

# Apuntes de clase

José Antonio de la Rosa Cubero

**Proposición 1.** 1.  $x^m = 1$  si y solo si  $n|m$ .

2.  $\text{ord}(x^k) = n/\text{gcd}(n, k)$

3.  $x^k$  es un generador de  $C_n$  si y solo si  $\text{gcd}(n, k) = 1$ .

4. El número de generadores distintos de  $C_n$  es exactamente  $\varphi(n)$ , la función totiente de Euler.

**Proposición 2.** Sean  $a, b \in G$  dos elementos de un grupo que conmutan entre sí, esto es, para los que  $ab = ba$ , y de manera que sus órdenes son primos relativos, esto es  $\text{gcd}(\text{ord}(a), \text{ord}(b)) = 1$ . Se tiene:

1.  $\langle a \rangle \cap \langle b \rangle = 1$ .

2. Demostrar que  $\text{ord}(ab) = \text{ord}(a) \text{ord}(b)$ .

**Teorema 1.** Sea  $n \geq 2$  y  $\alpha, \beta \in S_n$  dos permutaciones disjuntas. Entonces:

$$\text{ord}(\alpha\beta) = \text{mcm}(\text{ord}(\alpha), \text{ord}(\beta))$$

**Corolario 1.** Como consecuencia, si  $\alpha \in S_n \setminus \{\text{id}\}$ , entonces el orden es el mínimo común múltiplo de las longitudes de los ciclos disjuntos en que descompone.

*Demostración.* Teomemos  $\alpha, \beta \in S_n$  permutaciones disjuntas. Veamos que sus potencias también son disjuntas.

Supongamos que  $\alpha^k(x) \neq x$ . Entonces  $\alpha(x) \neq x$  y  $\beta(x) = x$  y finalmente  $\beta^k(x) = x$ .

Sean  $r = \text{ord}(\alpha)$ ,  $s = \text{ord}(\beta)$  y  $m = \text{mcm}(r, s)$  y

$$(\alpha\beta)^m = \alpha^m \beta^m = \text{id}$$

Sea  $k$  tal que  $\text{id} = (\alpha\beta)^k = \alpha^k \beta^k$ . Como  $\alpha^k$  y  $\beta^k$  son disjuntas, entonces  $\alpha^k = \text{id} = \beta^k$ .

Finalmente eso implica que tanto  $r$  como  $s$  dividen a  $k$  y por tanto  $m = \text{mcm}(r, s) | k$  □

**Proposición 3.**  $G$  generado por  $a \neq b$  tal que el orden de ambos elementos es 2 y conmutan.

Entonces  $G = \{1, a, b, ab\}$  y  $G$  es isomorfo al grupo de Klein.

**Proposición 4** (Clasificación de los grupos de orden 4 y 6). Si  $G$  es un grupo de orden 4, entonces es isomorfo a  $K$  o a  $C_4$ . Si  $G$  es un grupo de orden 6 entonces es isomorfo a  $C_6$  o a  $D_3$ .

*Demostración.* Si hay un elemento de orden 4, entonces  $\langle a \rangle = G$  y por tanto es isomorfo al grupo cíclico.

El siguiente caso es que no se verifique lo anterior. Todos los elementos tienen orden 2. Entonces  $G$  es abeliano. Elegimos dos elementos  $a, b$  distintos entre sí y del 1. Sea  $H = \langle a, b \rangle$ . Entonces  $H$  es el grupo de Klein por la proposición anterior. Como tiene orden 4,  $G = H$ .

$a \in G$  con  $|G| = 6$ . Y  $\text{ord}(a) \in \{2, 3, 6\}$ .

Primer caso,  $G$  es abeliano. No todos los elementos de  $G$  tienen orden 2, porque si no  $H = \langle a, b \rangle \leq G$  sería isomorfo al propio  $G$  pues  $a^2 = b^2 = 1$  y  $ab = ba$ , pero el orden de  $H$  es 4.

Así  $\text{ord}(a) = 6$  o  $\text{ord}(a) = 3$ . En el primer caso,  $\langle a \rangle = G$  y por tanto es cíclico.

Supongamos  $a$  de orden 3. Sea  $H = \{1, a, a^2\} \leq G$ .

$$[G : H] = \frac{|G|}{|H|} = \frac{6}{3} = 2$$

entonces:

$$H/G = \{H, Hb\}$$

con  $b \in G$  tal que  $b \notin H$ .  $G = H \cup Hb = \{1, a, a^2, b, ab, a^2b\}$ .

Han llamao a la puerta y me he perdido. □

Descripción de los subgrupos de  $G$ , para algunos grupos de orden finito.

**Teorema 2.** 1. Para cada divisor positivo  $d$  de  $n$ ,  $\langle x^{n/d} \rangle$  tiene orden  $d$ . Por tanto  $\langle x^{n/d} \rangle = C_d$ .

2. Sea  $H$  un subgrupo propio de  $C_n$ . Sea  $s = \min\{r \geq 1 : x^r \in H\}$ . Entonces  $s|n$  y  $H = \langle a^s \rangle$ .

3. Hay una biyección  $(d \mapsto \langle x^{n/d} \rangle)$  entre los divisores de  $n$  y los subgrupos de  $C_n$ .

4.  $d_1|d_2$  si y solo si  $\langle x^{n/d_1} \rangle \leq \langle x^{n/d_2} \rangle$