

Homomorfismos.

Def. Sean G y T grupos, y $f: G \rightarrow T$ una función. Decimos que f es homomorfismo, si

$$f(ab) = f(a)f(b), \forall a, b \in G.$$

Además, si

i) f es inyectiva, se dice que f es monomorfismo, o que f es un encaje de G en T .

ii) f es suprayectiva, se dice que f es epimorfismo.

iii) f es biyectiva, se dice que es isomorfismo.

También el homomorfismo $f: G \rightarrow T$ se dice que es

iv) endomorfismo si $G = T$.

v) automorfismo si $G = T$, y f es isomorfismo.

Denotamos por:

$$\text{Hom}(G) := \{f: G \rightarrow T \mid f \text{ es homomorfismo}\}$$

$$\text{End}(G) := \{f: G \rightarrow G \mid f \text{ es endomorfismo}\}$$

$$\text{Aut}(G) := \{f: G \rightarrow G \mid f \text{ es automorfismo}\}$$

Usamos los siguientes diagramas para los diversos tipos de funciones:

1) Homomorfismos.

$$G \xrightarrow{f} T$$

2) Monomorfismos.

$$G \hookrightarrow T$$

3) Epimorfismos.

$$G \xrightarrow{f} T$$

4) Isomorfismos.

$$G \xrightarrow{\sim} T$$

Si el diagrama cumple que:

$$\begin{array}{ccc} G & \xrightarrow{f} & T \\ & \searrow g & \downarrow h \\ & Z & \end{array} \quad \text{Con } g = f \circ h$$

Entonces es comunitativo.

Def. Un grupo G se dice que **está encajado en** o **inmerso en** un grupo T , si existe un monomorfismo f de G en T .

Def. Se dice que los grupos G y T son **isomorfos** si existe un isomorfismo f de G en T , a lo que se escribe $G \cong T$, $G \stackrel{f}{\cong} T$.

Proposición.

Sean G y T grupos, y $f: G \rightarrow T$. Entonces:

- i) $f(e_G) = e_T$.
- ii) $f(a^{-1}) = f(a)^{-1}$, $\forall a \in G$.
- iii) Si $H < G$, entonces $f(H) < T$.
- iv) Si $K < T$, entonces $f^{-1}(K) < G$ tal que $\text{Ker } f \subseteq f^{-1}(K)$.

Dem:

De (i):

Veamos que:

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \Rightarrow f(e_G) = e_T$$

De (ii):

Sea $a \in G$, entonces

$$e_T = f(e_G) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}) \Rightarrow f(a^{-1}) = f(a)^{-1}$$

De (iii):

Sean $a, b \in H$, entonces:

$$f(a) \cdot f(b)^{-1} = f(a b^{-1}) \in f(H), \text{ pues } H < G \Rightarrow a b^{-1} \in H. \text{ Luego } f(H) < T.$$

De (iv):

Probaremos que $\text{Ker } f < G$. Sean $a, b \in \text{Ker } f$, entonces:

$$f(ab^{-1}) = f(a) \cdot f(b)^{-1} = e_i \cdot e_i^{-1} = e_i \Rightarrow ab^{-1} \in \text{Ker } f$$

por tanto, $\text{Ker } f \subset G$. Sean ahora $g \in G$ y $n \in \text{Ker } f$, entonces:

$$f(gng^{-1}) = f(g) \cdot f(n) \cdot f(g^{-1}) = f(g) \cdot e_i \cdot f(g)^{-1} = e_i \Rightarrow gng^{-1} \in \text{Ker } f$$

entonces, $\text{Ker } f \trianglelefteq G$.

De (ii):

Como $K < T$, entonces $e_i \in K$, así $e_a \in f^{-1}(K)$, pues $f(e_a) = e_i \in K$, luego $f^{-1}(K) \neq \emptyset$. Sean $a, b \in f^{-1}(K)$, entonces:

$$f(ab^{-1}) = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b)^{-1} \in K$$

pues $f(a) \in K$ y $f^{-1}(b) \in K$, por ser $K < T$. Entonces $f^{-1}(K) \subset G$. Ahora, como

$$\text{Ker } f = f^{-1}(\{e_i\})$$

y $\{e_i\} \subseteq K$, entonces $\text{Ker } f \subseteq f^{-1}(K)$.

Proposición.

Sean $f: G \rightarrow T$ y $g: T \rightarrow U$ dos homomorfismos. Entonces:

- i) $g \circ f$ es homomorfismo
- ii) Si f y g son monomorfismos (epimorfismos e isomorfismos), $g \circ f$ también lo es.
- iii) Si f es monomorfismo, su inversa $f^{-1}: f(G) \rightarrow G$ es homomorfismo.

Dem:

De (i): Sean $a, b \in G$, entonces

$$\begin{aligned} g \circ f(ab) &= g(f(ab)) \\ &= g(f(a)f(b)) \\ &= g(f(a)) \cdot g(f(b)) \\ &= g \circ f(a) \cdot g \circ f(b). \end{aligned}$$

De (ii): es inmediato.

De (iii): Sean $x, y \in f(G)$, entonces $\exists a, b \in G$ m $x = f(a)$ y $y = f(b)$, asi:

$$\begin{aligned}f^{-1}(xy) &= f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab \\&= f^{-1}(f(a)) \cdot f^{-1}(f(b)) = f^{-1}(x) \cdot f^{-1}(y)\end{aligned}$$

q.e.d.

Proposición:

Sea $f: G \rightarrow T$ un homomorfismo. Entonces f es monomorfismo si y sólo si $\text{Ker } f = \{e_G\}$.

Dem:

\Rightarrow) Supongu que f es monomorfismo. Por una proposición anterior, $\{e_G\} \subseteq \text{Ker } f$. Sea ahora $a \in \text{Ker } f$, entonces $f(a) = e_T = f(e_G)$, por ser f monomorfismo, $f(a) = f(e_G) \Rightarrow a = e_G \Rightarrow a \in \{e_G\}$. Por tanto, $\text{Ker } f = \{e_G\}$.

\Leftarrow) Suponga que $\text{Ker } f = \{e_G\}$. Sean $a, b \in G$ m $f(a) = f(b)$, entonces:

$$\begin{aligned}f(ab^{-1}) &= f(a) \cdot f(b)^{-1} = f(a) \cdot f(a)^{-1} = e_T \Rightarrow ab^{-1} \in \text{Ker } f = \{e_G\} \\&\Rightarrow ab^{-1} = e_G \Rightarrow a = b.\end{aligned}$$

Por tanto, f es monomorfismo.

q.e.d.

Proposición.

Sea $f: G \rightarrow T$ un homomorfismo. Entonces f es isomorfismo si y sólo si existe un homomorfismo $g: T \rightarrow G$ tal que $f \circ g = id_T$ y $g \circ f = id_G$.

Dem:

\Rightarrow) Supongu que f es isomorfismo, entonces $\exists f': T = f(G) \rightarrow G$ es homomorfismo tal que

$$f' \circ f = id_T$$

$$f' \circ f = id_G$$

Por tanto, la g buscada es f^{-1} .

\Leftarrow) Supongamos que existe una función $g: \bar{T} \rightarrow G$ homomorfismo tal que $f \circ g = id_{\bar{T}}$ y $g \circ f = id_G$. Probaremos que f es monomorfismo y epimorfismo.

i) Se un $a, b \in G$ $\cap f(a) = f(b)$, entonces $a = g \circ f(a) = g \circ f(b) = b$. Por tanto, f es monomorfismo.

ii) Sea $x \in T$, existe $a = g(x)$ tal que $f(a) = f(g(x)) = f \circ g(x) = x$. Por tanto, f es epimorfismo.

Por i) y ii), f es isomorfismo.

q.e.d.

EJEMPLOS:

Teorema (de Correspondencia)

Sea G un grupo y $N \triangleleft G$. Denotamos por $\mathcal{H} = \{H \triangleleft G \mid N \subseteq H\}$, y $\bar{\mathcal{H}} = \{\bar{H} \mid \bar{H} < G/N\}$. Entonces existe una biyección $\bar{\Phi} : \mathcal{H} \rightarrow \bar{\mathcal{H}}$ dada como sigue:

$$\forall H \in \mathcal{H}, \bar{\Phi}(H) = \varphi(H)$$

donde $\varphi : G \rightarrow G/N$ es el epimorfismo canónico. La inversa de $\bar{\Phi}$ es $\psi : \bar{\mathcal{H}} \rightarrow \mathcal{H}$ es: $\forall \bar{H} \in \bar{\mathcal{H}}, \psi(\bar{H}) = \varphi^{-1}(\bar{H})$.

Dem:

Probaremos que $\bar{\Phi}$ y ψ están bien definidas. Para $\bar{\Phi}$:

a) Sea $H \in \mathcal{H}$, probaremos que $\bar{\Phi}(H) \in \bar{\mathcal{H}}$. En efecto, como $H \triangleleft G$, $e \in H \Rightarrow N = \varphi(e) \in \varphi(H) = \bar{\Phi}(H)$, así: $\bar{\Phi}(H) \neq \emptyset$. Sean $N_a, N_b \in \bar{\Phi}(H)$, entonces como φ es suprayectiva, $\exists a, b \in H$ m $\varphi(a) = N_a$ y $\varphi(b) = N_b$, como $a, b \in H$ y $H \triangleleft G$, entonces $a, b^{-1} \in H$, luego:

$$\begin{aligned} \varphi(a, b^{-1}) &= N_a, b^{-1} = N_a \cdot (N_b, 1^{-1}) \\ &= N_a(N_b)^{-1} \in \bar{\Phi}(H) \end{aligned}$$

por tanto, $\bar{\Phi}(H) < G/N$, así: $\bar{\Phi}(H) \in \bar{\mathcal{H}}$.

b) Claramente, si $H, K \triangleleft G$ m $N \subseteq H, K$, entonces $\bar{\Phi}(H) = \varphi(H)$ y $\bar{\Phi}(K) = \varphi(K)$, y $\bar{\Phi}(H) = \bar{\Phi}(K)$, pues $\varphi(H) = \varphi(K)$.

Para ψ :

c) Sea $\bar{H} \in \bar{\mathcal{H}}$. Probaremos que $\psi(\bar{H}) = \varphi^{-1}(\bar{H}) \in \mathcal{H}$. Como $\bar{H} < G/N$, entonces $N \in \bar{H}$, así: $e \in \varphi^{-1}(\{N\}) \subseteq \varphi^{-1}(\bar{H})$. Por tanto, $\varphi^{-1}(\bar{H}) \neq \emptyset$. Sean ahora $a, b \in \varphi^{-1}(\bar{H})$, entonces $N_a, N_b \in \bar{H} \Rightarrow N_a b^{-1} \in \bar{H}$, así: $a b^{-1} \in \varphi^{-1}(\bar{H})$. Por tanto, $\psi(\bar{H}) \triangleleft G$.

Probaremos que $N \subseteq \psi(\bar{H})$. En efecto, sea $a \in N$, entonces $\varphi(a) = N$, por tanto $a \in \varphi^{-1}(\{N\}) \subseteq \psi(\bar{H})$. Así: $N \subseteq \psi(\bar{H})$.

d) Claramente, si $\bar{H}, \bar{K} < G/N$, entonces $\psi(\bar{H}) = \psi(\bar{K})$.

Por a), b), c) y d), $\bar{\Phi}$ y $\bar{\Psi}$ están bien definidos. Ahora, para probar que $\bar{\Phi}$ es biyección, probaremos que $\bar{\Phi} \circ \bar{\Psi} = id_{\bar{H}}$ y $\bar{\Psi} \circ \bar{\Phi} = id_H$. Es decir:

$$i) \forall H \in \mathcal{H}, H = \bar{\Psi} \circ \bar{\Phi}(H) = \varphi^{-1}(\varphi(H))$$

$$ii) \forall \bar{H} \in \bar{\mathcal{H}}, \bar{H} = \bar{\Phi} \circ \bar{\Psi}(\bar{H}) = \varphi(\varphi^{-1}(\bar{H}))$$

Probaremos primero (i). Sea $H \in \mathcal{H}$, entonces $H < G$ y $N \leq H$.

- Sea $a \in H$, entonces $\varphi(a) \in \varphi(H)$, por tanto $a \in \varphi^{-1}(\varphi(H))$.

- Sea $a \in \varphi^{-1}(\varphi(H))$, entonces $\varphi(a) \in \varphi(H)$, entonces $\exists h \in H$ tal que $\varphi(a) = \varphi(h)$, por tanto $\varphi(a^{-1}) = \varphi(a) \cdot \varphi(h)^{-1} = N$, luego $a^{-1} \in \text{Ker } \varphi = N \leq H$, por tanto, $a = ah^{-1} \in H$.

Por tanto, $H = \varphi^{-1}(\varphi(H))$. Para (ii) es similar. Por (i) y (ii), $\bar{\Phi}$ es biyección, y $\bar{\Psi} = \bar{\Phi}^{-1}$.

Q.E.D.

Obs: Sea $\varphi: G \rightarrow G/N$ el epimorfismo canónico. Sea $H < G$ tal que $N \leq H$. Por una proposición anterior, $N < H$, luego podemos formar el grupo cociente $H/N = \{Nh \mid h \in H\}$, y entonces:

$$\varphi(H) = \{Nh \mid h \in H\} = H/N$$

Corolario.

Sea G grupo y $N \trianglelefteq G$. Entonces $\bar{H} < G/N \Leftrightarrow [H] < G$ tal que $N \leq H$ y $\bar{\Phi}(H) = \bar{H}$.

Además $\bar{H} \triangleleft G/N \Leftrightarrow H \triangleleft G$.

Dem:

4) Sea G un grupo cíclico generado por a , es decir:

$$G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

definimos $f: \mathbb{Z} \rightarrow G$ dada por: $f(m) = a^m, \forall m \in \mathbb{Z}$. f es suprayectiva, veamos que es epimorfismo. Para ello:

Sean $m, k \in \mathbb{Z}$, tomando a \mathbb{Z} como grupo aditivo:

$$f(m+k) = a^{m+k} = a^m \cdot a^k = f(m) \cdot f(k)$$

por lo tanto, f es homomorfismo, luego como es suprayectiva, es epimorfismo.

Así, por el PTI, f induce una función $\bar{f}: \mathbb{Z}/\text{Ker}(f) \rightarrow G$ dada por

$$\forall m \in \mathbb{Z}, \bar{f}(m + \text{Ker}(f)) = f(m) = a^m$$

donde \bar{f} es un isomorfismo. Como $\text{Ker}(f) \subset \mathbb{Z}$, entonces al ser G cíclico, existe $n \in \mathbb{N} \cap \text{Ker}(f) = n\mathbb{Z}$. Por lo tanto:

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G$$

$$m + n\mathbb{Z} \rightarrow a^m$$

Si $n=0 \Rightarrow n\mathbb{Z} = \langle 0 \rangle$. Luego

$$\mathbb{Z} \cong \mathbb{Z}/\langle 0 \rangle = \mathbb{Z}/n\mathbb{Z} \cong G$$

por lo tanto, G debe ser infinito, y $|a| = +\infty$.

Si $n \geq 1$, entonces $\mathbb{Z}/n\mathbb{Z} \cong G$. Como $|\mathbb{Z}/n\mathbb{Z}| = n$, entonces G es finito, y $|a| = n$.

Obs: La relación de "ser isomorfo" en la clase de todos los grupos es una relación de equivalencia.

Esto quiere decir que \cong induce una partición en la clase de todos los grupos.

5) Sea G grupo. Sabemos que S_G es grupo. Consideraremos los automorfismos de

G , $\text{Aut}(G)$.

Se tiene que $\text{Aut}(G) \subset S_G$. Sean $g \in G$ y definimos $i_g: G \rightarrow G$ dada como sigue:

$$\forall x \in G, i_g(x) = gxg^{-1}$$

Tenemos que $i_g \in \text{Aut}(G)$, $\forall g \in G$. En efecto: sea $g \in G$ fijo.

a) Sean $x, y \in G$. Entonces

$$i_g(xy) = gx y g^{-1} = gx g^{-1} g y g^{-1} = i_g(x) \cdot i_g(y)$$

b) Sean $x, y \in G$ s.t. $i_g(x) = i_g(y)$, entonces:

$$gxg^{-1} = gyg^{-1} \Rightarrow xg^{-1} = yg^{-1} \Rightarrow x = y$$

Otra forma de probar lo anterior, es probando que $\text{Ker}(i_g) = \{e\}$.

c) Sea $y \in G$. Entonces $\exists x = g^{-1}yg \in G$, entonces

$$\begin{aligned} i_y(x) &= gxg^{-1} \\ &= g(g^{-1}yg)g^{-1} = y \end{aligned}$$

Por a), i_g es homomorfismo, por b) es monomorfismo y c), es isomorfismo. Como $i_g: G \rightarrow G$, entonces $i_g \in \text{Aut}(G)$.

El automorfismo i_g es llamado el **automorfismo interior de G por g** . Denotemos $\text{Int}(G) = \{i_g: G \rightarrow G \mid g \in G\} \subseteq \text{Aut}(G)$. Más aún,

$$\text{Int}(G) \triangleleft \text{Aut}(G)$$

d) Sean $g, h \in G$. Para cada $x \in G$,

$$\begin{aligned} (i_g \circ i_h)(x) &= i_g(i_h(x)) \\ &= i_g(hxh^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= (gh) x (gh)^{-1} \end{aligned}$$

Luego, $\exists gg \in G$ tal que $i_g \circ i_g = i_{gg}$. Por tanto, $i_g \circ i_g \in \text{Int}(G)$.

e) Sea $g \in G$. Entonces $i_g^{-1} = i_{g^{-1}}$, en efecto, sea $x \in G$. Veamos que:

$$\begin{aligned}(i_g \circ i_{g^{-1}})(x) &= i_g(i_{g^{-1}}(x)) \\ &= (gg^{-1})x(gg^{-1}) \\ &= x = id_G(x)\end{aligned}$$

Así, $i_{g^{-1}} = i_g^{-1}$. Luego $i_g^{-1} = i_g \in \text{Int}(G)$.

Por d) y e), $\text{Int}(G) \subset \text{Aut}(G)$.

f) Sea $f \in \text{Aut}(G)$ y $g \in G$. Entonces $f \circ i_g \circ f^{-1} \in \text{Int}(G)$, en efecto:

Si $x \in G$:

$$\begin{aligned}(f \circ i_g \circ f^{-1})(x) &= f(i_g(f^{-1}(x))) \\ &= f(gf^{-1}(x)g^{-1}) \\ &= f(g) \cdot f(f^{-1}(x)) \cdot f(g^{-1}) \\ &= f(g) \cdot x \cdot (f(g))^{-1}\end{aligned}$$

Como $f(g) \in G$, entonces $f \circ i_g \circ f^{-1} = i_{f(g)} \in \text{Int}(G)$.

Por f), $\text{Int}(G) \subset \text{Aut}(G)$.

$\text{Int}(G)$ es llamado el grupo de los automorfismos interiores de G .

Teorema:

$$G/Z \cong \text{Int}(G)$$

Donde Z es el centro de G .

Dem:

Sea $\Psi: G \rightarrow \text{Int}(G)$ dada por: $\forall g \in G$

$$\Psi(g) := i_g$$

Probaremos que Ψ es endomorfismo.

i) ψ es homomorfismo.

Sean $g, g_1 \in G$, entonces:

$$\psi(gg_1) = i_{gg_1} = i_g \circ i_{g_1} = \psi(g) \circ \psi(g_1)$$

ii) Es claro que ψ es suprayectiva.

Por (i) y (ii), ψ es endomorfismo.

iii) $\text{Ker}(\psi) = Z$.

Sea $g \in G$.

$$\begin{aligned} g \in \text{Ker}(\psi) &\Leftrightarrow \psi(g) = \text{id}_G \Leftrightarrow \forall x \in G, \psi(g)(x) = \text{id}_G(x) = x \\ &\Leftrightarrow \forall x \in G, gxg^{-1} = x \Leftrightarrow \forall x \in G, gx = xg \\ &\Leftrightarrow g \in Z = Z(G) \end{aligned}$$

Como se cumple que ψ es endomorfismo y (iii), entonces por el PII, ψ induce un único isomorfismo $\bar{\psi}: G/Z \rightarrow \text{Int}(G)$ tal que

$$\bar{\psi} \circ \varphi = \psi$$

donde $\varphi: G \rightarrow G/Z$ es el epimorfismo canónico. Así pues:

$$G/Z \xrightarrow{\bar{\psi}} Z$$

$$gZ \mapsto \psi(g) = i_g$$

q.e.d.

Notemos que, como $\text{Int}(G)$ es grupo se tiene que $\text{id}_G \in \text{Int}(G)$, y $\text{id}_G = \text{id}_e$.

En G definimos la relación $\sim: \forall x, y \in G$,

$$\begin{aligned} x \sim y &\Leftrightarrow \exists g \in G \text{ m } y = gxg^{-1} \\ &\Leftrightarrow \exists g \in G \text{ m } i_g(x) = y. \end{aligned}$$

Se tiene que \sim es una relación de equivalencia en G . (probar).

Si $x \in G$ y $C(x)$ o C_x es la clase de equivalencia de G con representante x , ba-

jo la relación de equivalencia \sim , entonces $C(x)$ es llamada la clase de conjugación, y todo elemento de $C(x)$ se dice ser un conjugado de x . La relación \sim es llamada la relación de conjugación en G .

Def. Sea G grupo y \bar{X} un conjunto no vacío. Una representación permutacional de G por \bar{X} , es cualquier homomorfismo $\varphi: G \rightarrow S_{\bar{X}}$. Cuando esto ocurre, decimos que G actúa sobre \bar{X} a través de φ .

Por lo general, a φ de la definición anterior, se le conoce como una acción de G sobre \bar{X} .

En la prop. anterior vimos una representación permutacional, pues:

$$\text{Int}(G) \triangleleft \text{Aut}(G) < S_G$$

es decir, $\varphi: G \rightarrow S_G$. Por tanto, en ese ejemplo, G actúa sobre G .

Supóngase que G es grupo actuando en un conjunto $\bar{X} \neq \emptyset$ bajo la acción $\varphi: G \rightarrow S_{\bar{X}}$, donde $\varphi(g): \bar{X} \rightarrow \bar{X}$ es una biyección, la cual:

$$\forall x \in \bar{X}, \varphi(g)(x) \in \bar{X}$$

Para no hacer engorrosa la notación, denotamos por $\varphi_g: \varphi(g), \forall g \in G$; así que

$$\begin{aligned} \varphi_g: \bar{X} &\rightarrow \bar{X} \text{ es biyección} \\ x &\mapsto \varphi_g(x) \end{aligned}$$

Más aún, $\forall g \in G$ y $\forall x \in \bar{X}$, denotamos como

$$g \cdot x = \varphi_g(x) \in \bar{X}$$

Veamos las propiedades de φ .

PROPIEDADES.

i) φ es homomorfismo:

Como φ es homomorfismo, entonces $\forall g_1, g_2 \in G$:

$$\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$$

o sea, $\forall x \in \bar{X}$, $\varphi_{g_1 g_2}(x) = (\varphi_{g_1} \circ \varphi_{g_2})(x)$, es decir:

$$g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x)$$

ii) Como φ es homomorfismo, entonces

$$\varphi(e) = id_G$$

por lo tanto $\varphi_e(x) = id(x) = x$, $\forall x \in \bar{X}$. Por tanto:

$$e \cdot x = x$$

iii) $\forall g \in G$, $\varphi_g : \bar{X} \rightarrow \bar{X}$ es suprayectiva $\Leftrightarrow \forall x \in \bar{X} \exists y \in \bar{X} \text{ m } \varphi_g(y) = x$, i.e. $g \cdot y = x$. De otra forma

$$\varphi_g(\bar{X}) = \bar{X}$$

$$\Leftrightarrow g \cdot \bar{X} = \bar{X}, \text{ donde } g \cdot \bar{X} = \{g \cdot x \mid x \in \bar{X}\}$$

iv) $\forall g \in G$, $\varphi_g : \bar{X} \rightarrow \bar{X}$ es inyectiva, es decir, $\forall x, y \in \bar{X}$, i.e.

$$\text{Si } \varphi_g(x) = \varphi_g(y) \quad (g \cdot x = g \cdot y) \Rightarrow x = y$$

Veamos algunos ejemplos:

$$gg_1 \cdot x = y \Leftrightarrow g_1 \cdot x = \bar{g}^{-1} \cdot y$$

\Rightarrow Supongamos que $gg_1 \cdot x = y$. Veamos que

$$\begin{aligned} g_1 \cdot x &= e \cdot (g_1 \cdot x) = (eg_1) \cdot x \\ &= (\bar{g}^{-1}(gg_1) \cdot x) = \bar{g}^{-1} \cdot (gg_1 \cdot x) \\ &= \bar{g}^{-1} \cdot y. \end{aligned}$$

Obs: Sea G un grupo y $\bar{X} \neq \emptyset$. Entonces G actúa en \bar{X} bajo $\varphi \Leftrightarrow \exists$ una función $\psi : G \times \bar{X} \rightarrow \bar{X}$ m $\psi(x, g) = x \cdot g$, $\forall x \in \bar{X}$ y $g \in \bar{X}$, tal que

Se cumplen:

i) $(gg_1) \cdot x = g \cdot (g_1 \cdot x)$, $\forall g, g_1 \in G$, y $\forall x \in \bar{X}$.

ii) $\forall x \in \bar{X}$, $e \cdot x = x$.

iii) $\forall y \in G$, $y \cdot \bar{X} = \bar{X}$, donde $y \cdot \bar{X} = \{y \cdot x, \forall x \in \bar{X}\}$.

Dem:

\Rightarrow Se probó en las observaciones.

\Leftarrow Sea $\varphi: G \rightarrow S_{\bar{X}}$ dada como: $\varphi(g) = \varphi_g$, $\forall g \in G$, donde $\varphi_g: \bar{X} \rightarrow \bar{X}$ estú que $\varphi_g(x) = \psi(g \cdot x)$, $\forall x \in \bar{X}$ y $\forall g \in G$. Claramente φ_g estú bien definida, probaremos que φ lo estú, y que es una acción de G sobre \bar{X} .

Obs: Decimos: "G actúa en \bar{X} con acción $g \cdot x$ ".

EJEMPLOS.

i) Si G es grupo, entonces tenemos que G actúa en sí mismo por conjugación, es decir, $\forall g \in G$ y $\forall x \in G$:

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

esto pues $i: G \rightarrow S_G$, donde $i(g) = i_g$, $\forall g \in G$. Donde, $\forall g, x \in G$, $i_g: G \rightarrow G$ es tal que $x \mapsto i_g(x) = gxg^{-1} = g \cdot x$.

Posemos a otros detalles. Suponemos G actuando en \bar{X} con acción $g \cdot x$. Definimos la relación \sim en \bar{X} como: $\forall x, y \in \bar{X}, x \sim y \Leftrightarrow \exists g \in G \text{ m } g \cdot x = y$.

Tenemos que la relación \sim es una relación de equivalencia en \bar{X} :

i) Reflexiva.

$x \sim x$, pues $\exists e \in G \text{ m } e \cdot x = x$.

ii) Simétrica.

Si $x \sim y$, $\exists g \in G \text{ m } g \cdot x = y$. Como $e \cdot x = x$ y $e = g^{-1}g$, entonces $(g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y$, luego $x = g^{-1} \cdot y \Rightarrow g \cdot y = x$. Así, $y \sim x$.

iii) Transitiva.

Si $x \sim y$ y $y \sim z$, entonces $\exists g, g_1 \in G \text{ m } y \cdot x = z$ y $g \cdot y = z$. Luego como $(gg_1) \cdot x = g \cdot (g_1 \cdot x) = g \cdot y = z$, entonces $x \sim z$. ○

Sea G un grupo actuando sobre un conjunto $\bar{X} \neq \emptyset$, bajo acción $g \cdot x$.

Sobre \bar{X} hemos definido la relación de equivalencia \sim :

$$\forall x, y \in \bar{X}, x \sim y \Leftrightarrow \exists g \in G \text{ m } y = g \cdot x.$$

Las clases de equivalencia de \bar{X} bajo la relación de equivalencia \sim son llamadas las órbitas de G en \bar{X} , y si $x \in \bar{X}$, su clase con respecto a esta relación de equivalencia es llamada la órbita de el grupo G en \bar{X} con representante x .

Notemos que si C es la órbita de G en \bar{X} con representante x , entonces

$$\begin{aligned} C &= \{y \in \bar{X} \mid y = g \cdot x \text{ para algún } g \in G\} \\ &= \{g \cdot x \mid g \in G\} \\ &= G \cdot x \end{aligned}$$

Otra forma de enunciarlo es: $\forall x, y \in \bar{X}$,

$$\begin{aligned} x \sim y &\Leftrightarrow G \cdot x = G \cdot y \\ x \not\sim y &\Leftrightarrow G \cdot x \cap G \cdot y = \emptyset \end{aligned}$$

Además, como las clases inducen una partición en \bar{X} :

$$\bar{X} = \bigcup_{x \in X} G \cdot x$$

Si R es un conjunto completo de representantes:

$$\bar{X} = \bigcup_{x \in R} G \cdot x$$

Def. Se dice que \sim es transitiva si existe $x \in \bar{X}$ tal que $G \cdot x = \bar{X}$, esto es,
 $\forall y \in \bar{X} \exists g \in G \text{ m } y = g \cdot x$.

Def. Decimos que x es punto fijo bajo la acción de G sobre \bar{X} , $g \cdot x = x$, $\forall g \in G$.

Denotamos al conjunto de puntos fijos de G por \bar{X}^G , como:

$$\bar{X}^G = \{x \in \bar{X} \mid g \cdot x = x, \forall g \in G\}$$

por supuesto, $\forall x \in \bar{X}$:

$$x \in \underline{X}^G \Leftrightarrow G \cdot x = \{x\}$$

Por otro lado, sea $x \in \underline{X}$. Definimos:

Def. $\forall x \in \underline{X}$, el estabilizador de x es:

$$G_x = \{g \in G \mid g \cdot x = x\}$$

Sea $x \in \underline{X}$, entonces $G_x \neq \emptyset$, pues $e \in G$ es tal que $e \cdot x = x$.

Proposición:

$$\forall x \in \underline{X}, G_x = G \Leftrightarrow x \in \underline{X}^G$$

Dem:

Es inmediato de la definición.

f.o.u.

Proposición.

$$\forall x \in \underline{X}, G_x \subset G. \text{ Además } [G : G_x] = |G \cdot x|.$$

Dem:

Sean $x \in \underline{X}$ y $g, g_1 \in G_x$, esto es $g \cdot x = x$ y $g_1 \cdot x = x$. Como $g_1 \cdot x = x \Rightarrow x = g_1^{-1} \cdot x$, así $x = g \cdot x = g \cdot (g_1^{-1} \cdot x) = (g g_1^{-1}) \cdot x$, por tanto, $g g_1^{-1} \in G_x$. Luego $G_x \subset G$.

Por otro lado, definimos:

$$f: \underline{X}^G / G_x \rightarrow G \cdot x$$

$$g G_x \mapsto g \cdot x$$

Probaremos que f está bien definida.

a) Sean $g_1, g_2 \in G$ y $g_1 G_x = g_2 G_x$, esto es $g_1 \equiv g_2 \pmod{G_x} \Rightarrow g_1^{-1} g_2 \in G_x$, entonces $(g_1^{-1} g_2) \cdot x = x \Rightarrow g_1 \cdot x = g_2 \cdot x \Rightarrow f(g_1 G_x) = g_1 \cdot x = g_2 \cdot x = f(g_2 G_x)$.

Ahora con la inyectividad y suprayectividad.

b) Sean $g_1, g_2 \in G$ y $f(g_1 G_x) = f(g_2 G_x) \Rightarrow g_1 \cdot x = g_2 \cdot x \Rightarrow x = (g_1^{-1} g_2) \cdot x$.

$$x \Rightarrow g_1^{-1} g_2 \in G_x \Rightarrow g_1 \equiv_{G_x} g_2 \text{ mod } G_x \Rightarrow g_1 G_x = g_2 G_x$$

c) Sea $y \cdot x \in G_x$, entonces $\exists g \in G \setminus G_x \cap f(g G_x) = y \cdot x$.

Por tanto, f es biyección. Así:

$$[G : G_x] = |G \cdot x|.$$

q.e.d.

Supongase que X es finito, y sea R un conjunto completo de representantes de las órbitas de G en X . Denotemos por $R' = R \cap \bar{X}^G$. Entonces:

$$\begin{aligned} \bar{X} &= \bigcup_{x \in R} G \cdot x \\ \Rightarrow |\bar{X}| &= \left| \bigcup_{x \in R} G \cdot x \right| \\ &= \sum_{x \in R} |G \cdot x| \\ &= \sum_{x \in R'} |\{x\}| + \sum_{x \in R \setminus R'} |G \cdot x| \\ &= |R'| + \sum_{x \in R \setminus R'} |G \cdot x| \dots (1) \end{aligned}$$

R' denota a todos los representantes R cuya órbita conste de 1 sólo elemento, pues $x \in \bar{X}^G \Leftrightarrow G \cdot x = \{x\}$. Claramente $R' \subseteq \bar{X}^G$, pero $\bar{X}^G \subseteq R'$? Pues si debe suceder, ya que si $y \in \bar{X}^G$, $G \cdot y = \{y\}$, así $y \in R$, pues y se representa a sí mismo. Así: $R' = \bar{X}^G$. Retomando (1):

$$\begin{aligned} |\bar{X}| &= \sum_{x \in \bar{X}^G} |\{x\}| + \sum_{x \in R \setminus \bar{X}^G} |G \cdot x| \\ &= |\bar{X}^G| + \sum_{x \in R \setminus \bar{X}^G} |G \cdot x| \dots (2) \end{aligned}$$

(2) es llamada la ecuación de clase bajo la acción de G por \bar{X} . Si además G es finito:

$$|\bar{X}| = |\bar{X}^G| + \sum_{x \in R \setminus \bar{X}^G} \frac{|G|}{|G_x|}$$

EJEMPLOS.

1) Sea G grupo actuando sobre sí mismo por conjugación, es decir, $\forall g \in G \quad \forall x \in G \quad g \cdot x = gxg^{-1}$

para cada $x \in G$, tenemos que $G \cdot x$ es la clase de conjugación $C(x)$, es decir:

$$C(x) = G \cdot x = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$

Sea $x \in G$. Tenemos que

$$\begin{aligned} x \in \bar{X}^G &\iff g \cdot x = x, \quad \forall g \in G \\ &\iff gxg^{-1} = x, \quad \forall g \in G \\ &\iff gx = xg, \quad \forall g \in G \\ &\iff x \in Z = Z(G) \end{aligned}$$

Por tanto, $\bar{X}^G = Z$. Sea $x \in G$:

$$\begin{aligned} g \in G_x &\iff g \cdot x = x \\ &\iff gxg^{-1} = x \\ &\iff gx = xg \\ &\iff g\{x\} = \{x\}g \\ &\iff g \in N(\{x\}) = Z(x). \end{aligned}$$

Por tanto, $G_x = N(x) = N(\{x\})$. Así pues, la ecuación de clase con respecto a la acción de conjugación está dada como sigue:

$$|G| = |Z| + \sum_{x \in G \setminus Z} \frac{|G|}{|N(x)|}$$

con $|G| < \infty$.

Proposición.

Sea G un grupo finito de orden p^n , $p, n \in \mathbb{N}$ y p primo. Entonces, el c-

entro Z de G es diferente de $\langle e \rangle$.

Dem:

Sea R un conjunto completo de representantes en las clases de conjugación. Notemos que si:

$$x \in R \setminus Z \Rightarrow \frac{|G|}{|N(x)|} \geq 2, \text{ donde}$$

$$\frac{|G|}{|N(x)|} \mid p^n \Rightarrow \frac{|G|}{|N(x)|} = p^f, \text{ con } 1 \leq f < n, \quad (1 \leq f \text{ pues } s: f=0, \frac{|G|}{|N(x)|} = 1)_{**}$$

$$\text{Además, } f \neq n, \text{ pues } s: \text{Si fuera } f=n \Rightarrow p^n = |G| = |Z| + \sum_{x \in R \setminus Z} \frac{|G|}{|N(x)|} \geq p^n$$

$$\Rightarrow |Z| = 0_{**}.$$

Luego $p \mid \sum_{x \in R \setminus Z} \frac{|G|}{|N(x)|}$ donde $p \mid |G|$. Por la ecuación de clase:

$$p \mid \left(|G| - \sum_{x \in R \setminus Z} \frac{|G|}{|N(x)|} \right) = |Z|$$
$$\Rightarrow |Z| = p^s \text{ con } 1 \leq s \leq n$$

en particular, $Z \neq \langle e \rangle$.

g.e.d.

..

Corolario.

Sea G un grupo de orden p^2 con p primo. Entonces G es abeliano.

Dem:

Probaremos que $Z = G$. Claramente $Z \subseteq G$. Notemos que $|Z| = p$ ó p^2 .

Sea $a \in G$, y suponga que $a \notin Z$, luego $|Z| = p$.

Se tiene que $Z(a) = N(a) = \{g \in G \mid ga = ag\}$, así, como $Z \subseteq N(a) = Z(a)$, entonces:

$$|N(a)| \neq p \Rightarrow |N(a)| = p^2$$
$$\Rightarrow N(a) = G \Rightarrow a \in Z_{**}$$

por tanto, $Z = G$.

g.e.c.

Teorema (de Cauchy).

Todo grupo está encajado en algún grupo de permutaciones.

Dem:

Sea G grupo. Definimos la acción de G en sí mismo como: $\forall g \in G$ y $\forall x \in G$, $g \cdot x = gx$ (esta acción es llamada la acción de Caley).

Afirmamos que la acción $\varphi: G \rightarrow S_G$ de Caley es un monomorfismo, pues si $g \in G$ tal que $g \in \text{Ker}(\varphi)$.

$$\begin{aligned} g \in \text{Ker}(\varphi) &\Rightarrow \varphi(g) = \text{id}_G \\ &\Rightarrow \varphi_g = \text{id}_G \\ &\Rightarrow \forall x \in G, g \cdot x = x \\ &\Rightarrow \text{para } e \in G, g \cdot e = g \cdot e = e \\ &\Rightarrow g = e. \end{aligned}$$

Luego $\text{Ker}(\varphi) = \{e\}$

q.e.d.

Teorema.

Sea G grupo y $H \triangleleft G$. Consideramos el conjunto $\bar{X} = G/H$. Entonces \exists un homomorfismo $\varphi: G \rightarrow S_{\bar{X}}$ tal que $\text{Ker}(\varphi)$ es el máximo subgrupo normal de G contenido en H .

Dem:

Definimos la relación

$$g \cdot xH = gxH, \quad \forall g, x \in G.$$

Tenemos que en efecto, $g \cdot xH$ determina una acción de G por \bar{X} . En efecto

i) $\forall g, g_1 \in G$, y $\forall x \in G$: $(gg_1) \cdot xH = gg_1xH = g \cdot g_1xH = g \cdot (g_1 \cdot xH)$

ii) $\forall x \in G$, $e \cdot xH = exH = xH$.

iii) Probaremos que, $\forall g \in G$, $g \cdot \bar{X} = \bar{X}$, es decir $g \cdot G/H = G/H$. Sabemos que

$g \cdot G/IH \subseteq G/IH$. Recíprocamente, sea $yH \in G/IH$, entonces $g \cdot \bar{g}^{-1}yH = yH \in g \cdot G/IH$.

Por tanto, $\underline{g} \cdot \underline{X} = \underline{X}$.

Por (i), (ii) y (iii), $g \cdot xH$ es una acción. Sea $\ell: G \rightarrow S_{\underline{X}}$ dada como: $y \mapsto \ell(y)$, $y, \ell(y): \underline{X} \rightarrow \underline{X}$ dada como $\ell(y)(xH) = g \cdot xH$. Por ser $g \cdot xH$ una acción, ℓ está bien definida, y es homomorfismo.

a) $\text{Ker } \ell \subseteq H$.

Sea $g \in \text{Ker } \ell$, entonces $\ell_g = \text{id}_{\underline{X}}$. Por tanto, $\forall x \in G$, $g \cdot xH = xH$ (o $\ell_g(xH) = xH$), entonces $gxH = xH, \forall x \in G \Rightarrow gh = h \Rightarrow g \in H$. Por tanto, $\text{Ker } \ell \subseteq H$.

b) Maximalidad de $\text{Ker } \ell$

Sea $N \triangleleft G$ tal que $N \subseteq H$. Probaremos que $N \subseteq \text{Ker } \ell$. Sea $n \in N$. $\forall x \in G$ se tiene que $xnx^{-1} \in N$, por lo cual $xnx^{-1} \in H$, pues $N \subseteq H$. Así: $x \equiv_n x \text{ mod } H \Rightarrow xH = nxH = n \cdot xH, \forall x \in G$, lo cual implica que $n \in \text{Ker } \ell$.

q.e.d.

Corolario:

Sea G un grupo finito y $H \triangleleft G$, $H \neq G$ tal que $|G| \nmid [G:H]!$. Entonces, H contiene un subgrupo normal no trivial. En particular, G es simple.

Dem:

Sea $\underline{X} = G/IH$. Por un teorema anterior existe un homomorfismo $\ell: G \rightarrow S_{\underline{X}}$ tal que $\text{Ker } \ell$ es el máximo subgrupo normal de G contenido en H . Si $\text{Ker } \ell = \langle e \rangle$, entonces ℓ es monomorfismo, por lo cual $G \cong \ell(G) \subset S_{\underline{X}}$, con lo cual $|G| = |\ell(G)| \mid |S_{\underline{X}}| = [G:H]!$.

*. Por tanto $\text{Ker } \ell \neq \langle e \rangle$, y $\text{Ker } \ell \triangleleft G$ con $\text{Ker } \ell \subsetneq H$. Luego G no es simple.

q.e.d.

TEOREMAS DE SYLOW

p-grupos.

Proposición.

Sean p un número primo, G un grupo de orden p^n , $n \in \mathbb{N}$ actuando sobre un conjunto \bar{X} no vacío. Entonces:

$$|\bar{X}| \equiv |\bar{X}^G| \pmod{p}$$

Dem:

Sea R un conjunto completo de representantes bajo la relación de la acción de G por \bar{X} . Como $[G : G_x] = |G \cdot x|$ y $|G| = p^n$, entonces $p \mid |G \cdot x|$, $\forall x \in \bar{X}$, en particular:

$$\begin{aligned} & p \mid \sum_{x \in R \setminus \bar{X}} |G \cdot x| \\ \Rightarrow & p \mid |\bar{X}| - |\bar{X}^G| \\ \Rightarrow & |\bar{X}| \equiv |\bar{X}^G| \pmod{p} \end{aligned}$$

q.e.d.

Continúa en la sig. página.

Corolario.

Sea G un grupo finito y $H \subset G$ tal que $|H| = p^k$, con p primo y $k > 0$. Entonces

$$[N_G(H) : H] \equiv [G : H] \pmod{p}$$

Dem:

Sea $\underline{X} = G/H$ y $\ell : G \rightarrow S_{\underline{X}}$ dada por: $g \mapsto \ell_g$, donde $\ell_g : \underline{X} \rightarrow \underline{X}$ dada como $\ell_g(xH) = gxH$.

Por el teorema anterior, ℓ es una acción de G por \underline{X} . Como $H \subset G$, entonces $\psi : \ell|_H : H \rightarrow S_{\underline{X}}$ es un homomorfismo, luego H actúa sobre \underline{X}

Por acción:

$$h \cdot xH = hxH, \forall h \in H \text{ y } \forall x \in G.$$

Sea R un conjunto completo de representantes bajo la acción de H por \underline{X} . Si $x \in R$, con $x \notin \underline{X}^H$, entonces $p \mid \frac{|H|}{|\underline{X}_x|}$, lo cual implica.

$$p \mid \sum_{x \in R \setminus \underline{X}^H} \frac{|H|}{|\underline{X}_x|}$$

así que, por la ecuación de clase: $p \mid |\underline{X}| - |\underline{X}^H| \Rightarrow |\underline{X}^H| \equiv |\underline{X}| \pmod{p}$.

odp. Como $\underline{X} = G/H \Rightarrow |\underline{X}| = [G : H]$. Por tanto:

$$|\underline{X}^H| \equiv [G : H] \pmod{p}$$

Veamos qué pasa con \underline{X}^H . Sea $x \in G$.

$$xH \in \underline{X}^H \Leftrightarrow h \cdot xH = hxH = xH, \forall h \in H.$$

$$\Leftrightarrow \bar{x} \cdot h xH = H, \forall h \in H$$

$$\Leftrightarrow \bar{x} \cdot h x \in H, \forall h \in H.$$

$$\Leftrightarrow \bar{x} \cdot H x \subseteq H$$

$$\Leftrightarrow \bar{x} \cdot H x = H$$

$$\Leftrightarrow Hx = xH \Leftrightarrow x \in N_G(H).$$

$$\Leftrightarrow xH \in N_G(H)/H$$

por tanto: $\sum H = N_G(H)/H$. Así

$$[N_G(H):H] \equiv [G:H] \pmod{p}$$

q.e.d.

Teorema (de Cauchy).

Sea G un grupo finito, y p un número primo tal que $p \mid |G|$. Entonces,
 $\exists a \in G$ m $|a| = p$.

Dem:

(Bosquejo). Conocemos ya, por la ecuación de clase que

$$|\underline{X}| = |\overline{X}^H| \text{ mod}_p \quad \dots \quad (1)$$

tomando a \overline{X} como: $\overline{X} \subseteq G^P$ y $\overline{X} = \{(a_1, \dots, a_p) \in G^P \mid a_1 \cdot a_2 \cdot \dots \cdot a_p = e\}$.

Claramente $\overline{X} \neq \emptyset$, pues $(e, e, \dots, e) \in \overline{X}$. Definiremos una acción tal que:

$$\forall (a_1, \dots, a_p) \in G^P, e(a_1, \dots, a_p) = (a_p, a_1, \dots, a_{p-1})$$

pero el H debe ser tal que con esta acción se cumpla (1), tomemos $H = (\mathbb{Z}/p\mathbb{Z}, +)$. La acción la vamos a dar como:

$$[i] \cdot (a_1, a_2, \dots, a_{p-1}) = (a_{1+i}, a_{2+i}, \dots, a_{p+i})$$

Pensando que el $i+1$ en el a es $[i+1] = [i] + [1]$. Luego tomamos $f: \overline{X} \rightarrow G^{P-1}$, como:

$$f(a_1, \dots, a_p) = (a_1, \dots, a_{p-1})$$

Probar que f es función y que es biyectiva. As: $|\overline{X}| = |G|^{P-1} = |\overline{X}^H| \text{ mod}_p$. Pero $\overline{X}^H \neq \emptyset$, pues $(e, \dots, e) \in \overline{X}^H$. Si $|\overline{X}^H| = 1 \Rightarrow p \mid 1 \text{ **c}$. Por tanto $0, |\overline{X}^H| > 1$, as: $\exists a \in H, a \neq e \text{ y } g \cdot (a, \dots, a) = (a, \dots, a) \Rightarrow a^p = e$.

Obs: Sea G grupo y $H \leq G$ tal que $|H|=p^n$ con p primo y $n \geq 1$. Por una proposición anterior $[N_G(H):H] \equiv [G:H] \pmod{p}$.

2) Sea G un grupo finito con $|G|=p^n$, p primo y $n \geq 1$. Si G actúa en un $X \neq \emptyset$, entonces:

$$|X| = |\Sigma^G| \pmod{p}$$

Def. Sea p un número primo. Un grupo G se dice que es un p -grupo, si $\forall a \in G$:

$$|a| = p^m$$

para algún $m \in \mathbb{Z}^+ \cup \{0\}$ que depende de a .

Def. Sea G grupo y $H \leq G$. Decimos que H es un p -subgrupo de G , si H como grupo es p -grupo, con p primo.

Proposición.

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

Dem:

\Rightarrow) Supongamos que G es p -grupo. Como G es finito, $\exists m \in \mathbb{N}$ m $|G|=m$. Sea q un número primo tal que $q \mid |G|=m$. Por el Teorema de Cauchy, $\exists a \in G$ m $|a|=q$. Pero, como G es p -grupo, $p \mid |a|=q \Rightarrow p=q$. Por tanto, $|G|$ debe ser alguna potencia de p .

\Leftarrow) Sea $a \in G$. Como $|G|=p^n$, con $n \in \mathbb{N} \Rightarrow |a|=p^j$ donde $0 \leq j \leq n$, pues $|a| \mid |G|$. Por tanto, G es p -grupo.

g.o.d.

Corolario.

Sean p un número primo. Si G es p -grupo finito, entonces todo subgrupo de G es p -subgrupo de G .

TEOREMAS DE SYLLOW

Teorema (PTS).

Sea p un número primo y $m, n \in \mathbb{N}$ arbitrarios tales que $p \nmid m$. Entonces, todo grupo finito de orden $p^m n$ contiene un subgrupo de orden p^f , para cada $0 \leq f \leq n$; además, cada subgrupo de orden p^f con $f < n$, es normal en un subgrupo de orden p^{f+1} de dicho grupo.

Dem:

Procederemos por inducción sobre n .

1) Sea G un grupo de orden p^m . Como $p \nmid |G|$, por el teorema de Cauchy, $\exists a \in G$ m $|a|=p$. Así $\langle e \rangle$ y $\langle a \rangle$ son subgrupos de G de orden p^0 y p^1 y $\langle e \rangle \triangleleft \langle a \rangle$.

2)

EJEMPLOS.

I) Todo grupo G de orden 72 es no simple. En efecto, notemos que:

$$|G| = 72 = 2^3 \cdot 3^2$$

Consideremos el número n_3 , la cantidad de 3-subgrupos Sylow de G . Por la proposición anterior, $n_3 = 2^{k_1}$ con $k_1 = 0, 1, 2, 3$. Pero, como $n_3 \equiv 1 \pmod{3}$, entonces $k_1 = 0, 2$, así $n_3 = 1$ ó $n_3 = 4$. Si $n_3 = 1$, significa que G tiene un único 3-subgrupo Sylow, el cual debe ser normal $\Rightarrow G$ es no simple.

Si $n_3 = 4$, sea P un 3-subgrupo Sylow de G , entonces

$$n_3 = 4 = [G : N_G(P)]$$

con lo cual $|G| + [G : N_G(P)]! = 24 \Rightarrow G$ no es simple.