Semana 11: El teorema de Lagrange

1. Grupos cíclicos

Definición 11.1. Sea G un grupo y sea a un elemento cualquiera de éste. *El orden de a* es el menor entero positivo m de forma que $a^m = e$. Si dicho entero existe, decimos que *a tiene orden finito* y escribimos $\text{ord}(a) = m$, en caso contrario decimos que *a tiene orden infinito*.

En el caso del grupo de las raíces m-ésimas, la definición anterior coincide con la que se provee. La ventaja, por supuesto, es tener ahora un concepto que aplica a cualquier objeto que pertenezca a un grupo. Podemos considerar algunos ejemplos sencillos.

Ejemplo. El conjunto de números complejos $\Gamma_4 = \{1, i, -1, -i\}$ junto al producto complejo forma un grupo. Además, i es un generador del grupo pues $i^0 = 1$, $i^1 = i$, $i^2 = -1$ e $i^3 = -i$. En ese caso podemos afirma que Γ_4 es un grupo cíclico de orden 4.

Ejemplo. Una transposición α sobre un conjunto con n elementos tiene orden 2. Esto se debe simplemente a que $\alpha^2 = (1)$ como hemos mostrado con anterioridad.

Ejemplo. En general, si α es k-ciclo del grupo S_n, este debe tener orden k. Uno de los ejercicios de la semana pasada muestra que k es el menor entero positivo de forma que $\alpha^k = (1)$ lo cual garantiza que k es precisamente el orden de acuerdo a la definición.

Definición 11.2. Sea G un grupo cualquiera y sea a un elemento de dicho grupo. Definimos *el subgrupo cíclico generado por a* como el subgrupo

$$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}.$$

Si además $G = \langle a \rangle$, decimos que G es *un grupo cíclico* y en ese caso a se dice *un generador del grupo*.

Aunque no hemos usado esa terminología para describirlos, ya conocemos varios grupos que resultan cíclicos.

Ejemplo. El grupo aditivo de los enteros, es cíclico y tiene como generador al entero 1, en símbolos $\mathbb{Z} = \langle 1 \rangle$. En particular éste es un grupo cíclico de orden infinito.

Ejemplo. El grupo aditivo de los enteros módulo m, también es cíclico con generador $[1]_m$. En símbolos $\mathbb{Z}_m = \langle [1]_m \rangle$. Los enteros módulo m, constituyen un ejemplo de grupo cíclico de orden finito con orden m.

Ejemplo. El grupo de unidades módulo 8, $\mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$, tiene la peculiaridad que sus elementos son también sus inversos. Esto implica que si $a \in \mathbb{Z}_8^*$, entonces

$$a^m = \begin{cases} a & \text{si } m \text{ es impar} \\ [1]_8 & \text{si } m \text{ es par} \end{cases}$$

mostrando que ningún elemento del grupo lo genera o, en otras palabras, no es cíclico.

Proposición 11.1. *Sea G un grupo finito y sea a un elemento del grupo con orden finito. Entonces, el orden de a es el número de elementos en $\langle a \rangle$.*

Demostración. Observemos primero que la lista de elementos a^0, a^1, ... contiene al menos un elemento repetido al ser el grupo finito. Tomemos k como el menor elemento repetido, i.e., $a^k = a^j$ para algún $0 \leq j < k$. Si $j \geq 1$, entonces $a^{k-j} = e$ pero $k - j < k$ contradiciendo el hecho de ser k el menor repetido. Luego, $j = 0$ por lo que $a^k = e$ y además, k debe ser el orden de a pues cualquier número menor provocaría una contradicción con la elección de k. Por lo anterior, el conjunto $H = \{a^0, a^1, \ldots, a^{k-1}\}$ contiene elementos distintos entre sí y además, $H \subseteq \langle a \rangle$. Basta entonces probar la otra contención y para mostrarla tomamos $a^j \in \langle a \rangle$ y expresando $j = qk + r$ donde $r < k$ y en ese caso

$$a^j = a^{qk} a^r = a^r \in H$$

lo cual muestra que $\langle a \rangle \subseteq H$ mostrando que

$$\langle a \rangle = \{a^0, a^1, \ldots, a^{k-1}\}.$$ ■

Lema 11.2. *Sea G un grupo cualquiera y sea a un elemento de orden m. Entonces, $a^n = e$ implica $m \mid n$.*

Demostración. Por el teorema de la división expresamos $n = qm + r$ con $0 \leq r < m$. En ese caso,

$$e = a^n = a^{qm+r} = a^{qm} a^r = a^r$$

pero si $r > 0$, entonces $r < \text{ord}(a)$ lo cual es contradictorio por tanto $r = 0$ o en otras palabras $m \mid n$, como buscábamos. ■

Teorema 11.3. *Sea G un grupo cíclico de orden m y sea a un generador de G. Entonces, a^k es un generador si y sólo si $(m, k) = 1$.*

Demostración. Supongamos que a^k es un generador, en ese caso $a \in \langle a^k \rangle$, entonces existe un entero s de forma que $a = a^{ks}$ o en otras palabras, $a^{ks-1} = e$. Ahora, según el lema 11.2, debemos tener que $m \mid (ks - 1)$, lo que implica que existe un entero t tal que $-mt + ks = 1$, implicando con esto que 1 es una combinación lineal de m y k. Como el máximo común divisor es la mínima combinación lineal positiva, entonces $(m, k) = 1$. Supongamos ahora que $(m, k) = 1$. Por la identidad de Bézout, expresamos $1 = mt + ks$ y en ese caso

$$a = a^{mt+ks} = a^{mt} a^{ks} = a^{ks}$$

y en consecuencia $a \in \langle a^k \rangle$. Por hipótesis $G = \langle a \rangle$ obteniendo de esto $G \subseteq \langle a^k \rangle$ y de esto podemos concluir $G = \langle a^k \rangle$. ■

2. Clases laterales

Definición 11.3. Sea G un grupo y sea H un subgrupo de este. Para dos elementos $a, b \in G$ decimos que *a es congruente con b módulo H*, en símbolos $a \equiv b \mod H$, si $a^{-1}b \in H$.

No es casualidad que la relación anterior tenga la misma terminología y símbolos que la congruencia módulo n en los enteros. En realidad, esta última es un caso particular: Considerando $\mathbb{Z}$ como un grupo aditivo, el conjunto H_m, que contiene a todos los múltiplos de m, resulta un subgrupo. En ese caso, podemos observar que la definición obliga a tener $a \equiv b \mod H_m$ si y sólo si $b - a \in H_m$ o lo que es lo mismo, $b - a$ es un múltiplo de m. De esto podemos concluir que $a \equiv b \mod m$ si y sólo si $a \equiv b \mod H_m$. Lo anterior indica que la congruencia módulo un subgrupo es una generalización de la congruencia modular y como ésta, resulta una relación de equivalencia.

Proposición 11.4. *La congruencia módulo un subgrupo es una relación de equivalencia.*

Demostración. Ejercicio 11.9 ■

Definición 11.4. Sea G un grupo, H un subgrupo de éste y a un elemento de G. Definimos *la clase lateral izquierda de H determinada por a* como el conjunto

$$aH = \{ah \mid h \in H\}.$$

Es importante observar que si el grupo no es conmutativo, entonces no tienen por que coincidir una clase lateral izquierda con una derecha.

Ejemplo. Considerando $\mathbb{R}^2$ como un grupo aditivo a través de la suma. Hemos visto que una recta l que pasa por el origen es un subgrupo. Además, las clases laterales de l están dadas por los rectas paralelas a l. Así, a cada clase de equivalencia le corresponde un número real α de forma que $\alpha + l$ representa a la clase.

Lema 11.5. *Para un elemento a de un grupo y un subgrupo H, se tiene que*

$$aH = \{x \mid x \equiv a \mod H\}$$

Demostración. Es importante notar que el conjunto a la derecha, es simplemente la clase de equivalencia de a bajo la congruencia módulo H. Por esto, la denotaremos simplemente $[a]$. Probaremos primero que $aH \subseteq [a]$: Si $g \in aH$, entonces para algún elemento $h \in H$ podemos expresar $g = ah$ y como H es un subgrupo, entonces

$$g^{-1}a = (ah)^{-1}a = h^{-1} \in H.$$

En ese caso, según la definición de congruencia $g \equiv a \mod H$ con lo que $g \in [a]$. Probaremos ahora que $[a] \subseteq aH$: Si $g \in [a]$, entonces $g \equiv a \mod H$ por lo que $a^{-1}g \in H$ o en otras palabras, $a^{-1}g = h$ para algún $h \in H$, lo anterior implica simplemente que $g = ah$ y por tanto $g \in aH$· ■

Según el lema anterior, las clases de equivalencia módulo H coinciden con las clases laterales de H. Eso quiere decir que las clases laterales forman una partición de G. En particular,

- Si $aH \cap bH \neq \varnothing$, entonces $aH = bH$.
- $\bigcup_{a \in G} aH = G$.

Lema 11.6. *Entre dos clases laterales izquierdas cualquiera existe una función biyectiva.*

Demostración. Consideremos dos clases laterales, aH y bH. Entonces, para cada elemento $ah \in aH$ asociamos el elemento $bh \in bH$. Esta asociación es sobreyectiva por definición. Además, si $bh = bh'$, entonces por ley de cancelación $h = h'$ y en consecuencia $ah = ah'$ mostrando con esto que la asociación propuesta es una función biyectiva. ■

El concepto de clases laterales toma especial relevancia en caso de que el número de clases laterales sea finito. Esto implica una particular definición.

Definición 11.5. Si el número de clases laterales de un subgrupo H es finito, a dicho número se le denomina *el índice de H en G* y a dicho índice lo denotaremos como $[G : H]$.

Ejemplo. Considerando el grupo aditivo de $\mathbb{Z}_8$, entonces el subconjunto $H = \{0_8, 4_8\}$ es un subgrupo. Las clases laterales de H resultan:

$$0_8 + H = \{0_8, 4_8\}$$

$$1_8 + H = \{1_8, 5_8\}$$

$$2_8 + H = \{2_8, 7_8\}$$

$$3_8 + H = \{3_8, 8_8\}$$

Esto quiere decir que hay 4 clases laterales por lo que el índice del subgrupo resulta

$$[\mathbb{Z}_8, H] = 4.$$

Puede parecer que el índice sólo cobra sentido en caso de tener grupos finitos, sin embargo, es posible obtener índices finitos que involucren grupos y subgrupos no finitos. A continuación ilustramos esta posibilidad.

Ejemplo. Considerando a $\mathbb{Z}$ como grupo aditivo, el conjunto $2\mathbb{Z}$ es un subgrupo. No es difícil notar que $2\mathbb{Z}$ tiene sólo dos clases laterales izquierdas: $0 + 2\mathbb{Z}$ y $1 + 2\mathbb{Z}$. Esto se puede ver como una consecuencia del lema 11.5 pues la relación indicada en este caso, coincide con la congruencia módulo 2. Esto en particular se traduce en tener

$$[\mathbb{Z}, 2\mathbb{Z}] = 2.$$

Ejemplo. En general, el conjunto $m\mathbb{Z}$ de los múltiplos de m, tiene exactamente m clases laterales izquierdas distintas por la misma razón que el ejemplo anterior. De esta manera

$$[\mathbb{Z}, m\mathbb{Z}] = m.$$

3. El teorema de Lagrange

El caso finito del índice puede resolverse de manera muy sencilla. A este resultado se le conoce como el teorema de Lagrange, el cual consigue expresar el índice de los subgrupos de un grupo finito sin mucho trabajo. Además de plantearlo, exploraremos algunos resultados inmediatos de dicho teorema.

Teorema 11.7. *Para un subgrupo H de un grupo finito G, el orden de H divide al orden de G.*

Demostración. Consideremos $a_1H, a_2H, \ldots, a_kH$ las diferentes clases laterales de H. Entonces,

$$G = \bigcup_{i=1}^{k} a_iH$$

y al ser todos las clases laterales disjuntas, lo anterior se traduce en tener

$$|G| = \left|\bigcup_{i=1}^{k} a_iH\right| = \sum_{i=1}^{k} |a_iH|$$

Ahora, como cada clase lateral tiene lo mismos elementos y $eH = H$ es una clase lateral, entonces $|a_iH| = |H|$ para todo $1 \leq i \leq k$. En ese caso,

$$|G| = k|H|.$$ ■

Corolario 11.8. *Para un subgrupo H de un grupo finito G se tiene*

$$|G| = [G : H]|H|$$

Demostración. Basta observar la última igualdad en la prueba del teorema anterior:

$$|G| = k|H|$$

observando que son k las distintas clases laterales del subgrupo H. ■

Ejemplo. Según el teorema de Lagrange, cualquier subgrupo de S_3 debe tener como su orden a un número que divida a 6. Esto quiere decir que las únicas posibilidades para el orden de los subgrupos son 1, 2, 3 y 6. Todos los subgrupos de S_3 distintos del trivial y el mismo grupo, están distribuídos de la siguiente forma:

- Tres subgrupos de orden 2: $\{(1), (1\ 2)\}$, $\{(1), (1\ 3)\}$ y $\{(1), (2\ 3)\}$.
- Un subgrupo de orden 3: $\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$.

El ejemplo anterior puede ser engañoso pues nos hace creer que existe un subgrupo para cualquier divisor del orden de un grupo. Sin embargo, el recíproco teorema de Lagrange es falso en general, i.e., no para todo divisor del orden de un grupo existe un subgrupo con ese orden.

Ejemplo. Vamos a considerar el subgrupo A_4 del grupo S_4 definido por las 12 permutaciones:

$$(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4) \text{ y } (2\ 4\ 3).$$

De esta definición, se desprende de manera inmediata que A_4 tiene 8 permutaciones de orden 3. Si H fuera un subgrupo de orden 6 del grupo A_4 y a un elemento de orden 3, entonces, como H tiene índice 2 sobre A_4, las clases laterales H, aH y a^2H no pueden ser todas distintas. Pero la igualdad de cualquiera de éstas, implica que $a \in H$. Lo anterior indica que H debe contener a todos los elementos de orden 3 lo cual es contradictorio pues su orden sería distinto. Entonces, A_4 no admite un subgrupo de orden 6 a pesar de ser un divisor del orden de A_4.

Aparte de este corolario, el cual es un resultado inmediato del teorema, existen algunos otros resultados que conectan algunas particularidades.

Corolario 11.9. *Para un grupo finito G y un elemento a, el orden de a divide al orden de G.*

Demostración. Basta considerar el subgrupo generado por a, digamos H. Hemos probado ya que el orden de H coincide con el orden del elemento a y según el teorema de Lagrange, el orden de H divide a G. Luego, el orden de a divide al orden de G. ■

Corolario 11.10. *Si G es un grupo finito y a un elemento de éste, entonces*

$$a^{|G|} = e.$$

Demostración. Según el corolario anterior $\text{ord}(a)$ divide a $|G|$ por lo que existe k de forma que $|G| = k \cdot \text{ord}(a)$. En ese caso,

$$a^{|G|} = a^{k \cdot \text{ord}(a)} = \left(a^{\text{ord}(a)}\right)^k = e.$$ ■

Corolario 11.11. *Si el orden un grupo es un número primo, entonces el grupo es cíclico.*

Demostración. Si G es un grupo con orden primo y H es un subgrupo de G entonces, según el teorema de Lagrange, el orden de H divide al de G, lo cual implica que el orden de H o es 1 o p por lo que $H = \{e\}$ o $H = G$. Ahora, como el orden es primo, debe ser mayor que 1 por lo que debe existir $a \in G$ de forma que $a \neq e$ y en ese caso, el subgrupo generado por a es un subgrupo distinto al trivial. Bajo el comentario anterior, se debe tener $G = \langle a \rangle$ mostrando con esto que G es un grupo cíclico. ■

Ejercicios

Ejercicio 11.1. Encuentra el orden de cada uno de los siguientes elementos (si es que existe).

- 5 en el grupo aditivo de $\mathbb{Z}_{12}$.
- $\sqrt{3}$ en el grupo aditivo de $\mathbb{R}$.
- $\sqrt{3}$ en el grupo multiplicativo de $\mathbb{R}$.
- $-i$ en el grupo multiplicativo de $\mathbb{C}$.

Ejercicio 11.2. Encuentra todos los elementos de los siguientes subgrupos

- El subgrupo de $\mathbb{Z}$ generado por 7.
- El subgrupo de $\mathbb{Z}_{24}$ generado por 15.
- El subgrupo aditivo de $\mathbb{R}$ generado por 7.
- El subgrupo multiplicativo de $\mathbb{C}$ generado por 5.
- El subgrupo multiplicativo de $\mathbb{C}$ generado por i.
- El subgrupo multiplicativo de $\mathbb{C}$ generado por $2i$.
- El subgrupo multiplicativo de $\mathbb{C}$ generado por $(1+i)/\sqrt{2}$.

Ejercicio 11.3. Si $a^{22} = 1$, ¿cuáles son los posibles ordenes de a?

Ejercicio 11.4. Muestra que el orden de a y el orden de a^{-1} coinciden.

Ejercicio 11.5. Muestra que el orden de ab es el mismo que el de ba.

Ejercicio 11.6. Encuentra todos los subgrupos de los siguientes grupos aditivos

- $\mathbb{Z}_6$
- $\mathbb{Z}_{13}$.
- $\mathbb{Z}_{60}$.
- $\mathbb{Z}_{12}$.
- $\mathbb{Z}_{48}$.
- $\mathbb{Z}_{55}$

Ejercicio 11.7. Para un primo p, muestra que el grupo aditivo de $\mathbb{Z}_p$ solamente admite los subgrupos triviales.

Ejercicio 11.8. Muestra que el grupo aditivo de $\mathbb{Z}_n$ tiene un número par de generadores cuando $n \geq 2$.

Ejercicio 11.9. Prueba la proposición 11.4.

Ejercicio 11.10. Sea G un grupo y sean a y b elementos de G. Si a tiene orden p y b orden q de forma que p y q son primos distintos, muestra que

$$\langle a \rangle \cap \langle b \rangle = \{e\}.$$

Ejercicio 11.11. Sea p un número primo. Muestra que cualquier homomorfismo $\phi\colon \mathbb{Z}_p \to \mathbb{Z}_p$ es, o un isomorfismo o el homomorfismo trivial.

Para entregar: Ejercicio 11.7

Referencias

[Her90] Herstein, I. N.: *Álgebra moderna*. Editorial Trillas, 2ª edición, 1990.

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.