Subgrupos de Sylow

Sésar

1. Definición

Definition 1. Un grupo G es un **p-grupo** si $\forall g \in G$, $\mathrm{o}(g) = p^n$ para un cierto $n \in \mathbb{N}$.

Theorem 1. Sea G un grupo finito. Entonces G es un p-grupo si y solo si $|G| = p^n$ para un cierto $n \in \mathbb{N}$.

Demostración. Si $|G| = p^n$, entonces en particular, $\mathrm{o}(g)|p^n = |G|$, luego G es un p-grupo. Supongamos ahora que G es un p-grupo finito. Observamos primeramente $G = \langle g \rangle_{g \in G} = *_{g \in G} \langle g \rangle$. Como todo $\langle g \rangle$ tiene orden potencia de p, entonces G también tiene orden potencia de p. $\square$

Definition 2. Un **p-subgrupo** de G es un subgrupo $H \leq G$ que también es p-grupo.

Remark 1. Por el teorema de Lagrange, todo subgrupo de un p-grupo es un p-subgrupo.

Proposition 1. Supongamos que G es un p-grupo, X un conjunto finito y $\varphi : G \times X \to X$ una acción. Entonces

$$|X| \equiv |X_G| \mod p.$$

Demostración. Por la ecuación de acciones de grupos, obtenemos que

$$|X| - |X_G| = \sum |O_x| = \sum [G : G_x].$$

Como $G_x \leq G$, entonces G_x es un p-subgrupo y por tanto, $[G : G_x]$ es potencia de p. Esto implica que $[G : G_x] \equiv 0 \mod p$ y por tanto, $\sum [G : G_x] \equiv 0 \mod p$. De este modo, $|X| - |X_G| \equiv 0 \mod p$. $\square$

Corollary 1. Si $G \neq 1$ es un p-grupo finito, entonces $Z(G) \neq 1$.

Demostración. En primer lugar, tomando la acción conjugación en G, $X_G = Z(G)$ y por la proposición, obtenemos que $|G| \equiv |Z(G)| \equiv 0 \mod p$. Si $Z(G) = 1$, entonces $|G| \equiv |Z(G)| \equiv 1 \mod p$, contradiciendo el hecho de que G es un p-grupo. $\square$

Definition 3. Sea G un grupo finito y $p||G|$. Decimos que $P \leq G$ es un **p-subgrupo de Sylow** si P es un p-subgrupo y $p \nmid [G : P]$.

$$\mathrm{Syl}_p(G) := \{P \leq G \mid P \text{ es un } p\text{-subgrupo}, \ p \nmid [G : P]\}.$$

Remark 2. Un p-subgrupo de Sylow se caracteriza por el el p-subgrupo de G con la mayor potencia de p. Es decir, si $|G| = p^n m$ con $\mathrm{mcd}(m, p) = 1$, entonces $|P| = p^n$.

Example 1. Sea G es un p-grupo. Supongamos que P es un p-subgrupo de Sylow. Entonces tanto P como $[G : P]$ son múltiplos de p, salvo el caso $[G : P] = 1$, de donde concluímos que $P = G$. Por tanto, $\mathrm{Syl}_p(G) = \{G\}$.

Proposition 2. Sea G finito, $p||G|$ y supongamos que $P \in \mathrm{Syl}_p(G)$. Si existe $H \leq G$ tal que $P \leq H \leq G$, entonces $P \in \mathrm{Syl}_p(H)$.

Demostración. Tenemos que $[G : P] = [G : H][H : P]$. Como $p \nmid [G : P]$, en particular $p \nmid [H : P]$, por lo que P es de orden potencia máxima de p en H. □

2. Normalizador

Lemma 1. Sea G un grupo y $H \leq G$. Tomemos $X = \{xHx^{-1}\}_{x \in G}$. La apliación

$$\begin{aligned} \phi : G \times X &\to X \\ (g, xHx^{-1}) &\mapsto g \cdot (xHx^{-1}) = (gx)H(x^{-1}g^{-1}) \end{aligned}$$

Es una acción transitiva.

Demostración. En primer lugar, para todo $x \in H$, tenemos que $e \cdot (xHx^{-1}) = (ex)H(x^{-1}e^{-1}) = xHx^{-1}$. Por otro lado, si $g_1, g_2 \in G$, tenemos que

$$g_1 \cdot (g_2 \cdot (xHx^{-1})) = g_1 \cdot ((g_2x)H(x^{-1}g_2^{-1})) = (g_1g_2x)H(x^{-1}g_2^{-1}g_1^{-1}) = (g_1g_2) \cdot (xHx^{-1}),$$

luego ϕ cumple con las propiedades de una acción sobre grupos. Veamos ahora que es transitiva. Basta con ver que $xHx^{-1} = x \cdot H$, luego $xHx^{-1} \in O_H$ para todo $x \in G$, es decir, $X = O_H$. □

Definition 4. Sea G un grupo y $H \leq G$. Definimos el **normalizador** de H al estabilizador de G en H de la acción del lemma.

$$N_G(H) := G_H.$$

Proposition 3. sea G grupo y $H \leq G$. Entonces

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

Demostración. Basta calcular el estabilizador de la acción definida previamente.

$$G_H = \{g \in G \mid g \cdot H = H\} = \{g \in H \mid gHg^{-1} = H\},$$

obteniendo al igualdad deseada. □

Theorem 2. Sea G grupo y $H \leq G$. Entonces

$$H \trianglelefteq N_G(H) \leq G.$$

Además, $N_G(H)$ es el mayor subgrupo con estas características.

Demostración. En primer lugar, si $h \in H$, entonces es fácil comprobar que $hHh^{-1} = H$, luego $h \in N_G(H)$. Por otro lado, el estabilizador de una acción es siempre subgrupo de G, luego $N_G(H) \leq G$. Finalmente, veamos que H es un subgrupo normal. En particular, por definición del normalizador, si $g \in N_G(H)$, entonces $gHg^{-1} = H$, lo que implica que $N \trianglelefteq N_G(H)$.

Supongamos que K es un subgrupo que satisface también que $H \trianglelefteq K \leq G$. En particular, si $x \in K$, entonces por ser H subgrupo normal de K, $xHx^{-1} = H$, por lo que $x \in N_G(H)$. □

Proposition 4. $[G : N_G(H)]$ es el número de conjugadas de H.

Demostración. Como la acción definida previamente es transitiva, entonces

$$|X| = \frac{|G|}{|G_H|} = \frac{|G|}{|N_G(H)|} = [G : N_G(H)].$$

Finalmente, como X es el conjunto de las conjudas de H, se tiene el resultado. □

Theorem 3. Sea G finito y $P \leq G$ un p-subgrupo. Si $p|[G : P]$, entonces $P < N_G(P)$.

Demostración. Basta probar que existe un $x \in N_G(P) \setminus P$, es decir, que existe un $x \in G \setminus P$ tal que $xPx^{-1} = P$.

En primer lugar, tomemos la acción traslación por la izquierda ϕ sobre las clases laterales por la izquierda $X = \{xP\}_{x \in G}$. Sabemos que $G_{xP} = xPx^{-1}$, entonces en particular $G_P = P$. Como además, la acción es transitiva, tenemos que $|X| = [G : P]$, por lo que $p||X|$.

Consideremos ahora $\phi|_P$, la restricción de la acción en P. Como P es un p-grupo, entonces $|X| \equiv |X_P| \bmod p$. Por el párrafo anterior, $p||X_P|$. Como P es un punto fijo en $\phi|_P$, entonces en particular $|X_P| > 1$ —puesto que si $|X_G| = 1$ entonces $p \nmid |X_P|$—, por lo que existe un $x \in G$ tal que $xP \in X_P$ y que $xP \neq P$.

Como $xP \neq P$, en particular tenemos que $x \notin P$. Por otro lado, como $xP \in X_G$, entonces $|O_{xP}| = 1$, por lo que por el teorema de la órbita estabilizadora, $|P| = |G_{xP}| = |xPx^{-1}|$. Es decir, como $xPx^{-1} = G_{xP} \leq G$ con la misma cardinalidad, entonces $xPx^{-1} = P$, por lo que $x \in N_G(P)$. □

Corollary 2. Sea $G \neq 1$ un p-grupo finito. $P < G \Rightarrow P < N_G(P)$.

Demostración. Sabemos que como $P \leq G$, entonces P es un p-subgrupo. Por otro lado, $P \neq G$ implica que $[G : P] \neq 1$ y como $G \neq 1$ es p-grupo, $p|[G : P]$. Estamos en las condiciones del teorema anterior, por lo que la tesis se cumple. $\square$

3. Teorema de existencia

Lemma 2. Sea G un p-grupo finito con $G = p^n$. Entonces para todo $r \leq n$, existe un $H \leq G$ tal que $|H| = p^r$.

Demostración. Realicemos inducción sobre la potencia de p. Si $n = 1$. Entonces $|G| = p$ y por lo tanto $G \cong C_p$. Todo grupo cíclico de orden primo tiene como únicos subgrupos el trivial y el total, respectivamente de órdenes p^0 y p^1, por lo que existen tales subgrupos. Supongamos que es cierto para un cierto $n \in \mathbb{N}$ y sea G un p-grupo de orden $|G| = p^{n+1}$.

Si G es abeliano, entonces por el teorema de Cauchy para grupos abelianos, existe un $g \in G$ tal que $\mathrm{o}(g) = p$. De este modo, $G/\langle g\rangle$ es un p grupo de orden p^n y por hipótesis de inducción, existen subgrupos $H' \leq G/\langle o\rangle$ de orden $|H'| = p^r$. Por el teorema de correspondencia, $H' = H/\langle o\rangle$ donde $H \leq G$ con $|H| = p^{r+1}$, de donde se obteienen todos los subgrupos.

Por otro lado, si G no es abeliano, entonces $Z(G) \neq G$. Por otro lado, como G es un p-grupo, $Z(G) \neq 1$, por lo que $G/Z(G)$ y $Z(G)$ son ambos p-grupos de orden menor que p^n. Por hipótesis de inducción, existen subgrupos de todas las potencias en ambos grupos y por el teorema de correspondencia, los subgrupos de $G/Z(G)$ se relacionan con los subgrupos de G con su correspondiente orden. $\square$

Lemma 3. Sea p primo, $a, m \in \mathbb{N}$ con $m \neq 0$. Entonces

$$\binom{p^a m}{p^a} \equiv m \mod p.$$

Demostración. Por el binomio de Newton, tenemos que

$$(1+x)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} x^i + x^p.$$

Por tanto, como $p \mid \binom{p}{i}$, tenemos que $(1+x)^p \equiv 1 + x^p \mod p$. De este modo, se puede probar mediante inducción que $(1+x)^{p^a} \equiv 1 + x^{p^a} \mod p$. Por lo tanto, de manera general tenemos que

$$(1+x)^{p^a m} \equiv (1 + x^{p^a})^m \mod p.$$

Ahora bien, por un lado, el binomio de la izquierda se descompone por el binomio de Newton como

$$(1+x)^{p^a m} = \sum_{i=0}^{p^a m} \binom{p^a m}{i} x^i,$$

donde en la posición $i = p^a$ obtenemos el monomio $\binom{p^a m}{p^a} x^{p^a}$. Por otro lado, podemos descomponer el binomio de la derecha como

$$(1 + x^{p^a})^m = \sum_{j=0}^{m} \binom{m}{j} x^{p^a j},$$

donde en la posición $j = 1$ obtenemos el monomio $\binom{m}{1} x^{p^a} = m x^{p^a}$. Como es una congruencia de polinomios, en particular el coeficiente de cualquier monomio debe ser congruente con su correspondiente del mismo grado, por lo que $\binom{p^a m}{m} \equiv m \mod p$. □

Theorem 4 (Existencia)**.** Sea G un grupo finito y $p||G|$. Entonces

$$\mathrm{Syl}_p(G) \neq \varnothing.$$

Demostración. Supongamos que $|G| = p^n m$ donde $\mathrm{mcd}(|G|, m) = 1$. Sea $X = \{P \subseteq G \mid |P| = p^n\}$. Podemos observar que $X \neq \varnothing$ porque podemos tomar cualquier colección de elementos de G con esa cardinalidad. Por otro lado, por combinatoria,

$$|X| = \binom{p^n m}{p^n} \equiv m \mod p,$$

por lo que podemos deducir que $p \nmid |X|$. Definamos ahora la siguiente aplicación:

$$\begin{aligned} \phi : G \times X &\to X \\ (g, P) &\mapsto gP. \end{aligned}$$

Se puede demostrar rutinariamente que ϕ es una acción transitiva. Por el teorema de la ecuación de las órbitas, como p no divide a $|X|$, entonces existe un $A \in X$ tal que $p \nmid |O_A|$.

Así, por el teorema de la órbita estabilizadora, $p \nmid [G : G_A]$. Como $p^n||G|$, concluimos que $p^n \mid |G_A|$, y por tanto $p^n \leq |G_A|$. Por otro lado, si $g \in G_A$ y $a \in A$, entonces $ga \in gA = A$, por lo que $G_A A = A$, lo que implica que $G_A \subseteq A$ y, por tanto, $|G_A| \leq |A| = p^n$. De esta manera, $|G_A| = p^n$ y se deduce que $G_A \in \mathrm{Syl}_p(G)$. □

Corollary 3. Sea G grupo finito y $p||G|$. Entonces existe un p-subgrupo $H \leq G$ de orden cualquier potencia de p.

Demostración. Como p divide al orden de G, entonces existe un p-subgrupo de Sylow $P \in \mathrm{Syl}_p(G)$. Como P es en particular un p-grupo, entonces existen subgrupo de orden cualquier potencia de p. □

Corollary 4 (Teorema de Cauchy)**.** Si G es un grupo finito y $p||G|$, entonces $\exists g \in G$ tal que $\mathrm{o}(g) = p$.

Demostración. Por el corolario anterior, existen p-subgrupos del orden cualquier potencia de p. En particular, existe un $H \leq G$ tal que $|H| = p$, por lo que $H \cong C_p$, es decir, $H = \langle a \rangle$ con $\mathrm{o}(g) = p$. □

4. Teorema de conjugación

Lemma 4. Sea G grupo finito y $p||G|$. Si $H \leq G$ es un p-subgrupo y $P \in \mathrm{Syl}_p(G)$, entonces existe un $g \in G$ tal que $H \leq gPg^{-1}$.

Demostración. Tomemos la acción traslación ϕ de G sobre el conjunto X de las clases laterales de P. Como la acción es transitiva, entonces $|X| = [G : G_P] = [G : P]$ y como $P \in \mathrm{Syl}_p(G)$, entonces $p \nmid |X|$.

Consideremos ahora $\phi|_H$, la restricción de la acción en H. Como H es un p-grupo, tenemos que $|X| \equiv |X_H| \mod p$ y por el comentario anterior, $p \nmid |X_H|$, por lo que $X_H \neq \varnothing$ y existe un $gP \in X_H$. De este modo, para todo $h \in H$, $(hg)P = gP$, es decir, $h \in gPg^{-1}$. De este modo, $H \leq gPg^{-1}$. □

Theorem 5 (Conjugación)**.** Todos los p-subgrupos de Sylow son conjugados entre sí.

Demostración. Sean $P, Q \in \mathrm{Syl}_p(G)$. Como en particular Q es un p-subgrupo de G, entonces existe un $g \in G$ tal que $Q \leq gPg^{-1}$. Como $|Q| = |gPg^{-1}|$, se tiene entonces que $Q = gPg^{-1}$. □

Corollary 5 (Dominancia)**.** Todo p-subgrupo está contenido en un p-subgrupo de Sylow.

Demostración. Si $H \leq G$ es un p-subgrupo y $P \in \mathrm{Syl}_p(G)$, entonces existe un $g \in G$ tal que $H \leq gPg^{-1}$. Como los p-subgrupos de Sylow son conjugados entre sí, entonces $gPg^{-1} \in \mathrm{Syl}_p(G)$. □

Lemma 5. Sea G grupo y $p||G|$ y $P \in \mathrm{Syl}_p(G)$. Entonces

$$\mathrm{Syl}_p(G) = \{P\} \Leftrightarrow P \trianglelefteq G.$$

Demostración. Que P sea el único p-subgrupo es equivalente a que $gPg^{-1} = P$ para todo $g \in G$ —por el teorema de conjugación— y por definición, $P \trianglelefteq G$. □

Remark 3. Si $P \in \mathrm{Syl}_p(G)$, entonces como $P \trianglelefteq N_G(P) \leq G$, por un lado tenemos que $P \in \mathrm{Syl}_p(N_G(P))$ y como $P \trianglelefteq N_G(P)$, por el lema anterior $\mathrm{Syl}_p(N_G(P)) = \{P\}$.

Corollary 6. Sea G grupo finito, $p||G|$ y $P \in \mathrm{Syl}_p(G)$. Entonces

$$N_G(N_G(P)) = N_G(P).$$

Demostración. Es fácil observar que $N_G(P) \leq N_G(N_G(P))$. Por otro lado, sea $x \in N_G(N_G(P))$, entonces $xN_G(P)x^{-1} = N_G(P)$. Además, como $P \leq N_G(P)$, entonces $xPx^{-1} \leq xN_G(P)x^{-1} = N_G(P)$. Por el teorema de conjugación, $xPx^{-1} \in \mathrm{Syl}_p(G)$ y como $xPx^{-1} \leq N_G(P) \leq G$, entonces $xPx^{-1} \in \mathrm{Syl}_p(N_G(P)) = \{P\}$. De este modo, $xPx^{-1} = P$, por lo que $x \in N_G(P)$. □

5. Teorema de cardinalidad

Theorem 6 (Cardinalidad)**.** Sea G finito y $p||G|$ y sea $n_p := |\operatorname{Syl}_p(G)|$. Entonces

1. $n_p = [G : N_G(P)]$ para todo $P \in \operatorname{Syl}_p(G)$.
2. $n_p|[G : P]$ para todo $P \in \operatorname{Syl}_p(G)$.
3. $n_p \equiv 1 \mod p$.

Demostración. Sea $X = \operatorname{Syl}_p(G)$ y ϕ la acción por conjugación de G sobre X. Entonces por un lado, $G_P = N_G(P)$. Además, como la acción es transitiva, tenemos que $n_p = |X| = [G : G_P] = [G : N_G(P)]$. De este modo, como $n_P = [G : N_P(G)] = \frac{[G:P]}{[N_G(P):P]}$, en particular, $n_p|[G : P]$.

Tomemos ahora la restricción $\phi|_P$ de esta acción en P. Como P es un p-grupo, entonces $n_p = |X| \equiv |X_P| \mod p$. Por un lado, es fácil observar que $P \in X_P$. Veamos que sólo existe un único punto fijo. Sea $Q \in X_P$. Entonces $gQg^{-1} = Q$ para todo $g \in P$, por lo que $P \leq N_G(Q)$. En particular, $Q, P \in \operatorname{Syl}_p(N_G(Q)) = \{Q\}$, implicando que $P = Q$. Luego $|X_P| = 1$. $\square$