AMPLIACIÓN DE MATEMÁTICAS

EL TEOREMA DE LAGRANGE.

El Teorema de Lagrange pone en relación la Teoría de Grupos con la divisibilidad entre números enteros.

Definición 1. *Dado un grupo* $(\mathbb{G}, *)$ *y un subgrupo de él* $N \trianglelefteq \mathbb{G}$*, se define la relación* $\sim_N$ *sobre* $\mathbb{G}$ *por*

$$g \sim_N g' \qquad \Leftrightarrow \qquad g * g'^{-1} \in N \qquad \text{para todo} \qquad g, g' \in \mathbb{G}.$$

Proposición 1. *Dado un grupo* $(\mathbb{G}, *)$ *y un subgrupo de él* $N \trianglelefteq \mathbb{G}$ *la relación* $\sim_N$ *es una relación de equivalencia.*

Demostración:

- $g * g^{-1} = e \in N$ (**reflexiva**).
- Si $g * g'^{-1} \in N$, entonces $(g * g'^{-1})^{-1} = g' * g^{-1} \in N$ (**simétrica**).
- Si $g * g'^{-1} \in N$ y $g' * g''^{-1} \in N$, entonces $g * g''^{-1} = g * g'^{-1} * g' * g''^{-1} \in N$ (**transitiva**)$\square$

Vamos a considerar el **conjunto cociente** respecto de esta relación $\sim_N$ y lo denotamos por

$$\mathbb{G}/\sim_N = \mathbb{G}/N.$$

Ejemplo 1. *Sea* $\mathbb{G} = \mathbb{Z}$ *un grupo, tomamos como subgrupo* $N = n\mathbb{Z}$*, el subgrupo de los múltiplos de* $n \in \mathbb{N}$*. En este caso la relación de equivalencia* $\sim_N$ *es la congruencia módulo n habitual*

$$k_1 \equiv k_2 \text{ mód } n \qquad \Leftrightarrow \qquad k_1 - k_2 \in n\mathbb{Z} \qquad \Leftrightarrow n | k_1 - k_2.$$

En este caso, como sabemos, el conjunto cociente es

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Observación 1. *Si la relación $\sim_N$ es una **congruencia**, ya sea por que el grupo es abeliano o por que el subgrupo sea normal, entonces el conjunto cociente $\mathbb{G}/N$ tiene una estructura natural de grupo. En lo que sigue, **no necesitamos** la estructura de grupo del conjunto cociente.*

Necesitamos estudiar alguna propiedad del conjunto cociente $\mathbb{G}/N$.

Observación 2.

- *Si $[g] \in \mathbb{G}/N$, entonces*

$$\begin{aligned}[g] &= \{h \in \mathbb{G} \ : \ h \sim_N g \ \} \\ &= \{h \in \mathbb{G} \ : \ h * g^{-1} \in N \ \} \\ = \{h \in \mathbb{G} \ : \ h = m * g \ \ &\textit{donde} \ \ m \in N \ \} = N * g.\end{aligned}$$

  La última igualdad solo es una notación.
- *Si $N * g_1, N * g_2 \in \mathbb{G}/N$, entonces o bien $g_1 \sim_N g_2$ y así $N * g_1 = N * g_2$ o bien $N * g_1 \bigcap N * g_2 = \emptyset$ (una relación de equivalencia produce clases de equivalencias disjuntas dos a dos).*
- *Lo anterior parece que tiene utilidad en los llamados "Métodos de descomposición inteligentes para **códigos** error-corrección".*

Definición 2. *Dado un grupo $(\mathbb{G}, *)$ y un subgrupo de él $N \trianglelefteq \mathbb{G}$, denotamos por $[\mathbb{G} : N]$ al **cardinal** del conjunto cociente $\mathbb{G}/N$, al cuál se le llama **índice** de N en $\mathbb{G}$.*

Lema 1. **A:** *Dado $g \in \mathbb{G}$, la siguiente aplicación es una **biyección***

$$\begin{array}{rccccc} \varphi & : & N & \to & N * g & \\ & & m & \to & \varphi(m) & = \ m * g. \end{array}$$

B: *Para todo $g_1, g_2 \in \mathbb{G}$, se tiene que*

$$Card\, N * g_1 = Card\, N * g_2 = Card\, N,$$

es decir toda clase de equivalencia respecto de la relación $\sim_N$ tiene el mismo número de elementos.

Demostración: Por la definición que tenemos de la clase de equivalencia $N * g$, φ esta bien definida como aplicación y claramente es **suprayectiva**. Solo falta ver que es inyectiva. Así

$$\varphi(m_1) = \varphi(m_2) \qquad \Leftrightarrow \qquad m_1 * g = m_2 * g \qquad \Leftrightarrow \qquad m_1 = m_2 * g * g^{-1} = m_2 \square$$

Ya está todo preparado para dar el Teorema de Lagrange.

Teorema 1. *(**de Lagrange**). Dado un grupo $(\mathbb{G}, *)$ **finito** y un subgrupo de él $N \trianglelefteq \mathbb{G}$, entonces el orden de N divide al orden de $\mathbb{G}$, ($|N| \,|\, |\mathbb{G}|$). De forma más precisa*

$$|N|[\mathbb{G} : N] = |G|$$

Demostración: Como la relación $\sim_N$ es de equivalencia, las clases de equivalencia que genera son disjuntas y así

$$\mathbb{G} = \bigcup_{g \in \mathbb{G}} N * g = \bigcup_{[g] \in \mathbb{G}/N} N * g$$

y por tanto

$$|G| = |N|[\mathbb{G} : N] \ \square$$

El **Teorema de Lagrange** tiene muchas aplicaciones. Veamos algunas de ellas.

Ejemplo 2. *Un grupo de orden 50 solo puede tener subgrupos de orden $1, 2, 5, 10$ o 25.*

Corolario 1. *Un grupo **finito** $\mathbb{G}$ tiene orden **primo** si y solo si no tiene subgrupos propios (es decir $\{e\}$ y $\mathbb{G}$ son los únicos subgrupos del grupo).*

Demostración:

- Si $|\mathbb{G}|$ es primo solo 1 y $|\mathbb{G}|$ dividen al orden de $\mathbb{G}$, luego por el Toerema de Lagrange solo $\{e\}$ y $\mathbb{G}$ pueden ser subgrupos de $\mathbb{G}$.
- Suponemos ahora que $|\mathbb{G}| = pn$, que el orden de $\mathbb{G}$ no es primo. Entonces por ser el grupo finito, para todo elemento $a \in \mathbb{G} \backslash \{e\}$, este elemento tendrá un orden $Ord(a) = k \leq |\mathbb{G}|$ (como vimos al estudiar grupos cíclicos). Entonces

  $$\{a, a^2, ..., a^k = e\} = A$$

  es un subgrupo de $\mathbb{G}$. Si $k < |\mathbb{G}|$, A es un subgrupo propio de $\mathbb{G}$. Si $k = |\mathbb{G}|$, entonces se toma $b = a^p$ y

  $$\{b = a^p, b^2, ..., (b^p)^n = a^{|\mathbb{G}|} = e\} = B$$

  es un subgrupo propio de $\mathbb{G}$ $\square$

Observación 3. *De lo anterior se deduce que todo **grupo de orden primo es cíclico**.*

Claro, si tomamos $a \in \mathbb{G}\backslash\{e\}$ y consideramos el orden del elemento, $Ord(a) = k$, se tiene que

$$\{a, a^2, ..., a^k = e\} = A$$

es un subgrupo de $\mathbb{G}$. Luego por ser de orden primo, $k = |\mathbb{G}|$. Lo que dice que a es un generador del grupo y por tanto éste es cíclico $\square$

Corolario 2. *Sea* $\mathbb{G} =< g >$ *un* ***grupo cíclico*** *de orden* m. *Entonces todos los generadores del grupo vienen dados por* g^k *donde* $m.c.d.(k, m) = 1$.

Demostración: $\mathbb{G} = \{g, g^2, ..., g^k, ..., g^m = e\ \}$ y así todos los elementos del grupo son de la forma g^k.

- Si $m.c.d.(k, m) = d > 1$, tenemos que $k = dn_1$, $m = dn_2$ con $n_2 < m$. Entonces

  $$(g^k)^{n_2} = g^{dn_1 n_2} = (g^m)^{n_1} = e.$$

  De lo que se deduce que $Ord(g^k) \leq n_2 < m$, luego g^k no es un generador del grupo.
- Si $m.c.d.(k, m) = d = 1$, por el Lema de Bezout existen $r, s \in \mathbb{Z}$ de modo que $rk + sm = 1$. Así

  $$g = g^{rk} * g^{sm} = (g^k)^r * (g^m)^s = (g^k)^r \in < g^k > .$$

  De lo que se sigue que $< g > \subseteq < g^k >$, y como el subgrupo generado por g es todo el grupo, $< g >= \mathbb{G}$, necesariamente $< g >=< g^k >$. Por tanto g^k es otro generador del grupo $\square$

Observación 4. *Del corolario anterior y de la definición de la función de Euler se deduce que el número de generadores de un grupo cíclico finito* G *es exactamente* $\phi(|G|)$.

Esta observación la recordaremos cuando hablemos de **elementos primitivos** de cuerpos finitos.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es