Apuntes de clase

José Antonio de la Rosa Cubero

Proposición 1. *Si G contiene un elemento x que tiene exactamente dos conjugados, entonces G admite un subgrupo normal propio.*

Demostración. Sea $x \in G$ tal que $|\mathrm{cl}(x)| = 2$. En particular $x \neq 1$.

Consideramos $N = c_G(x) = \mathrm{Stab}_G(x)$. Sabemos que $[G : N] = |\mathrm{cl}(x)| = 2$ por lo tanto, $N \lhd G$.

Por otro lado, como $x \in N = \{g \in G : gx = xg\}$ tenemos $N \neq 1$. Por tanto N es un subgrupo normal propio de G.

□

Proposición 2. *Sea G un grupo y consideremas la acción por conjugación. La órbita es:*

$$O(H) = \{gHg^{-1} : g \in G\}$$

y el estabilizador

$$\mathrm{Stab}_G(H) = \{g \in G : gH = Hg\}$$

que se llama el normalizador de H en G.

$$\mathrm{Fix}(G) = \{H \leq G : H \trianglelefteq G\}$$

Si G es finito, entonces $|O(H)|$ es finito. Esto es, el número de conjugados de H es finito.

$$|O(H)| = [G : N_G(H)]$$

entonces $|O(H)| \mid |G|$.

Definición 1 (p-grupo)**.** Sea p un número primo. Un grupo finito no trivial G diremos que es un p-grupo si todo elemento de G tiene orden una potencia de p.

Ejemplos:

1. Para cada $n \geq 1$, C_{p^n} es un p-grupo. Porque si $a \in C_{p^n}$, entonces $\mathrm{ord}(a)$ divide a $|C_{p^n}| = p^n$ y $\mathrm{ord}(a) = p^k$.

2. $C_p \times \cdots \times C_p$ es un p-grupo. Todo elemento de G tiene orden una potencia de p tal que esa potencia sea menor que n.

3. Si G es un grupo con $|G| = p^n$ para $n \geq 1$, entonces, razonando como en el ejemplo 1, G es un p-grupo.

Teorema 1 (Teorema de Cauchy)**.** *Sea G un grupo finito. Para cada primo p divisor de $|G|$ existe $x \in G$ tal que* $\mathrm{ord}(x) = p$*. Entonces existe un $H \leq G$ tal que $|H| = p$.*

Demostración. Sea $n = |G|$ y $p|n$ un primo. Sea:

$$X := \{(x_1, \ldots, x_p) \in G^p : \prod_{i=1}^{p} x_i = 1\}$$

Como $|G| = n$, entonces $|X| = n^{p-1}$, ya que el último elemento viene determinado por los anteriores.

Consideramos $\sigma = (1 \quad 2 \quad \ldots p) \in S_p$ y $H = \langle \sigma \rangle = \{1, \sigma, \ldots, \sigma^{p-1}$. Definimos la siguiente acción de H sobre X:

$$^{\sigma^0}x = x$$

para $1 \leq j \leq p-1$:

$$^{\sigma^j}(x_1, \ldots, x_p) = (x_{j+1}, \ldots, x_p, x_1, \ldots, x_j)$$

Vemos la órbita:

$$O((x_1, \ldots, x_p)) = \{(x_1, \ldots, x_p), \ldots, (x_p, x(1), \ldots, x_{p-1})\}$$

que tiene orden 1 o p.

Los elementos de orbita de orden 1 son los puntos fijos $x \in \mathrm{Fix}(X)$, pero en ese caso $x_i = x$ para todo $i \in \{1, \ldots, n\}$.

Puesto que $(1, \ldots, 1) \in \mathrm{Fix}(X)$ tenemos que no es vacío. Tenemos:

$$|X| = |\mathrm{Fix}(X)| + \sum_{x \notin \mathrm{Fix}(X)} |O(x)| = |\mathrm{Fix}(X)| + \sum_{x \notin \mathrm{Fix}(X)} p = r + ps$$

o sea, que $n^{p-1} = r + ps$, tenemos que $p|r$ ya que divide a n y en particular $r \geq 2$.

Esto implica que existe un $(x, \ldots, x) \in \mathrm{Fix}(X)$ distinto al que ya conocemos, el $(1, \ldots, 1)$ y por tanto $x \neq 1$. Como $(x, \ldots, x) \in X$ por definición, tenemos que $x \cdots x = x^p = 1$ y $x \neq 1$. Concluimos que existe un $x \in X$ tal que $\mathrm{ord}(x) = p$.

$\square$

Corolario 1. G es un p-grupo si y solo si $|G| = p^n$ para algún $n \geq 1$.

Demostración. Sea $m = |G|$, $m \geq 1$. Sea q un divisor primo de m.

Sea q un divisor primo de m. Por el teorema de Cauchy, existe $x \in G$ tal que el orden de x es q. Por otro lado, como G es un p-grupo, entonces $\mathrm{ord}(x) = p^k$, con lo que $q = p^k$ lo que implica que $k = 1$ y $p = q$.

Si el único divisor primo de m es p, entonces existe un n tal que $m = p^n$.

□