Real Bermúdez Jesús M.

June 16, 2003

1.

2.

3.

4.

5. Teoremas de Sylow

5.1. Acciones de Grupo

Definición 5.1
Sea G un grupo y X un conjunto no vacío. Decimos que *G actúa en X* si existe un homomorfismo

$$\varphi : G \to S_X$$

El Homomorfismo φ es llamado una *representación permutacional* de G en X.
Si $\varphi : G \to S_X$ es un homomorfismo, entonces:

$$\forall g \in G \Rightarrow \varphi(g) \in S_X$$

$$\Rightarrow \varphi(g) : X \to X \quad biyección \quad \forall x \in X, \varphi(g)(x) \in X$$

Denotemos $\forall g \in G$,

$$\varphi_g := \varphi(g) \Rightarrow \forall x \in X, \varphi_g(x) = \varphi(g)(x)$$

, por lo tanto $\varphi : G \to S_X$ es homomorfismo. Por lo tanto $\varphi_g : X \to X$ biyección. Más aún, denotemos: $\forall g \in G, forall x \in X$ $\varphi_g(x) = g \cdot x \in X$.

Propiedades 5.2

1. $\forall g, g_1 \in G$ $\varphi(gg_1) = \varphi(g)\varphi(g_1)$ es decir $\varphi_{gg_1} = \varphi_g \circ \varphi_{g_1}$.
   O sea $\forall x \in X$
   $$(gg_1) \cdot x = g \cdot (g_1 \cdot x)$$
2. $\varphi(e) = e_X$ es decir, $\varphi_e = e_X \Rightarrow \forall x \in X, e \cdot x = x$.
3. $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$ es decir, $\varphi_{g^{-1}} = \varphi_g^{-1}$ o equivalentemente $\varphi_{g^{-1}} \circ \varphi_g = e_X = \varphi_g \circ \varphi_{g^{-1}} \Rightarrow g^{-1} \cdot (g \cdot x) = x = g \cdot (g^{-1} \cdot x) \quad \forall x \in X$.
4. $\in G$ y $\forall x, y \in X$ si $y = g \cdot x \Rightarrow^{-1} \cdot x$.
5. $\forall g \in G$ y $\forall x, y \in X$ si $g \cdot x = g \cdot y \Rightarrow x = y$.
6. $\forall g \in G$, entonces $g \cdot X = X$ donde $g \cdot X = \{g \cdot x | x \in X\}$(ya que $\varphi_g : X \to X essuprayectiva) \Rightarrow \varphi_g(x) = X$, donde
   $$\begin{aligned} \varphi_g(x) &= \{\varphi_g(x) | x \in X\} \\ &= \{g \cdot x | x \in X\} \\ &= g \cdot X. \end{aligned} \tag{1}$$

Ejemplo

Sea G grupo, y sea $X = G$. Sea $\varphi : G \to S_G$ dada por $\forall g \in G$, $\varphi(g) = \varphi_g$ donde $\varphi_g : X \to X$ dada por $\varphi_g(x) = g \cdot x := gxg^{-1}$, es decir, φ_g es un automorfismo interior de G.
Se tiene en efecto que:

$$\varphi : G \to S_G \quad es \quad un \quad homomorfismo$$

es decir, $\forall g, g_1 \in G$

$$\varphi(gg_1) = \varphi(g)\varphi(g_1);$$

o sea

$$\varphi_{gg_1} = \varphi_g \varphi_(g_1)$$

equivalentemente $\forall x \in G$

$$\begin{aligned} gg_1 \cdot x &= g \cdot (g_1 \cdot x) \\ &= (gg_1) \times (gg_1)^{-1} \\ &= g(g_1 \times g_1^{-1})g^{-1} \\ &= g(g_1 \cdot x)g^{-1} \\ &= g \cdot (g_1 \cdot x) \end{aligned} \tag{2}$$

En este caso, φ es llamada la *acción de conjugación.*

Sea $\varphi : G \to S_X$ una representación permutacional o una acción. Definimos la relación sobre X: $\forall x, y \in X \quad x \sim y \Leftrightarrow$ $existe \quad g \in G \quad tal \quad que \quad y = g \cdot x$. Tenemos que $\sim$ es una relación de equivalencia sobre X.

1. Reflexiva.- Si $x \sim y, x \sim x, \forall x \in X$ pues $x = e \cdot x$.
2. Simétrica.- Si $x \sim y \Rightarrow \quad existe \quad g \in G$ tal que $y = g \cdot x \Rightarrow x = g^{-1} \cdot y \Rightarrow y \sim x$.
3. Transitiva.- Si $x \sim y$ y $y \sim z \Rightarrow \quad existe \quad g \in G$ tal que $g = g \cdot x$ y existe $g_1 \in G$ talq ue $z = g_1 \cdot y \Rightarrow z = g_1 \cdot y = g_1 \cdot (g \cdot x) = (g_1 g) \cdot x \Rightarrow x \sim z$

Así esta relación de equivalencia induce una partición en X por las clases de equivalencia llamadas *órbitas de G en X.*

Si $x \in X$, denotamos a su órbita como $O(x)$ donde:

$$\begin{aligned} y \in O(x) &\Leftrightarrow y \sim y \\ &\Leftrightarrow \quad existe \quad g \in G \quad tal \quad que \quad y = g \cdot x \\ &\Leftrightarrow y \in G \cdot x \end{aligned} \tag{3}$$

donde $G \cdot x = \{g \cdot x | g \in G\}$ =órbita, es decir,

$$O(x) = G \cdot x$$

.

Luego, $y \in G \cdot x \Leftrightarrow G \cdot x = G \cdot y$ ó $y \notin G \cdot x \Leftrightarrow G \cdot x \cap G \cdot y = \emptyset$.

Sea $\{x_i | i \in I\}$ un conjunto completo de representantes bajo esta relación, entonces:

$$X = \cup_{i \in I} G \cdot X_i = unión \quad disjunta.$$

Si la relación de equivalencia consta de una órbita, entonces decimos que la relación es *transitiva*, es decir; $\forall x, y \in X$ $x \sim y$.

Definición 5.3

Pra cada $x \in X$, se define el *estabilizador de x* como: $G_X := \{g \in G | g \cdot x = x\}$, notemos que: $\forall x \in X \quad e \cdot x = x \Rightarrow e \in G_X \quad (G_X \neq \emptyset)$.

Denotemos por:

$$\begin{aligned} X^G &:= \{x \in X | g \cdot x\} \\ &= \{x \quad \forall g \in G\} \subset G \\ &= conjunto \quad de \quad puntos \quad fijos \end{aligned} \tag{4}$$

$x \in X^G \Leftrightarrow g \cdot x = x \forall g \in G \Leftrightarrow G \cdot x = \{x\}$. Así si $|x| < +\infty$. Tenemos que $x = \cup_{i \in I} G \cdot x_i$ donde $\{x_i\}_{i \in I}$ representa un conjunto completo de representantes en las órbitas de G en X $\Rightarrow$

$$\begin{aligned} |x| &= \sum_{i \in I} |G \cdot x_i| \\ &= |x^G| + \sum_{i \in I \quad y \quad x_i \notin x^G} |G \cdot x_i| \quad = |x^G| + \sum_{i \in I \quad y \quad x_i \notin x^G} [G : G_{x_i}] \end{aligned} \tag{5}$$

Por lo tanto $|x| = |x^G| + \sum_{i \in I \quad y \quad x_i \notin x^G} [G : G_{x_i}]$, si además $|G| < +\infty$, entonces:

$$|x| = |x^G| + \sum_{i \in I \quad y \quad x_i \notin x^G} \frac{|G|}{|G^{x^i}|} \tag{6}$$

En particular, si consideramos la acción de conjugación:

$$|G| = |Z| + \sum_{i \in I \quad y \quad x_i \notin x^G} \frac{|G|}{|N_G(x_i)|} \tag{7}$$

Ejmeplo

Sea G grupo. Entonces, la relación de conjugación, $\forall x, y, g \in G$

$$g \cdot x = gxg^{-1}$$

y

$$y \sim x \Leftrightarrow y = gxg^{-1}$$

$$\begin{aligned} G \cdot x &= C(x) \\ &= \{gxg^{-1} | g \in G\} \end{aligned} \tag{8}$$

$$\begin{aligned} G_X &= \{g \in G | gxg^{-1} = x\} \\ &= \{g \in G | gx = xg\} \\ &= N_G(x) \end{aligned} \tag{9}$$

$$\begin{aligned} x \in X^G = G^G &\Leftrightarrow gxg^{-1} = x \quad \forall g \in G \\ &\Leftrightarrow gx = xg \quad \forall g \in G \\ &\Leftrightarrow x \in Z \end{aligned} \tag{10}$$

Por lo tanto $X^G = Z$

Proposición 5.4
Para todo $x \in X$, $G_X < G$

Demostración

Sean $g, g_1 \in G_X$. Veamos que $gg_1^{-1} \in G_X$. Tenemos que $g \cdot x = x = g_1 \cdot x \Rightarrow g_1^{-1}x = x$.
Por lo tanto $gg_1^{-1} \cdot x = g \cdot (g_1^{-1} \cdot x) = g \cdot x = x \Rightarrow gg_1^{-1} \in G_X$
Por lo tanto $G_X < G$

q.e.d.

Corolario
Para todo $x \in G$, $N_G(x) < G$.

Proposición 5.5
Para todo $x \in G$;

$$|G \cdot x| = [G : G_X]$$

En particular, si G es finito entonces $|G \cdot x| = \frac{|G|}{|G_X|}$.

Demostración

Sea $\varphi : G \cdot x \to G/_I G_X$

1. φ está bien definida:
   Si g, g_1 tal que $g \cdot x = g_1 \cdot x \Rightarrow (g_1^{-1}) \cdot x = x \Rightarrow g_1^{-1}g \in G_X \Rightarrow gG_X = g_1G_X$.
2. φ es inyectiva:
   $\varphi(g \cdot x) =' varphi(g_1 \cdot x)$ entonces $gG_X = g_1G_X \Rightarrow g_1^{-1}g \in G_X \Rightarrow g_1^{-1}g \cdot x = x \Rightarrow g \cdot x = g_1 \cdot x$.
3. φ es suprayectiva (es inmediata).

por lo tanto $|G \cdot x| = [G : G_X]$.

q.e.d.

Corolario
Para toda $x \in G$, $|c(x)| = [G : N_G(x)]$

Proposición 5.6
Si G es grupo con $|G| = p^n$ con p primo y $n \geq 1$ entonces $Z \neq < e >$.

Demostración

Bajo la notación anterior, tenemos que si $Z \neq G \Rightarrow$ existe $i \in I$ tal que $x_i \notin Z \Rightarrow \frac{|G|}{|N_i(x_i)|||G|=p^n} \Rightarrow p|\frac{|G|}{|N_G(x_i)|} \Rightarrow p|\sum_{i\in I \quad y \quad x_i \notin x^G} \frac{|G|}{|N_G(x_i)|} - |G| = -|Z| \Rightarrow |Z| > 1 \Rightarrow z \neq < e >$.

q.e.d.

Observación
G es Abeliano si y sólo si $G = Z$

Proposición 5.7
Supóngase que G es finito con $|G| = p^n$ con $ngeq1$, p primo. Si x es finito no vacío y G actúa en X, entonces:

$$|x| \equiv |x^G| \quad mod \quad p$$

Demostración

Tomemos $\{x_i | i \in I\}$ un conjunto completo de representantes en las órbitas de G en X, entonces:

$$|x| = |x^G| + \sum_{x_i \in X^G} \frac{G}{Gx_i}$$

puesto que $p|\frac{|G|}{|Gx_i|}$ con $x_i \notin X^G \Rightarrow p|\sum_{x_i} \notin X^G \frac{|G|}{|Gx_i|=|x|-|X^G| \quad mod \quad p}$.

q.e.d.

Teorema 5.8 (de Cauchy)
Si G es un grupo finito y p es un número primo tal que $p||G|$, entonces existe $a \in G$, $a \neq e$ tal que $a^p = e$

Demostración
Sea $X = \{(a_1, ..., a_p) \in G \times G \times ... \times G = G^p | a_1...a_2 = e\}$.
Notemos que: $X \neq \emptyset$ pues $(e, ..., e) \in X$. Denotemos por $n = |G|$ tenemos:

1. $|X| = n^{p-1}$. Definimos $h : X \to G^{p-1}$ dada por $h(a_1, ..., p) = (a_1, ..., p-1) \quad \forall (a_1, ..., a_p) \in X$. Entonces h es *biyección*:

   a) h es inyectiva:
   $h(a_1, ..., a_p) = h(b_1, ..., b_p) \Rightarrow (a_1, ..., a_{p-1}) = (b_1, ..., b_{p-1}) \Rightarrow a_i = b^i \quad \forall i \in \{1, 2, ..., p-1\}$ donde $a_1 \cdot ... \cdot a_p = e = b_1 \cdot ... \cdot b_p \Rightarrow a_p = b_p$.
   Por lo tanto $(a_1, ..., a_p) = (b_1, ..., b_p)$

   b) h es suprayectiva:
   Sea $(a_1, ..., a_{p-1}) \in G^{p-1}$, $ap = a_{p-1}^{-1} \cdot ... \cdot a_1^{-1} \in G \Rightarrow h(a_1, ..., a_p) = (a_1, ..., a_{p-1})$.
   Por lo tanto $|X| = |G^{p-1}| = n^{p-1}$, en particular $p||X|$.

   Consideremos el grupo cíclico $H = \mathbb{Z}/p\mathbb{Z}$ de p elementos.

   Redefinimos a X como:
   $$X = \{(a_{[1]}, ..., a_{[p]}) | a_{[1]} \cdot ... \cdot a_{[p]} = e\}$$
   donde $[k] \in H \quad (k \in \mathbb{Z})$. Definimos $\forall [k] \in H$, $\varphi_{[k]} : X \to X$ dada por $\varphi_{[k]}(a_{[1]}, ..., a_{[p]}) = (a_{[k+1]}, ..., a_{[p+k]})$.

2. $\varphi_{[k]}$ está bien definida:

   Sea $k' \in [k] \Rightarrow k \equiv k' \quad mod \quad p \Rightarrow k+i \equiv k'+i \quad mod \quad p, \forall i \in \mathbb{Z} \Rightarrow (a_{[1+k]}, ..., a_{[p+k]}) = (a_{[1+k']}, ..., a_{[p+k']}) \Rightarrow \varphi_k(a_{[1]}, ..., a_{[p]}) = \varphi_{k'}(a_{[1]}, ..., a_{[p]})$. Además $\forall [k] \in H$.

   $a_{[1+k]} \cdots a_{[p+k]} = a_{[1]} \cdot a_{[i+1]} \cdots a_{[p]} a_{[1]} \cdots a_{[i-1]} = e$ donde $1 \leq i \leq p$ y $[i] = [1+k]$

3. $\varphi_{[k]}$ es inyectiva:

   $\varphi_{[k]}(a_{[1]}, ..., a_{[p]}) = \varphi_{[k]}(b_{[1]}, ..., b_{[p]}) \Rightarrow (a_{[1+k]}, ..., a_{[p+k]}) = (b_{[1+k]}, ..., b_{[p+k]}) \Rightarrow a_{[i+k]} = b_{[i+k]}, \forall \quad i \leq i \leq p \Rightarrow a_{[i]} = b_{[i]}, \forall \quad 1 \leq i \leq p$.

4. φ_k es suprayectiva:

   Sea $(b_{[1]}, ..., b_{[p]}) \in X$. Sea $a_{[1]} = b_{[1-k]}, a_{[2]} = a_{[2-k]}, ..., a_{[p]} = b_{[p-k]}$, entonces tenemos que :

$$a_{[1]} \cdots a_{[p]} = b_{[1-k]} \cdots _[p-k] = e$$

   y

$$\varphi(a_{[1]} \cdots a_{[p]}) = (b_{[1]} \cdots b_{[p]})$$

   Por lo tanto $\varphi_{[k]}$ es biyección.

   Ahora bien, sea $\varphi : H \to S_x$ dada por:

$$\varphi_{[k]} := \varphi_{[k]}$$

   .

   Se tiene que φ está bien definida:

   Si $k' \in [k] \Rightarrow k' = k \quad mod \quad p, \Rightarrow \varphi_{k'} = \varphi_k$. Además φ *es homomorfismo*, es decir, $\forall [k], [k'] \in H$

$$\varphi([K] + [K]i) = \varphi_{[k]} \circ \varphi_{[K]i}$$

   En efecto :

$$\begin{aligned}(\varphi_{[k]} \circ \varphi_{[k']})(a_{[1]}, ..., a_{[p]}) &= \varphi(\varphi_{[k']}(a_{[1]}, ..., a_{[p]})) \\ &= \varphi_{[k]}(a_{[1+k']+...+a_{[p+k]}}) \\ &= (a_{[i+k+k']}, ..., a_{[1+k+k']}) \\ &= \varphi_{[k+k']}(a_{[1]}, ..., a_{[p]}) \in X\end{aligned} \tag{11}$$

   Por lo tanto $\varphi_{[k+k']} = \varphi_{[k]+[k']} = \varphi_{[k]} \cdot \varphi_{[k']}$.

   De aquí que:

$$|X| = |X^H| + \sum_{x \in X^H} \frac{|H|}{|Hx|}$$

   la suma variando en un conjunto de representantes completo de las órbitas de H en X con xX^H.

   Notemos que si $x \notin X^H, \quad (x \in X) \Rightarrow \frac{|H|}{|Hx|} > 1$ y $\frac{|H|}{|Hx|}||H| = p \Rightarrow \frac{|H|}{|Hx|} = p, \quad con \quad x \notin X^H$. Teniendo que $|x| = n^{p-1}$, obtenemos $n^{p-1} = |X^H| + tp, \quad t \in \mathbb{N}$ como $p|n^{p-1} \Rightarrow p||X^H|$ en particular $|X|^H > 1$. pero $(a_{[1]}, ..., a_{[p]}) \in X^H \Leftrightarrow [k] \cdot (a_{[1]}, ..., a_{[p]}) = (a_{[1]}, ..., a_{[p]}), \forall [k] \in K \Leftrightarrow (a_{[1+k]}, ..., a_{[p+k]}) = a_{[1]}, ..., a_{[p]}, \forall \quad k \in \mathbb{Z} \Leftrightarrow a_{[1]} = ... = a_{[p]}$.

   Así $X^H = \{(a_1, ..., a_p) \in G^p | a^p = e\}$ como $|X^H| > 1$ con $(e_1 ... e) \in X^H \Rightarrow$ existe $a \in G$, $a \neq e$ tal que $a^p = e$

q.e.d.

Observación

La cantidad de elementos de G de orden p es $|X^H| - 1$, donde $|X^H| - 1 = (-pt - 1) + n^{p-1} = n^{p-1} - pt - 1$, por lo tanto $|X^H| - 1 \equiv -1 \quad mod \quad p$.

Definición 5.9

Sea G un grupo y p un número primo. Decimos que G es un $p - grupo$ si $\forall g \in G, |g| = p^m$ para algún $m \geq 0$.

Proposición 5.10

Sea G un grupo finito y p u número primo. Entonces G es $p - primo$ si y sólo si $|G| = p^n$ para algún $n \geq 0$

Demostración

Supongamos que G es un p-grupo; con $|G| = m$. Si $m = 1 \Rightarrow m = p^0$. Supongamos que $m > 1$. Sea q número primo tal que: $q|m = |G|$, por el teorema de Cauchy existe $a \in G, a \neq e$ tal que $|a||q \Rightarrow |a| = q$, pero por hipótesis $|a| = pt$ con $t \geq 1 \Rightarrow q = pt \Rightarrow q = p$ y $t = 1$.

Por lo tanto $m = p^n$,con $n \geq 1$.

Recíprocamente, supóngase que $|G| = p^n$ con $n \geq 0$. Sea $g \in G \Rightarrow |g|||G| = p^n \Rightarrow |g| = p^2$, con $t \geq 0$.

Por lo tanto G es p grupo.

q.e.d.

Definición 5.11

Sea G grupo y $H < G$. Si p es número primo, decimos que H es $p-$subgrupo de G si H es $p - subgrupo$.

Proposición 5.12

Sea H un $p - subgrupo$ de G con G finito. Entonces

$$[G : H] \equiv [N_G(H) : H] \quad mod \quad p$$

Demostración

Sabemos que $\varphi : G \to S_X$ dada por $\varphi(g) = \varphi_g$ donde $\varphi_g(xH) = gxH, \forall x \in G$, es un homomorfismo de G en S_X con $X = G/_I H \Rightarrow \psi = \varphi|_H : H \to S_X$ es un homomorfismo. Así que H actúa sobre X con

$$h \cdot (xH) = hxH, \forall h \in H, \forall x \in G$$

Sea $x \in G$, $xH \in X^H \Leftrightarrow h \cdot xH = xH_1 \quad \forall h \in H \Leftrightarrow hxH = xh, \forall h \in H \Leftrightarrow x^{-1}hxH = H, \forall h \in H \Leftrightarrow x^{-1}hx \in H, \forall h \in H \Leftrightarrow x^{-1}Hx \subset H \Leftrightarrow x^{-1}Hx = H \in N_G(x) \in N_G(H)/_I H$

Por lo tanto $X^H = N_G(H)/_I H \Rightarrow [G : H] = |X| = |X^H| + \sum_{x \notin X^H} \frac{|H|}{|H_X|} = [N_G(H) : H] + tp$

Por lo tanto $[G : H] = [N_G(H) : H] \quad mod \quad p$.

q.e.d.

5.2. Teoremas de Sylow

Teorema 5.13 (Primer Teorema de Sylow)

Sea G un grupo finito con $|G| = p^n m$ donde $n \geq 1, m \geq 1$, p es número primo y $(p, m) = 1$. Entonces, para cada $0 \leq k < n$ existe un subgrupo de orden p^k con $0 \leq k < n$ es normal en un subgrupo de orden p^{k+1}.

Demostración

Si $k = 0$ basta tomar $H_0 =< e >$. Para $k = 1$, considerando el Teorema de Cauchy, tenemos que existe $a \in G, a \neq e$ tal que $a^p = e \Rightarrow |a| = p_1 :=< a >$ es tal que $|H_1| = p$ y $H_0 \lhd H_1$ por inducción, supóngase construídos subgrupos $H_0 \lhd H_1 \lhd ... \lhd H_k$ tales que $|H_i| = p^i, 0 \leq i \leq k \quad con \quad k < n$, construyamos un subgrupo H_{k+1} de G tal que $|H_{k+1}| = p^{k+1}$ y $H_k \lhd H_{k+1}$ como $|H_k| = p^k$, entonces: $[G : H_k] \equiv [N_G(H_k) : H_k] \quad mod \quad p$, donde $[G : H_k] = \frac{|G|}{|h_k|} = p^{n-k}m \quad (n - k > 0) \Rightarrow p|[N_G(H_k) : H_k] = |N_G(H_k)/H_k|$.

Por el teorema de Cauchy existe $[H] < N_G(H_k)/H_k$ tal que $|[H]| = p$. Por el teorema de correspondencia, existe $H_{k+1} < N_G(H_k)$ con $H_{k+1} \supseteq H_k$ tal que $[H] = H_{k+1}/H_k \Rightarrow p = |[H]| = |H_{k+1}/H_k| = \frac{|H_{k+1}|}{|H_k|} = \frac{|H_{k+1}|}{p^k} \Rightarrow |H_{k+1}| = p^{k+1}$. Finalmente, como $H_k < H_{k+1} < N_G(H_k) \Rightarrow H_k \lhd H_{k+1}$ con $|H_{k+1}| = p^{k+1}$

q.e.d.

Corolario

En las condiciones del teorema anterior, se tiene que existe $P < G$ tal que $|P| = p^n$.

Lema de Zorn 5.14

Sea $(x, <)$ parcialmente ordenado tal que toda cadena de X tiene una cota superior en X entonces X tiene un máximal.(Una cadena es: C $\subset Xtalquetodoelementoen Cestárelacionado$)

Definición 5.15

Sea G grupo, y sea p número primo.Un p-subgrupo de G maximal es llamado *p-subgrupo sylow de G.*

Observaciones
Aplicando el Lema de Zorn; se prueba que todo grupo tiene p-subgrupos Sylow para cada primo p.

Proposición 5.16 ıG grupo finito con $|G| = p^n m$, con $n, m \geq 1$, p primo y $(p, m) = 1$, entonces para $P \neq < e >$ p-subgrupo de G se tienen las siguientes equivalencias:

1. P es p-subgrupo Sylow.
2. —P—=p$^n(|P|, [G : P]) = 1$

Demostración

1) $\Rightarrow$ 2). Se tiene que P es p-subgrupo maximal , es decir, si H es p-subgrupo de G tal que $P < H \Rightarrow P = H$. Si $|P| = p^t$ con $t < n$, por el primer Teorema de Sylow, se tiene que $H < G$ tal que $P \lhd H$ y $|H| = p^{t+1}$ lo cual es una contradicción. Por lo tanto $|P| = p^n$.

$ii) \Rightarrow iii)$. Si $|P| = p^n \Rightarrow [G : P] = m$ con $(p, m) = 1 \Rightarrow (|p|, [G : P]) = 1$

$iii) \Rightarrow i)$. Sea $t \geq 0$ tal que $|P| = p^t$. Puesto que $(p^t, p^{n-t}m) = 1 \Rightarrow t = 0 \quad ó \quad t = n$. Si $t = 0 \Rightarrow P =< e >$ lo cual no puede ser $\Rightarrow t = n \Rightarrow |P| = p^n$. Además, P es p-subgrupo Sylow, ya que en caso contrario, existiría $H < G$ tal que $|H| = p^k$ con $P < H, P \neq H \Rightarrow p^n < p^k \Rightarrow p^k | p^n m$, lo cual es una contradicción.

3. q.e.d.

Definición 5.17
Sea H y K subgrupos de G.Decimos que H y K son *conjugados* si existe $x \in G$ tal que $H = xKx^{-1}$

Observaciones
Si G es grupo y $H < G$. Entonces:

1. $\forall x \in G, xHx^{-1} < G$
2. $|H| = |xHx^{-1}| \quad \forall x \in G.$

Proposición 5.18
Si G grupo finito con $|G| = p^n m$ y P es p-subgrupo Sylow de G. Entonces, todo conjugado de P es un p-subgrupo Sylow de G.

Demostración

Es inmediata definiendo

$$H \to xHx^{-1}$$
$$h \mapsto xhx^{-1}$$

q.e.d.

Proposición 5.19
Sea G grupo finito con $|G| = p^n m$ $(n, mgeq1$, p primo y $(p, m) = 1)$. Sea P un p-subgrupo Sylow de G. Entonces si P es el único p-subgrupo Sylow de G entonces $P \lhd G$.

Demostración

Por demostrar que $\forall x \in G$ $P = xPx^{-1}$. Si $x \in G \Rightarrow xPx^{-1}$ es un p-subgrupo Sylow de G entonces $xPx^{-1} = P$.
Por lo tanto $P \lhd G$.

q.e.d.

Segundo Teorema de Sylow 5.20

Sea G grupo finito con $|G| = p^n m$ con $n, m \geq 1$, p número primo y $(p, m) = 1$. Sea P un p-subgrupo Sylow de G, y sea H un p-subgrupo de G. Entonces existe $x \in G$ tal que $H < xPx^{-1}$. En particular, los p-subgrupos Sylow de G son conjugados.

Demostración

Sabemos que

$$\begin{aligned} \varphi : G &\to S_X \\ g &\mapsto \varphi_g \end{aligned}$$

donde $X = G/_I P$ y $\forall g \in G$ $\varphi_g : X \to X$ dada por $\varphi_g(xP) = gxP \quad \forall x \in G$ es un homomorfismo.

Restringiendo a H, tenemos que la función $\psi : \varphi|_H : H \to S_X$es un homomorfismo. Así H actúa sobre X como: $h \cdot (xP) = hxP \forall h \in H$ y $x \in G$. Como H es p-subgrupo de G, se tiene que:

$$|x| \equiv |x^H| \quad mod \quad p$$

donde $|x| = [G : P] = m \Rightarrow p \nmid |x^H|$. En particular, $x^H \neq \emptyset$. Sea $x \in G$

$$\begin{aligned} xP^H &\Leftrightarrow hxP = x =\in H \\ &\Leftrightarrow x^{-1}hxP = P \forall h \in H \\ &\Leftrightarrow x^{-1}h^{\in}P \forall h \in H \qquad \Leftrightarrow h \in xPx^{-1} \forall h \in H \Leftrightarrow H < xP^{-1}x \end{aligned}$$

Por lo tanto $x^H = \{xP | H < xP^{-1}x\} \neq \emptyset \Rightarrow$ existe $x \in G$ tal que $H < xPx^{-1}$. En particular, si $|H| = p^n \Rightarrow |H| = p^n \leq |xPx^{-1}| \Rightarrow |H| = xPx^{-1}$

q.e.d.

Corolario

En las mimas condiciones del teorema anterio. Sea p un p-subgrupo Sylow de G. Entonces $P \lhd G$ si y sólo si P es el único p-subgrupo Sylow de G.

Demostración

Seupongamos que $P \lhd G$. Sea G un p-subgrupo Sylow de G. Por el Segundo Teorema de Sylow, existe $x \in G$ talque $Q = xPx^{-1}$. Como $P \Rightarrow Q = xPx^{-1}$.

Por lo tanto P es el único p-subgrupo Sylow de G.

Recíprocamente si $x \in G \Rightarrow xPx^{-1}$ es p-subgrupo Sylow de G. Por unicidad $xPx^{-1} = P \Rightarrow P \lhd G$

q.e.d.

Corolario

En las mimas condiciones del Teorema anterior. Sea P un p-subgrupo Sylow de $N_G(P)$; además P es el único p-subgrupo Sylow de $N_G(P)$

Demostración

Tenemos que $|p| = p^n$. si Q fuera p-subgrupo sylow de $N_G(P) \Rightarrow |Q| = p^k$ para algún $kgeq0$ donde $p^k = |Q|||N_G(P)|$ y $|N_G(P)||G| \Rightarrow p^k||G| = p^n m \Rightarrow p^k|p^n \Rightarrow 0 \leq k \leq n$.Como $P \lhd N_G(P)$ y $|P| = p^n \Rightarrow P$ es un p-subgrupo Sylow de $N_G(P)$. Por el corolario anterior, P debe ser el único p-subgrupo Sylow en $N_G(P)$

q.e.d.

Corolario
En las condiciones anteriores. Si P es p-subgrupo Sylow de G, entonces $N_G(N_G(P)) = N_G(P)$

Demostración

Es claro que $N_G(P) \subseteq N_G(N_G(P))$. Sea k=N$_G(P).Pordemostrarque$:N$_G(K) \subset K \Rightarrow xKx^{-1} = K$ como $P < K \Rightarrow xPx^{-1} < xKx^{-1} = K$ donde xPx^{-1} es p-subgrupo Sylow de G $\Rightarrow P = xPx^{-1} \Rightarrow x \in K$.
Por lo tanto $N_G(K) \subseteq K$, por lo que $N_G(K) = K$.

q.e.d.

Tercer Teorema de Sylow 5.21
Sea G grupo finito con $|G| = p^n m$ con $n, m \geq 1$, p número primo y $(p, m) = 1$. Sea P un p-subgrupo Sylow de G. Denotemos por n$_p alacantidadde$p-subgrupos Sylow de G.$Entonces$:

1. $n_p = [G : N_G(p)]$
2. $n_p || G|$
3. $n_p \equiv 1 \quad mod \quad p$

Demostración

Sea X el conjunto de los p-subgrupos Sylow de G. Es decir:

$$X = \{xPx^{-1} | x \in G\}$$

además $n_p = |X|$. Notemos que si $x, y \in G$ entonces $xPx^{-1} = yPy^{-1} \Leftrightarrow y^{-1}xP(y^{-1}x)^{-1} = y^{-1}xPxy = P \Leftrightarrow y^{-1}x \in N_G(P) \Leftrightarrow xN_G(P) = yN_G(P)$ o equivalentemente $xPx^{-1} \neq yPy^{-1}N_G(P) \neq yN_G(P)$.
Por lo tanto $n_p = [G : N_G(P)]$. Esto Prueba 1).

2) $n_p = [G : N_G(P)] = \frac{|G|}{|N_G(P)|} || G|$.

3) Sea $\varphi : P \to S_X$ dada como sigue: Sea $g \in P$ y sea $\varphi_g : X \to X$ dada por $\varphi_g(Q) = gQg^{-1} \in X$. Se tiene que φ está bien definida y determina una acción de P en X.
Como P es p-subgrupo Sylow, bajo esta acción, se tiene que: $|X| \equiv |X^p| \quad mod \quad p$, es decir; $n_p \equiv |X^p| \quad mod \quad P$. Veamos que $|X^p| = 1$. Notemos que $p \nmid n_p = [G : N_G(P)] \Rightarrow X^p \neq \emptyset$.
Sea $Q \in X$ entonces

$$\begin{aligned} Q \in X^p &\Leftrightarrow gQg^{-1} = Qquad \in P \\ &\Leftrightarrow P < N_G(a) \\ \Rightarrow Q &= P \end{aligned}$$

Por lo tanto $X^p = \{p\} \Rightarrow |X^p| = 1$. Por lo tanto $n_p \equiv 1 \quad mod \quad p$.

q.e.d.

Ejemplos

1. Sean p,q números primos con $p < q$ y sea G un grupo de orden pq. Entonces:
   a) Un q-subgrupo Sylow es normal en G. En particular G no es simple.
   b) Si $p \nmid (q - 1)$, entonces G es cíclico.

Solución

i) Tenemos que $n_q || G| = pq$, de donde $n_q 1 \quad mod \quad q \Rightarrow q \nmid n_q \Rightarrow n_q \equiv 1$, p donde $n_q \equiv 1 \quad mod \quad q$.
Puesto que $q \nmid (p - 1)$. Por lo tanto $n_q = 1$, por lo que un q-subgrupo Sylow de G debe ser normal.

Tenemos que $n_p||G| = pq$ y $n_p \equiv 1 \quad mod \quad p \Rightarrow p \nmid n_p, n_p = 1, q$.

Puesto que $p \nmid (q-1) \Rightarrow n_p = 1$.Por lo tanto Un p-subgrupo Sylow y q-subgrupos Sylow de G $\Rightarrow P \lhd G, Q \lhd G$ con $PQ \lhd G$ y $|PQ| = \frac{|p||Q|}{|P \cap Q|} \Rightarrow |PQ| = pq$ (Pues si $a \in P \cap Q \Rightarrow |a|||p| = p \quad y \quad |a|||Q| = q \Rightarrow |a| = 1 \quad y \quad a = e. \therefore P \cap Q =< e >$).

Por lo tanto $G = PQ$ y $P \cap Q =< e >$, con $P, Q \lhd G \Rightarrow G \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, entonces $G \cong \mathbb{Z}/qp\mathbb{Z}$ =grupo cíclico de orden pq.

q.e.d.

2. Encuentre los 2 y 3 subgrupos

Solución

$S_3 = \{e, \pi, \pi^2, \sigma, \sigma, \sigma\pi, \sigma\pi^2\}$ donde $|\sigma| = 2$, $|\pi| = 3$ y $\pi\sigma = \sigma\pi^2$.

Como $|S_3| = 3! = 2 \cdot 3$. Por el ejemplo anterior, un 3-Sylow de S_3 debe ser Normal, es decir; $n_3 = 1$, como $|\pi| = 3$ entonces $G =< \pi >$ es un 3-subgrupo Sylow de S_3. Si P es un $2-Sylow$, $P \cap Q =< e >$. Notemos que $n_2 \equiv 1 \quad mod \quad 2$ y $n_2|6 \Rightarrow n_2 = 1 \quad ó \quad 3 \Rightarrow P_1 =< \sigma >$ es un 2-subgrupo Sylow de S_3. También $(\sigma\pi)^2 = \sigma\pi\sigma\pi = \sigma\sigma\pi^2\pi = \sigma^2\pi^3 = e$

Por lo tanto $|\sigma\pi| = 2 \Rightarrow P_2 =< \sigma\pi >$ es un 2-subgrupo Sylow de S_3.

Finalmente $\sigma\pi^2\sigma\pi^2 = \sigma\pi\pi\sigma\pi^2 = \sigma\pi\sigma\pi^2 = \pi^2 = \sigma\pi\sigma\pi = e$.

Por lo tanto $|\sigma\pi^2| = 2 \Rightarrow P_3 =< \sigma\pi^2 >$ es un 2-subgrupo Sylow de S_3

3. Sea G un grupo con $|G| = 21$. Analizando el grupo G se tiene que:

   a) G no es simple. Sea Q un 7-subgrupo Sylow de G $\Rightarrow Q \neq G$ con $|G| = 21 \nmid [G : Q]! = 3! = 6$.
   Por un corolario, G no es simple, más aún se establece que existe $N \lhd G$ tal que N es el máximo subgrupo Normal de G contenido en Q.
   Puesto que $|Q| = 7$ y $N \neq< e >$, entonces $N = Q \Rightarrow Q \lhd G$ y $n_7 = 1$.

   b) $N_3 = 1$ o 7, si $n_3 = 1 \Rightarrow$ un 3-subgrupo Sylow de G es normal. Luego G sería cíclico de orden 21, i.e., $G \cong \mathbb{Z}/21\mathbb{Z}$.
   Si $n_3 = 7$, entonces G no es Abeliano, además si P es un 3-Sylow de G, entonces $PQ < G$ y $P \cap Q =< e >\Rightarrow |PQ| = |P||Q| = 21 \Rightarrow G = PQ$.
   Por lo tanto si $P =< a >$ y $Q =< b >\Rightarrow |a| = 3, |b| = 7$ y
   $G = \{e, a, a^2, b, b^2, b^3, b^4, b^5, b^6, ab, ab^2, ab^3, ab^4, ab^5, ab^6, a^2b, a^2b^2, a^2b^3, a^2b^4, a^2b^5, a^2b^6\}$