## C. Relacionando Propiedades de $H$ con Propiedades de $G/H$

Sea $G$ un grupo y $H$ un subgrupo normal de $G$. Probar:

1. Si $x^2 \in H$ para cada $x \in G$, entonces cada elemento de $G/H$ es su propio inverso.

Si $x^2 \in H$, entonces $x^2H = H$, esto es equivalente a decir que $xH = x^{-1}H$

2.AAAAAAA
3. AAAAAAAAAAAAAAAAAAAA

4. Cada elemento de $G/H$ posee una raíz cuadrada si y solo si para todo $x \in G$ hay un $y \in G$ tal que $xy^2 \in H$.

Si cada $Hx \in G/H$ posee una raíz cuadrada, hay $Hy$ tal que $Hx = Hy^2$, es decir $xy^{-2} \in H$. Las implicancias se leen en sus respectivas direcciones.

5. $G/H$ es cíclico si y solo si hay un elemento $a \in G$ con la siguiente propiedad: por cada $x \in G$, hay $n$ tal que $xa^n \in H$.

Si $G/H$ es cíclico, sease $\langle aH \rangle$ su generador, luego existe $xH \in \langle aH \rangle$ tal que $xH = a^nH$, para algún $n \in \mathbb{N}$, luego $x^{-1}a^n \in H$.

Si para todo $x \in G$, existe $n$ tal que $xa^n \in H$, etonces $xa^nH = H \iff a^nH = x^{-1}H$, luego esta definición corresponde a grupo cíclico.

6. Si $G$ es un grupo abeliano, sea $H_p$ el conjunto de todos los $x \in G$ cual orden es una potencia de $p$. Probar que $H_p$ es un subgrupo de $G$. Probar que $G/H_p$ no posee elementos cual orden es ua potencia de $p$ (elemento no nulo.)

(i)Sea $a, b \in H_p$, luego $\text{ord}\,(a) = p^n$ y $\text{ord}\,(b) = p^m$, suponer que $m > n$. Luego $\text{ord}\,(ab) = p^m$, $ab \in H_p$.
(ii) Sea $a^{p^n} = e, luego e = a^{-p^n} = (a^{-1})^{p^n}$.
(iii) Sea $e \in G$, luego $e^{p^n} = e$ para todo $n \in \mathbb{N}$.
(iv) Supongamos que $a^p \in H_p$. Por definición, esto significa que el orden de $a^p$ es una potencia de $p$, es decir, existe un $n \in \mathbb{N}$ tal que:

$$\text{ord}(a^p) = p^n.$$

Por lo tanto, se cumple que:

$$(a^p)^{p^n} = e.$$

Reescribiendo la expresión, obtenemos:

$$a^{p^{n+1}} = e.$$

Esto implica que el orden de $a$, denotado como $\text{ord}(a)$, debe dividir $p^{n+1}$. Es decir, existe un entero $m$ tal que:

$$\text{ord}(a) = p^m.$$

Dado que $p^m$ es una potencia de $p$, se concluye que $a \in H_p$, como queríamos demostrar.

7.
(a) Si $G/H$ es abeliano, probar que $H$ contiene todos los conmutadores de $G$.

Si $G/H$ es abeliano, entonces $Hab = Hba$, luego $Haba^{-1}b^{-1} = H$, entonces $aba^{-1}b^{-1} \in H$

(b)

Sean $g, g' \in G$. Como $G/H$ es abeliano, para cualesquiera $g, g' \in G$ se tiene

$$g\,g'H = g'H\,g.$$

Esto implica que el conmutador

$$[g, g'] = g\, g'\, g^{-1}\, g'^{-1} \in H.$$

Dado que $H \subseteq K$, se tiene $[g, g'] \in K$. Por lo tanto,

$$g\, g' = [g, g']\, g'\, g,$$

y al pasar al cociente obtenemos

$$gK\ g'K = g'K\ gK.$$

Concluimos que $G/K$ es abeliano.

Sea $k, k' \in K$. Dado que $k, k' \in G$ y $G/H$ es abeliano, el conmutador

$$[k, k'] = k\, k'\, k^{-1}\, k'^{-1} \in H.$$

Luego, en el cociente $K/H$ se tiene

$$kH\, k'H = k'H\, kH.$$

Por lo tanto, $K/H$ es abeliano.

En consecuencia, si $G/H$ es abeliano, entonces tanto $G/K$ como $K/H$ son abelianos.

## D. Propiedades de $G$ determinadas por propiedades de $G/H$ y $J$

Hay propiedades de grupo donde si se cumplen en $G/H$ y en $H$, entonces se cumplen en $G$. Sea $G$ un grupo y $H$ un subgrupo normal de $G$. Probar:

1. Si cada elemento de $G/H$ posee orden finito y cada elemento de $H$ posee orden finito, entonces cada elemento de $G$ posee orden finito.

Sea $Hx$ con $x \in G$ en $G/H$, se tiene que hay $n \in \mathbb{N}$ tal que $Hx^n = H$, es decir $x^n \in H$, Luego, para elemento en $H$ posee orden finito, es decir, hay $m \in \mathbb{N}$ tal que $h^m = e$, luego esto se cumple para todo $x \in G$, ya que, $x^n \in H$, entonces $(x^n)^m = e$. Luego cada $x \in G$ posee orden finito.

2. Si cada elemento de $G/H$ posee una raíz cuadrada y cada elemento de $H$ posee raíz cuadrada, entonces cada elemento de $G$ posee una raíz cuadrada.

Sea $Hx$ con $x \in G$ en $G/H$, existe $Hy$ tal que $Hx = Hy^2$ es decir $x(y^{-1})^2 \in H$, luego cada $h \in H$ posee una raíz cuadrada también, por lo que $h = (h')^2$, luego como todo $x(y^{-1})^2 \in H$ con $x, y \in G$, cada $g \in G$ posee raíz cuadrada.

3. Sea $p$ un número primo. Si $G/H$ y $H$ son *p-grupos*, entonces $G$ es un *p-grupo*.

Sea $Hx \in G/H$, se tiene que $Hx^{p^n} = H$, es decir $x^{p^n} \in H$, luego todo $h \in H$ cumple que $h^{p^m} = e$, como todo $x \in G$ cumple que $x^{p^n} \in H$, $(x^{p^n})^{p^m} = x^{p^{m+n}}$, luego $G$ es un p-grupo.

4. Si $G/H$ y $H$ son finitamente generados, entonces $G$ es finitamente generado.

Sea $G/H$ finitamente generado por los cosets $Hx_1, \ldots, Hx_n$ y $H$ finitamente generado por $h_1, \ldots, h_m$. Entonces, para cualquier $g \in G$, se tiene que $gH$ se puede escribir como un producto de los cosets $Hx_i$, de modo que existe $h \in H$ y enteros $a_1, \ldots, a_n$ tales que

$$g = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} h.$$

Pero como $h$ se puede expresar como un producto de $h_1, \ldots, h_m$, se sigue que $g$ es producto de los elementos del conjunto finito

$$\{x_1, \ldots, x_n, h_1, \ldots, h_m\}.$$

Por tanto, $G$ es finitamente generado.

## E. Orden de Elementos en Grupos Cocientes

Sea $G$ un grupo y $H$ un subgrupo normal de $G$. Probar:

1. Por cada elemento $a \in G$, el orden del elemento $Ha$ en $G/H$ es un divisor del orden de $a \in G$.

Sea $\varphi : G \to G/H : a \mapsto Ha$ dado que $G/H$ es la imagen homomorfa de $G$. Luego se tiene que $\operatorname{ord}\varphi(a) \mid \operatorname{ord}(a)$ por ejercicio anterior, equivalentemente, $\operatorname{ord}(Ha) \mid \operatorname{ord}(a)$

2. Si $(G : H) = m$, el orden de cada elemento de $G/H$ es divisor de $m$.

Se tiene que $(G : H)$ es el orden de $G/H$, luego por teorema, para $Hg \in G/H$, $\operatorname{ord}(Hg) \mid |G/H|$.

3. Si $(G : H) = p$ con $p$ primo, entonces el orden de cada elemento $a \notin H$ en $G$ es un múltiplo de $p$.

$|G| = p \cdot |H|$, luego como para $g \notin H$, $\operatorname{ord}(g) \mid |G|$, es decir $\operatorname{ord}(g) \mid p \cdot |H|$, luego $\operatorname{ord}(g) \nmid |H|$, por lo que es múltiplo de $p$.

4. Si $G$ posee un subgrupo normal de índice $p$, donde $p$ es primo, entonces $G$ posee almenos un elemento de orden $p$.

Suponer que $G$ es finito, como $(G : H) = p$, entonces $G/H$ es cíclico, luego, como $G$ es finitio $p \mid |G|$, por lo que posee un elemento de orden $p$. Luego como es cíclico de orden $p$, cada elemento de $G$ es generador de $G$. Luego $G/H \cong \mathbb{Z}_p$.

5. Si $(G : H) = m$, entonces $a^m \in H$ para todo $a \in G$.

Se tiene que $\operatorname{ord}(Hx) \mid m$, luego $Ha^m = H$, luego $a^m \in H$.

6. En $\mathbb{Q}/\mathbb{Z}$, cada elemento posee orden finito.

Sea $\mathbb{Q}/\mathbb{Z} = \{\frac{m}{n} + \mathbb{Z} \mid (m, n) = 1\}$. Luego para $\frac{m}{n} + \mathbb{Z}$ en el conjunto se cumple que $n(\frac{m}{n} + \mathbb{Z}) = m + n\mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}$.

## F. Cociente de un Grupo por Su Centro

El centro de un grupo $G$ es el subgrupo normal $C$ de $G$ consistiendo de todos los elementos de $G$ que conmutan con cada elemento de $G$. Suponer que el grupo cociente $G/C$ es grupo cíclico. Sease generado por $Ca \in G/C$. Probar:

1. Por cada $x \in G$, hay algún entero $m$ tal que $Cx = Ca^m$.

Como $G/C$ es cíclico, todo elemento $Cx$ con $x \in G$ es generado por una potencia de $Ca$, es decir, hay $m$ tal que $Cx = (Ca)^m = Ca^m$.

2. Por cada $x \in G$ hay algún entero $m$ tal que $x = ca^m$, donde $c \in C$.

Por el punto anterior, $Cx = Ca^m$, es decir, existen $c_1, c_2$ que: $c_1 x = c_2 a^m \iff x = c_1^{-1} c_2 a^m$, luego tomar $c = c_1^{-1} c_2$.

3. Para cualquier par de elementos $x, y \in G$, $xy = yx$.

Por punto anterior $x = ca^m$ y $y = c'a^n$, luego $xy = ca^m c' a_n$, como $c, c' \in C$ subgrupo normal, estos conmutan, es decir $ca^m c' a^n = c' a^n c a^m = yx$.

4. Luego Si $G/C$ es cíclico, se cumple que $xy = yx$, es decir, que $G$ es abeliano.

## G. Usando la Ecuación de Clase para Determinar el Tamaño del Centro

Sea $G$ un grupo finito. Un par de elementos $a, b \in G$ se dicen conjugados de uno y de otro si y solo si $a = xbx^{-1}$, para algún $x \in G$. Esto es una relación $a \sim b$ de equivalencia en $G$, la clase de equivalencia de cualquier elemento $a$ se dice *clase de conjugación*. Entonces $G$ es particionado en clases de conjugación. (El tamaño de cada clase de conjugación divide a $|G|$.)

Sean $S_1, S_2, \ldots, S_t$ las distintas clases de conjugación de $G$ y sea $k_1, k_2, , k_t$ sus respectivos tamaños, entonces $|G| = k_1 + k_2 + \cdots + k_t$ (Esta es la ecuación de clase de $G$)

Sea $G$ un grupo cual orden es una potencia de $p$, sease $|G| = p^k$. Sea $C$ el centro de $G$.

1. La clase de conjugación contiene a $a$ si y solo si $a \in C$.

Si $a \in [a]$, se tiene que $a \sim a$, es decir $a = xax^{-1}$ o equivalentemente $ax = xa$, por lo que $a \in C$.

2. Sea $c$ el orden de $C$. Entonces $|G| = c + k_s + k_{s+1} + \cdots + k_t$, donde $k_s, \ldots, k_t$ son los tamaños de todas las clases de conjugación de elementos $x \notin C$.

Se tiene que cada elelemtno de $C$ es su propia clase de equivalencia, es decir para $a \in C$, $[a]$ contiene solamente $a$, por lo que en conjunto todas estas representan $|C| = c$ clases de equivalencia, luego tomando la ecuación de clase,

$$|G| = k_1 + k_2 + \cdots + k_t$$

podemos sumar el tamaño de las clases de conjugación de elementos de $C$, (las cuales aportan indidividualmente 1 en tamaño) obteniendo $c$ y dejar la ecuación como:

$$|G| = c + k_s + k_{s+1} + \cdots + k_t$$

3. Por cada $i \in \{s, s+1, \ldots, t\}$, $k_i$ es una potencia de $|G|$.

Vimos en $13-I6$ que el número de conjugados es un factor de $(G : C)$, luego el tamaño de cada clase de conjugación es un factor de $|G|$, luego $k_i = p^{j_i}$.

4. Despejando la ecuación $|G| = c + k_s + \cdots + k_t$ para $c$, explicar por que $c$ es un múltiplo de $p$.

Se tiene que $c = |G| - (k_s + \cdots + k_t)$, luego $|G| = p^k$ y cada $k_i = p^{j_i}$, con $j_i \neq 0$, por lo que $p \mid c$.

*Podemos concluir por la parte* 4 *que* $C$ *debe contener más de un solo elemento e. De hecho* $|C|$ *es múltiplo de* $p$.

5. Probar: Si $|G| = p^2$, $G$ debe ser abeliano.

Si $|G| = p^2$, $|C| = p, p^2$ (no puede ser 1 ya que debe ser múltiplo de $p$!). Si $|C| = p^2$, entonces $G = C$ y entonces todo elemento conmuta, asi que es directamente abeliano.

Si $|C| = p$, entonces $|G/C| = p$, por lo que $G/C$ es cíclico, luego por ejercicio $F$, $G$ es abeliano.

6. Probar que si $|G| = p^2$, entonces $G \cong \mathbb{Z}_{p^2}$ o $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Si $G$ es cíclico, hay un elemento $a$ que genera todo el grupo, es decir, posee orden $p^2$ , luego $\langle a \rangle = \mathbb{Z}_{p^2}$

Si no es cíclico, por teorema de Lagrange hay un subgrupo de orden $p$, ciclico, luego $|G - H| = p$, por lo que también es cíclico, luego tomando el mapeo $f : G \to \mathbb{Z}_p \times \mathbb{Z}_p : f(ab = (a, b)$ obtenemos un isomorfismo.

## Inducción en $|G|$: Un Ejemplo

1. Si $\text{ord}(a) = tp$ (para algún entero $t$), ¿Cuál es el elemento de $G$ que posee orden $p$?.

$\text{ord}(a) = tp$, es decir $a^{tp} = e = (a^t)^p$. Luego $\text{ord}(a^t) = p$