Apuntes de clase

José Antonio de la Rosa Cubero

Proposición 1. *Sea G un grupo finito y $H \leq G$ tal que $[G : H] = p$ siendo p el menor primo que divide al orden de G.*

Entonces $H \trianglelefteq G$.

Demostración. Consideramos

$$G/H = \{xH : x \in G\}$$

y la acción por traslación ${}^{g}(xH) = (gx)H$ y ρ la representación asociada.

Veamos que $\ker \rho \leq H$. $\ker \rho = \{\rho(g)(xH) = xH \forall x \in G\} = \{(gx)H = xH \forall x \in G\}$

Si $g \in \ker \rho$ entonces $(gx)H = xH$ para todo $x \in G$. En particular para $x = 1$ se tendrá

$$gH = H$$

y por lo tanto $g \in H$.

Por el primer teorema de isomorfía tenemos que $G/\ker \rho \cong \operatorname{Im} \rho$

$$[G : \ker \rho] = |\operatorname{Im} \rho|$$

$\operatorname{Im} \rho \leq S(G/H) \cong S_p$ y como $|G/H| = [G : H] = p$, tenemos que $\operatorname{Im}(\rho)|p!$ como queríamos ver.

Veamos que $[H : \ker(\rho)]|(p-1)!$.

Consideramos

$$\ker(\rho) \leq H \leq G$$

Luego

$$[G : \ker \rho] = [G : H][H : \ker \rho] = p[H : \ker \rho]$$

Como el segundo miembro del producto divide a $p!$, tenemos que $[G : \ker \rho]|(p-1)!$.

Ahora tenemos que ver que $[H : \ker \rho] = 1$.

Supongamos que no fuera 1. Elegimos un primo q que divida a $[H : \ker \rho]$.

Por transitividad, $q|\,|H|$ e igualmente $q|\,|G|$.

Como por el apartado anterior, tenemos que $[H : \ker\rho] | (p-1)!$ y $q | [H : \ker\rho]$, luego $q < p$, lo cual contradice que p es el menor primo que divide al orden de G.

Consecuentemente $[H : \ker\rho] = 1$, por tanto $H = \ker\rho$ y por tanto $H \trianglelefteq G$ pues el núclao es siempre normal en el dominio de ρ.

□

Proposición 2. *Sea G un p-grupo y H normal en G de orden p.*

Entonces $H \leq Z(G)$.

Demostración. Consideramos $|G| = p^n$, $n \geq 1$, $H \trianglelefteq G$ y $|H| = p$.

Como $H \trianglelefteq G$ entonces $gHg^{-1} = H$ para toda $g \in G$.

Entonces podemos considerar la acción por conjugación de G sobre H.

$$^{g}h = ghg^{-1}$$

Entonces

$$|H| = |\mathrm{Fix}(H)| \sum_{h \notin \mathrm{Fix}(H)} [G : \mathrm{Stab}_G(h)]$$

Si $h \notin \mathrm{Fix}(H)$, $[G : \mathrm{Stab}_G(h)] > 1$, y como $[G : \mathrm{Stab}_G(h)] \mid |G| = p^n$ luego existe un $r \geq 1$ tal que $[G : \mathrm{Stab}_G(h)] = p^r$.

Consecuentemente $p | \sum_{h \notin \mathrm{Fix}(H)} [G : \mathrm{Stab}_G(h)]$ y como $|H| = p$ entonces $p \mid |\mathrm{Fix}(H)|$.

$h \in \mathrm{Fix}(H) \iff O(h) = \{h\}$ o equivalentemente $ghg^{-1} = h$ para toda $g \in G$, es decir, si $gh = hg$ o lo que es lo mismo, si $h \in Z(G)$.

Por tanto, $\mathrm{Fix}(H) = H \cap Z(G)$.

Como $p \mid |H \cap Z(G)|$ y $H \cap Z(G) \leq H$ entonces $|H \cap Z(G)| \mid |H| = p$

Luego $|H \cap Z(G)| = p = |H|$ y entonces $H \cap Z(G) = H$ lo que implica que $H \leq Z(G)$.

□

Clasificación de grupos abelianos finitos

Proposición 3. *Sea A un p-grupo abeliano finito con $|A| = p^n$, $n \geq 1$. Entonces existen enteros $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1$ y tales que $\sum \beta_i = n$ y*

$$A \cong C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_t}}$$

Además esta expresión es única (salvo el orden). Esto es, si

$$A \cong C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_s}}$$

y $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_s \geq 1$ y tales que $\sum \alpha_i = n$ entonces $s = t$ $\alpha_i = \beta_i$ para todo $1 \leq i \leq t$.

Definición 1 (p-grupo abeliano elemental)**.** Un p-grupo abeliano finito E diremos que es un p-grupo abeliano elemental si $x^p = 1$ para todo $x \in E$.

Un ejemplo de p-grupo abeliano elemental es $C_p \times \cdots \times C_p$.

Lema 1. *Sea E un p-grupo abeliano elemental. Entonces para cada $x \in E$ existe un $M \leq E$ tal que E es el producto directo interno de M y $\langle x \rangle$, es decir, $E \cong M \times \langle x \rangle$.*

Demostración. Si $x = 1$, basta tomar $M = E$.

Supongamos $x \neq 1$. Entonces $\text{ord}(x) = p$.

Sea
$$\Sigma = \{H \leq E : x \notin H\}$$

Sabemos que no es vacío pues $\{1\} \in \Sigma$.

Sea $M \in \Sigma$ el elemento de mayor orden.

Aseguramos que $[E : M] = p$. Sabemos ya que $[E : M] \,|\, |E| = p^n$, luego $[E : M] = p^r$ con $r \geq 1$.

Si $[E : M] = p$, veamos que E es el producto directo interno de M y $\langle x \rangle$.

Como E es abeliano, M y $\langle x \rangle$ son subgrupos normales.

$M \cap \langle x \rangle = \{1\}$ si $y \in M \cap \langle x \rangle$. Entonces $y = x^j$ y tenemos que $\langle x^j \rangle \leq M$. Como $x \notin M$, entonces $j = 0$ y por tanto $y = 1$. Si no $\langle x^j \rangle = \langle x \rangle$.

En tercer lugar, $M\langle x \rangle = E$. Aplicamos el tercer teorema de isomorfía a $M \leq E$ y $\langle x \rangle \leq E$ y obtenemos:

$$M\langle x \rangle / \langle x \rangle \cong M/(M \cap \langle x \rangle) = M/\{1\} = M$$

Como $[E : M] = p$, tenemos que $\frac{E}{M} = p$, y po tanto $|M| = \frac{|E|}{p} = \frac{p^n}{p} = p^{n-1}$.

Entonces $|M\langle x \rangle| = p^{n-1}p = p^n = |E|$, con lo que $M\langle x \rangle = E$.

Por tanto, $E \cong M \times \langle x \rangle$.

Supongamos que no ocurriera que $[E : M] = p$, es decir, $[E : M] = p^i$, con $i \geq 2$.

Consideramos E/M, que es también un p-grupo abeliano y elemental.

$yM \in E/M$ implica $(yM)^p = y^p M = M$ y entonces $y \in E$ implica que $y^p = 1$ y entonces cualquier elemento distinto de M en E/M tiene orden p.

Elegimos $yM \in E/M$, $yM \neq M$ y $yM \notin \langle xM \rangle$.

$xM \in E/M$, $xM \neq M$, $\text{ord}(xM) = p$ tenemos $\langle xM \rangle \leq E/M$ y como $|E/M| = p^2$ y $|\langle xM \rangle| = p$ tenemos que $\langle xM \rangle < E/M$ y entonces existe yM en las condiciones anteriores.

Además podemos asegurar que $xM \notin \langle yM \rangle$ porque xM, yM tienen ambos orden p.

Consideramos la proyección canónica $\pi : E \longrightarrow E/M$, dada por $\pi(a) = aM$.

Sea $H = \pi(\langle yM \rangle) = \{a \in E : \pi(a) \in \langle yM \rangle\} = \{a \in E : aM \in \langle yM \rangle\}$.

Como $xM \notin \langle yM \rangle$ entonces $x \notin H$.

Si $a \in M$, tenemos que $aM = M \in \langle yM \rangle$, $a \in H$, es decir, $M \leq H$.

Como $y \in H$ y también $y \notin M$, entonces $M < H$ y ya hemos llegado a la contradicción:

$$x \notin H \implies H \in \Sigma$$

y $M < H$, en contra de la elección de M.

$\square$