MATE6201-0U1
Prof. Luis A. Medina
10.00 - 11.20
CNL-A-207

Algebra Moderna

Alec Zabel-Mena

Universidad de Puerto Rico, Recinto de Rio Piedras

29.08.2022

Lectura 1: Grupos y Subgrupos

Definición. Sea G un conjunto no vacío junto a una operación binaria $\cdot$. Decimos que el par $(G, \cdot)$ es un **grupo** si:

(1) $a \cdot b \in G$ para $a, b \in G$.

(2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para $a, b, c \in G$

(3) Existe un $e \in G$ tal que $a \cdot e = e \cdot a = a$ para toda $a \in G$.

(4) Para toda $a \in G$, existe una $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Si $a \cdot b = b \cdot a$ para toda $a, b \in G$, entoces decimos que G es un grupo **Abeliano**.

Ejemplo 1. (1) Los naturales $\mathbb{N}$ junto a la multiplicación se satisface los primeros tres axiomas, pero no es un grupo. De hecho, $\mathbb{N}$ forma un estructura llamado un “monoide”.

(2) El grupo mas pequeño es el conjunto $\{e\}$, que denotamos como $\langle e \rangle$. $\langle e \rangle$ es, trivialmente, un grupo Abeliano.

(3) Los enteros $\mathbb{Z}$ junto con adición $+$ forma un grupo Abeliano por la commutatividad de adición de los enteros.

(4) El conjunto $GL(n, \mathbb{R})$ de matrices $n \times n$ con entradas reales, nosingular forman un grupo con respecto a multiplicación de matrices. $GL(n, \mathbb{R})$ no es un grupo Abeliano.

(5) Sea S cualquier conjunto y $A(S)$ el conjunto de todas las funciónes 1–1 y sobre llevando elementos de S a elementos de S. Entonces $A(S)$ es un grupo no Abeliano con respecto a composición de funciónes, $\circ$. Si S tiene n elementos, entonces exscribimos $A(S) = S_n$. $A(S)$ también no se Abeliano ya que para funciónes cualquieras f, g, $f \circ g \neq g \circ f$.

Definición. Sea G un grupo. El **orden** de un grupo es su cardinalidad, y escribimos $\operatorname{ord} G = |G|$. Decimos que G es **finito** si $\operatorname{ord} G$ es finito; de lo contrario, G es **infinito**.

Definición. Sea G un grupo, y $a \in G$. El **orden** de a, denotado $\operatorname{ord} a$, es el menor entero positivo n tal que $a^n = e$ y escribimos $\operatorname{ord} a - n$. Si tal n no existe, entonces decimos que a es de orden **infinita**, y decimos que a es un elemento **torsión**.

Ejemplo 2. (1) Considera $\mathbb{C}^* = \mathbb{C}\backslash 0$, entonces $\mathbb{C}^*$ tiene orden infinita, note que si $\alpha = \exp(\frac{2i\pi}{5}) \in \mathbb{C}^*$, entonces $\alpha \neq 1$, para $j \neq 1, 2, 3, 4$, pero $\alpha^5 = 1$. Entonces $\operatorname{ord} \alpha = 5$.

(2) Considere $A \in GL(6, \mathbb{R})$ con la forma

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Entonces

$$A^3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

entonces, $A^3 = I$.

(3) En $\mathbb{R}^* = \mathbb{R}\backslash 0$, $\mathbb{R}^*$ es infinito, y $\operatorname{ord} 2$ es infinito.

Definición. Sea G un grupo y $H \subseteq G$ no vacío. Entonces decimos que H es un **subgrupo** de G si H es un grupo bajo la misma opearación de G. Escribimos $H \leq G$.

Ejemplo 3. (1) Considere $GL(n, \mathbb{R})$ y sea $SL(n, \mathbb{R})$ los elementos $A \in GL(n, \mathbb{R})$ tales que $\det A = 1$. Entonces $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.

(2) Sea $C(\mathbb{R})$ el conjunto de todas las funciones continuas sobre $\mathbb{R}$. Entonces $C(\mathbb{R})$ es un grupo bajo la suma de funciónes $+$. Sea $C^1(\mathbb{R})$ el conjunto de funciónes primer diferenciables continuas sobre $\mathbb{R}$ Es decir, que f' existe y es continua. Observe lo siguiente:

(a) $(f+g)' = f' + g'$

(b) $f' + (g+h)' = (f+g)' + h'$.

(c) $c' = 0$, entonces $0 \in C^1(\mathbb{R})$

(d) $f' - f' = -f' + f' = 0$.

Suponiendo que $f', g', h' \in C^1(\mathbb{R})$, son continuas, entonces vemos que los funciones de arriba tambien son continuas. Entonces $C'(\mathbb{R}) \leq C(\mathbb{R})$.

Lema 1. *Sea G un grupo y $H \subseteq G$ no vacío. Si tenemos que $ab \in H$, implicat que $ab^{-1} \in H$, entonces $H \leq G$.*

Proof. Como $H \neq \emptyset$, sea $a \in H$. Entonces $aa^{-1} = e \in H$. Luego, tambien tenemos qie $ea^{-1} = a^{-1} \in H$. Finalmente, tenemos que si $b \in H$, entonces $ab^{-1} \in H$, por lo tanto $b^{-1} \in H$, entonces $a(b^{-1})^{-1} = ab \in H$. ∎

Ejemplo 4. (1) Considere a los enteros pares $2\mathbb{Z}$. Sean $2n, 2m \in 2\mathbb{Z}$. Noten que $2n - 2m = 2(n-m) \in 2\mathbb{Z}$. Entonces $2\mathbb{Z} \leq \mathbb{Z}$.

(2) Si G es un grupo, entonces $\langle e \rangle$ y G son subgrupos de G. Llamamos a $\langle e \rangle$ el grupo **trivial**.

(3) Si G es un grupo, y $a \in G$, entonces el conjunto $\langle a \rangle = \{a^j : j \in \mathbb{Z}\}$ es un subgrupo de G, llamado el **subgrupo generado por** a.

(4) Si G es un grupo, y $a \in G$, entonces $C(a) = \{g \in G : ag = ga\}$ y $Z(G) = \{g \in G : ag = ga \text{ para toda } a \in G\}$ son subgrupos. Nota que $Z(G) = \bigcap C(a)$. Llamamos a $C(a)$ el **cnetralizador** de a y $Z(G)$ el **centro** de G.

(5) Sea G un grupo y $H \leq G$, y sea $a \in G$, entonces $a^{-1}Ha \leq G$. Llamamos a $a^{-1}Ha$ el **conjugado** de H **con respecto** a a.

Definición. Suponga que G y H son grupos. Un mapa $\phi : G \to H$ se llama un **homomorphismo** si para toda $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$. Si ϕ es $1-1$ y sobre, entonces lo llamamos un **isomorphismo**. Si ϕ es un isomorphismo, y $G = H$, entonces llamamos a ϕ un **automorphismo**.

Lectura 2: Grupos y Subgrupos

Ejemplo 5. (1) Considera $\mathbb{R}$ bajo la suma $+$ y $\mathbb{R}^+$ bajo la multiplicacón, $\cdot$. Sea $\phi : \mathbb{R} \to \mathbb{R}^+$ definido por $\phi : x \to \exp x$. Entonces ϕ es un homomorfismo, ya que

$\exp(x+y) = \exp x + \exp y$. De igual forma, nota que ϕ es $1-1$ y sobre, por lo tanto, existe inverso; de hecho, $\phi^{-1} = \log$, que tambien es un homomorfismo Pues, tenemos ϕ es un isomorphismo y que $\mathbb{R} \simeq \mathbb{R}^+$.

(2) Sea $\phi : GL(n, \mathbb{R}) \to \mathbb{R}^*$ dado por $\phi : A \to \det A$. Entonces ϕ es un homomorphismo ya que $\det AB = \det A \det B$. Nota que $GL(n, \mathbb{R})$ no es Abeliano, pero $\mathbb{R}^*$ si, por lo tanto $GL(n\mathbb{R}) \not\simeq \mathbb{R}^*$. Esto también dice que no existe inverso $\det^{-1}$. Esto nos dice que los homomorfismos solo preservan el estructura de grupos, pero nada mas de eso.

(3) Considere $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ dado por $\phi(m) = m \mod n$. Entonces $\phi(m+k) = (m+k) \mod n \equiv m \mod n + k \mod n = \phi(m) + \phi(k)$. Así que ϕ es un homomorfismo.

(4) Sea G y H grupos, y sea $\phi : G \to H$ un homomorfismo de G sobre H. Entonces si G es Abeliano, también lo es H. Nota que para $h, h' \in H$, exists $g, g' \in G$ con $\phi(g) = h$ y $\phi(g') = h'$. Entonces $hh' = \phi(g)\phi(g') = \phi(gg') = \phi(g'g) = \phi(g')\phi(g) = h'h$.

(5) Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $x \to 5x$. Entonces $\phi(x+y) = 5(x+y) = 5x+5y = \phi(x)+\phi(y)$.

(6) Suponga que G es Abeliano y defina $\phi : G \to G$ por la regla $\phi(a) = a^{-1}$. Entonces tenemos que $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$. Así que ϕ es un homomorfismo. Nota también que por la ley de inversos de elementos, que ϕ es sobre. También tenemos que ϕ es $1-1$ ya que $a^{-1} = b^{-1}$ implica que $a = b$, por unicidad de inversos. Por lo tanto ϕ es un automorfismo.

(7) Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $x \to x^2$. ϕ no es un homomorfismo ya que en general, $(x+y)^2 \neq x^2 + y^2$. Peros, si tomamos la mapa $\psi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ dado por la misma regla, entonces ψ es un homomorfismo.

Definición. Sea G y H grupos, y $\phi : G \to H$ un homomorfismo de G hacia H. Definimos el **kernel** de ϕ como el conjunto $\ker \phi = \{a \in G : \phi(a) = e'\}$ donde e' es la identitad de H. Definimos también la **imagen** del homoorphismo como el conjunto $\Im\phi = \phi(G) = \{\phi(a) : a \in G\}$.

Lema 2. *Sea G y H grupos y $\phi : G \to H$ un homomorfismo de G hacia H. Entonces $\ker \phi \leq G$ y $\phi(G) \leq H$.*

Proof. Nota por definicion qiue $\ker \phi \subseteq G$. Tambien tenemos que $e \in \ker \phi$ por el ley de homomorpfismo. Entonces $\ker \phi$ no es vacio. Ahora, sea $a, b \in \ker \phi$. Entonces, tenemos $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e'e' = e'$, pues $ab^{-1} \in \ker \phi$. ∎

Ejemplo 6. (1) Considere $\phi : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ dado por $m \to m \mod 12$. Entonces $\ker \phi = \langle 12m \rangle = 12\mathbb{Z}$. Tambien $\phi(\mathbb{Z}) = \mathbb{Z}/12\mathbb{Z}$; pues ϕ es sobre.

(2) Considere $\phi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ dado por $m \to 3m$. ϕ es un homomorfismo, y $\ker \phi = \{x \in \mathbb{Z}/12\mathbb{Z} : 3x \equiv_{12} 0\} = \{0, 4, 8\} = \langle 4 \rangle$. De igual manera, $\phi(\mathbb{Z}/12\mathbb{Z}) = \{0, 3, 6, 9\} = \langle 3 \rangle$.

(3) Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $m \to 5m$. Entonces $\ker \phi = \langle 5m \rangle = \langle 0 \rangle = 5\mathbb{Z}$. Nota que como ϕ es $1 - 1$, si $a \in 5\mathbb{Z}$, entonces $a = 5m \equiv_5 0$. Note tambien que $\phi(\mathbb{Z}) = 5\mathbb{Z}$, por lo tanto ϕ es sobre, asi que tenemos $\mathbb{Z} \simeq 5\mathbb{Z}$.

(4) Sea D_n el grupo dihedral sobre un polygano regular de n-vertices. Recuerda que $r^n = t^2 = e$ y que $tr^j = r^{n-j}t$. Considere la homomorfismo $\phi : D_8 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donde $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ es un grupo bajo la suma de productos directos. Entonces si $\phi(r) = (1, 0)$ y $\phi(t) = (0, 1)$ entonces tenemos que $\ker \phi = \langle r^2 \rangle$ y $\phi(D_8) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lectura 3: Grupos Cíclicos, Clases Laterales, y La Teorema de Lagrange.

Definición. Sea G un grupo. Definimos un **grupo cíclico** de G **generado** por un elemento $a \in G$ de ser el subgrupo de G $\langle a \rangle = \{aj : j \in \mathbb{Z}\}$. Llamamos a a el **generador** del grupo. Si $G = \langle a \rangle$ para algun $a \in G$, entonces decimos que G es **cíclico**.

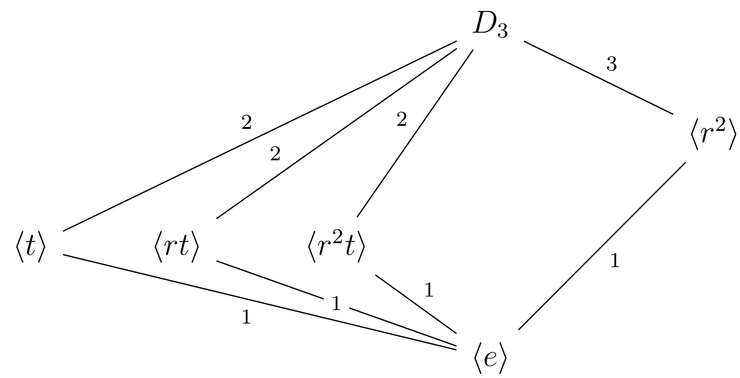
Ejemplo 7. (1) Considere el grupo $\langle A \rangle$, donde

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Nota que $A^4 = I$, entonces $\langle A \rangle = \{I, A, A^2, A^3\}$ es un subgrupo de orden $\operatorname{ord} A = 4$ del grupo $GL(4, \mathbb{R})$.

(2) Considere el grupo dihedral $D_3 = \{e, r, r^2, t, rt, r^t\}$ Los sobgrupos de D_3 son los sigu-

ientes en la reticulo de subgrupos sigueinte con los ordenes anotados:



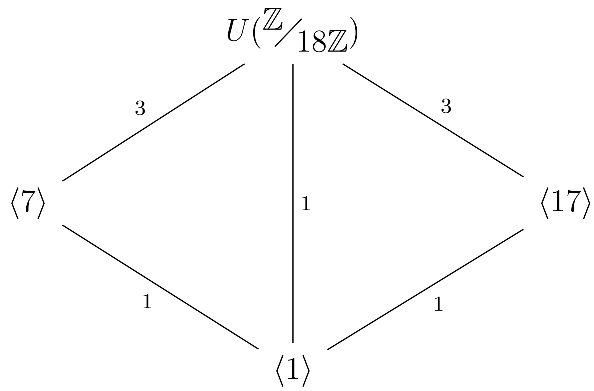
Teorema 3 (Teorema Fundamental de Grupos Cíclicos)**.** *Todo subgrupo de un grupo cíclico es cíclico. mas aún si $G = \langle a \rangle$ es un grupo cíclico de orden $G = n$, entonces G tiene un subgrupo de orden d por cada divisor d de n.*

Proof. Sea $G = \langle a \rangle$ y $H \leq G$. Observe qu si $H = \langle e \rangle$, entonces terminamos. Pues suponga que $H \neq \langle e \rangle$. Entonces existe un $h \in H$ con $h \neq e$. Es decir, que $h = a^j$ para alguna $j \in \mathbb{Z}$. Nota que si $j > 0$ entonces h es una potencia positiva de j; de igual manera, si $j < 0$ entonces $h^{-j} = (h^{-1})^j$ es una potencia psotiva de j. Es decir, H tiene potencias positivas. Por lo tanto, por el principio de buen orden, existe una potencia positiva mas peqeño, sea a^m. Sea $h \in H$, entonces $h = a^k$ para algún $k \in \mathbb{Z}$. Entonces por la teorema de división, existe $q, r \in \mathbb{Z}$ tales que $k = qm + r$ y $0 \leq r < m$. Entonces $a^k = a^{qm+r} = a^{qm}a^r i = (a^m)^q a^r$. Como $a^k \in H$, y $a^m \in H$, es necesario tener $(a^m)^q a^r \in H$ para preservar que $H \leq G$. Entonces, si $a^r \neq e$, tenemos una potencia de a mas pequeño que a^m, lo cual no puede pasar. Es decir $a^r = e$, y $a^k = (a^m)^q$. Es decir todo elemento de h es una potencia del elemento a^m, por lo tanto $H = \langle a^m \rangle$ es cíclico.

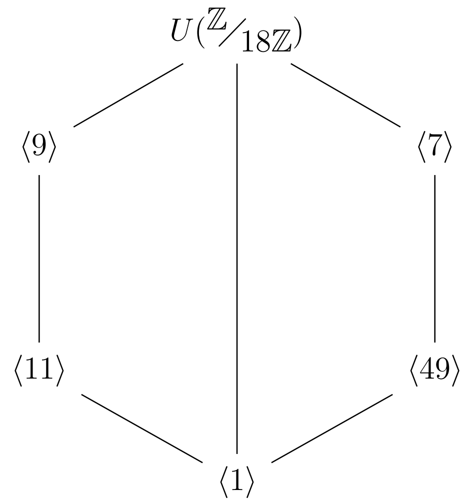
Ahora sea $\operatorname{ord} G = n$ y sea d un divisor positivo de n. Como $d|n$, entonces existe un $k \in \mathbb{Z}^+$ con $n = kd$. Ahora considere el subgrupo $\langle a^k \rangle$ Entonces sea $j \in \mathbb{Z}$ y considere $(a^k)^j$. Nota que $(a^k)^d = a^{kd} = a^n = e$, y si $0 < d < j$ entonces $(a^k)^j = a^{kj} \neq e$ por lo tanto $\operatorname{ord} a^k = d$, lo cual dice que $\operatorname{ord} \langle a^k \rangle = d$. ∎

Ejemplo 8. (1) Sea $U(\mathbb{Z}/18\mathbb{Z}) = \{1, 5, 7, 11, 13, 17\}$ el grupo de unidades dde $\mathbb{Z}/18\mathbb{Z}$. Observe que $U(\mathbb{Z}/18\mathbb{Z}) = \langle 5 \rangle$, y que $\operatorname{ord} U(\mathbb{Z}/18\mathbb{Z}) = \operatorname{ord} \langle 5 \rangle = 6$. Entonces $U(\mathbb{Z}/18\mathbb{Z})$

tiene los siguientes subgrupos mostrado en la siguiente reticulo con ordenes anotados:



(2) El grupo de unidades de $\mathbb{Z}/50\mathbb{Z}$, $U(\mathbb{Z}/50\mathbb{Z}) = \langle 3 \rangle$ tiene el siguiente retículo de subgrupos:



Teorema 4 (Criterio de Igualdad de Potencias)**.** *Suponga que G es un grupo. Sea $a \in G$, y sea $i, j \in \mathbb{Z}$ tales que $a^i = a^j$. Si a es de orden infinito, entonces $i = j$; de igual manera, si* $\operatorname{ord} a = n$, *entonces* $i \equiv j \mod n$.

Corolario. *Sí $j \in \mathbb{Z}^+$, entonces $\langle a^j \rangle = \langle a^{(j,n)} \rangle$, y* $\operatorname{ord} a^j = \frac{n}{(j,n)}$, *donde (j, n) es el maximo común divisor de j y n.*

Corolario. *Sí $G = \langle a \rangle$, y* $\operatorname{ord} G = \operatorname{ord} \langle a \rangle = n$, *entonces a^j es generador de G sí y solo sí $(j, n) = 1$. La cantidad de generadores de G está dado por $\phi(n)$ donde ϕ es la función Euler-ϕ.*

Ejemplo 9. Considere de nuevo $U(\mathbb{Z}/50\mathbb{Z}) = \langle 3 \rangle$. Tenemos que $\phi(50) = 20$, así que los generadores de $U(\mathbb{Z}/_{50\mathbb{Z}})$ son potencias 3^j donde $(j, n) = 1$. Es decir, los generadores son:

$$3^1 \qquad 3^3 \qquad 3^7 \qquad 3^9 \qquad 3^{11} \qquad 3^{13} \qquad 3^{17} \qquad 3^{19}$$

Teorema 5. *Sea G un grupo cíclico. Entonces $G \simeq \mathbb{Z}$ ó $G \simeq \mathbb{Z}/_{n\mathbb{Z}}$ para algún $n \in \mathbb{Z}^+$.*

Proof. Sea G un grupo cíclico. Suponga que G es infinito. Como los elementos de G son de la forma a^j para $j \in \mathbb{Z}$, considere el mapa $\phi : G \to \mathbb{Z}$ dado por $a^j \to j$. Entonces ϕ es un homomorfismo de G sobre $\mathbb{Z}$, ya que j corresponde a la potencia de uno de los infinito elementos de G. Mas aún, ϕ es 1–1, ya que $a^i = a^k$ implica que $i = k$. Es decir ϕ define un isomprfismo entre G y $\mathbb{Z}$.

De igaul forma, suponga que $\operatorname{ord} G = n$. Nota entonces que G tiene la forma $G = \{a^j : j \in \mathbb{Z}/_{n\mathbb{Z}}\}$. Define entonces $\phi : G \to \mathbb{Z}/_{n\mathbb{Z}}$ dado por $a^j \to j \mod n$. ϕ es un homomorfismo de G sobre $\mathbb{Z}/_{n\mathbb{Z}}$, por definición. ϕ tambien es 1–1 ya que $a^i = a^j$ implica $i \equiv j \mod n$. Esto define un isomorfismo de G sobre $\mathbb{Z}/_{n\mathbb{Z}}$. ■

Ejemplo 10. Considere $\mathbb{C}$ y sea $i \in \mathbb{C}$. Entonces $\langle i \rangle = \{1, i, -1, -i\}$ por multiplicación, así que $\operatorname{ord} \langle i \rangle = \operatorname{ord} i = 4$. Por la teorema anterior, esto hace $\langle i \rangle \simeq \mathbb{Z}/_{4\mathbb{Z}}$.

Definición. Sea G un grupo y $H \leq G$. Sí $a \in G$ definimos la **clase lateral por la derecha** de H **generado** por a de ser el conjunto $Ha = \{ha : h \in H\}$. De igual forma, definimos la **clase lateral por la izquierda** de H **generado** por a de ser el conjunto $aH = \{ah : h \in H\}$.

Definición. Sea G un grupo y $H \leq G$. Defina la relación $\equiv$ sobre G de la siguiente forma: $a \equiv b$ sí y solo sí $ab^{-1} \in H$. Llamamos a $\equiv$ **congruencia modulo** H. Escribimos $a \equiv b \mod H$, ó simplements $a \equiv_H b$.

Lema 6. *Sea G un grupo y $H \leq G$. Entonces la relación de congruencia modulo H sobre G es una relación de equivalencia.*

Proof. Como $H \leq G$, tenemos que $e = aa^{-1} \in H$, así que $a \equiv a \mod H$. Ahora, suponga que $a \equiv b \mod H$, entonces $ab^{-1} \in H$. Entonces $(ab^{-1})^{-1} = ba^{-1} \in H$, por lo tanto $b \equiv a \mod H$. Finalmente, sea $a \equiv b \mod H$, y $b \equiv c \mod H$. Entonces $ab^{-1}, bc^{-1} \in H$, así que $(ab^{-1})(bc^{-1}) = a(bb^{-1})c^{-1} = ac^{-1} \in H$, así que $a \equiv c \mod H$. ■

Corolario. *Los clases de equivalencia de $\equiv_H$ sobre G son precisamente los clases laterales por la izquierda aH.*

Proof. Exercise. ■

Corolario. *Tenemos que* $\operatorname{ord} H = |aH|$.

Proof. Considere la mapa $f : H \to aH$ dado por la regla $h \to ah$. A todo $ah \in H$ podemos asignarlo a h, así que f lleva H sobre aH. De igual forma, si $ah = ah'$ para $h, h' \in H$, entonces por cancelación $h = h'$. Es decir f es 1–1. ∎

Corolario. *La cantidad de clases laterales por la izquierda de H en G es la misma que la del los clases laterales por la derecha de H en G.*

Proof. Considere la mapa $f : aH \to Ha$. ∎

Definición. Sea G un grupo y $H \leq G$. Definimos el **indice** de H en G, denotado por $[G : H]$, de ser la cantidad de clases laterales de H en G.

Teorema 7 (La Teorema de Lagrange)**.** *Sea G un grupo y $H \leq G$. Entonces tenemos*

$$\operatorname{ord} G = [G : H] \operatorname{ord} H$$

Proof. Sabemos que $G = \bigcup_{a \in H} aH$ es una unión disjunta. Como $aH \cap bH = \emptyset$ sí y solo sí $a \neq b$, entonces tenemos repeticiones. Ahora suponga que el conjunto de clases laterales de H en G está indexado por J. Entonces tenmos que

$$\operatorname{ord} G = \sum_{j \in J} |a_j H| = \sum_{j \in J} \operatorname{ord} H = |J| \operatorname{ord} H$$

Nota que $|J| = [G : H]$. ∎

Corolario. *Si G y H son finito, entonces el orden de H divide el orden de G. Mas aún, tenemos que* $\frac{\operatorname{ord} G}{\operatorname{ord} H} = [G : H]$