C. Consecuencias Elementales del Teorema de Langrange

Sea G un grupo finito. Probar:

1. Si G posee orden n, entonces $x^n = e$ para todo $x \in G$

Sea x de orden m, entonces $\langle x \rangle$ posee m elementos, por lo que $m \mid n$, es decir $n = km$, luego $x^n = x^{km} = (x^m)^k = e^k = e$.

2. Sea G de orden pq con p, q primos. Entonces G es ciclico o cada elemento $x \neq e$ posee orden p o q.

Si $|G| = pq$, los subgrupos proios poseen p o q elementos, es decir para $H \subseteq G$, $|H| = p, q$, es decir, es cíclico, por lo que (sin pérdida de generalidad, tomando p) $h \in H \Longrightarrow h^p = e$. Si $|H| = pq$, entonces existe a tal que $a^{pq} = e$ y el orden de a es pq, por lo que $|\langle a \rangle| = pq$, entonces $\langle a \rangle = G$.

3. Sea G de orden 4. Entonces G es cíclico o cada elemento de G es su propio inverso. Concluir que cada grupo de orden 4 es abeliano.

Sea $|G| = 4$, entonces $|H| = 2$ por Lagrange, es decir es cíclico donde $h^2 = e \Longleftrightarrow h = h^{-1}$, luego $G = \{e, a, b, c\}$, pero $ab \neq a, b$ por cancelación, por lo que $c = ab$, luego por las mismas razones $c = ba$, es decir $ab = ba$. Luego si $|H| = 4$, $G = H$ y $G = \{e, a, a^2, a^3\}$ y $\varphi : \mathbb{Z}_4 \to G$ comprende un isomorfismo. Por lo que es abeliano.

4. Si G posee un elemento de orden p y un elemento de orden q, donde $(p, q) = 1$, entonces el orden de G es múltiplo de pq.

Se tiene que $p \mid |G|$ y $q \mid |G|$, luego p, q son coprimos, por lo que ninguno posee factores en común del otro, por lo que $pq \mid |G|$ es decir $|G| = pqk$.

5. Si G posee un elemento de orden k y un elemento de orden m, entonces $|G|$ es un múltiplo de $\operatorname{lcm}(k, m)$.

Si $(k, m) \geq 1$, $k \mid |G|$ y $m \mid |G|$, por lo que $|G|$ es múltiplo común de k y m, es decir $\operatorname{lcm}(k, m) \mid |G|$.

6. Sea p primo. En cualquier grupo finito, el número de elementos de orden p es múltiplo de $p - 1$

D. Más Consecuencias del Teorema de Lagrange

Sea G un grupo finito, sea H y K un subgrupo de G. Probar:

1. Suponer $H \subseteq K$. Entonces $(G : H) = (G : K)(K : H)$.

Por definición $(G : H) = \frac{|G|}{|H|}$, luego como $H \subseteq K$, $(K : H) = \frac{|K|}{|H|} \Longrightarrow |H| = \frac{|K|}{(K:H)}$.

Juntando todo: $(G : H) = \frac{|G|}{|K|} \cdot (K : H) = (G : K)(K : H)$.

2. El orden de $H \cap K$ es divisor común del orden de H y el orden de K.

Hay que probr que $H \cap K$ es subgrupo de H y K.

Sea $x \in H \cap K$, luego $x^{-1} \in H$ y $x^{-1} \in K$, por lo que $x^{-1} \in H \cap K$.
Sea $a, b^{-1} \in H \cap K$, luego $a, b^{-1} \in H$ y $a, b^{-1} \in K$, por lo que $ab^{-1} \in H, K$, luego $ab^{-1} \in H \cap K$.

Por Lagrange, $|H \cap K| \mid H, K$

3. Sea H de orden m y K de orden n, donde m, n son coprimos. Entonces $H \cap K = \{e\}$.

Como m, n son coprimos, por lo que el "único factor cómún" es el 1, por el punto anterior esto quiere decir que $|H \cap K| = 1$, luego $H \cap K = \{e\}$.

4. Suponer que H y K no son equivalentes y ambos poseen como orden el mismo número primo p. Entonces $H \cap K = \{e\}$

Como $|H \cap K| \mid p$ y $|H \cap K|$ es divisor propio del orden de los grupos, $|H \cap K| = 1$, luego $H \cap K = \{e\}$.

5. Suponer que H posee índice p y K posee índice q donde p y q son primos distintos, entonces el índice de $H \cap K$ es múltiplo de pq.

Como $(G : H) = p$ y $(G : K) = q$, por ley de torres (de grupos) $(G : H \cap K) = (G : K)(K : H \cap K)$ y $(G : H \cap K) = (G : H)(H : H \cap K)$, por lo que $p, q \mid (G : H \cap K)$, es decir $pq \mid (G : H \cap K)$.

6. Si G es grupo abeliano de orden n y m es un entero tal que m y n son coprimos, entonces la función $f(x) = x^m$ es un automorfismo de G.

Homomorfismo: $f(xy) = (xy)^m = x^m y^m = f(x)f(y)$.
Inyectividad: Sea $x^m = y^m$, luego $(xy^{-1})^m = e$, por ejercicio anterior, $m \mid n$, pero son coprimos, por lo que la única opcion es que $xy^{-1} = e$, es decir $x = y$.
Sobreyectividad: Directamente para todo x^m se puede definir x.

E. Propiedades Elementales de Cosets

Sea G un grupo y H un subgrupo de G. Sean a, b elementos de G. Probar:

1. $Ha = Hb$ si y solo si $ab^{-1} \in H$.

Si $Ha = Hb$, entonces $h_1 a = h_2 b$, luego $h_1 ab^{-1} = h_2$, es decir $Hab^{-1} = H$, $ab^{-1} \in H$. Las implicancias se leen en sus respectivas direcciones.

2. $Ha = H$ si y solo si $a \in H$.

Es la misma demostración anterior tomando $b = e$

3. Si $aH = Ha$ y $bH = Hb$, entonces $(ab)H = H(ab)$.

$abh_1 = a(h_2 b) = (h3a)b$, luego $(ab)H = H(ab)$

4. Si $aH = Ha$, entonces $a^{-1}H = Ha^{-1}$.

$a^{-1}h_1 = (h_1^{-1}a)^{-1} = (ah_2^{-1})^{-1} = h_2 a^{-1} \iff a^{-1}H = Ha^{-1}$

5. Si $(ab)H = (ac)H$, entonces $bH = cH$

$abh_1 = ach_2 \iff bh_1 = ch_2 \iff bH = cH$.

6. El número de cosets derechos de H es equivalente al número de cosets izquierdos de H.

Esto viene directo de las biyecciones $\varphi : H \to aH$ y $\phi : H \to Ha$ y de la definición de índice.

7. Si J es un subgrupo de G tal que $J = H \cap K$, entonces para cualquier $a \in G$, $Ja = Ha \cap Ka$. Concluir que si H y K poseen indice finito en G, entonces su intersección también posee índice finito.

Esto ya fué probado, la primera implicacia es trivial por doble contención, Luego la segunda implicancia es directa ya que el orden es divisor común del orden de H y K.

F. Estudio de Todos los Grupos de Seis Elementos

Sea G cualquier grupo de orden 6. Por Teorema de Cauchy G posee un elemento de orden 2 y un elemento b de orden 3. Por ejercicio anterior, los elementos:

$$\{e, a, b, b^2, ab, ab^2\}$$

son distintos, y como G posee solo seis elementos, estos son todos los elementos de G. Entonces ba es uno de los elementos, e, a, b, b^2, ab o ab^2.

1. Probar que ba no puede ser igual a e, a, b o b^2, entonces $ba = ab$ o $ba = ab^2$.

(i) $ba = e \iff ba^2 = a \iff b = a$. No
(ii) $ba = a \iff ba^2 = a^2 \iff b = e$. No
(iii) $ba = b \iff a = e$. No.
(iv) $ba = b^2 \impliedby b = a$.

Luego las únicas posibilidades son $ba = ab$ y $ba = ab^2$.

2. Si $ba = ab$. Probar que $G \cong \mathbb{Z}_6$

Si $ba = ab$, se tiene que a, b conmutan, entonces $\langle ab \rangle = \langle a \rangle \times \langle b \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

3. Si $ba = ab^2$. Probar que $G \cong S_3$

Como $a^2 = e$, $b^3 = e$ y $ba = ab^2 \iff a^{-1}ba^2 = b^2 = b^{-1}$, los elementos describen S_3. Luego $G \cong S_3$

G. Estudio de Todos los Grupos de 10 Elementos

Sea G un grupo cualquiera de orden 10.

1. Razonar como en el ejercicio anterior para mostrar que $G = \{e, a, b, b^2, b^3, b^4, ab, ab^2, ab^3, ab^4\}$ donde a posee orden 2 y b posee orden 5.

Sea $|G| = 10$, por teorema de Cauchy, G posee un elemento a de orden 2 y un elemento b de orden 5, luego todos los elementos de la forma a^ib^j, $0 \leq i \leq 2$, $0 \leq j \leq 5$ son diferentes al ser $2, 5$ coprimos.

2. Probar que ba no puede ser igual a e, a, b^2, b^3 o b^4.

(i) $ba = e \iff b = a^{-1} = a$. No
(ii) $ba = a \iff b = e$. No
(iii) $ba = b \iff a = e$. No
(iv) $ba = b^2 \iff a = b$. No
(v) $ba = b^4 \iff a = b^3$. No

3. Probar que si $ba = ab$, entonces $G \cong \mathbb{Z}_{10}$

G es generado por ab, como conmutan y 2 y 5 son coprimos, se tiene que es equivalente al producto directo:

$$\langle ab \rangle \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10}$$

4. Si $ba = ab^2$. Probar que $ba^2 = a^2b^4$ y concluir que $b = b^4$, lo que es imposible, pues b posee orden 5. Entonces $ba \neq ab^2$.

Si $ba = ab^2$, entonces $ba^2 = baa = ab^2a = abba = abab^2 = a(ba)b^2 = aab^2b^2 = a^2b^4$. Luego $ba^2 = a^2b^4$, $b = b^4$. Pero esto es imposible, pues b tiene orden 5. La suposición inicial es falsa.

5. Si $ba = ab^3$. Probar que $ba^2 = a^2b^3 = a^2b^4$. Concluir que $b = b^4$ y llegar a una contradicción.

$ba = ab^3 \implies ba^2 = ab^3a = ab^2(ba) = ab^2ab^3 = ab(ba)b^3 = abab^3b^3 = a(ba)b^6 = aab^3b^6 = a^2b^9$. Luego $ba^2 = a^2b^9 = a^2b^4$, por lo que $b = b^4$. Contradicción, la suposición inicial es falsa.

Probar que si $ba = ab^4$, entonces $G \cong D_5$ (D_5 siendo el grupo de simetrías del pentágono).

Si $a^2 = e$ y $b^5 = e$ y $ba = ab^4 \implies a^{-1}ba = b^{-1}$. Luego $G \equiv D_5$

0.1 H. Estudio de Todos los Grupos de Ocho Elementos

Sea G un grupo cualquiera de orden 8. Si G posee un elemento de orden 8, entonces $G \equiv Z_8$. Entonces asumir que G no posee elementos de orden 8, entonces todos los elementos $\neq e$ en G poseen orden 2 o 4.

1. Si cada $x \neq e$ en G posee orden 2, sea a, b, c los tres elementos. Probar que $G =, a, b, c, ab, bc, ac, abc\}$. Concluir que $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Todo elemento de la forma $a^ib^jc^k$ con $0 \leq i, j, k \leq 2$. Luego como todo elemento es de orden 2, en particular permutan entre sí ya que $a = a^{-1}$. Luego $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

2. Asumir que en Hb hay un elemento de orden 2 (sea b) este elemento). Si $ba = a^2b$, probar que $b^2a = a^4b^2$, entonces $a = a^4$, lo cual es imposible. Concluir que $ba = ab$ o $ba = a^3b$.

$b^2a = b(ba) = ba^2b = (ba)ab = a^2(ba)b = a^4b^2$, luego $b^2a = a^4b^2 \iff a = a^4$, luego $a = e$, pero esto es una contradicción ya que $|G| = 8$.

3. Sea b como en (2). Probar que si $ba = ab$, entonces $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Si $|a| = 4$ y $|b| = 2$ y todo elemento conmuta, luego $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$

4. Sea b como en la parte (2). Probar que si $ba = a^3b$, entonces $G \cong D_4$.

Si $|a| = 4$ y $|b| = 2$, luego si $ba = a^3b \iff bab^-1 = a^-1$, por lo que $G \cong D_4$

I. Elementos Conjugados

Si $a \in G$, un conjugado de a es cualquier elemento de la forma xax^{-1}, donde $x \in G$. Probar:

1. La relación "a es eqvuialente a el conjugado de b" es una relación de equivalencia en G (Escribir $a \sim b$ para denotar la relación)

(i) $a \sim a$: $a = xax^{-1} \iff x^{-1}ax = a$
(ii) Si $a \sim b$: $a = xbx^{-1} \iff x^{-1}ax = b$, entonces $b \sim a$
(iii) Si $a \sim b$ y $b \sim c$, $a = xbx^{-1}$ y $b = xcx^{-1}$, luego $a = x(xcx^{-1})x^{-1} = x^2c(x^2)^{-1}$.

Luego $\sim$ es una relación de equivalencia.

(*) Para cualquier elemento $a \in G$, el centralizador de a, denotado por C_a, es el conjunto de los elementos en G que conmutan con a, eso es:

$$C_a = \{x \in G : xa = ax\} = \{x \in G : xax^{-1} = a\}$$

2. Para cualquier $a \in G$, C_a es subgrupo de G.

(i) $x, y \in C_a$, entonces $a = xax^{-1}$, $a = yay^{-1}$, entonces $a = x(yay^{-1})x^{-1} = (xy)a(xy)^{-1}$, por lo que $xy \in C_a$
(ii) Sea $x \in C_a$, entonces $a = xax^{-1} \iff a = x^{-1}ax$, por lo que $x^{-1} \in C_a$

(iii) $a = ea = eae = eae^{-1}$, luego $e \in C_a$

3. $x{-}1ax = y^{-1}ay$ si y solo si xy^{-1} conmuta con a si y solo si $xy^{-1} \in C_a$

Si $x^{-1}ax = y^{-1}ay \Longleftrightarrow a = xy^{-1}ayx^{-1} = xy^{-1}a(x^{-1})^{-1}$, entonces xy^{-1} comuta con a y $xy^{-1} \in C_a$.

4. $x^{-1}ax = y^{-1}ay$ si y solo si $C_a x = C_a y$.

Como $x^{-1}ax = y^{-1}ay$, entonces $xy^{-1} \in C_a$, esto es equivalente a que $C_a xy^{-1} = C_a$, luego $C_a x = C_a y$.

5. Hay una correspondencia uno-a-uno entre el conjunto de todos los conjugados de a y el conjunto de todos los cosets de C_a.

Sea $\varphi : \{xax^{-1} \mid a \in G\} \to \{yC_a \mid y \in G\} : x^{-1}ax \mapsto xC_a$

Inyectividad: Si $xC_a = yC_a$, entonces $x^{-1}ax = y^{-1}ay$ por punto anterior
Sobreyectividad: Para $xC_a \in \{yC_a \mid y \in G\}$ siempre se puede definir $x^{-1}ax$ tal que $\varphi(x^{-1}ax) = xC_a$

Luego se tiene una correspondencia uno-a-uno (biyectividad).

6. El número de conjugados distintos de a es igual a $(G : C_a)$, el índice de C_a en G. Entonces el tamaño de cada clase es factor de G.

Como C_a subgrupo. Por teorema y por la biyección:

$\frac{|G|}{|C_a|} = |\{yC_a \mid y \in G\}| = (G : C_a)$

J. Grupo Actuando en un Conjunto

Sea A un conjunto y sea G cualquier subgrupo de S_A. G es un grupo de permutaciones de A, decimos que es un grupo actuando en el conjunto A. Asumir que G es un grupo finito, si $u \in A$, la órbita de u (con respecto a G) es el conjunto:

$$O(u) = \{g(u) \mid g \in G\}$$

1. Se define una relación $\sim$ en A por $u \sim v$ si y solo si $g(u) = v$. Probar que $\sim$ es una relación de equivaqlencia en A y que las órbitas son sus clases de equivalencia.

(i) $u \sim u \Longleftrightarrow g(u) = u = g^{-1}(u)$.
(ii) Si $x \sim y$, entonces $g(x) = y$, luego $g \in G$, por lo que $g^{-1} \in G$, luego $g^{-1}(g(x)) = x = g^{-1}(y)$, por lo que $y \sim x$.
(iii) Si $x \sim y$ y $y \sim z$: $g_1(x) = y$ y $g_2(y) = z$, luego $g_2(g_1(x)) = g_2(y) = z$. Por lo que $x \sim z$

Si $u \in A$, el estabilizador de u es el conjunto $G_u = \{g \in G : g(u) = u\}$, este es el conjunto de todas las permutaciones en G que dejan u fijo.

2. Probar que G_u es un subgrupo de G.

(i) $e \in G_u$, ya que $e \in G$ y $e(u) = u$
(ii) Sea $g_1, g_2 \in G_u$: $g_1(g_2(u)) = g_1(u) = u$
(iii) Sea $g \in G_u : g(u) = u \Longleftrightarrow g^{-1}(u) = u$

3. AAAAAAAAAAAAAAAA

4. Sea $f, g \in G$. Probar que f y g están en el mismo coset izquierdo de G_u si y solo si $f(u) = g(u)$.

$f, g \in xG_u \Longleftrightarrow fG_u = gG_u$, esto implica que $fg^{-1} \in G_u$, es decir $fg^{-1}(u) = u$, luego $f(u) = g(u)$.

5. Usar la parte 4 para mostrar que el número de elementos en $O(u)$ es igual a el índice de G_u en G:

Sea $\varphi : \{gG_u \mid g \in G\} \to O(u) : fG_u \mapsto f(u)$

Inyectividad: $f(u) = g(u) \iff fG_u = gG_u$ (punto anterior)
Sobreyectividad: Para $f(u) = v$ en $O(u)$, siempre se puede definir fG_u.

Luego, hay una bitección entre $\{gG_u \mid g \in G\}$ y $O(u)$, luego:

$$\frac{|G|}{|G_u|} = (G : G_u) = |\{gG_u \mid g \in G\}| = |O(u)|$$