Apuntes de clase

José Antonio de la Rosa Cubero

Ejemplo: Para todo $n \in \mathbb{N}$, $\mu_n = \langle \xi_1 \rangle$, es decir, las raíces de la unidad es un grupo cíclico.

Esto es debido a que $\xi_1^k = \xi_k$.

Otro ejemplo: Vamos a ver que $\mathbb{Z}_7^\times$ es cíclico:

$$\langle 2 \rangle = \{1, 2, 4\}$$

No ha habido suerte. Probemos con el siguiente:

$$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^\times$$

Otro ejemplo: Veamos que pasa con S_n:

$$\langle S_n \rangle = \{(12), (13), \ldots, (1n)\} = \{(12), (23), \ldots, (n-1n)\}$$

que se deducen de que:

$$(ij) = (1i) \cdots (ij)$$

y:

$$(1i)(ii+1)(1i) = (1i+1)$$

Proposición 1. *Sea G un grupo y X, Y subconjuntos de G. Entonces, si $H = \langle X \rangle$ y $K = \langle Y \rangle$. Entonces:*

$$H \bigwedge K = \langle X \cup Y \rangle$$

Proposición 2. *Sea f un homormofismo de grupos y X un subconjunto de G. Entonces:*

$$f(\langle X \rangle) = \langle f(X) \rangle$$

Proposición 3. *En particular, la imagen directa de un subgrupo cíclico de G es un subgrupo cíclico de G'.*

Proposición 4. *Sea f un homomorfismo de grupos y X' subconjunto de G'. Entonces:*

$$\langle f^{-1}(X') \rangle = f^{-1}(\langle X' \rangle)$$

Definición 1. Sea G un grupo y H un subgrupo. Definimos dos realciones binarias asociadas a H como sigue.

$$x \sim_I y \iff y^{-1}x \in H$$

y

$$x \sim_D y \iff xy^{-1} \in H$$

Proposición 5. *Tenemos que* $\sim_I, \sim_D$ *son relaciones de equivalencia en* G.

Definición 2. Denotaremos por G/H al conjunto cociente de G por $\sim_I$ y H/G al conjunto cociente de G por $\sim_D$.

$$[x]_I = \{y \in G : y \sim_I x\} = \{y \in G : x^{-1}y \in H\} = xH$$

donde la última igualdad es fácil demostrarla por doble inclusión.

Del mismo modo $[x]_D = Hx$.

Definición 3. A la clase de equivalencia xH (Hx) se le llama la clase lateral de x por la izquierda (derecha) módulo H.

Tenemos:

$$G/H = \{xH : x \in G\}$$

Y:

$$H/G = \{Hx : x \in G\}$$

Proposición 6. *1.*

$$x \in xH, x \in Hx$$

2.

$$xH = yH \iff y^{-1}x \in HHx = Hy \iff xy^{-1} \in H$$

3.

$$xH \neq yH \iff xH \cap yH = \emptyset, Hx \neq Hy \iff Hx \cap Hy = \emptyset$$

4. Tanto G/H *como* H/G *son particiones de* G.

5. Los conjuntos xH, Hx *son biyectivos a* H.

6. Existe una biyección entre G/H *y* H/G.

Demostración. Del 1 al 4 son propiedades generales de conjuntos.

La propiedad 5, se demuestra tomando $t(h) := xh$ (o $s(h) := hy$) y viendo que es biyectiva.

Sea $\lambda(xH) := Hx^{-1}$. □

Definición 4. Sea G un grupo finito y H un subgrupo de G. Definimos el índice de H en G como el cardinal del conjunto G/H (que coincide con el de H/G). Lo denotaremos por $[G : H]$. Es decir, el número de clases a la izquierda (derecha) módulo H.

Teorema 1 (de Lagrange)**.** *Sea G un grupo finito y H un subgrupo. Entonces:*

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

Demostración. Supongamos $[G : H] = r$ y sea

$$G/H = \{x_1H, \ldots, x_rH\}$$

por el apartado 4 de la proposición anterior, todas esas clases forman una partición. Luego:

$$G = \bigcup_{i=1}^{r} x_iH$$

y $x_iH \cap x_jH = \emptyset$, luego:

$$|G| = \sum |x_iH| = \sum |H| = r\,|H|$$

□

Ejemplo: Tomamos el grupo S_3 y $A_3 \leq S_3$.

$$|S_3/A_3| = [S_3 : A_3] = \frac{|S_3|}{|A_3|} = 2$$

$$S_3/A_3 = \{A_3, (12)A_3\}$$

$$A_3/S_3 = \{A_3, A_3(12)\}$$

Corolario 1. El orden de $H\,\mathrm{Sub}(G)$ divide al orden de G.

Definición 5 (Orden de un elemento)**.** Sea G un grupo y $a \in G$. Definimos el orden de a, que denotaremos por $\mathrm{ord}(a)$ como el menor entero positivo tal que $a^n = 1$.

Si no existe $n > 0$ tal que $a^n = 1$, diremos que a tiene orden infinito.

Si G es un grupo finito, todos sus elementos tienen orden finito.
Si $a^n = a^m$, entonces, $a^{|n-m|} = 1$.
Además:

$$\operatorname{ord}(a) = 1 \iff a = 1$$

En $\mathbb{Z}$, el único elemento de orden finito es 0.
En μ_n, ξ_1 tiene orden n.
Si $\alpha = (x_1 \dots x_k) \in S_n$ entonces $\operatorname{ord}(\alpha) = k$
En Q_2:

$$\operatorname{ord}(i) = \operatorname{ord}(j) = \operatorname{ord}(k) = 4$$

$$\operatorname{ord}(-i) = \operatorname{ord}(-j) = \operatorname{ord}(-k) = 4$$

$$\operatorname{ord}(-1) = 2$$

$$\operatorname{ord}(1) = 1$$

En D_4:

$$\operatorname{ord} sr^k = \operatorname{ord}(r^2) = 2$$

para $k \in \{0, \dots, 3\}$:

$$\operatorname{ord}(r) = \operatorname{ord}(r^3) = 4$$

$$\operatorname{ord}(1) = 1$$

Luego no es isomorfo a Q_2.