AMPLIACIÓN DE MATEMÁTICAS

GRUPOS CÍCLICOS.

Los grupos que pueden ser generados por un único elemento se llaman **Grupos Cíclicos**. Un único elemento como generador hace que sea fácil trabajar con ellos. Además, más adelante, veremos que los grupos multiplicativos de los cuerpos finitos son todos cíclicos, algo que tiene implicaciones en criptografía.

Definición 1. *Sea* $(\mathbb{G}, *)$ *un grupo.*

A: *Si existe* $\{g_1, g_2, ..., g_n\} \subseteq \mathbb{G}$*, un subconjunto finito de* $\mathbb{G}$*, de modo que*

$$< g_1, g_2, ..., g_n >= \mathbb{G}$$

se dice que $\mathbb{G}$ *está finitamente generado.*

B: *Si existe* $g \in \mathbb{G}$ *de modo que* $< g >= \mathbb{G}$*, se dice que* $\mathbb{G}$ *es un* ***grupo cíclico*** *y que* g *es un* ***generador*** *de* $\mathbb{G}$*.*

Ejemplos 1.

1. $< 2 >= 2\mathbb{Z}$*, así el grupo* $(2\mathbb{Z}, +)$ *es cíclico y 2 es un generador.*
2. $< 1 >= \mathbb{Z}$*.*
3. $(\mathbb{R}, +)$ *no está finitamente generado.*

Definición 2. *Sea* $(\mathbb{G}, *)$ *un grupo. Sea* $g \in \mathbb{G}$*. Se llama* ***orden*** *de* g *al* ***menor*** *entero* $k \in \mathbb{N}\backslash\{0\}$ *de modo que*

$$g^k = g * g * ...{}_{k-veces}... * g = e.$$

Escribiremos $Ord(g) = k$*.*

Puede haber elementos de un grupo con orden infinito (por ejemplo $2 \in (\mathbb{Z}, +)$) lo cuál no es muy interesante. En los **grupos** finitos (de orden finito) todos sus elementos tiene orden finito.

Proposición 1. *Sea* $(\mathbb{G}, *)$ *un grupo finito.*

- *Todo elemento* a *de* $\mathbb{G}$ *tiene orden finito.*
- *Si* $a \in \mathbb{G}$ *y* n *es su orden entonces* $\{a, a^2, ..., a^n = e\}$ *forma un subgrupo cíclico de* $\mathbb{G}$.

Demostración: Tomemos un elemento $a \in \mathbb{G}$ y consideramos el conjunto de las potencias del elemento a,

$$\{a, a^2, ..., a^k, ...\}$$

(solo operamos a con el mismo). Como $\mathbb{G}$ es finito estas potencias de a se tienen necesariamente que repetir. Sea $k, r \in \mathbb{N}$ de modo que

$$a^k = a^{k+r} \;\Leftrightarrow\; a^k = a^k * a^r,$$

ahora multiplicando por el inverso de a^k tenemos que $e = a^r$. Ahora solo hace falta tomar el menor de los $r \in \mathbb{N}$ con $a^r = e$ para conseguir el orden de a.

Consideremos ahora

$$\{a, a^2, ..., a^n = e\}.$$

Todas estas potencias son distintas, de los contrario existirían $k, r \in \mathbb{N}$ con $k + r \leq n$ de modo que $a^k = a^{k+r}$ y por el argumento anterior $a^r = e$. Lo cuál no es posible ya que $r < n$ y por definición de n (el orden de a) es el **menor** natural que verifica $a^n = e$.

Sean ahora $a^{k_1}, a^{k_2} \in \{a, a^2, ..., a^n = e\}$. Claramente $(a^{k_2})^{-1} = a^{n-k_2} \in \{a, a^2, ..., a^n\}$ y además

$$a^{k_1}(a^{k_2})^{-1} = a^{k_1}a^{n-k_2} = a^{k_1+n-k_2} \in \{a, a^2, ..., a^n = e\}$$

(claro, como $0 < k_1 + n - k_2 < 2n$, si $0 < k_1 + n - k_2 \leq n$ es clara la pertenencia anterior, si $k_1 + n - k_2 = n + r$ con $r < n$ entonces $a^{k_1+n-k_2} = a^{n+r} = a^n a^r = a^r$).

Por la caracterización de subgrupos vemos que $\{a, a^2, ..., a^n = e\}$ es un subgrupo de $\mathbb{G}$ de orden exactamente n ($|\{a, a^2, ..., a^n = e\}| = n$). Además, claramente $< a >= \{a, a^2, ..., a^n = e\}$, luego es un subgrupo cíclico $\square$

Propiedades de los **grupos finitos cíclicos** son las siguientes.

Proposición 2. *Si* $(\mathbb{G}, *)$ *es un grupo finito cíclico y* a *es un generador, entonces*

$$\mathbb{G} = \{a, a^2, ..., a^k, ..., a^{|\mathbb{G}|} = 1\}$$

(donde 1 es el elemento neutro y $a^k = a * a * a * ...{}_{k-veces}... * a$*).*

Demostración: Sea n el orden de a, que sabemos que existe por ser $\mathbb{G}$ finito. Por la proposición anterior sabemos que

$$< a >= \{a, a^2, ..., a^n = 1\} \subseteq \mathbb{G}$$

es un subgrupo cíclico de $\mathbb{G}$. Como a es un generador de $\mathbb{G}$, esto solo puede ocurrir si

$$n = |\{a, a^2, ..., a^n = 1\}| = |\mathbb{G}|\square$$

Proposición 3. *Todo subgrupo de un grupo cíclico finito es a su vez cíclico.*

Demostración: Sea $\mathbb{G} =< a >$, un grupo cíclico finito con a un generador. Sea S un subgrupo de $\mathbb{G}$ ($S \trianglelefteq \mathbb{G}$). Como $\mathbb{G} = \{a, a^2, ..., a^k, ..., a^{|\mathbb{G}|} = 1\}$, tomamos $a^{k_0} \in S$ de modo que

$$k_0 = \text{mín}\{k \ : \ a^k \in S \ \}.$$

Solo nos falta ver que $< a^{k_0} >= S$. Como S es subgrupo es claro que $< a^{k_0} > \subseteq S$. Sea ahora $a^k \in S$. Si $k_0|k$ es claro que $a^k \in < a^{k_0} >$. Si no, por el Teorema del Resto, $k = qk_0 + r$ con $r < k_0$ y así

$$a^k = a^{qk_0+r} = (a^{k_0})^q * a^r \qquad \Rightarrow ((a^{k_0})^q)^{-1} a^k = a^r \in S$$

lo cuál no es posible ya que por elección de k_0, éste es el menor natural de modo que al elevar a a él, ésta potencia pertenece a $S\square$

Proposición 4. *Si* S *es un subgrupo de un grupo cíclico finito* $\mathbb{G}$*, entonces el orden del subgrupo divide al orden del grupo (* $|S| \mid |\mathbb{G}|$*).*

Demostración: Sea a un generador de $\mathbb{G}$, con orden de a igual a $|\mathbb{G}|$ y sea a^{k_0} un generador de S con orden $|S|$. Entonces $(a^{k_0})^{|S|} = a^{k_0|S|} = 1$, como el orden de a es $|\mathbb{G}|$ se tiene que

$$k_0|S| = m.c.m(k_0, |\mathbb{G}|).$$

De la definición de máximo común múltiplo y su caracterización como el producto de los primos divisores comunes o no, se sigue que $|S|$ divide a $|\mathbb{G}|\square$

Esta propiedad de que el orden del subgrupo divide al orden del grupo es una propiedad general de los grupos finitos. En el caso de grupos cíclicos es más o menos sencillo de probar. En el caso general, el **Teorema de Lagrange**, nos va a llevar un poco más de trabajo.

Antes de avanar más, veamos algunos ejemplos del cálcuo de ordenes de elementos de un grupo.

Ejemplo 1. *Sea* $(\mathbb{Z}_5\backslash\{0\}, \times) = (\{[1], [2][3], [4]\}, \times)$.

Éste es un grupo multiplicativo, ya que 5 es primo y sus congruencias todas tienen inverso.

- [1] tiene orden 1 claramente.
- [2] tiene orden 4, ya que $[2^4] = [16] = [1]$ y $[2^2] = [4]$ y $[2^3] = [3]$. Luego [2] es un generador del grupo.
- [3] tiene orden 4, ya que $[3^4] = [81] = [1]$ y $[3^2] = [4]$ y $[3^3] = [2]$. Luego [3] es un generador del grupo.
- [4] tiene orden 2, ya que $[4^2] = [16] = [1]$.

Ejemplo 2. *Sea* $(\mathbb{Z}_9^*, \times) = (\{[1], [2], [4], [5], [7], [8]\}, \times)$.

Éste es un grupo multiplicativo como hemos visto anterioremente. Además, $|\mathbb{Z}_9^*| = 6$

- [2] tiene orden 6, ya que $[2^6] = [64] = [1]$ y $[2^2] = [4], [2^3] = [8], [2^4] = [16] = [7]$ y $[2^5] = [32] = [5]$. Luego [2] es un generador del grupo.
- [4] tiene orden 3, ya que $[4^3] = [64] = [1]$ y $[4^2] = [16] = [7]$.
- [5] tiene orden 6, ya que $[5^2] = [25] = [7]$ y $[5^3] = [125] = [8]$. Como el grupo es finito y cíclico (ya que 2 es un generador), entonces el orden de [5] tiene que dividir al del grupo; como este orden no es ni 2 ni 3, solo puede ser 6.
- [7] tiene orden 3, ya que $[7^2] = [14] = [5]$ y $[7^3] = [343] = [1]$.
- [8] tiene orden 2, ya que $[8^2] = [64] = [1]$.

Siempre encontramos que el orden de un elemento divide al orden del grupo, ya que el orden del elemento es igual al orden del subgrupo que engendra en el grupo.

Ejemplo 3. *Sea un grupo* $(\mathbb{G}, *)$ *y sean* $a, b \in \mathbb{G}$. *Hay que probar que*

1. *Si* $Ord(a) = n$ *y* $n = pq$, *entonces* $Ord(a^p) = q$.
2. $Ord(a^{-1}) = Ord(a)$ *y* $Ord(ab) = Ord(ba)$ *(*$\mathbb{G}$ *no tiene por que ser conmutativo).*
3. *Si* a *y* b *conmutan y tienen ordenes finitos primos entre si, entonces* $< a > \bigcap < b >= \{e\}$.

Demostración:

- En el primer caso, por definición de orden
$$e = a^n = (a^p)^q.$$
Si $Ord(a^p) = r < q$, entonces $e = (a^p)^r$ y se tendría que $Ord(a) \leq pr < n$, lo que contradice la hipótesis.
- $e = a^n$, despejando $(a^n)^{-1} = e$, como $(a^n)^{-1} = (a^{-1})^n$, deducimos que $Ord(a^{-1}) = n$.

  Por otro lado si $Ord(ab) = 1$, entonces a y b son inversos y $Ord(ba) = 1$. Ahora se procede por inducción.
- Si $c \in < a > \bigcap < b >$ se tiene que $c = a^n = b^k$ para ciertos $n, k \in \mathbb{N}$. c está dentro de grupos finitos y ciclícos, luego existe $Ord(c)$ con $Ord(c)|Ord(a)$ y $Ord(c)|Ord(b)$. Como ambos ordenes son primos entre si, se tiene que $Ord(c) = 1$ y así $c = e\square$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es