Grupos finitos

Notas de clase de
Eugenio Miranda Palacios
para el curso 2010/2011
Adaptadas por Manuel Bullejos
para el curso 2020/2021

Índice

5. G-conjuntos y p-grupos.

5.1. Acciones de un grupo sobre un conjunto

Definición 5.1. Sea G un grupo y sea X un conjunto no vacío. Una *acción de G sobre X* es una ley de composición externa

$$G \times X \to X, \quad (x, s) \mapsto {}^x s$$

Renombramos ${}^x s = xs$

$G \xrightarrow{\rho} S_X$, $g \mapsto \rho(g): X \to X$, $x \mapsto \rho(g)(x)$, $G \times X \to X$, $(g, x) \mapsto \rho(g)(x) \overset{\text{not}}{=} g_x \overset{\text{not}}{=} gx$

Recuerda a una operación externa, como en esp. vect. (escalar por vector)

sujeta a dos condiciones:

1. $\forall x, y \in G,\ \forall s \in X \quad {}^{(xy)}s = {}^x({}^y s)$.
2. $\forall s \in X,\ {}^1 s = s$.

Dada una acción de G sobre X, diremos que *G opera sobre X* y también se dice que *X es un G-conjunto*. Al grupo G le llamamos *dominio de operadores*.

Designamos como S_X al grupo de permutaciones del conjunto X con la composición de aplicaciones.

Teorema 5.2. *Una estructura de G-conjunto sobre X (una acción de G sobre X) es equivalente a un homomorfismo de grupos $\phi : G \to S_X$.*

Demostración. Sea X un G-conjunto. Para cada $x \in G$ fijo consideramos la aplicación $\phi_x : X \to X$ dada por $\phi_x(s) = {}^x s$.

Entonces para todo $s \in X$ tenemos $\phi_x\phi_y(s) = {}^x({}^y s) = {}^{xy} s = \phi_{xy}(s)$, así que $\phi_x\phi_y = \phi_{xy}$; además $\phi_1(s) = {}^1 s = s$ luego $\phi_1 = 1_S$. En particular $\phi_x\phi_{x^{-1}} = \phi_{xx^{-1}} = \phi_1 = 1_S = \phi_{x^{-1}}\phi_x$, luego $\phi_{x^{-1}} = \phi_x^{-1}$ y ϕ_x es una permutación de X. Definimos ahora $\phi : G \to S_X$ por $\phi(x) = \phi_x$. Ahora $\phi(xy) = \phi_{xy} = \phi_x\phi_y = \phi(x)\phi(y)$. Luego ϕ es un homomorfismo de grupos.

A la inversa, sea $\phi : G \to S_X$ un homomorfismo de grupos. Definimos una aplicación $G \times X \to X$ por $(x, s) \mapsto {}^x s = \phi(x)(s)$. Entonces ${}^x({}^y s) = \phi(x)(\phi(y)s) = (\phi(x)\phi(y))s = \phi(xy)s = {}^{(xy)}s$; ${}^1 s = \phi(1)s = 1_S(s) = s$ y la aplicación es una acción de G sobre X. □

Definición 5.3. El núcleo $\ker\phi$ del homomorfismo ϕ del teorema 5.2 se llama *núcleo de la acción*

$$\ker\phi = \{x \in G;\ {}^x s = s, \forall s \in X\},$$

y es el conjunto de elementos de G que dejan fijo a todo $s \in X$.

Definición 5.4. La acción de G sobre X se llama *fiel* o *efectiva* si el morfismo ϕ del teorema 5.2 es inyectivo o, equivalentemente, si su núcleo es trivial.

Definición 5.5.

1. Para cada $s \in X$ llamamos *órbita de s* al conjunto

$$Orb(s) = \{{}^x s;\ x \in G\} \subseteq X.$$

2. Para cada $s \in X$ llamamos *estabilizador* o *grupo de isotropía* de s al subgrupo de G,
$$St(s) = \{x \in G;\ {}^x s = s\} \leq G.$$

Definición 5.6. Si X consta de una sola órbita (es decir, si para cualesquiera $s, t \in X$ existe un $x \in G$ tal que $s = {}^x t$), diremos que G *actúa transitivamente* sobre X.

Dado un G-conjunto X podemos definir una relación binaria en X así:

$$s \sim t \text{ si, y sólo si, existe } x \in G \text{ tal que } s = {}^x t.$$

Observamos entonces que:

1. La relación $\sim$ recién definida es una relación de equivalencia.
2. Las clases de equivalencia bajo $\sim$ son las órbitas.
3. El conjunto de órbitas es una partición de G.

Tenemos también

Lema 5.7. *Para la relación anterior, $s \sim t \Rightarrow St(s)$ y $St(t)$ son conjugados en G.*

Demostración. Es fácil comprobar que si $t = {}^g s$ entonces $St(t) = gSt(s)g^{-1}$. □

El inverso del lema anterior es falso.

Ejemplo 5.1. El grupo S_n actúa de forma evidente sobre el conjunto $\mathbf{n} = \{0, 1, \ldots, n-1\}$; ${}^\sigma i = \sigma(i)$, y el morfismo asociado es la identidad $Id : S_n \to S_n$. Además esta acción es transitiva.

En general el grupo de permutaciones S_X actúa transitivamente sobre X, para cualquier conjunto X.

Ejemplo 5.2. Sea X un conjunto arbitrario no vacío, $n > 0$ un natural y sea $X^n = X \times \cdots \times X$. Sea $G = S_n$ el grupo de permutaciones de n elementos. Definimos $G \times X^n \to X^n$ así:

$${}^\sigma(x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Es inmediato comprobar que X^n es un G-conjunto.

Ejemplo 5.3. Sea X un conjunto no vacío arbitrario y G un grupo cualquiera. Definimos una acción de G sobre X por ${}^x s = s$ para todo $x \in G$ y todo $s \in X$. Esta acción se llama *trivial* de G sobre X. El estabilizador de cualquier $s \in X$ es todo G y la órbita se reduce al mismo s.

Ejemplo 5.4. Hacemos actuar al grupo D_4 sobre los cuatro vértices del cuadrado. Numeramos estos vértices sucesivamente 1, 2, 3, 4. Sea $r \in D_4$ la rotación de ángulo $\pi/2$ radianes, y sea s la reflexión en la línea diagonal que pasa por 1 y 3. Entonces las permutaciones de los vértices correspondientes son:

$$r \mapsto \rho = (1\ 2\ 3\ 4) \qquad s \mapsto \sigma = (2\ 4)$$

Ya que la representación por permutaciones es un homomorfismo, la permutación correspondiente a sr es $\sigma\rho = (1\ 4)(2\ 3)$. La acción de D_4 sobre los cuatro vértices del cuadrado es fiel ya que sólo la identidad fija todos los vértices. El estabilizador de cualquier vértice i es el subgrupo de orden 2 generado por la reflexión sobre la diagonal que pasa por i

Ejemplo 5.5. Sea $X = G$ un grupo. G actúa sobre sí mismo de tres formas diferentes:

1. *Por conjugación:* ${}^x s = xsx^{-1}$.
2. *Por traslación por la izquierda:* ${}^x s = xs$.
3. *Por traslación por la derecha:* ${}^x s = xs^{-1}$.

Es inmediato comprobar que con cualquiera de ellas G es un G-conjunto.

En el primer caso:

- El estabilizador de $s \in G$,

$$St(s) = \{x \in G;\ xsx^{-1} = s\} = C_G(s),$$

  es el *centralizador* de s en G.

- Mientras que la órbita $Orb(s) = \{xsx^{-1};\ x \in G\} = Conj(s)$ es la *clase de conjugación* de s en G.

En el segundo caso:
El estabilizador de $s \in G$, $St(s) = \{x \in G;\ xs = s\} = 1$ se reduce al subgrupo trivial, mientras que la órbita $Orb(s) = \{xs \mid x \in G\}$ es el grupo total, la acción es transitiva.

Esta acción también es fiel y por tanto el morfismo inducido $\phi : G \to S_G$ es inyectivo y nos permite identificar G con un subgrupo de un grupo de permutaciones. Este resultado es conocido como teorema de Cayley y lo destacamos en el siguiente

Teorema 5.8 (Cayley)**.** *Todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.*

Igual ocurre en la traslación por la derecha.

Ejemplo 5.6. Las tres operaciones del ejemplo 5.5 pueden generalizarse al conjunto $\mathcal{P}(G)$ (conjunto de las partes de G):

Todo grupo tiene una representación fiel sobre un conjunto

$G \overset{\text{tr. izq.}}{\longmapsto} S_G$ $\qquad$ $G \cong Im(\text{tr. izq}) \leq S_G$

$g \mapsto g \cdot ()$ $\quad g_h = g \cdot h$

1. Sea $T \subset G$; ${}^xT = xTx^{-1}$. El estabilizador es el normalizador de T en G: $St(T) = N_G(T) = \{x \in G;\, xTx^{-1} = T\}$. La órbita es la *clase de conjugación* de T en G: $Orb(T) = \{xTx^{-1};\, x \in G\}$.

   Notemos que si $T \leq G$ es un subgrupo, entonces cualquier conjugado de T, $xTx^{-1} \leq G$ también es un subgrupo y por tanto la acción por conjugación de G sobre $\mathcal{P}(G)$ induce una acción de G sobre $SubGr(G)$ el retículo de subgrupos de G.

2. Sea $T \subset G$; ${}^xT = xT = \{xt;\, t \in T\}$. Es particularmente interesante el caso en que T es un subgrupo de G. Entonces el estabilizador de T es $St(T) = \{x \in G;\, xT = T\} = T$ y la órbita es $Orb(T) = \{xT \mid x \in G\} = G/_T \sim$, el conjunto de clases por la izquierda de T en G.

   A un conjunto de representantes de estas órbitas (es decir, un conjunto con un y sólo un elemento de cada órbita) le llamamos *transversal* de T en G.

   Un análisis análogo podemos hacer en el tercer caso.

   El caso que acabamos de ver es especialmente típico, como veremos a continuación.

5.2. Fórmula de clases

Teorema 5.9. *Sea X un G-conjunto, entonces para cada $s \in X$ se tiene una biyección*

$$Orb(s) \cong G/_{St(s)} \sim .$$

Y como consecuencia se tiene que $|Orb(s)| = [G : St(s)]$, que es un divisor del orden de G.

Demostración. Definimos

$$f : G/_{St(s)} \sim \to Orb(s) \text{ por } f(xSt(s)) := {}^xs,$$

está claro que f está bien definida ya que $\forall g \in St(s), {}^{(xg)}s = {}^x({}^gs) = {}^xs$. Además si ${}^xs = {}^ys$, entonces ${}^{y^{-1}x}s = s$ lo que implica que $y^{-1}x \in St(s)$ o equivalentemente $xSt(s) = ySt(s)$ y concluimos que f es inyectiva.

Por otro lado f es sobreyectiva ya que los elementos de $Orb(s)$ son de la forma ${}^xs$ para algún $x \in G$ y se tiene que $f(xSt(s)) = {}^xs$.

Por último, la igualdad $|Orb(s)| = [G : St(s)]$ se deduce de ser $|G/_{Sta(s)\sim}| = [G : St(s)]$. □

Si consideramos la acción por conjugación de G sobre si mismo y aplicamos el Teorema 5.9 tenemos

Corolario 5.10. *El número de conjugados de $x \in G$ es igual a*

$$|Conj(x)| = [G : C_G(x)] = |G|/|C_G(x)|.$$

Puesto que el conjunto de órbitas determina una partición de X, si tomamos una trasversal Δ, esto es un conjunto de representantes de cada órbita, tenemos que

$$|X| = \sum_{s\in\Delta} |Orb(s)| = \sum_{s\in\Delta} [G : St(s)].$$

Diremos que un elemento $s \in X$ es un "*punto fijo*" si ${}^x s = s, \forall x \in G$. Está claro que s es un punto fijo si, y sólo si, $Orb(s) = \{s\}$. Denotaremos $Fix(X)$ al conjunto de puntos fijos y observamos que $Fix(X) \subseteq \Delta$, para toda trasversal. Separando entonces los puntos fijos de la trasversal, reescribimos la fórmula anterior en el siguiente

Teorema 5.11 (Fórmula de descomposición en órbitas)**.**
Si X es un G-conjunto, $Fix(X)$ es el conjunto de puntos fijos y Δ es una trasversal, entonces

$$|X| = |Fix(X)| + \sum_{s\in\Delta, s\notin Fix(X)} [G : St(s)].$$

Si consideramos ahora la acción por conjugación de G sobre si mismo, tenemos que

$$Fix(G) = \{s \in G;\ xsx^{-1} = s,\ \forall x \in G\} = Z(G).$$

Entonces el Teorema 5.11 nos dice

Corolario 5.12 (Fórmula de clases)**.**

$$|G| = |Z(G)| + \sum_{s\in\Delta'} [G : C_G(s)]$$

donde la suma se toma sobre el conjunto $\Delta' = \Delta\backslash Z(G) = \{x \in \Delta;\ x \notin Z(G)\}$ de representantes de clases que tienen más de un elemento.

La fórmula de clases admite la siguiente generalización bastante útil:
Sea $H \trianglelefteq G$. Hacemos actuar a G sobre H por conjugación: ${}^x h = xhx^{-1}$.
El estabilizador de un elemento $h \in H$ es

$$St(h) = \{x \in G;\ xhx^{-1} = h\} = C_G(h).$$

Un elemento $h \in H$ será un punto fijo para esta acción si su órbita tiene un sólo elemento o equivalentemente si $G = C_G(h)$, que significa que $h \in Z(G)$. Así $Fix(H) = H \cap Z(G)$ y la fórmula de clases nos diría:

Teorema 5.13 (Fórmula de clases general)**.**
Para todo subgrupo normal $H \trianglelefteq G$ se tiene

$$|H| = |H \cap Z(G)| + \sum_{h\in\Delta'} [G : C_G(h)]$$

donde Δ' es un conjunto de representantes de órbitas con más de un elemento. En particular si H es finito, $[G : C_G(h)]$ es finito para todo $h \in H$, aunque G no lo sea.

5.3. Aplicaciones: p-grupos

Definición 5.14. Sea p un primo, diremos que un grupo G es un p-grupo si todo elemento de G tiene orden una potencia de p.

Claramente todo grupo finito con orden una potencia de p es un p-grupo, nuestro objetivo será probar el recíproco de este enunciado, esto es, que los p-grupos finitos todos tienen orden una potencia de p.

El estudio de los p-subgrupos de un grupo será esencial a la hora de clasificar grupos finitos y su importancia será manifiesta en las secciones siguientes.

Teorema 5.15 (Cauchy)**.** *Sea G un grupo finito tal que p divide al orden de G. Entonces G tiene un elemento (o equivalentemente un subgrupo) de orden p.*

Demostración. Vamos a distinguir dos casos y en ambos haremos la demostración por inducción sobre el orden de G.

Caso 1: G **abeliano.**

Claramente si $|G| = 1$ el teorema es cierto. Además si G es cíclico el teorema también es cierto pues hemos demostrado que en un grupo cíclico para todo divisor de su orden existe un único subgrupo de orden ese divisor. Si ese divisor es un primo p, el subgrupo ha de estar generado por un elemento de orden p.

Supongamos entonces que G es un grupo no trivial y no cíclico y que el teorema es cierto para todo grupo de orden menor que $|G|$. Sea $x \in G$ un elemento no trivial y sea $H = \langle x \rangle \leq G$ el subgrupo generado por x. Ha de ser $H \neq G$ por no ser G cíclico.

Si $p||H|$, por hipótesis de inducción H tendría un subgrupo de orden p y por tanto también lo tendría G. Supongamos entonces que p no divide a $r = |H| = o(x)$. Entonces p y r son coprimos y tendríamos que x^p es también un generador de H, esto es $H = \langle x \rangle = \langle x^p \rangle$.

Por ser G abeliano $H \trianglelefteq G$ y podemos considerar el grupo cociente G/H además $p||G| = |G/H| \cdot |H|$ y p no divide $|H|$, por tanto $p||G/H| < |G|$ y ha de existir (por hipótesis de inducción) un elemento $gH \in G/H$ de orden p y por tanto $(gH)^p = 1H$ de donde $g^p \in H$ y es la menor potencia positiva de g que está en H, por tanto ha de existir un $s < r$ con $g^p = (x^p)^s$ (recuerda que x^p también genera H). Así gx^{-s} es un elemento no trivial tal que $(gx^{-s})^p = 1$ y por tanto tiene orden p.

Caso 2: G **no abeliano.**

Consideramos $Z(G)$ el centro de G. Si $p||Z(G)|$, por ser este abeliano y el caso 1, tendría un elemento de orden p y entonces también lo tendría G.

Supongamos entonces que p no divide al orden de $Z(G)$. Tomándo módulo p en la fórmula de clases, Teorema 5.12,

$$|G| = |Z(G)| + \sum_{s \in \Delta'} [G : C_G(s)]$$

tenemos que $\sum_{s\in\Delta'}[G : C_G(s)] \equiv -|Z(G)| \not\equiv 0 \mod p$ y ha de existir $s \in \Delta'$ tal que p no divida a $[G : C_G(s)]$. Pero p divide a $|G| = [G : C_G(s)]|C_G(s)|$ y

por tanto p ha de dividir a $|C_G(s)| < |G|$ y por hipótesis de inducción $C_G(s)$ sería un subgrupo de G que tiene un elemento de orden p y por tanto también lo tendría G. □

Corolario 5.16. *Un grupo finito es un p-grupo si y sólo si $|G|$ es una potencia de p.*

Demostración. Si suponemos que p y q son dos primos que dividen al orden de G, el teorema de Cauchy nos asegura la existencia de elementos de orden p y de orden q por tanto G no puede ser un p-grupo a menos que p sea el único primo que divide al orden de G. □

Podemos aplicar ahora la fórmula de clases Teorema 5.13 a p-grupos y obtenemos

Teorema 5.17. *Sea G un p-grupo finito y H un subgrupo normal no trivial de G. Entonces $Z(G) \cap H \neq 1$.*

Demostración. La fómula de clases nos dice

$$|H| = |H \cap Z(G)| + \sum_{h \in \Delta'} [G : C_G(h)].$$

Tomando módulo p, puesto que el orden de H y el índice $[G : C_G(h)]$ son divisores del orden de G, que es una potencia de p, tendríamos que $|H \cap Z(G)| \equiv 0 \mod p$ y por ser $|H \cap Z(G)| \geq 1$, ya que $1 \in H \cap Z(G)$, tendríamos que $|H \cap Z(G)|$ es un múltiplo no nulo de p y por tanto $H \cap Z(G) \neq 1$. □

Tomando como H el propio G tenemos

Corolario 5.18 (Teorema de Burnside)**.** *Cualquier p-grupo finito G tiene centro no trivial.*

Otro corolario interesante sería

Corolario 5.19. *Sea G un p-grupo, H un subgrupo normal suyo de orden p. Entonces $H \subset Z(G)$.*

Demostración. Puesto que $1 \neq H \cap Z(G) \leq H$ y H no tiene subgrupos propios (por tener orden p), ha de ser $H \cap Z(G) = H$. □

Teorema 5.20. *Sea $|G| = p^n$. Entonces $|Z(G)| \neq p^{n-1}$.*

Demostración. En la relación de problemas 4, probamos que no puede haber un grupo no abeliano G con $G/Z(G)$ cíclico. Esdecir, si $G/Z(G)$ es cíclico, entonces $G = Z(Z)$ y G es abeliano. Así si $|G| = p^n$ y $|Z(G)| = p^{n-1}$ tendríamos $|G/Z(G)| = p$ y sería cíclico lo que contradice lo anterior. □

Corolario 5.21. *Todo grupo de orden p^2 es abeliano.*

5.4. Teoremas de Sylow

El matemático noruego Peter Ludwig Mejdell Sylow (1832-1918) se dedica a estudiar p-subgrupos de un grupo finito G y prueba los teoremas que hoy en día llevan su nombre y que han mostrado su utilidad en la clasificación de grupos finitos..

Teorema 5.22 (Primer Teorema de Sylow)**.**
Sea G un grupo finito de orden $|G| = n$, y sea p un primo. Para toda potencia $p^i \mid n$ existe un subgrupo $H < G$ de orden $|H| = p^i$.

Demostración.
Inducción sobre i. Si $i = 0$ tomamos $H = 1$.

Sea ahora $i > 0$ y supongamos el teorema cierto para toda potencia p^j con $j < i$. Ahora hacemos inducción sobre $|G|$. Si $|G| = p^i$ tomamos $H = G$. Sea $|G| > p^i$ y supongamos cierto el teorema para todo grupo de orden menor. Distinguimos dos casos:

- $\exists K < G$ tal que $p \nmid [G : K]$. Entonces $p^i || K|$ y por la hipótesis de inducción, $\exists H < K < G$ tal que $|H| = p^i$.
- $\forall K < G$, $p \mid [G : K]$. Consideramos la fórmula de clases, y despejamos el primer término:
$$|Z(G)| = |G| - \sum_{x \in \Delta'} [G : C_G(x)]$$

Todos los términos del segundo miembro son divisibles por p, así que el primer miembro también es divisible por p.

Por el teorema de Cauchy, $\exists K < Z(G)$ (y por tanto normal en G) tal que $|K| = p$. Consideramos el grupo cociente G/K.

$|G/K| = |G|/|K| = |G|/p$ es divisible por p^{i-1} y por tanto (por la otra hipótesis de inducción) existe un subgrupo suyo $\bar{L} \leq G/K$ de orden p^{i-1}.

Por la correspondencia entre los subgrupos de un cociente y los del grupo original (tercer teorema de isomorfía) , $\exists H < G$ tal que $H > K$ y $\bar{L} = H/K$.

Pero por el teorema de Lagrange, su orden será:

$$|H| = |H/K||K| = p^{i-1}p = p^i$$

□

Definición 5.23. Sea p^k la máxima potencia de p que divide al orden de G. Todo subgrupo H de G tal que $|H| = p^k$ se llama *p-subgrupo de Sylow de G.*

Corolario 5.24 (Primer teorema de Sylow "sensu stricto")**.**
Para todo grupo finito G y todo primo p existe un p-subgrupo de Sylow de G.

El segundo teorema de Sylow estudia el número de subgrupos de Sylow de un grupo finito.

Lema 5.25. *Sea P un p-subgrupo de Sylow de G y sea H un p-subgrupo del normalizador $N_G(P)$. Entonces $H \subseteq P$*

Demostración. Por el segundo teorema de isomorfía, aplicado a $H \leq N_G(P)$ y $P \trianglelefteq N_G(P)$, tenemos

$$\frac{HP}{P} \cong \frac{H}{H \cap P}$$

y por tanto $[HP : P] = [H : H \cap P]$ es un divisor común de $[G : P]$ y $|H|$ que son primos relativos. Luego $[HP : P] = 1$, $HP = P$, lo que implica $H \subseteq P$. □

Teorema 5.26 (Segundo teorema de Sylow)**.**
Sea $|G| = n = p^k m$ con $(p, m) = 1$. Llamamos n_p al número de p-subgrupos de Sylow del grupo G.

1. *Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow.*
2. *Todos los p-subgrupos de Sylow son conjugados entre sí.*
3. *$n_p = [G : N_G(P)]$ para cualquier p-subgrupo de Syloy P. Además $n_p \mid m$ y $n_p \equiv 1 \pmod{p}$*

Demostración.
(1).- Sea

$$S = Syl_p(G) = \{P;\ P \text{ es un } p\text{-subgrupo de Sylow de } G\},$$

y sea H un p-subgrupo arbitrario de G.

Notar que si $P \in S$ y $g \in G$, entonces $|P| = |gPg^{-1}|$ y por tanto $gPg^{-1} \in S$. Podemos entonces hacer actuar a G sobre S por conjugación.

Sea P_1 un p-subgrupo de Sylow cualquiera y sea $T = Orb(P_1)$ su órbita bajo la acción de G. Sabemos que $|T| = [G : N_G(P_1)] \mid [G : P_1] = m$ y por tanto es primo relativo con p.

Consideramos ahora la acción de H sobre T también por conjugación. Por la fórmula de descomposición en órbitas,

$$|T| = \sum_{P \in \Delta} [H : Stab_H(P)].$$

Ahora $Stab_H(P) = N_G(P) \cap H < N_G(P)$ y es un p-grupo. Por el Lema 5.25 anterior, $N_G(P) \cap H < P$ y por tanto $Stab_H(P) = N_G(P) \cap H = P \cap H$. Nos queda $|T| = \sum_{P \in \Delta} [H : P \cap H]$.

Todos los sumandos del segundo miembro son divisores de $|H|$ y por tanto son potencias de p. Como el primer miembro no es divisible por p, existe un $P \in T$ tal que $[H : P \cap H] = 1$. Así que $H = H \cap P$, luego $H \subseteq P$ con lo que hemos demostrado el primer punto. Observese que el grupo P que contiene a H es conjugado a P_1 que es arbitrario.
(2).- Sean ahora P_1 y P_2 dos p-subgrupos de Sylow arbitrarios. En la demostración anterior tomamos $H = P_2$ y obtenemos que $P_2 \subseteq P$ que es conjugado

a P_1. Contando órdenes, $P_2 = P$, con lo que obtenemos el punto 2. Obsérvese que esto implica que $S = T$.
(3).- Sea $n_p = |S| = |T| = [G : N_G(P_1)] \mid [G : P_1] = m$. Para demostrar la segunda condición, tomamos $H = P_1$ en la acción arriba descrita. Entonces $P_1 \subseteq P \Leftrightarrow P_1 = P$ y por tanto hay una única órbita con un elemento y todas las demás tienen cardinal divisible por p, así que $n_p \equiv 1 \pmod{p}$.

□

Como consecuencia inmediata tenemos

Corolario 5.27. *Sea P un p-subgrupo de Sylow de G. Entonces:*

P es el único p-subgrupo de Sylow de $G \Leftrightarrow P$ es un subgrupo normal de G.

Teorema 5.28. *Sea G un grupo finito que tiene un único subgrupo de Sylow para cada primo que divida al $|G|$. Entonces G es producto directo de sus subgrupos de Sylow.*

Demostración. Supongamos $|G| = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ la descomposición en primos distintos del orden de G. Sean P_i el único p_i-subgrupo de Sylow de G para $i = 1, \cdots, r$. Probemos las tres condiciones que han de cumplirse para que G sea el producto directo de los P_i:

1. $P_i \trianglelefteq G, i = 1, \cdots, r$, por el Corolario 5.27.

2. $P_i \cap P_j = 1$ si $i \neq j$, por tener orden primos relativos. Además veamos que $|P_1 \cdots P_i| = |P_1| \cdots |P_i| = p_1^{e_1} \cdots p_i^{e_i}$ para todo $i \leq r$, por inducción sobre i. Para $i = 2$, por ser P_1 y P_2 ambos subgrupos normales, tenemos

$$|P_1 P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = |P_1||P_2| = p_1^{e_1} p_2^{e_2}.$$

   ya que $P_1 \cap P_2 = 1$. Inductivamente,

$$|P_1 \cdots P_{i+1}| = \frac{|P_1 \cdots P_i||P_{i+1}|}{|P_1 \cdots P_i \cap P_{i+1}|}$$

   Pero, por hipótesis de inducción $|P_1 \cdots P_i| = p_1^{e_1} \cdots p_i^{e_i}$ que es primo relativo con $p_{i+1}^{e_{i+1}}$ de donde $P_1 \cdots P_i \cap P_{i+1} = 1$ y deducimos que

$$|P_1 \cdots P_{i+1}| = |P_1| \cdots |P_{i+1}| = p_1^{e_1} \cdots p_{i+1}^{e_{i+1}}.$$

   Concluimos además que para todo $i < r$ los órdenes de $P_1 \cdots P_i$ y P_{i+1} son primos relativos y por tanto $P_1 \cdots P_i \cap P_{i+1} = 1, i = 1, \ldots, r-1$.

3. Por último $P_1 P_2 \cdots P_r = G$ ya que $|P_1 \cdots P_r| = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = |G|$.

Por tanto $P_1 \cdots P_r = G$, como producto directo. □

5.4.1. Ejemplos

Ejemplo 5.7. Si p no divide al orden de G, el único p-subgrupo de Sylow de G es el grupo trivial (y todas las partes del segundo teorema de Sylow son triviales). Si $|G| = p^k$, entonces el mismo G es su único p-subgrupo de Sylow.

Ejemplo 5.8. Un grupo abeliano finito tiene un único p-subgrupo de Sylow para cada primo p. Este subgrupo está formado por todos los elementos cuyo orden es una potencia de p y se llama la *componente p-primaria* del grupo abeliano.

Ejemplo 5.9. S_3 tiene tres 2-subgrupos de Sylow: $< (12) >, < (13) >$ y $< (23) >$. Tiene un único (por tanto normal) 3-subgrupo de Sylow: $< (123) > = A_3$. Nótese que $3 \equiv 1 \pmod 2$.

Ejemplo 5.10. A_4 tiene un único 2-subgrupo de Sylow: $< (12)(34), (13)(24) > = V$. Tiene cuatro 3-subgrupos de Sylow: $< (123) >, < (124) >, < (134) >$ y $< (234) >$. Nótese que $4 \equiv 1 \pmod 3$.

Ejemplo 5.11. S_4 tiene $n_2 = 3$ y $n_3 = 4$. Ya que S_4 contiene un subgrupo isomorfo a D_4, todo 2-subgrupo de Sylow de S_4 es isomorfo a D_4.

Ejemplo 5.12. Sea p un primo. Todo p-subgrupo de S_p tiene orden p, es cíclico y contiene $p-1$ ciclos de longitud p, todos ellos generadores. El número total de ciclos de longitud p en S_p es $(p-1)!$, así que en este caso $n_p = (p-2)!$. Este es también el índice $[S_p : N_{S_p}(P)]$ siendo P un p-subgrupo de Sylow. Por el teorema de Lagrange, $|N_{S_p}(P)| = p(p-1)$.

Calculamos ahora el centralizador (luego nos hará falta): $\sigma \in C_{S_p}(P)$ si y sólo si $\sigma \in C_{S_p}((i_1 \dots i_p))$ para cualquier ciclo no trivial de P. Como todos los ciclos de longitud p son conjugados en S_p, $[S_p : C_{S_p}(P)] = (p-1)!$, luego $|C_{S_p}(P)| = p$ y como P es abeliano, $P = C_{S_p}(P)$ es un subgrupo propio de $N_{S_p}(P)$.

Ejemplo 5.13. Sea p un primo y $G = GL_2(\mathbb{Z}_p)$.

Calculemos $|G|$: Una matriz es invertible si y sólo si las filas son vectores linealmente independientes. La primera fila puede ser cualquiera de los $p^2 - 1$ vectores no nulos de $\mathbb{Z}_p^2$. La segunda fila es uno de los $p^2 - p$ vectores que no están en la recta vectorial generada por la primera, así que en total tenemos $|G| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$.

La máxima potencia de p que divide a $|G|$ es exactamente p, así que todo p-subgrupo de Sylow de G tiene orden p y es cíclico.

$H = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}_p\}$ y $K = \{\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}_p\}$ son dos subgrupos distintos de G de orden p, luego $n_p \geq p+1$.

$D = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \mid a, b \in \mathbb{Z}_p^\times\}$ normaliza a H, $|D| = (p-1)^2$ y $D \cap H = 1$, luego DH es un subgrupo de $N_G(H)$ y $|N_G(H)| \geq |DH| = p(p-1)^2$. De donde $n_p = [G : N_G(H)] = \frac{|G|}{|N_G(H)|} \leq p+1$. En resumen, $n_p = p+1$, $N_G(H) = DH$.