Teorema (Cauchy)

Sea G un grupo finito y p un divisor primo de $|G|$. Entonces G tiene un elemento de orden p.

Dem:

Supongamos que el resultado es falso y supongamos que G es un contraejemplo de orden $|G|$ mínimo. Es decir, $p \mid |G|$ pero G no tiene elementos de orden p y $|G|$ es mínimo. Recordemos que $|cl_G(g)| = [G : C_G(g)]$ así que $p \mid |cl_G(g)| |C_G(g)|$ por Lagrange. Supongamos que $|cl_G(g)| > 2$ y así $|C_G(g)| < |G|$. Si $p \mid |C_G(g)|$ por como se escogió a G, $C_G(g)$ debe de contener un elemento de orden p, lo que implica que G tiene un elemento de orden p ∇_0^∇. Entonces $p \mid |cl(g)|$. Como las clases de conjugacion particionan a G, $|G| = c_1 + \cdots + c_k$ donde k son las distintas clases de

conjugación y c_i su respectivo tamaño. Si $c_i \geq 2$, entonces $p \mid c_i$. Digamos que $c_1, \dots, c_n \geq 2$ y $c_{n+1}, \dots, c_k = 1$. Entonces $|G| = c_1 + \cdots + c_n + 1 + \cdots + 1$. Como $p \mid |G|$ y $p \mid c_i$ $\forall$ $\forall 1 \leq i \leq n$, $p \mid \underbrace{1 + \cdots + 1}_{k-n}$. Recordemos que $|cl_G(g)| = 1 \Leftrightarrow g \in Z(G)$ $\therefore |Z(G)| = k - n$ y $p \mid |Z(G)|$

Por la elección de G, $Z(G)$ contiene un elemento de orden p si $n \geq 1$. Si $n = 0$, $G = Z(G)$ entonces G es abeliano y por la proposición anterior, G tiene un elemento de orden p ! $\forall$

Prop. Sea p un número primo y G un p-grupo finito. Entonces $Z(G) \neq e$.

Dem:

Como G es un p-grupo, $|G| = p^k$ p.a. $k > 0$. Entonces $p \mid |cl(g)|$ para $g \in G$ siempre y cuando $|cl(g)| > 1$. Sean $c_1, \dots, c_k$ los tamaños de las respectivas clases de conjugación distintas de G. Entonces $|G| = c_1 + \cdots + c_k$. Digamos que $c_1, \dots, c_n \geq 2$ y $c_{n+1}, \dots, c_k = 1$.

Entonces $|G| = c_1 + \cdots + c_n + 1 + \cdots + 1$. Como $p \mid |G|$ y $p \mid c_i$ $\forall 1 \leq i \leq n$, $p \mid \underbrace{1 + \cdots + 1}_{k-n}$.

Recordemos que $|cl_G(g)| = 1 \Leftrightarrow g \in Z(G)$ $\therefore |Z(G)| = k - n$ y $p \mid |Z(G)|$. $\therefore Z(G) \neq e$.

Teoremas de Sylow

Lema: Sea $n=p^\ell m$ con p primo. Entonces $\binom{n}{p^a}\equiv m \bmod p$.

$$\binom{n}{m}=\frac{n!}{m!(n-m)!}$$

Dem:

Dados dos polinomios $f(x)=\sum_{j\geq 0} a_j x^j$ y $g(x)=\sum_{j\geq 0} b_j x^j$ con coeficientes en $\mathbb{Z}$, usaremos la notación $f(x)\equiv g(x) \bmod p$ para indicar que para cada $j\geq 0$ $a_j \equiv b_j \bmod p$. Así, tenemos que $(x+1)^p \equiv x^p+1 \bmod p$ ya que los coeficientes $\binom{p}{j}\equiv 0 \bmod p$ para $1\leq j\leq p-1$. Se sigue que $(x+1)^{p^2}\equiv (x^p+1)^p \equiv x^{p^2}+1 \bmod p$. Continuando de esta manera $(x+1)^{p^\ell}\equiv x^{p^\ell}+1 \bmod p$. Entonces $(x+1)^n \equiv (x+1)^{p^\ell m}\equiv (x^{p^\ell}+1)^m \bmod p$. Comparando los coeficientes de x^{p^ℓ} de ambos lados, tenemos que $\binom{n}{p^\ell}\equiv\binom{m}{1}=m \bmod p$.

Teorema (Sylow E)

Sea G un grupo finito de orden $p^l m$ con p primo y $p \nmid m$. Entonces G tiene un subgrupo H de orden p^l.

Dem:

Sea Ω el conjunto de todos los subconjuntos $X \subseteq G$ tales que $|X| = p^l$. Entonces $|\Omega| = \binom{|G|}{p^l} \equiv m \not\equiv 0 \mod p$ por el lema anterior y porque $p \nmid m$. Para cada $g \in G$ y $X \subseteq G$ se tiene que $|X| = |gX|$, entonces G actua en Ω por multiplicación. Como $p \nmid |\Omega|$, debe existir una orbita $\mathcal{O}$ tal que $p \nmid |\mathcal{O}|$. Sea $X \in \mathcal{O}$. Por el FCP, tenemos que $|\mathcal{O}| = |G|/|H|$ donde $H = G_X$ es el estabilizador de X. Como $p^l \mid |G|$ pero p no divide a $|\mathcal{O}|$ $p^l \mid |H|$, en particular, $p^l \leq |H|$. Ahora, fijemos $x \in X$. Para $h \in H$, $hx \in hX = h \cdot X = X$ ya que H es el estabilizador de X. Se sigue que $Hx \subseteq X$ y así $|H| = |Hx| \leq |X| = p^l$.

Por lo tanto, $|H| = p^l$.