$, $|\tilde{S}| = p^{i-m}$ $\quad (n-m \geq i-m \geq 1)$

  $\tilde{S} = S/Z(G) \quad \Rightarrow \quad |S| = |\tilde{S}|\,|Z(G)| = p^i$

ii) $(0 \leq i \leq n-1,\ |S| = p^i \Rightarrow \exists\, T \leq G \quad |T| = p^{i+1}$ y $S \trianglelefteq T)$

Como $S \subsetneq G \Rightarrow S \subsetneq N_G(S)$ se podría aplicar Cauchy directamente

Ahora $N_G(S)/S$ es un p-grupo finito $\Rightarrow$ por la parte (i) $\exists\, H \leq N_G(S)/S$ $|H| = p$ y por el Teorema de Correspondencia $H = T/S$, $S \leq T \leq N_G(S)$

$\Rightarrow |T| = |H|\,|S| = p^{i+1}$ y $S \trianglelefteq T$

$\square$

En general esto no vale para cualquier grupo G que no sea un p-grupo

Ejemplos se dan con S_n

TEOREMAS DE SYLOW

G grupo finito, p primo

Definición: un p-subgrupo de Sylow de G ($\to$ p-Sylow) es un subgrupo H tal que $|H| = p^n$ donde $|G| = p^n k$, $(p,k) = 1$

ie. $|H|$ es la mayor potencia de p que divide a $|G|$

Primer Teorema de Sylow: supongamos que $|G| = p^n k$, $(p,k) = 1$. Entonces $\forall\, 0 \leq i \leq n$, G posee un subgrupo de orden p^i. En particular G posee un p-Sylow

Demostración:

Notemos que un p-Sylow es un p-grupo

Por la primera parte de la proposición anterior, basta probar que G contiene un p-Sylow

- Caso G abeliano ($G = Z(G)$): supongamos que $p \mid |G|$ $(n>0)$

  Sea $G[p] = \{x \in G \mid p^i x = 0$, para algún $i \geq 0\}$ (elementos de G cuyo orden es potencia de p)

  $G[p]$ es subgrupo de G: $p^i x = 0$, $p^j y = 0$

  Sea $l = \max(i,j)$ $\quad p^l(x-y) = p^l x - p^l y = 0 - 0 = 0$

  esto no vale cuando G es no abeliano

  $G[p]$: componente p-primaria de G

  Como $G[p]$ es p-grupo $\Rightarrow |G[p]| = p^m$, para algún $0 < m \leq n$

  Si fuese $m < n$: $\left|G/G[p]\right| = p^{n-m} \cdot k$, $n-m>0$ o sea $p \mid \left|G/G[p]\right|$

  Por Cauchy $\Rightarrow \exists\, \bar{a} \in G/G[p]$ tal que $|\bar{a}| = p$: $\underbrace{pa\,G[p]}_{\bar{a}} = \underbrace{G[p]}_{0}$

  $\Rightarrow p \cdot a \in G[p] \Rightarrow \exists\, l$ tal que $p^l(pa) = 0 \Rightarrow p^{l+1} a = 0$

  $\Rightarrow a \in G[p] \Rightarrow \bar{a} = \bar{0}$

  Pero esto contradice $|\bar{a}| = p$, luego $m = n$ y $G[p]$ es p-Sylow de G

- Caso G no abeliano ($Z(G) \lneq G$):

Hacemos inducción en el orden de G

La afirmación es cierta si $|G|=1$ (pues $\nexists$ primo que divida a 1)

Supongamos $|G|>1$ y que el Teorema vale para grupos de orden $<|G|$

Por la Ecuación de clases (acción por conjugación):

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G:G_i] \quad , \quad G_i \lneq G$$

Si $p \nmid |Z(G)|$

Podemos suponer también que $p \mid |G|$ (si no, es trivial)

$\Rightarrow \exists\ 1 \leq i \leq r$ tal que $p \nmid [G:G_i]$, de donde $p^n \mid |G_i|$ $\quad (|G| = p^n \cdot k, (n,k)=1)$

Por HI ($|G_i|<|G|$) G_i posee un subgrupo de orden p^n y este es un p-Sylow de G

Supongamos que $p \mid |Z(G)|$ $\quad (|Z(G)|<|G|)$

$$|Z(G)| = p^m d \quad , \quad 0<m\leq n \quad (d,p)=1$$

Por lo visto en el caso abeliano, $Z(G)$ contiene un subgrupo T con $|T|=p^m$

Además $T \trianglelefteq G$ (pues $T \leq Z(G)$)

$|G/T| = p^{n-m} \cdot k$. Como $m>0 \Rightarrow n-m<n$ y $|G/T|<|G|$

Por HI, $\exists\ \tilde{H}$ de G/T con $|\tilde{H}| = p^{n-m}$

Por el Teorema de Correspondencia $\Rightarrow \tilde{H} = H/T$, $T \leq H \leq G$

$|H| = |T||\tilde{H}| = p^m \cdot p^{n-m} = p^n$ $\quad \therefore$ H es un p-Sylow de G

$\square$

Segundo Teorema de Sylow: sea G grupo finito y p primo

Sean $S \leq G$ tal que $|S| = p^i$, $i \in \mathbb{N}_0$ y H un p-subgrupo de Sylow de G

Entonces $\exists a \in G$ tal que $S \leq aHa^{-1}$ (S no neces. dentro de H pero sí podemos decir que está dentro de algún conjugado)

En particular: S p-Sylow $\Leftrightarrow$ S y H son conjugados

Demostración: sea S p-Sylow de G

Consideremos la acción de S en $X = \{Hx \mid x \in G\} = {}_H\backslash G$ dada por:

$$g \cdot Hx = Hxg^{-1}$$ (ejercicio: probar que es una acción)

Por la ecuación de clases:

$$\underbrace{[G:H]}_{\text{coprimo con } p} = |X| = |X^S| + \sum_i [S:S_i] \quad , \quad S_i \lneq S$$

En particular, como S es un p-subgrupo $\Rightarrow p \mid [S:S_i] \quad \forall i$

$\Rightarrow |X^S| \neq \emptyset \quad \Rightarrow \exists\, a \in G$ tal que $Hag^{-1} = Ha \quad \forall g \in S$

y esto ocurre $\Leftrightarrow aga^{-1} \in H \quad \forall g \in S$

$\Leftrightarrow aSa^{-1} \subseteq H$

$\Leftrightarrow S \subseteq a^{-1}Ha$

$\square$

Notar que si tenemos 2 p-subgrupos de Sylow (?) son conjugados del mismo p

Corolario: sea $H \leq G$. H es el único p-Sylow de $G \Leftrightarrow H \trianglelefteq G$

Tercer Teorema de Sylow: sea G grupo finito, p primo y sea $n_p = |\{p\text{-subgrupos de Sylow de } G\}|$. Entonces $n_p \mid |G|$ y $n_p \equiv 1\ (p)$

Demostración:

Podemos suponer que $p \mid |G|$

Sean $S_1, \dots, S_{n_p}$ los p-Sylow distintos de G y sea $X = \{S_2, \dots, S_{n_p}\}$

sacamos S_1

S_1 actúa en X por conjugación: $x \cdot S_j = x S_j x^{-1}$

Buena definición:

Si fuese $x S_j x^{-1} = S_1 \quad (j \geq 2, x \in S_1) \Rightarrow S_j = x^{-1} S_1 x = S_1$ Abs!

Por la ecuación de clases:

$$n_p - 1 = |X| = |X^{S_1}| + \sum_{i=1}^{k} \underbrace{[S_1 : H_i]}_{\text{divisible por } p\ \forall i} \quad , \quad H_i \lneq S_1$$

Si $S_j \in X^{S_1}$, $2 \leq j \leq n_p \Rightarrow x S_j x^{-1} = S_j \quad \forall x \in S_1 \Leftrightarrow S_1 \leq N_G(S_j)$

Pero también tenemos $S_j \trianglelefteq N_G(S_j)$

$\Rightarrow S_1$ y S_j son p-Sylow de $N_G(S_j)$

Por el 2° Teorema de Sylow $\Rightarrow S_1 = S_j$, $j \geq 2$ Abs!

$\therefore X^{S_1} = \emptyset \Rightarrow p \mid |X| = n_p - 1$ y así $n_p \equiv 1\ (p)$

Notemos que $n_p = [G : N_G(S)]$, $S = S_1$ p-Sylow

En general, si $H \leq G$ cualquiera, la cantidad de conjugados de H es $[G : N_G(H)]$ (ejercicio)

En particular $n_p \mid |G|$

$\square$

(Acá termina la parte de grupos)