Lección nº 3 Junio, 2021

Capítulo 3

Teoremas de Sylow

Consideremos $p \geq 2$ un número primo.

Definición. Un grupo G se llama un *p-grupo* si todo elemento de G tiene orden igual a una potencia de p.

Proposición 3.1. *Sea G un grupo finito. G es un p-grupo si y solo si $|G| = p^n$ para algún entero $n \geq 1$.*

Ejercicio 3.2. Demostrar la proposición anterior.

El siguiente resultado ya ha sido probado como una consecuencia de la ecuación de clases en el capítulo anterior. Lo enunciamos nuevamente aquí por conveniencia.

Teorema 3.3. *Si G es un p-grupo finito con $|G| > 1$, entonces $|Z(G)| \geq p$.*

Ejemplos 3.4. (1) $\mathbb{Z}/p^n\mathbb{Z}$ es un p-grupo.

(2) Si G es un p-grupo, $|G| = p^2$, entonces G es abeliano.

Notación: Sea G un grupo finito, p primo tal que $p \mid |G|$. Notaremos como $p^a \mid\mid |G|$ si a es el índice tal que

$$p^a \mid |G| \quad \text{y} \quad p^{a+1} \nmid |G|,$$

o equivalentemente

$$|G| = p^a m, \quad p \nmid m.$$

Definición. Sea G un grupo finito con $p^a \mid\mid |G|$. Un subgrupo $P \leq G$ se llama un *p-subgrupo de Sylow de G* si

$$|P| = p^a.$$

Se denota

$$\mathrm{Syl}_p(G) = \{P \leq G \mid P \text{ es } p\text{-subgrupo de Sylow}\}.$$

Teorema 3.5 (Primer Teorema de Sylow)**.** *Si G es un grupo finito, con $p \mid |G|$, entonces G tiene un p-subgrupo de Sylow.*

Lema 3.6. *Sea $n = p^a m$, $p \nmid m$, con p un primo. Entonces*

$$\binom{n}{p^a} \equiv m \pmod{p}.$$

Demostración del lema. Veamos las siguientes congruencias

$$\begin{aligned}(x+1)^p &\equiv x^p + 1 \pmod{p}\\ (x+1)^{p^2} &\equiv x^{p^2} + 1 \pmod{p}\\ &\vdots\\ (x+1)^{p^a} &\equiv x^{p^a} + 1 \pmod{p}.\end{aligned}$$

Pero

$$(x+1)^n = (x+1)^{p^a m} = \left((x+1)^{p^a}\right)^m \equiv (x^{p^a}+1)^m \pmod{p}.$$

Comparando a ambos lados el coeficiente de x^{p^a} deducimos que

$$\binom{n}{p^a} \equiv m \pmod{p}.$$

□

Demostración del Primer Teorema de Sylow. Supongamos que $|G| = p^a m$, $p \nmid m$. Sea $X = \{A \subseteq G \,|\, |A| = p^a\}$; así, por el lema anterior

$$|X| = \binom{|G|}{p^a} \equiv m \pmod{p},$$

lo que implica que $p \nmid X$ pues $p \nmid m$.

Definamos una acción de G sobre X.

$$\begin{aligned}G \times X &\longrightarrow X\\ (g, A) &\longmapsto gA.\end{aligned}$$

Descomponiendo X en órbitas, $|X| = \sum_{i=1}^{k} |O_i|$, con $O_1, \ldots, O_k$ órbitas distintas. Como $p \nmid |X|$ existe $O = O_i$ tal que $p \nmid |O|$.

Sea $A \in X$ tal que $O = G \cdot A$ (órbita que contiene a A), entonces

$$G_A = \mathrm{Stab}_G(A) \leq G.$$

Sabemos que

$$|O| = [G\colon G_A] = \frac{|G|}{|G_A|},$$

como $p \nmid |G|$ se sigue $p \nmid \frac{|G|}{|G_A|}$; pero $p^a \,||\, |G|$, así $p^a \mid |G_A|$, de donde $p^a \leq |G_A|$.

Afirmamos que $|G_A| = p^a$, entonces G_A es un p-subgrupo de Sylow de G. Sea $a \in A$, así para todo $h \in G_A = \mathrm{Stab}_G(A)$ se verifica

$$h \cdot a \in h \cdot A = A,$$

en consecuencia $G_A \cdot a \subseteq A$.
Así, $|G_A \cdot a| \leq |A| = p^a$; pero se tiene la biyección

$$\begin{array}{rcl} G_A & \longleftrightarrow & G_A \cdot a \\ g & \longmapsto & g \cdot a, \end{array}$$

lo que implica que $|G_A| = |G_A \cdot a| \leq p^a$, y por tanto $|G_A| = p^a$. Este grupo de Sylow es un estabilizador de un subconjunto $A \subseteq G$ de orden p^a. □

Si $P \leq G$ es un p-subgrupo de Sylow, entonces para todo $g \in G$, gPg^{-1} es un p-subgrupo de Sylow.

Ejercicio 3.7. Probar que $gG_Ag^{-1} = G_{g_A}$.

Observación. Si $p \nmid |G|$ en el Primer Teorema de Sylow, entonces el p-subgrupo de Sylow es trivial.

Proposición 3.8. *Sea G un grupo finito, $H \leq G$. Sea $S \in \mathrm{Syl}_p(G)$ un p-subgrupo de Sylow de G. Entonces existe $g \in G$ tal que*

$$H \cap gSg^{-1} \leq H$$

es un p-subgrupo de Sylow de H.

Observación. Si $p \mid |G|$ y $p \mid |H|$, este subgrupo es no trivial.

Demostración. Sea S un p-subgrupo de Sylow de G. Consideremos la acción de H sobre G/S

$$\begin{array}{rcl} H \times G/S & \longrightarrow & G/S \\ (h, gS) & \longmapsto & hgS. \end{array}$$

Calculemos

$$\begin{aligned} \mathrm{Stab}_H(xS) &= \{h \in H \mid hxS = xS\} \\ &= \{h \in H \mid x^{-1}hxS = S\} \\ &= \{h \in H \mid h \in xSx^{-1}\} \\ &= H \cap xSx^{-1}. \end{aligned}$$

Como S es p-subgrupo de Sylow de G entonces, $p \nmid |G/S|$ y G/S es la unión disjunta de H-órbitas, es decir

$$|G/S| = \sum |O_{\bar{x}_i}|,$$

con $\bar{x}_i \in G/S$ ($\bar{x}_i = x_iS$), y $O_{\bar{x}_i}$ son las distintas órbitas concluimos que existe $O = H \cdot gS$ tal que $p \nmid |O| = [H : \mathrm{Stab}_H(gS)] = |H|/|\mathrm{Stab}_H(gS)|$. Luego, como $p^b \,||\, |H|$ tenemos

$$p \nmid \frac{|H|}{|\mathrm{Stab}_G(gS)|},$$

lo que implica $p^b \,||\, |\mathrm{Stab}_H(gS)| = |H \cap gSg^{-1}|$, de donde $p^b \mid |H \cap gSg^{-1}|$ y así $p^b \leq |H \cap gSg^{-1}|$.

Ahora, $|H \cap gSg^{-1}| \mid |H|$ y $|gSg^{-1}|$ es potencia de p, entonces $|H \cap gSg^{-1}| = p^b$; lo que a su vez implica que $H \cap gSg^{-1}$ sea un p-subgrupo de Sylow de H. □

Corolario 3.9. *Sea $H \leq G$ un grupo finito y $p \geq 2$ un primo. Si G contiene un p-subgrupo de Sylow, entonces H contiene un p-subgrupo de Sylow.*

Observación. Sea G un grupo finito que admite un monomorfimos $f\colon G \to G'$ en un grupo G'. Si G' tiene un p-subgrupo de Sylow, entonces G también.

Ejemplo 3.10. Sea G un grupo finito y llamemos $n = |G|$. A la acción regular por izquierda

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & xy \end{array}$$

le corresponde un homomorfismo $\phi\colon G \to \mathrm{Sym}(G) = S_n$, y de hecho ϕ es un monomorfismo. Así

$$\begin{array}{rcl} G \hookrightarrow S_n & \hookrightarrow & \mathrm{GL}(n, \mathbb{F}_{p^n}) \\ \sigma & \longmapsto & I_\sigma. \end{array}$$

Por tanto, $G \hookrightarrow \mathrm{GL}(m, \mathbb{F}_{p^n})$.

$\mathrm{GL}(m, \mathbb{F}_{p^n})$ se identifica con el conjunto de todas las bases del espacio vectorial $\mathbb{F}_{p^n}^m$. Luego, si $q = p^n$

$$\begin{aligned} |\mathrm{GL}(m, \mathbb{F}_q)| &= (q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}) \\ &= q^{\frac{m(m-1)}{2}} \prod_{i=1}^{m} (q^i - 1) \\ &= p^{\frac{nm(m-1)}{2}} \prod_{i=1}^{m} (p^{in} - 1), \end{aligned}$$

por lo que $p^{\frac{nm(m-1)}{2}} \mid\mid |\mathrm{GL}(m, \mathbb{F}_q)|$.

Ejercicio 3.11. Sea

$$H = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; * \in \mathbb{F}_{p^n} \right\}.$$

Demostrar que $|H| = p^{\frac{nm(m-1)}{2}}$ y $H \leq \mathrm{GL}(m, \mathbb{F}_q)$. Por ende , H es un p-subgrupo de Sylow de $\mathrm{GL}(m, \mathbb{F}_{p^n})$.

Ejercicio 3.12. Sea P un p-subgrupo de Sylow de G (finito) y $H \leq G$ un p-subgrupo. Entonces

$$H \cap N_G(P) = H \cap P.$$

Proposición 3.13. *Sea G un grupo de orden p^a, $a \geq 1$. Entonces G contiene un subgrupo normal de orden p^{a-1}. Además, existen subgrupos $G_1, G_2, \ldots, G_{a-1}$ con*

$$G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_{a-1} \triangleleft G_a = G,$$

tales que $|G_i| = p^i$.

Demostración. De la proposición, existe $G_{a-1} \triangleleft G$ con $|G_{a-1}| = p^{a-1}$. G_{a-1} es un p-grupo de orden p^{a-1}, entonces existe $G_{a-2} \triangleleft G_{a-1}$ con $|G_{a-2}| = p^{a-2}$. Más precisamente, se puede alcanzar que $G_i \triangleleft G$ para todo i. □

Teorema 3.14. *Sea G un grupo con $|G| = p^a$. Entonces para todo $0 \leq b \leq a-1$, existe un subgrupo normal $G_b \trianglelefteq G$ tal que $|G_b| = p^b$ y se tiene además que*

$$G_i \trianglelefteq G_{i+1} \quad \forall\, i,$$

y tenemos una cadena de subgrupos

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_{a-1} \trianglelefteq G_a = G.$$

Además, G_{i+1}/G_i es cíclico de orden p.

Demostración. Se demostrará el resultado por inducción con respecto a a ($|G| = p^a$). Si $a = 1$ no hay nada que probar.

Sea $a \geq 2$. Como G es un p-grupo, $|Z(G)| \geq p$ y es un p-grupo. Por el Teorema de Cauchy, existe $x_1 \in Z(G)$ tal que $x_1^p = 1$, es decir $|\langle x_1\rangle| = p$ y $\langle x_1\rangle \trianglelefteq G$. Definamos $G_1 = \langle x_1\rangle$, $|G_1| = p$ y $G_1 \trianglelefteq G$. Así, G/G_1 es un p-grupo y $|G/G_1| = p^{a-1}$. Por inducción existen subgrupos normales $\overline{G_i} \trianglelefteq G/G_1$ con $|\overline{G_i}| = p^{i-1}$ y $\overline{G_i} \trianglelefteq \overline{G_{i+1}}$ para $i \in \{2, \ldots, a-1\}$. Por tanto

$$\overline{G_1} = \{1\} \trianglelefteq \overline{G_2} \trianglelefteq \cdots \trianglelefteq \overline{G_{a-1}} \trianglelefteq \overline{G_a} = \overline{G} = G/G_1.$$

Ahora, $\overline{G_i} = G_i/G_1$, con $G_i \trianglelefteq G$, $|G_i| = p^i$. Así, tenemos

$$G_0 = \{1\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_{a-1} \trianglelefteq G_a = G,$$

con $|G_i| = p^i$, y $|G_{i+i}/G_i| = p$ pues este es cíclico de orden p. □

Definición. Un grupo G se dice *nilpotente* si existen $G_i \trianglelefteq G$, $0 \in \{1, \ldots, n\}$ tales que

$$\{1\} = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

y G_{i+1}/G_i es cíclico para todo $i \in \{0, \ldots, n-1\}$.

Corolario 3.15. *Sea $p \leq 2$ y G un p-grupo. Entonces G es nilpotente.*

Teorema 3.16 (Segundo y tercer teorema de Sylow)**.** *Sean $p \geq 2$ primo, $a \in \mathbb{Z}^+$ y G un grupo tales que $p^a || \, |G|$. Sea además $P \leq G$ un p-grupo y $S \in \mathrm{Syl}_p(G)$ un p-subgrupo de Sylow. Entonces existe $g \in G$ tal que*

$$P \leq gSg^{-1}.$$

En particular, si P también es un grupo de Sylow, entonces

$$P = gSg^{-1}.$$

Es decir que $\mathrm{Syl}_p(G)$ es la clase de conjugación de S.

Demostración. Sea $X = \{xS \,|\, x \in G\} = G/S$. Como $p^a || \, |G|$, entonces existe $m \in \mathbb{Z}^+$ tal que $|G| = p^a m$ y $p \nmid m$, así

$$|X| = \frac{|G|}{|S|} = \frac{p^a m}{p^a} = m,$$

de modo que $p \nmid |X|$. P opera sobre G mediante la siguiente acción

$$\begin{aligned} P \times X &\to X \\ (g, xS) &\mapsto gxS. \end{aligned}$$

Luego, de la ecuación de clases, existe una órbita $O = P \cdot xS$, con $x \in G$, tal que $p \mid |O|$. Por otro lado sabemos que $|O| \mid |P|$, y entonces $|O| = 1$. Así, para todo $g \in P$ tenemos que

$$\begin{aligned} g \cdot xS = xS &\Rightarrow x^{-1}gxS = S \\ &\Rightarrow x^{-1}gx \in S \\ &\Rightarrow g \in xSx^{-1}. \end{aligned}$$

De donde $P \leq xSx^{-1}$. En particular, si $|P| = p^a$ entonces $P = xSx^{-1}$, es decir que los p-grupos de Sylow son conjugados. □

Corolario 3.17. *Sea G un grupo finito y $P \in \mathrm{Syl}_p(G)$, entonces*

$$\left|\mathrm{Syl}_p(G)\right| = [G\colon N_G(P)]$$

y

$$\left|\mathrm{Syl}_p(G)\right| \mid [G\colon P] = m,$$

con $m \in \mathbb{Z}^+$ tal que $|G| = p^a m$, $p \nmid m$.

Demostración. Consideremos la acción de G sobre $\mathrm{Syl}_p(G)$ dada por

$$\begin{aligned} G \times \mathrm{Syl}_p(G) &\to \mathrm{Syl}_p(G) \\ (g, S) &\mapsto gSg^{-1}. \end{aligned}$$

Veamos primero que $\mathrm{Syl}_p(G) = \mathrm{Orb}_G(P)$. En efecto: Si $S \in \mathrm{Syl}_p(G)$, como $P \in \mathrm{Syl}_p(G)$, por el teorema anterior existe $g \in G$ tal que $S = gPg^{-1} \in \mathrm{Orb}_G(P)$. Recíprocamente es claro que $gPg^{-1} \in \mathrm{Syl}_p(G)$ para cualquier $g \in G$. Notemos además que $\mathrm{Stab}_G(P) = \{g \in G \mid gPg^{-1} = P\} = N_G(P)$. De esta manera

$$\left|\mathrm{Syl}_p(G)\right| = |\mathrm{Orb}_G(P)| = [G\colon \mathrm{Stab}_G(P)] = [G\colon N_G(P)].$$

Para la segunda igualdad basta notar que

$$\frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|}\frac{|N_G(P)|}{|P|} = \left|\mathrm{Syl}_p(G)\right|\frac{|N_G(P)|}{|P|},$$

donde $\dfrac{|N_G(P)|}{|P|}$ es entero pues $P \leq N_G(P)$. □

Observación. Sea G un grupo finito, $S \in \mathrm{Syl}(G)$. Las siguientes afirmaciones son equivalentes

(1) $S \trianglelefteq G$;

(2) $\mathrm{Syl}_p(G) = \{S\}$;

(3) Todo p-subgrupo de G está contenido en S.

(4) Para todo automorfismo $\alpha\colon G \xrightarrow{\sim} G$, se tiene que $\alpha(S) = S$ (a un grupo que cumpla con esta propiedad se lo llama grupo característico).

Ejercicio 3.18. Probar la observación anterior.

Lema 3.19. *Sean G un grupo finito, $S \in \mathrm{Syl}_p(G)$ y P un p-subgrupo de $N_G(S)$, entonces $P \leq S$.*

Demostración. Como $P \leq N_G(S)$ y $S \trianglelefteq N_G(S)$, entonces $PS \leq N_G(S)$. Luego,

$$|PS| = \frac{|P|\,|S|}{|P \cap S|}.$$

De modo que $|PS|$ es una potencia de p y por tanto PS es un $p-$subgrupo de $N_G(S)$. Por otro lado, como S es un $p-$subgrupo de Sylow de G, se tiene que

$$p^a = |S| \leq |PS| \leq |G| = p^a m$$

con $a, m \in \mathbb{N}$. Esto implica que $|PS| = p^a n$, con $1 \leq n \leq m$, pero como PS es un $p-$grupo, entonces $n = 1$. Finalmente tenemos $PS = P$ y eso implica que $P \leq S$. □

Corolario 3.20. *Sean $S, S' \in \mathrm{Syl}_p(G)$ y $S' \leq N_G(S)$, entonces $S = S'$.*

Demostración. Se sigue directo del lema anterior. □

Teorema 3.21 (Teorema de conteo de Sylow)**.** *Sean G un grupo finito, $p \geq 2$ un número primo y notamos $n_p(G) = \left|\mathrm{Syl}_p(G)\right|$. Entonces*

i. $n_p(G) \equiv 1 \pmod{p}$;

ii. Si $p^e \leq [S\colon S \cap T]$, con $e \geq 1$ y para cualquier par $T, S \in \mathrm{Syl}_p(G)$, $T \neq S$, entonces

$$n_p(G) \equiv 1 \pmod{p^e}.$$

iii. Si $|G| = p^a m$, $p \nmid m$, entonces $n_p(G) \mid m$.

Demostración. Sea $P \in \mathrm{Syl}_p(G)$. P actúa sobre $\mathrm{Syl}_p(G)$ mediante la siguiente acción

$$\begin{aligned} P \times \mathrm{Syl}_p(G) &\to \mathrm{Syl}_p(G) \\ (g, S) &\mapsto gSg^{-1}. \end{aligned}$$

i. Primeramente notemos que $\mathrm{Orb}_P(P) = \{gPg^{-1} \mid g \in P\} = \{P\}$ y por tanto $|\mathrm{Orb}_P(P)| = 1$. Sea $S \in \mathrm{Syl}_p(G)$, $S \neq P$. Utilizando el Lema 3.19 aplicado a $N_P(S) \leq N_G(S)$, tenemos que $N_P(S) \leq S$, por tanto $N_P(S) \leq P \cap S \leq N_P(S)$. Es decir que $N_P(S) = P \cap S$ y

$$|\mathrm{Orb}_P(S)| = |P\colon \mathrm{Stab}_P(S)| = |P\colon N_P(S)| = |P\colon P \cap S|\,.$$

Como $P \neq S$ entonces $P \cap S \neq P$ (pues si no, $S \leq P$ lo que no se puede pues $|S| = |P|$ y $S \neq P$), y así

$$|\mathrm{Orb}_P(S)| = \frac{|P|}{|P \cap S|} = p^b,$$

con algún $b \in \mathbb{N}$. En resumen, la cantidad de grupos que pertenecen a $\mathrm{Syl}_p(G)$ es de 1 más un múltiplo de p, es decir que $n_p(G) \equiv 1 \pmod{p}$.

ii. Se sigue directamente por lo visto en i.

iii. Se sigue del corolario 3.17.

□

3.1. Aplicaciones

Ejemplo 3.22. Sea G un grupo de orden $|G| = 360 = 2^3 \cdot 3^2 \cdot 5$. Utilizando el teorema anterior, literal iii. con $p = 3$, $a = 2$ y $m = 2^3 \cdot 5$ tenemos que

$$n_3(G) \mid 2^3 \cdot 5 = 40,$$

entonces $n_3(G) \in \{1, 2, 4, 8, 5, 10, 20, 40\}$. Pero por el literal i. tenemos que $n_3(G) \equiv 1 \pmod 3$, y por tanto $n_3(G) \in \{1, 4, 10, 40\}$.

Ejemplo 3.23. Sea G un grupo de orden $|G| = pq$, con $p > q$ primos tales que $p \not\equiv 1 \pmod q$. Sean además P un $p-$grupo de Sylow y Q un $q-$grupo de Sylow. Por el teorema 3.21, literal i. sabemos que $n_p(G) \equiv 1 \pmod p$ y $n_q(G) \equiv 1 \pmod q$, así, existen $k, h \geq 0$ enteros tales que $n_p(G) = 1 + kp$ y $n_q(G) = 1 + kq$. Por otro lado, nuevamente por el teorema anterior, literal iii., se tiene que $n_p(G) \mid q$ y $n_q(G) \mid p$. Luego $1 + kp \mid q < p$, por lo que k debe ser necesariamente 0 y $n_p(G) = 1$, lo que a su vez implica que $P \trianglelefteq G$.

Por otro lado, como $n_q(G) = 1 + hq \mid p$, existe $l \geq 0$ entero tal que $(1 + hq)l = p$. Como p es un número primo tenemos dos opciones:
Si $1 + hq = p$ y $l = 1$, se contradice el hecho que $p \not\equiv 1 \pmod q$ entonces no es posible. Tendríamos entonces que $1 + hq = 1$ y $l = p$, por tanto $h = 0$. Así $n_q(G) = \left|\mathrm{Syl}_q(G)\right| = 1$ y $Q \trianglelefteq G$. Por otro lado, tenemos $pq = |P|\,|Q| = |P \cap Q|\,|PQ|$. Hay cuatro opciones posibles

(1) Si $|P \cap Q| = pq$ y $|PQ| = 1$ entonces $pq = |P \cap Q| \leq |P| = p$ lo cual no es posible.

(2) Si $|P \cap Q| = p$ y $|PQ| = q$ entonces $p = |P \cap Q| \leq |Q| = q$ lo cual tampoco se puede.

(3) Si $|P \cap Q| = q$ y $|PQ| = p$ entonces $PQ = P$, lo cual implica que $Q \leq P$, lo cual no es posible pues por el teorema de Lagrange tendríamos que $q = |Q| \mid |P| = p$.

Tenemos el caso restante $|P \cap Q| = 1$ y $|PQ| = pq = |G|$, es decir que $P \cap Q = \{1\}$ y $PQ = G$.

Todos los $g \in G$ se escribirán de manera única como $g = ab$, con $a \in P$ y $b \in Q$. Notemos además que G es conmutativo, es decir que $g = ab = ba$ para todo $g \in G$. En efecto: como Q es un subgrupo normal, $aba^{-1} \in aQa^{-1} = Q$, entonces $(aba^{-1})b^{-1} \in Q$ y de la misma forma se puede ver que $a(ba^{-1}b^{-1}) \in P$. Así, $aba^{-1}b^{-1} \in P \cap Q = \{1\}$, es decir que $ab = ba$. Podemos definir entonces la aplicación

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

que establece un isomorfismo entre G y $P \times Q$. Además, como P y Q son cíclicos de órdenes coprimos, concluimos G es un grupo cíclico de orden pq.

Ejercicio 3.24. Si n y m son números enteros tales que $(n, m) = 1$, entonces $C_n \times C_m \cong C_{mn}$.

Si G es un grupo con $|G| = pq$, $p > q$, G no es conmutativo. Además, existen p estructuras distintas para G, pues existen p p-subgrupos de Sylow de G, y cada $Q \in \mathrm{Syl}_q(G)$

Ejemplo 3.25. Sea G un grupo con $|G| = 2p$, p un primo impar. Entonces, se tiene que $G \cong \mathbb{Z}/2p\mathbb{Z}$ o $G \cong D_{2p}$.

Todo p-subgrupo de Sylow P es cíclico de orden p. Por tanto, todo 2-subgrupo de Sylow es cíclico de orden 2. Sea $\alpha \in G$ con $|\alpha| = p$, es decir $\alpha^p = 1$. Así

$$|G/\langle\alpha\rangle| = 2 \Longrightarrow \langle\alpha\rangle \trianglelefteq G.$$

Luego, $n_p = 1 \pmod p$ y $n_p \mid 2$, lo que implica que $n_p = 1$. En consecuencia, existe un único p-subgrupo de Sylow $\langle\alpha\rangle$.

Sea $\langle\beta\rangle$ un 2-subgrupo de Sylow ($\beta^2 = 1$). Así, tenemos

$$\beta\alpha\beta^{-1} \in \langle\alpha\rangle \Longrightarrow \beta\alpha\beta^{-1} = \alpha^k \quad k \in \mathbb{Z},\ 0 < k < p,$$

de donde

$$\beta(\beta\alpha\beta^{-1})\beta^{-1} = \beta\alpha^k\beta^{-1} = (\alpha^k)^k,$$

por tanto $\alpha = \alpha^{k^2}$ y en consecuencia $k^2 \equiv 1 \pmod p$. Esto implica que $k \equiv 1 \pmod p$ o $k \equiv p-1 \pmod p$. Así, tenemos 2 casos

(1) $\beta\alpha\beta = \alpha$, es decir, $\alpha\beta = \beta\alpha$; por lo tanto, G es conmutativo. Pero $G = \langle\alpha\rangle\langle\beta\rangle$, y $\langle\alpha\rangle \cap \langle\beta\rangle = \{1\}$, lo que implica que $G \cong \mathbb{Z}/2p\mathbb{Z}$ y es cíclio.

(2) $\beta\alpha\beta = \alpha^{-1}$, entonces

$$G = \langle\alpha, \beta\rangle = \langle\alpha, \beta \,|\, \alpha^p = \beta^2 = 1,\ \beta\alpha = \alpha^{-1}\beta\rangle = D_{2p}.$$

Ejemplo 3.26. Vamos a encontrar todos los grupos de orden 8.

$$\mathbb{Z}/p\mathbb{Z}, \quad (\mathbb{Z}/2\mathbb{Z})^3, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad D_8, \quad Q_8.$$

Ejemplo 3.27. Sea G finito con $|G| = p^2q$, p y q primos distintos, entonces G no es simple. En efecto, se verifica que G tiene un p-subgrupo de Sylow y G tiene un q-subgrupo de Sylow.

Notemos que

$$\begin{aligned} n_p &\equiv 1 \pmod p \quad n_p \mid q \\ n_q &\equiv 1 \pmod q \quad n_q \mid p^2 \end{aligned}$$

Si $n_p = 1$ o $n_q = 1$, entonces G no es simple (un tal subgrupo de Sylow sería normal). Ahora, supongamos que $n_p > 1$ y $n_q > 1$, entonces $n_p = 1 + kp \mid q$ y así $q > p$ (con $k \geq 1$ ya que $n_p > 1$). Además, como $n_q \mid p^2$ y $n_q > 1$, entonces $n_q \in \{p, p^2\}$.

Si $Q, Q' \in \mathrm{Syl}_q(G)$, $Q \neq Q'$, $Q \cap Q' = \{1\}$. Así, $|Q \setminus \{1\}| = q - 1$ para todo $Q \in \mathrm{Syl}_q(G)$. Por tanto

$$\left| \bigcup_{Q \in \mathrm{Syl}_q(G)} (Q \setminus \{1\}) \right| = n_q(q-1).$$

Supongamos que $n_q = p^2$, entonces en G hay $p^2 = p^2q - p^2(q-1)$ elementos de orden distinto de q. Todo p-grupo de Sylow P tiene orden p^2, lo que implica que P sería el único p-subgrupo de Sylow de G, es decir $n_p = 1$, lo que contradice que $n_p > 1$.

Así, $n_q = p \equiv 1 \pmod q$, y entonces $q \mid p-1$, es decir $q < p$, lo que es absurdo. Por ende, $n_p \leq 1$ o $n_q \leq 1$ y por lo tanto G no es simple.

Ejercicio 3.28 (Desafiante)**.** Suponga que $|G| = pql$, con p, q, l primos distintos y que G no es abeliano ¿Es G un grupo simple?