6. $\mathcal{G}$-conjuntos y P-grupos

6.1. Definiciones y $\mathcal{G}$-conjuntos

Definición

Sea $\mathcal{G}$ un grupo, $\emptyset \neq X$ un conjunto. Una acción de $\mathcal{G}$ sobre X (por la izquierda) es una aplicación

$$\begin{aligned} ac: \mathcal{G}\times X &\longrightarrow X \\ (g,x) &\longmapsto ac(g,x) = {}^{g}x \end{aligned}$$

¡El orden!

que verifica:

i) ${}^{1}x = x \quad \forall x\in X$

ii) ${}^{g}({}^{h}x) = {}^{(gh)}x \quad \forall x\in X,\ \forall g,h\in \mathcal{G}$

Cuando ocurre esto, diremos que $\mathcal{G}$ actúa u opera por la izquierda sobre X. Al conjunto X se le llama $\mathcal{G}$-conjunto a izquierda. Y a la aplicación ac se le llama aplicación de $\mathcal{G}$-estructura.

Ejemplo

siempre actúa el 1.

i) La acción trivial $ac: \mathcal{G}\times X \longrightarrow X$, $ac(g,x)=x$ $\forall g\in\mathcal{G},\ x\in X$.

ii) La acción por restricción de un subgrupo $H\leq\mathcal{G}$ sobre X

$$\begin{tikzcd} H\times X \arrow[r, "ac_H"] \arrow[dr, "i_1"'] & X \\ & \mathcal{G}\times X \arrow[u, "ac_{\mathcal{G}}"'] \end{tikzcd}$$

iii) La acción natural de S_n sobre $X=\{1,2,\dots,n\}$ dada por

$$\begin{aligned} ac: S_n\times X &\longrightarrow X \\ (\sigma,i) &\longmapsto ac(\sigma,i) = {}^{\sigma}i = \sigma(i) \end{aligned}$$

Proposición

Sea $\mathcal{G}$ un grupo, X un conjunto no vacío. Dar una acción de $\mathcal{G}$ sobre X equivale a dar un homomorfismo de grupos de $\mathcal{G}$ en $\mathrm{Perm}(X)$. → Date cuenta de que al llegar a X sólo alteramos el orden de los elementos de X

-Demostración-

$\Rightarrow$)

Sea $\begin{aligned} ac: \mathcal{G}\times X &\longrightarrow X \\ (g,x) &\longmapsto ac(g,x)={}^{g}x \end{aligned}$ luego $\forall g\in\mathcal{G}$ definimos $\varphi_g: X\longrightarrow X$ una aplicación dada por

φ_g es la acción para cada $g\in\mathcal{G}$

$\varphi_g(x) = {}^{g}x$ $\forall x\in X$. Veamos que φ_g nos permite construir ese homomorfismo.

i) $\varphi_1 = id_X$

ii) $\varphi_{gh} = \varphi_g\varphi_h$ $\forall g,h\in\mathcal{G}$

} Es reescribir las propiedades de las acciones

↳ Esto es una composición

Porque en ese caso pertenece a un grupo y es una alteración del orden.

¿Por qué tener una inversa nos da la pertenencia?

$id_X = \varphi_1 = \varphi_{gg^{-1}} = \varphi_g\varphi_{g^{-1}}$ pero $id_X = \varphi_{g^{-1}}\varphi_g$ luego $\forall g\in\mathcal{G}$ tenemos una inversa $\Rightarrow \varphi_g\in\mathrm{Perm}(X)$.

luego $\begin{aligned} \phi: \mathcal{G} &\longrightarrow \mathrm{Perm}\,X \\ g &\longmapsto \varphi_g \end{aligned}$ es el homomorfismo de grupos que buscamos.

$\Leftarrow$]

Sea $\Phi : G \longrightarrow Perm(X)$ un homomorfismo de grupos, definimos $ac : G \times X \longrightarrow X$
$(g, x) \longmapsto \Phi(g)(x) = {}^{g}x$

que cumple que:

i) ${}^{1}x = \Phi(1)(x) = x$

ii) ${}^{g}({}^{h}x) = \Phi(g)(\Phi(h)(x)) = \Phi(gh)(x) = {}^{(gh)}x$ $\square$

Al homomorfismo ϕ se le reconoce como la representación de G por permutaciones. Además, como ϕ es un homomorfismo podemos calcular su núcleo luego

$$Ker(\phi) = \{g \in G \mid \Phi(g) = id_X\} = \{g \in G \mid {}^{g}x = x \quad \forall x \in X\}$$

y lo llamaremos núcleo de la acción; en el caso de que $Ker(\phi) = 1$, diremos que la acción es fiel

Ejemplo

i) La acción trivial.

$$\phi : G \longrightarrow Perm(X)$$
$$g \longmapsto g$$

ii) La acción por restricción Será fiel sii ϕ_G es fiel

$$\phi_H : H \longrightarrow Perm(X)$$
$$h \longmapsto (\phi_G \circ i)(h)$$

iii) La acción natural

$$\phi : S_n \longrightarrow Perm(X) = S_n$$
$$\sigma \longmapsto \sigma$$

Es fiel pues para $\sigma \in S_n$, $\sigma(i) = i \ \forall i \in X \Rightarrow \sigma \equiv 1$

iv) La acción de D_4 sobre $X = \{1, 2, 3, 4\}$

¡Inyectiva $\Rightarrow$ fiel!

$ac : D_4 \times X \longrightarrow X \qquad ac(g, x) = {}^{g}x = \Phi(g)(x)$

$\phi : D_4 \longrightarrow Perm(X) = S_4 \qquad \phi(r) = (1234) \quad \sigma(s) = (2\,4)$

Además, ϕ es inyectivo y por tanto será fiel

v) La acción por traslación

$ac : G \times G \longrightarrow G \qquad ac(g, h) = {}^{g}h = gh$

$\phi : G \longrightarrow Perm\, G \qquad \phi(g)(h) = gh$

$Ker\, \phi = 1$ luego es fiel

Es trivialmente fiel pues $gh = h$ sii $g = 1 \Rightarrow$ $\phi(g) = id_G$ sii $g = 1$

Teorema de Cayley

Todo grupo finito es isomorfo a un subgrupo de un grupo de Permutaciones

- Demostración -

1er T° isomorfía

$\Phi/_{Ker\Phi} \cong Im\,\Phi \Rightarrow \Phi \cong Im\,\Phi$ ¿Por qué $Ker\,\Phi = 1$? ¿Qué nos garantiza que Φ es fiel?

Porque podemos usar la acción por traslación que es fiel.

Ejemplo

i) Acción por traslación de $\mathcal{G}$ sobre $P(\mathcal{G})$:

$$ac: \mathcal{G} \times P(\mathcal{G}) \longrightarrow P(\mathcal{G})$$
$$(g, A) \longmapsto ac(g, A) = {}^{g}A = gA = \{ga \mid a \in A\}$$

ii) Acción por traslación de $\mathcal{G}$ sobre $\mathcal{G}/_{H^{\sim}}$

$$ac: \mathcal{G} \times \mathcal{G}/_{H^{\sim}} \longrightarrow \mathcal{G}/_{H^{\sim}}$$
$$(g, xH) \longmapsto {}^{g}xH = gxH$$

iii) Acción por conjugación

$$ac: \mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}$$
$$(g, h) \longmapsto ac(g, h) = ghg^{-1}$$

$${}^{1}h = 1h1^{-1} = h$$

$${}^{(gd)}h = gh\,d(h)^{-1} = g(hdh^{-1})g^{-1}$$

$$\Phi: \mathcal{G} \longrightarrow Perm(\mathcal{G})$$
$$g \longmapsto \Phi(g)(h) = ghg^{-1}$$

, $\Phi(g) = \varphi_g$ es el automorfismo interior definido por g

$Ker\,\Phi = \{g \in \mathcal{G} \mid ghg^{-1} = h\} = \{g \in \mathcal{G} \mid gh = hg\} = Z(\mathcal{G})$

iv) Acción por conjugación de $\mathcal{G}$ sobre $P(\mathcal{G})$

$$ac: \mathcal{G} \times P(\mathcal{G}) \longrightarrow P(\mathcal{G})$$
$$(g, A) \longmapsto ac(g, A) = {}^{g}A = gAg^{-1} = \{gag^{-1} \mid a \in A\} \subset \mathcal{G}$$

v) Acción por conjugación de $\mathcal{G}$ sobre $Subg(\mathcal{G})$

$$ac: \mathcal{G} \times Subg(\mathcal{G}) \longrightarrow Subg(\mathcal{G})$$
$$(g, H) \longrightarrow ac(g, H) = {}^{g}H = gHg^{-1}$$

que es lo que se conoce por subgrupo conjugado.

Definición

Sea $\mathcal{G}$ un grupo, X un $\mathcal{G}$-conjunto, podemos definir la siguiente relación de equivalencia

$$y \sim x \Leftrightarrow \exists g \in \mathcal{G} \quad y = {}^{g}x$$

A la clase de equivalencia de cada $x \in X$ se llama órbita de x, es decir

$$\boxed{Orb(x) = \{y \in X \mid y = {}^{g}x, g \in \mathcal{G}\}}$$

De donde, podemos definir el conjunto cociente $X/_{\sim} = \{Orb(x) : x \in X\}$. Además, se cumplen las siguientes propiedades:

S1

i) $Orb(x) = Orb(y)$ sii $y = x$ → ¿$y \sim x$ mejor?

ii) $Orb(x) \neq Orb(y)$ sii $Orb(x) \cap Orb(y) = \emptyset$

iii) $X = \bigcup_i Orb(x_i)$ unión disjunta. → Me dan una partición

Ejemplos

Sea $X = \{1,2,3,4\}$ y $S_4 \times X \longrightarrow X$, $(\sigma, i) \longmapsto {}^{\sigma}i = \sigma(i)$

i) $H = \langle (123) \rangle$

$Orb(1) = \{ i \in X \mid \sigma \in H, \sigma(i) = 1 \} = \{1,2,3\}$

$Orb(2) = Orb(3) = Orb(1)$

$Orb(4) = \{4\}$

ii) $H = A_4$

$Orb(1) = X = Orb(2) = Orb(3) = Orb(4)$

iii) $H = V$

$Orb(1) = X = Orb(2) = Orb(3) = Orb(4)$

iv) $H = \langle (1234) \rangle$

$Orb(i) = X \quad \forall i \in \{1,2,3,4\}$

Definición

Diremos que una acción sobre un g-conjunto X es transitiva cuando $X/\sim$ es unitario, es decir

$\forall x,y \in X \; \exists g \in G \mid y = {}^{g}x$ → Todos los elementos se relacionan entre sí.

Por otro lado, bajo el mismo contexto, definimos como el estabilizador o grupo de isotropía de $x \in X$ como

$Stab_G(x) = \{ g \in G \mid {}^{g}x = x \} \leq G$ Los elementos de G que dejan fijo a x

Si es $\forall x \in X$ tenemos $Ker\,\phi$

Ejemplo

Sea $X = \{1,2,3,4\}$ y $S_4 \times X \longrightarrow X$, $(\sigma, i) \longmapsto {}^{\sigma}i = \sigma(i)$

i) $H = S_{\{1,2,3,4\}}$

$Stab_H(1) = \{ \sigma \in H \mid \sigma(1) = 1 \} = 1 = Stab_H(2) = Stab_H(3)$

$Stab_H(4) = H$

ii) $H = A_4$

$Stab_H(1) = \{1, (234), (243)\} = \langle (234) \rangle$

$Stab_H(2) = \langle (134) \rangle$

$Stab_H(3) = \langle (124) \rangle$

$Stab_H(4) = \langle (123) \rangle$

(iv) $H = V$

$Stab_H(1) = 1 = Stab_H(2) = Stab_H(3) = Stab_H(4)$

(v) $H = \langle (1234) \rangle$

$Stab_H(1) = 1 = Stab_H(2) = Stab_H(3) = Stab_H(4)$

Proposición

Cierto para grupos no finitos.

Tengo definida una acción

Sea $\mathcal{G}$ un grupo finito que actúa sobre $\mathbb{X}$. Entonces:

$\forall x \in \mathbb{X}$, $Orb(x)$ es un conjunto finito y $|Orb(x)| = [\mathcal{G} : Stab_{\mathcal{G}}(x)]$ (Es ver que $Orb(x) \cong \frac{\mathcal{G}}{Stab_{\mathcal{G}}(x)}$ $\forall x \in \mathbb{X}$)

Esto → En particular, el cardinal de la órbita es un divisor del orden de $\mathcal{G}$.

-Demostración-

Sabemos $Stab_{\mathcal{G}}(x) \leq \mathcal{G}$ y consideramos las clases laterales por la izquierda de $\mathcal{G}/_{Stab_{\mathcal{G}}(x)}\sim$. Podemos construir

$$\phi : \mathcal{G}/_{Stab_{\mathcal{G}}(x)}\sim \longrightarrow Orb(x)$$
$$g\,Stab_{\mathcal{G}}(x) \longmapsto {}^{g}x$$

$y \underset{Stab}{\sim} z$ sii $y \in x\,Stab_{\mathcal{G}}(z)$

ϕ está bien definida

Sean $g \in \mathcal{G}$, $g' \in \mathcal{G}$ tal que $g\,Stab_{\mathcal{G}}(x) = g'\,Stab_{\mathcal{G}}(x) \Rightarrow g = g'h$, $h \in Stab_{\mathcal{G}}(x)$ tenemos que

${}^{g}x = {}^{g'h}x = {}^{g'}({}^{h}x) = {}^{g'}(x)$

$h \in Stab_{\mathcal{G}}(x)$

Entonces:

$$\phi(g\,Stab_{\mathcal{G}}(x)) = \phi(g'\,Stab(x))$$

ϕ es sobreyectiva:

$\forall y \in Orb(x) \Rightarrow y = {}^{g}x$, $g \in \mathcal{G} \Rightarrow y = \phi(g\,Stab_{\mathcal{G}}(x))$ sobreyectiva

Por def de órbita

ϕ inyectiva

Sean $g, g' \in \mathcal{G} \mid \phi(g\,Stab_{\mathcal{G}}(x)) = \phi(g'\,Stab_{\mathcal{G}}(x)) \Rightarrow {}^{g}x = {}^{g'}x \Rightarrow x = {}^{g^{-1}}({}^{g}x) = {}^{g^{-1}}({}^{g'}x) = {}^{g^{-1}g'}x \Rightarrow g^{-1}g' \in Stab_{\mathcal{G}}(x)$

$\Rightarrow g\,Stab_{\mathcal{G}}(x) = g'\,Stab_{\mathcal{G}}(x)$.

Por tanto, se tiene que para $x \in \mathbb{X}$ $Orb(x)$ es finita y $|Orb(x)| = [\mathcal{G} : Stab_H(x)]$ pues ϕ es un isomorfismo.

Ejemplo

Sea $\mathfrak{X}=\{1,2,3,4\}$ y $\begin{array}{l} S_4\times\mathfrak{X}\longrightarrow\mathfrak{X} \\ (\sigma,i)\longmapsto {}^{\sigma}i=\sigma(i)\end{array}$

i) $H=<(123)>$

$$|Orb(4)|=3 \qquad [H:Stab_H(i)]=\frac{|H|}{|Stab_H(i)|} \Rightarrow |Stab_H(i)|=1$$

Repetirlos demás

Proposición

Sea $\mathcal{G}$ un grupo que actúa sobre $\mathfrak{X}$. Entonces, si x, y están en la misma órbita, se tiene que $Stab_{\mathcal{G}}(x)$ y $Stab_{\mathcal{G}}(y)$ son subgrupos conjugados.

↳ $\exists g\in\mathcal{G} \mid g\, Stab_g(x) g^{-1}=Stab_g(y)$

-Demostración- ¡Esta doble inclusión hecha por Dorora no demostrando!

Si $\underline{x,y\in Orb(x)}$, $x\in\mathfrak{X} \Rightarrow Orb(x)=Orb(y)\Rightarrow y\sim x\Rightarrow \exists g\in\mathcal{G}\mid y={}^{g}x \Rightarrow x={}^{g^{-1}}y$. Vamos a ver que

$$Stab_{\mathcal{G}}(y)=g\,Stab_{\mathcal{G}}(x)\,g^{-1}$$

$\forall h\in Stab_{\mathcal{G}}(x)$, ${}^{ghg^{-1}}y={}^{gh}({}^{g^{-1}}y)={}^{gh}x={}^{g}({}^{h}x)={}^{g}x=y \Rightarrow \underline{ghg^{-1}\in Stab_{\mathcal{G}}(y)}\Rightarrow \underline{g\,Stab_{\mathcal{G}}(x)g^{-1}\subset Stab_{\mathcal{G}}(y)}$

$\forall h\in Stab_{\mathcal{G}}(y)$, ${}^{g^{-1}hg}x=x \Rightarrow g^{-1}hg\in Stab_{\mathcal{G}}(x)\Rightarrow g\,Stab_{\mathcal{G}}(y)g^{-1}\subset Stab_{\mathcal{G}}(x)$ □

↳ ${}^{h}y=y \qquad y={}^{g}x \qquad {}^{g^{-1}}({}^{h}({}^{g}x))=x$

Definición

Sea $\mathfrak{X}$ un $\mathcal{G}$-conjunto, un elemento $x\in\mathfrak{X}$ se dice que es fijo por la acción si ${}^{g}x=x \ \forall g\in\mathcal{G}$. Definimos por tanto:

$$\boxed{Fix(\mathfrak{X})=\{x\in\mathfrak{X}\mid {}^{g}x=x,\ \forall g\in\mathcal{G}\}}$$ → Es el "contrario" al núcleo $Ker\,\phi=\{g\in\mathcal{G}\mid {}^{g}x=x\ \forall x\in\mathfrak{X}\}$

Además, $x\in Fix(\mathfrak{X})\Leftrightarrow Orb(\mathfrak{X})=x \Longleftrightarrow Stab_{\mathcal{G}}(x)=\mathcal{G}$.

↳ El grupo completo, es sencillo de demostrar, se basa en usar las defs.

En el caso de que $\underline{\mathfrak{X}\text{ sea finito}}$, $\mathfrak{X}/_{\sim}=\{Orb(x_1),\dots,Orb(x_n)\}$ y por tanto

dará una partición — $|Orb(x\in Fix)|=1$ — Proposición

$$\boxed{|\mathfrak{X}|=\sum_{i=1}^{n}|Orb(x_i)|=|Fix(\mathfrak{X})|+\sum_{x_i\notin Fix(\mathfrak{X})}|Orb(x_i)|=|Fix(\mathfrak{X})|+\sum_{x_i\notin Fix(x_i)}[\mathcal{G}:Stab_{\mathcal{G}}(x_i)] \qquad (1)}$$

Acción por traslación

Hemos considerado la acción por la derecha.

Sabemos que si $\mathcal{G}\neq 1$, $ac:\begin{array}{l}\mathcal{G}\times\mathcal{G}\longrightarrow\mathcal{G}\\ (g,h)\longmapsto gh\end{array}$ entonces:

i) $Orb(h)=\{y\in\mathcal{G}\mid y={}^{g}h\}=\{gh\mid g\in\mathcal{G}\}=\mathcal{G}\ \ \forall h\in\mathcal{G}$

ii) La acción por traslación es transitiva

iii) $Stab_G(h) = \{g \in G \mid {}^g h = h\} = \{g \in G \mid gh = h\} = 1$

iv) $Fix(G) = \{h \in G \mid {}^g h = h \ \forall g \in G\} = \{h \in G \mid gh = h \ \forall g \in G\} = \emptyset$

Acción por conjugación

Sabemos que si $G \neq 1$, $ac: G \times G \longrightarrow G$ entonces:

$$(g,h) \longmapsto ghg^{-1}$$

El conjunto de los conjugados de h lo llamamos así

i) $Orb(h) = \{y \in G \mid {}^g y = ghg^{-1}\}_{g \in G} = \{ghg^{-1} \mid g \in G\} = Cl_G(h)$ (clase de conjugación de h en G)

ii) $Stab_G(h) = \{g \in G \mid {}^g h = h\}_{ghg^{-1}=h} = \{g \in G \mid gh = hg\} = C_G(h)$ (centralizador de h en G)

iii) $|Cl_G(h)| = [G : C_G(h)] \underset{\text{si } G \text{ finito}}{=} \dfrac{|G|}{|C_G(h)|} \Rightarrow |Cl_G(h)|$ divisor de $|G|$

iv) $Fix(G) = \{h \in G \mid {}^g h = h \ \forall g \in G\} = \{h \in G \mid ghg^{-1} = h \ \forall g \in G\} = \{h \in G \mid gh = hg \ \forall g \in G\} = Z(G)$

De (i) deducimos la fórmula de las clases de conjugación de G como:

$$|G| = |Z(G)| + \sum_{\substack{h \notin Z(G) \\ h \in \Gamma}} |Cl_G(h)| = |Z(G)| + \sum_{\substack{h \notin Z(G) \\ h \in \Gamma}} [G : C_G(h)]$$

donde Γ son los representantes de clases de conjugación. En caso de que $H \trianglelefteq G$ podemos obtener la fórmula de clases generalizada

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

Pensar con tranquilidad

Definiendo ahora la acción sobre $Sub_G(G)$ como

grupo de los subgrupos

$$ac: G \times Sub_G(G) \longrightarrow Sub_G(G)$$
$$(g,H) \longmapsto gHg^{-1}$$

de manera que:

i) $Orb(H) = \{{}^g H = gHg^{-1} \mid g \in G\} =$ conjugados de H luego $Orb(H) = \{H\}$ sii $H \trianglelefteq G$

ii) $Stab_G(H) = \{g \in G \mid {}^g H = H\} = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\} = N_G(H)$ conocido como normalizador de H en G. Además, es el mayor subgrupo en G que contiene a H como subgrupo normal.

iii) $Fix(Sub_G(G)) = \{H \leq G \mid {}^g H = H \ \forall g \in G\} = \{H \leq G \mid gHg^{-1} = H \ \forall g \in G\} = \{H \leq G \mid H \trianglelefteq G\}$

En el caso finito:

$$\boxed{|Orb(H)| = [G : N_G(H)] \text{ es un divisor de } |G|}$$

Esto se cumple aunque no sea finito

En tanto, el número de subgrupos conjugados divide al orden de G. Necesitamos finitud.

Ejemplo

Calcular las clases de conjugación de D_4:

$$Cl_{D_4}(1) = \{ s^i r^j 1 (s^i r^j)^{-1} \} = 1$$

$$Cl_{D_4}(r) = \{ s^i r^j r (s^i r^j)^{-1} \} = \{ s^i r^{j+1} r^{-j} s^{-i} \} = \{ s^i r s^{-i} \} = \{ \underset{i=0}{r}, \underset{i=1}{r^3} \}$$

$$Cl_{D_4}(r^2) = \{ r^2 \}$$

$$Cl_{D_4}(s) = \{ s, sr^2 \}$$

$$Cl_{D_4}(sr) = \{ sr, sr^3 \}$$

4.2. P-grupos

Definición

Sea $p \in$ Número primo, un grupo G se dice que es un p-grupo si todo elemento tiene como orden una potencia de p.

Ejemplo

$\mathbb{Z}_8$ pues $O(x) = 2^3 \ \forall x \in \mathbb{Z}_8$

Teorema de Cauchy

Si G es un grupo finito y p es un primo que divide al orden de G entonces, G tiene un elemento de orden p.

Además, tendrá un subgrupo de orden p que será un p-grupo

-Demostración-

Se define $X = \{ (a_1, \dots, a_p) \in G^p \mid a_1 a_2 \dots a_p = 1 \}$. Entonces:

$$\text{si } |G| = n \Rightarrow |X| = n^{p-1} \text{ ¿-1?}$$

$$(\underbrace{a_1 \dots a_{p-1}}_{VR_n^{p-1}}, a_p)$$

Sea ahora $\sigma = (1, 2, \dots, p) \in S_p$ y defino

$$ac: H \times X \longrightarrow X$$

$$(\sigma^i, (a_1, a_2 \dots a_p)) = (a_{\sigma^i(1)}, a_{\sigma^i(2)} \dots a_{\sigma^i(p)})$$

Veamos quién es $|Orb(a_1, \dots a_p)| = [H : Stab_H(a_1, \dots a_p)] \Rightarrow |Orb(a_1, \dots, a_p)|$ divide $|H|$ $\to 1$, p

Supongamos que r es el número de órbitas con 1 elemento y s el número de órbitas con p elementos. Entonces $|X| = r + sp = n^{p-1}$

$Orb(a_1, \ldots, a_p) = \{(a_1, \ldots, a_p), \ldots, (a_p, a_1, \ldots, a_{p-1})\}$

La órbita es unitaria sii $a_1 = a_2 = \ldots = a_p$ $r \geq 1$

Por hipótesis $p \mid n$, pero $r = n^{p-1} - sp$, $p \mid r \Rightarrow r \geq 2$. Por lo tanto $\exists a \in \mathcal{G}, a \neq 1$ $(a, \ldots, a) \Rightarrow a^p = 1$

y por tanto $|a| = p$, es decir, $\langle a \rangle$ es un p-subgrupo de orden p. $\square$

Corolario

Sea $\mathcal{G}$ un grupo finito, entonces:

$\mathcal{G}$ es un p-grupo $\Leftrightarrow |\mathcal{G}| = p^n$ para algún $n \in \mathbb{N}$

-Demostración-

$\Leftarrow$] Si $|\mathcal{G}| = p^n \Rightarrow \forall x \in \mathcal{G}$ $o(x) \mid p^n \Rightarrow o(x) = p^i$ para algún $i \in \mathbb{N}$

$\Rightarrow$] Supongamos que $q \mid |\mathcal{G}|$ primo $\Rightarrow$ por el Teorema de Cauchy $\exists x \in \mathcal{G} \mid o(x) = q$, $q = p^r$ para algún $r \in \mathbb{N} \Rightarrow$

$r = 1$ y $p = q$. Es decir, el único primo que divide al orden de $\mathcal{G}$ es $p \Rightarrow |\mathcal{G}| = p^n$ para algún $n \in \mathbb{N}$. $\square$

Teorema de Burnside

Si $\mathcal{G}$ es un p-grupo finito no trivial entonces $|Z(\mathcal{G})| \geq p$, y en particular, $Z(\mathcal{G}) \neq 1$

-Demostración-

En particular es p^n para $n \in \mathbb{N}$

i) Si $\mathcal{G}$ es abeliano $\Rightarrow Z(\mathcal{G}) = \mathcal{G} \Rightarrow |Z(\mathcal{G})| = |\mathcal{G}| \geq p$ por ser $\mathcal{G}$ un p-grupo

ii) Si $\mathcal{G}$ es no abeliano $\Rightarrow Z(\mathcal{G}) \lneq \mathcal{G}$ y por la fórmula de las clases

$$p^n = |\mathcal{G}| = |Z(\mathcal{G})| + \sum_{\substack{h \notin Z(\mathcal{G}) \\ h \in \Gamma}} [\mathcal{G} : C_{\mathcal{G}}(h)]$$

Como $\mathcal{G}$ es finito $\Rightarrow [\mathcal{G} : C_{\mathcal{G}}(h)] \mid |\mathcal{G}| = p^n$ $\forall h \in \Gamma \Rightarrow [\mathcal{G} : C_{\mathcal{G}}(h)] = p^i$ para algún $i \in \mathbb{N}$, $\forall h \in \Gamma$

Entonces $p \mid [\mathcal{G} : C_{\mathcal{G}}(h)]$ $\forall h \in \Gamma \Rightarrow p \mid |Z(\mathcal{G})| \Rightarrow |Z(\mathcal{G})| \geq p$ $\square$

No entiendo estos últimos razonamientos

Corolario

Induce que sea p-grupo ($\mathcal{G}$ debe ser finito)

Si $|\mathcal{G}| = p^n$, p primo entonces $|Z(\mathcal{G})| \neq p^{n-1}$. En particular, si $|\mathcal{G}| = p^2 \Rightarrow \mathcal{G}$ es abeliano.

-Demostración-

finito y abeliano   el contrario

Si $|\mathcal{G}| = p^n$ y $|Z(\mathcal{G})| = p^{n-1} \Rightarrow |\mathcal{G}/Z(\mathcal{G})| = p \Rightarrow \mathcal{G}/Z(\mathcal{G})$ es cíclico de orden p $\Rightarrow$ es abeliano

entonces $\mathcal{G} = Z(\mathcal{G})$!!   Por ser finito

$|Z(\mathcal{G})| \mid |\mathcal{G}|$

Si $|\mathcal{G}| = p^2$, como $|Z(\mathcal{G})| \neq 1$, como $Z(\mathcal{G}) < \mathcal{G} \Rightarrow |Z(\mathcal{G})| = \begin{cases} 1 \Rightarrow Z(\mathcal{G}) = 1 \text{ !!} \\ p \Rightarrow |Z(\mathcal{G})| = p^{n-1} \text{ !!} \\ p^2 \Rightarrow |Z(\mathcal{G})| = \mathcal{G} \Rightarrow \mathcal{G} \text{ es abeliano} \end{cases}$

por ser subgrupo y $\mathcal{G}$ un p-grupo.

$\square$

Teorema

Sea $\mathcal{G}$ un grupo finito con $|\mathcal{G}|=n$ y sea p un primo. Entonces, para toda potencia p^i que divida a n existe un subgrupo de ese orden $\rightarrow$ Aplicar T^a de Cauchy

-Demostración-

Inducción en i:

Caso base $i=1$ $\rightarrow$ Teorema de Cauchy

1ª HI: Para $j<i$, si $p^j \mid n \Rightarrow \exists H < \mathcal{G} \mid |H| = p^j$

Paso i: Si $|\mathcal{G}| = p^i r$ hacemos inducción sobre r

Caso base $r=1$: $H=\mathcal{G}$

Si $r>1$, 2HI: Cierto para todo grupo de orden divisible por p^i que sea de la forma $p^i m$ con $m<r$. Es decir, $\exists H<\mathcal{G}$ con $|H|=p^i$ y vamos a ver qué ocurre con $\mathcal{G}$.

i) Si existe $K \lneq \mathcal{G}$ de manera que $p \nmid [\mathcal{G}:K]$, como $|\mathcal{G}| = [\mathcal{G}:K]|K| \wedge p^i \mid \mathcal{G}$ por 2HI $\Rightarrow p^i \mid |K| \Rightarrow$ ($|K|<r$)

$\exists H < K < \mathcal{G}$ de manera que $O(H) = p^i$

ii) Si para cualquier $K \lneq \mathcal{G}$ $p \mid [\mathcal{G}:K]$, por la fórmula de las clases

p divide a ambos

$$|Z(\mathcal{G})| = |\mathcal{G}| - \sum_{\substack{h \notin Z(\mathcal{G}) \\ h \in T}} [\mathcal{G} : C_{\mathcal{G}}(h)] \Rightarrow p \mid Z(\mathcal{G})$$

y por el T^a de Cauchy $\exists K < Z(\mathcal{G})$, $|K|=p$.

Como $K < Z(\mathcal{G}) \Rightarrow K \trianglelefteq \mathcal{G}$ y puedo tomar cocientes

$$|\mathcal{G}/K| = \frac{|\mathcal{G}|}{p} \Rightarrow p^{i-1} \mid |\mathcal{G}/K| = |\mathcal{G}|$$

y por la 1HI $\exists L < \mathcal{G}/K \mid |L| = p^{i-1}$. Ahora, por el 3TI $L = H/K$ $K \trianglelefteq H < \mathcal{G} \Rightarrow |H| = |\frac{H}{K}| \cdot |K| = p^i$ $\square$

4.3 Grupos de Sylow (1872)

Definición

Si $\mathcal{G}$ es un grupo finito y p un primo que divide al orden de $\mathcal{G}$, un p-subgrupo de Sylow de $\mathcal{G}$ es un p-subgrupo de $\mathcal{G}$ cuyo orden es la máxima potencia de p que divide al orden de $\mathcal{G}$, es decir, si $|\mathcal{G}| = p^k m$ $\wedge$ $mcd(p,m)=1$, un p-subgrupo de $\mathcal{G}$ es de Sylow si $|H| = p^k$

Ejemplo

$|\mathcal{G}|=24=2^3 3$

- P: 2-subgrupo de Sylow, $|P|=8$
- Q: 3-subgrupo de Sylow, $|Q|=3$

Corolario (Primer Teorema de Sylow)

Para todo grupo finito $\mathcal{G}$ y todo divisor primo p de su orden, existe al menos un p-subgrupo de Sylow.

Observación

Si $|\mathcal{G}|=p^n m$, $mcd(p,m)=1$, P es un p-subgrupo de Sylow de $\mathcal{G}$, $H<\mathcal{G}$, $P<H$. Entonces $[H:P] \mid [\mathcal{G}:P]=m$; por tanto, $p \nmid [H:P]$, como $[\mathcal{G}:H] \mid [\mathcal{G}:P] \Rightarrow p \nmid [\mathcal{G}:H]$

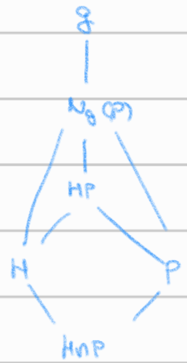
Lema

Si P es un p-subgrupo de Sylow de un grupo finito $\mathcal{G}$ y H es un p-subgrupo de $N_{\mathcal{G}}(P)$, entonces H está contenido en P.

$N_{\mathcal{G}}(P) = Stab_{\mathcal{G}}(P) = \{g\in\mathcal{G} \mid gPg^{-1}=P\}$

-Demostración-

Como $P \trianglelefteq N_{\mathcal{G}}(P)$ y $H<N_{\mathcal{G}}(P)$ entonces $HP<N_{\mathcal{G}}(H)$ y $P\cap H \trianglelefteq H$



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

Supongamos $1 \neq r := [HP:P] = [H:H\cap P] \Rightarrow p \nmid r$. Por otra parte, $r=[H:H\cap P]$ y H es un p-grupo $\Rightarrow p^i \mid r$ para algún $i\in\mathbb{N}$. !!

Entonces $r=1 \Rightarrow HP=P \Rightarrow H<P$

Segundo Teorema de Sylow

Sea $\mathcal{G}$ un grupo finito, p primo, $|\mathcal{G}|=p^k m$, $mcd(p,m)=1$ y n_p el nº de p-subgrupos de Sylow de $\mathcal{G}$.

i) Todo p-subgrupo de $\mathcal{G}$ será subgrupo de un p-subgrupo de Sylow de $\mathcal{G}$.

ii) Cualesquiera dos p-subgrupos de Sylow son conjugados

iii) $n_p \mid m$ y $n_p \equiv 1 \mod (p)$

-Demostración-

Si $S = Sub_p(\mathcal{G}) = \{P \mid P$ p-subg Sylow $\}$, $|S| = n_p$ y puedo considerar la acción por conjugación

$$\mathcal{G} \times S \longrightarrow S$$
$$(g, P) \longmapsto {}^gP = gPg^{-1} \in S$$

bien definida.

Sea $P_1 \in S$, entonces:

$\Rightarrow Orb(P_1) = \{gP^{-1}g \mid g \in \mathcal{G}\}$

$\Rightarrow Stab_{\mathcal{G}}(P_1) = \{g \in \mathcal{G} \mid gP_1g^{-1} = P_1\} (= N_{\mathcal{G}}(P_1))$

$\Rightarrow |Orb(P_1)| = [\mathcal{G} : N_{\mathcal{G}}(P_1)]$

$P_1 < N_{\mathcal{G}}(P_1) < \mathcal{G}$

$[\mathcal{G} : P_1] = \underbrace{[\mathcal{G} : N_{\mathcal{G}}(P_1)]}_{= |Orb(P_1)|} [N_{\mathcal{G}}(P_1) : P_1] \Rightarrow |Orb(P_1)| \mid [\mathcal{G} : P_1] = m$

luego $mcd(|Orb(P_1)|, p) = 1$

i) Sea H un p-subgrupo de $\mathcal{G}$, consideramos ahora la siguiente acción:

$$H \times Orb(P_1) \longrightarrow Orb(P_1)$$
$$(h, P) \longmapsto {}^hP = hPh^{-1} \in Orb(P_1)$$

$- Stab_H(P) = \{h \in H \mid hPh^{-1} = P\} = H \cap N_{\mathcal{G}}(P) < H$ $\left\{ \Rightarrow H \cap N_{\mathcal{G}}(P) < H \cap P < H \cap N_{\mathcal{G}}(P) \right.$

$H \cap N_{\mathcal{G}}(P) < P$ ↳ Lema último

De donde $N_{\mathcal{G}}(P) = H \cap P$ pues $N_{\mathcal{G}}(P) \not\subset P$ pues contendría más cosas.

$$|Orb(P_1)| = \sum_P [H : Stab_H(P)] = \sum_P [H : H \cap P] \Rightarrow$$ cada sumando divide a $|H| \Rightarrow$ es una potencia de p.

Pero $p \nmid |Orb(P_1)| \Rightarrow \exists P \in Orb(P_1) \mid [H : H \cap P] = 1 \Rightarrow H \cap P = H \Rightarrow H < P$. Además, P es conjugado de P_1

ii) Sean P_1, P_2 dos p-subgrupos de Sylow, tomando $H = P_2 \overset{\text{ap. anterior}}{\Rightarrow} \exists P$ p-subgrupo de Sylow de $\mathcal{G}$, conjugado de P_1 tal que $P_2 < P$, pero $|P_2| = |P| \Rightarrow P_2 = P$

iii) $Orb(P_1) = S \Rightarrow n_p = |S| = |Orb(P_1)| = [\mathcal{G} : N_{\mathcal{G}}(P_1)] \Rightarrow n_p \mid m$

Si $H = P_1$ (ap 1) $n_p = |Orb(P_1)| = \sum_P [P_1 : P_1 \cap P] \Rightarrow [P_1 : P_1 \cap P] \Rightarrow [P_1 : P_1 \cap P] = 1$ y

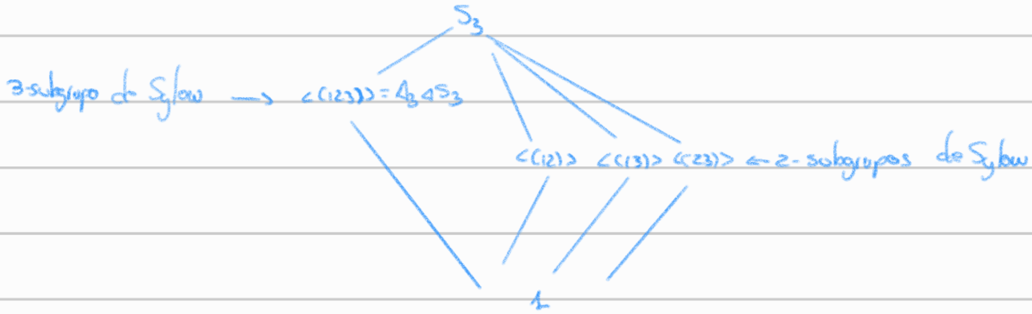
los demás son múltiplos de p $\Rightarrow n_p \equiv 1$ mod p

Ejemplos

i) $C_n = \langle x \mid x^n = 1\rangle$. Si $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, para cada $i = 1 \ldots k$ $\exists P_i$ p-subgrupo de Sylow de C_n que será cíclico de orden $p_i^{t_i}$, los p_i-subgrupos son $C_{p_i^{t_i}}$

ii) S_3, $|S_3| = 2\cdot 3$

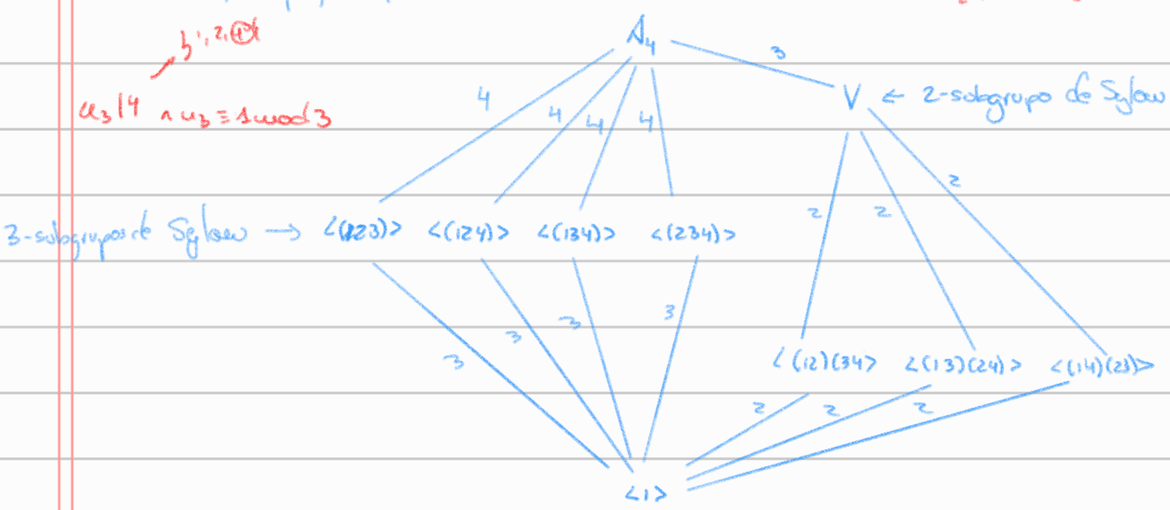
2-subgrupos de Sylow de $S_3 \xrightarrow{2TS} n_2 \mid 3 \wedge n_2 \equiv 1 \mod 2 \Rightarrow n_2 \in \{1,3\}$



iii) A_4, $|A_4| = 12 = 2^2 \cdot 3$

$n_2 \mid 3 \wedge n_2 \equiv 1 \mod 2$ $n_2 \in \{1,3\}$

$n_3 \mid 4 \wedge n_3 \equiv 1 \mod 3$ $\rightarrow \{1,2,4\}$



iv) S_4: $|S_4| = 24 = 2^3 \cdot 3$

$$\left.\begin{array}{l} n_2 \mid 3 \\ n_2 \equiv 1 \mod 2 \end{array}\right\} \Rightarrow n_2 = 1, n_2 = 3$$

$n_2 \mid 3$ $n_2 \equiv 1 \mod 2$

$n_2 \in \{1,3\}$

$|Q| = 8$ 2-subgrupo de Sylow.

Si $n_2 = 1 \Rightarrow$ todas las trasposiciones están en $Q \Rightarrow$ como todas las trasposiciones generan S_4

∃ un elemento de orden 2.

$\Rightarrow Q = S_4$!!

$\underline{n_2 = 3}$ $\quad$ $\underline{V \text{ es un 2-subgrupo}}$

- Si $V < Q_1$

$$\left.\begin{array}{l} Q_2 = \alpha Q_1 \alpha^{-1} \supseteq V \\ Q_3 = \beta Q_1 \beta^{-1} \supseteq V \end{array}\right\} \Rightarrow V < Q_i \ \forall i \Rightarrow Q_i = V = \langle (j\,k) \rangle$$

$n_3 \mid 8 \rightarrow \{1,2,4,8\}$

$$\left.\begin{array}{l} n_3 \mid 8 \\ n_3 \equiv 1 \mod 3 \end{array}\right\} \Rightarrow n_3 = 1 \text{ ó } n_3 = 4 \rightarrow \langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle$$

Corolario

Sea P un p-subgrupo de Sylow de un grupo finito de G.

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

- Demostración -

Los p-subgrupos de Sylow son todos conjugados

$\Rightarrow$) Si P es único p-subgrupo de Sylow $\Rightarrow \forall g \in G \; gPg^{-1}$ es un p-subgrupo de Sylow $\Rightarrow gPg^{-1} = P \; \forall g \in G \Rightarrow P \trianglelefteq G$.

$\Leftarrow$) Sea Q un p-subgrupo de Sylow, $\exists g \in G \mid gPg^{-1} = Q$, como $P \trianglelefteq G$ $P = Q$.

↳ suponer que hay otro y ver que es el único.

Ejemplo

Si $|G| = 35$ entonces es resoluble.

$|G| = 7 \cdot 5 \Rightarrow$ habrá 5-subgrupos de Sylow y 7-subgrupos de Sylow

De donde sale H?

$$\left.\begin{array}{l} n_7 \mid 5 \\ n_7 \equiv 1 \bmod 7 \end{array}\right\} \Rightarrow n_7 = 1 \Rightarrow \exists! P < G \text{ 7-subgrupo de Sylow}, P \trianglelefteq G \Rightarrow H \sim \mathbb{Z}_7 \text{ resoluble por ser abeliano}$$

$$|G/P| = \frac{|G|}{|P|} = 5 \Rightarrow G/P \simeq \mathbb{Z}_5, \text{ resoluble}$$

Entonces G es resoluble.

Teorema

Sea G un grupo finito, en el que todos sus subgrupos de Sylow son normales. Entonces, G es el producto directo interno de sus subgrupos de Sylow.

- Demostración -

Razonamiento por órdenes

Por ser únicos

Pero si suponemos que no con el orden de los elementos.

Por ser finito podemos dividir en prod. cíclicos.

$G = H \times K$ sii $H, K \trianglelefteq G$, $HK = G$ $\wedge$ $H \cap K = 1$ $\rightarrow$ Caracterización

Supongamos que $|G| = p_1^{n_1} \cdots p_k^{n_k}$ y llamamos P_i al único p_i-subgrupo de Sylow $\Rightarrow P_i \trianglelefteq G \; \forall i$, $|P_1 \ldots P_k| = |G|$

por lo tanto $P_1 \times \ldots \times P_k = G$.

$(P_1 \ldots P_{i-1}) \cap P_i = 1 \quad \forall i = 2 \ldots k$

$$\text{Sea } x \in (P_1 \ldots P_{i-1}) \cap P_i \Rightarrow \left.\begin{array}{l} O(x) \mid |P_1 \cdots P_{i-1}| = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} \\ O(x) \mid |P_i| = p_i^{n_i} \end{array}\right\} \Rightarrow O(x) = 1 \Rightarrow x = 1$$

Ejemplo

$|G| = 35$ ¿Por? De donde sale ese isomorfismo

$\mathbb{Z}_7 \simeq H$ 7-subgrupo de Sylow

$$Q: \left.\begin{array}{l} n_5 \mid 7 \\ n_5 \equiv 1 \bmod 5 \end{array}\right\} \Rightarrow n_5 = 1$$