Apuntes de clase

José Antonio de la Rosa Cubero

Subgrupos, generadores y retículos

Definición 1 (Subgrupo)**.** Sea G un grupo. Un subgrupo de G es un subconjunto H de G no vacío que verifica:

1. Para cualesquiera $x, y \in H$, se tiene que $xy \in H$.
2. $1 \in H$.
3. Para todo $x \in H$ entonces $x^{-1} \in H$.

Por tanto H con el producto en G tiene estructura de grupo.
Cuando H sea subgrupo de G, lo escribiremos de la forma: $H \leq G$.
Ejemplos:

1. Para todo grupo G, $\{1\}$ y el propio G se llaman los subgrupos impropios de G. Al subgrupo $\{1\}$ se le llama también el subgrupo trivial.

   El resto de subgrupos, en caso de haberlos, se llaman subgrupos propios.
2. $\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$.
3. $\mu_n \leq \mathbb{C}^\times$ para todo $n \in \mathbb{N}$.
4. Si $m|n$, entonces $\mu_m \leq \mu_n$.

Proposición 1. *Sea G un grupo y $H \leq G$ si y solo si para todo $x, y \in H$ tenemos que:*

$$xy^{-1} \in H$$

Proposición 2. *Sea G un grupo finito. sea $\emptyset \neq H \subseteq G$. Entonces H es un supgrupo de G si y solo si $xy \in H$.*

Ejemplos:
Si tomamos D_n tenemos el subgrupo de las rotaciones o $\{1, r^k s\}$.
Tomando S_4, tenemos $\{(12)(34), (13)(24), (14)(23)\}$. Se llama el subgrupo de Klein de S_4.

Proposición 3. *Sea f un homomorfismo de grupos:*

1. *$H \leq G$, entonces $f(H) \leq G'$.*
2. *$H' \leq G'$, entonces $f^{-1}(H) \leq G$.*
3. *$\ker f \leq G$, $\operatorname{Im} f \leq G'$*
4. *f es monomorfismo si y solo si $\ker f = \{1\}$ y f es epimorfismo si y solo si $\operatorname{Im} f = G'$.*

Demostración. Sean $x', y' \in f(H)$, existen $x, y \in H$ tal que $x' = f(x)$, $y' = f(y)$.

$$x'(y')^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$$

$H' \leq G'$, entonces $f^{-1}(H) \subseteq G$ y como $f(1) = 1 \in H'$, sabemos que f^{-1} no es vacío. Sean $x, y \in f^{-1}(H')$,

$$f(x)f^{-1}(y)$$

□

Grupos alternados Si $(x_1, \ldots, x_n)$ es un r-ciclo en s_n, entonces

$$(x_1 \ldots x_r) = (x_1 x_2) \cdots (x_{r-1} x_r)$$

Todo ciclo se expresa como producto de transposiciones, pero dicha expresión no tiene por qué ser única. Incluso productos de distinta longitudes pueden dar el mismo ciclo.

Como consecuencia, todo elemento de s_n se expresa como producto de transposiciones, aunque no de manera única.

Teorema 1. *Sea $n \geq 2$ y $\alpha \in s_n$. Supongamos que $\alpha = \tau_1 \cdots \tau_s = \tau'_1 \cdots \tau'_r$ donde las taus son trasposiciones.*

Entonces $r \equiv s \mod 2$.

Demostración. Probamos primero para la identidad. Basta ver que id $= (12)(12)$ y por lo tanto que $r \equiv 0 \mod 2$. Supongamos otra descomposición. Supongamos cierto para r.

Elegimos $m \in \{1, \ldots, n\}$ que aparezca en alguna de las trasposiciones.

Sea τ_j la primera en la que aparezca m. $\tau_j = (mx)$. Aseguramos que $j < r$, porque si no

$$\mathrm{id}(x) = \tau_1 \cdots \tau_r(x) = \tau_1 \cdots \tau_{r-1}(m) = m \neq x$$

Asi $j < r$ y podemos considerar τ_{j+1}. $\tau_j\tau_j + 1 = (ab)(mc)$, en algunos casos porque conmuta, en otros por otros motivos. Donde c es igual a x o a y.

Repetimos el proceso, pero m no puede aparecer en la última transposición, en un número finito de pasos llegamos a que $\mathrm{id} = \tau_1' \cdots \tau_{r-2}$ y por hipótesis de inducción $r - 2 \equiv 0 \mod 2$ y $r \equiv 0 \mod 2$.

Por otro lado, si expresamos otro elemento de s_n como dos productos distintos de transposiciones, entonces podríamos poner la identidad como las transposiciones por el inverso del otro producto posible, con lo que queda $r + s \equiv 0 \mod 2$.

$$\mathrm{id} = \tau_1 \cdots \tau_r (\tau_1' \cdots \tau_s')^{-1}$$

□

Definición 2. Diremos que una permutación es par (impar) si se expresa como producto de un número par (impar) de transposiciones.

Ejemplo: la identidad es siempre par. En general un r-ciclo es par si r es impar y es impar si r es par.

Definición 3. Definimos que la signatura de una permutación como

$$s(\alpha) = \begin{cases} 1 & \text{si es par} \\ 1 & \text{si es impar} \end{cases}$$

Proposición 4. *La signatura es un homomorfismo entre s_n y $\mu_2 = \{1, -1\}$*

Definición 4. Sea $n \geq 2$, definimos el n-ésimo grupo alternado, que denotaremos por A_n, como:

$$A_n := \{\alpha \in s_n : s(\alpha) = 1\}$$

Es un subgrupo de s_n, ya que $A_n = \ker s$.

Proposición 5. *El orden del grupo alternado A_n es $\frac{n!}{2}$.*