Apuntes de clase

José Antonio de la Rosa Cubero

Definición 1 (Centro de un grupo)**.** Sea G un grupo. Se define su centro como

$$Z(G) = \{a \in G : ax = xa \forall x \in G\}$$

Proposición 1. *El centro de un grupo es siempre un subgrupo normal en G.*

Observación 1. $Z(G)$ es abeliano siempre.

Observación 2. G es abeliano si y solo si coincide con su centro.

Proposición 2. *A_3 coincide con su centro y $Z(A_n) = \{\mathrm{id}\}$ para $n > 3$.*

Demostración. $A_3 = \{\mathrm{id}, (1 \quad 2 \quad 3), (1 \quad 3 \quad 2)\} = \langle (1 \quad 2 \quad 3) \rangle$ es abeliano, luego coincide con su centro.

Sea $n > 3$ y $\sigma \in A_n \setminus \{\mathrm{id}\}$. Existe un α con el que no conmuta. Existen i, j distintos tales que $\sigma(i) = j$. Elegimos k, l distintos tales que tampoco coinciden con i o j. Podemos elegirlos porque $n \geq 4$. Sea $\alpha = (j \quad k \quad l) \in A_n$. Entonces

$$\sigma\alpha(i) = \sigma(i) = j$$
$$\alpha\sigma(i) = \alpha(j) = k$$

Luego $\sigma\alpha \neq \alpha\sigma$, y por tanto $\sigma \notin Z(A_n)$, y como era arbitrario $Z(G) = \{\mathrm{id}\}$. □

Proposición 3. *Demostrar que $Z(D_n) = \{1, r^m\}$ si n es par y $Z(D_n) = \{\mathrm{id}\}$ si n es impar.*

Demostración.

$$D_n = \langle r, s : r^n = 1 = s^2, sr = r^{-1}s \rangle = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$$

Observamos que $r^k s \notin Z(D_n)$.

$$(r^k s)r = r^{k-1}s \neq r^{k+1}s = r(r^k s)$$

puesto que si no tendríamos que $\mathrm{ord}(r) = 2 \neq n$.

¿Cuándo $r^k \in Z(D_n)$? Evidentemente, conmuta con r^j para cualquier j. Veamos cuando conmuta con las simetrías $r^j s$. Esto ocurre cuando

$$r^{k+j} = r^{j-k}$$

y esto es lo mismo que

$$r^k = r^{-k}$$

o lo que es lo mismo, que $(r^k)^2 = 1$, es decir, el orden es 2.

Como $\text{ord}(r^k) = \frac{n}{\gcd(n,k)}$, y por tanto $n = 2\gcd(n,k)$ y n ha de ser par.

En el caso que $n = 2m$ sea par $m = \gcd(2m, k)$, tenemos que $k = m$ y por tanto $Z(D_{2m}) = \{\text{id}, r^m\}$.

□

Definición 2 (Automorfismo)**.** Sea G un grupo. Un automorfismo de G es un isomorfismo $f : G \longrightarrow G$.

$$\text{Aut}(G) = \{f : G \longrightarrow G : f \text{ es isomorfismo}\}$$

$\text{Aut}(G)$ con la composición es un grupo.

Proposición 4. *Sea C_n el grupo cíclico de orden n. Existe un isomorfismo entre $\mathbb{Z}_n^\times \cong \text{Aut}(G)$.*

Demostración. Si $\theta : C_n \longrightarrow G$ es un homomorfismo de grupos con $\theta(x) = g$, entonces $\text{ord}(g)|n$ y $\theta(x^k) = g^k$.

La segunda igualdad es obvia por definición de homomorfismo.

Puesto que θ es un hmomorfismo:

$$1 = \theta(1) = \theta(x^n) = \theta(x)^n = g^n$$

Por tanto g tiene orden finito y además $\text{ord}(g)|n$.

Demostremos que para cada $g \in G$ tal que $\text{ord}(g)|n$ existe un único homomorfismo de grupos $\theta_g : C_n \longrightarrow G$ tal que $\theta_g(x) = g$.

La unicidad es obvia, dado que es el grupo cíclico.

Veamos la existencia. Definimos $\theta_g : C_n \longrightarrow G$ por $\theta_g(x^k) = g^k$ para $0 \leq k < n$. Veamos que θ_g es un homomorfismo. Hay que ver que

$$\theta_g(x^k x^r) = \theta_g(x^k)\theta_g(x^r)$$

Vemos que:

$$\theta_g(x^k x^r) = \theta_g(x^s) = g^s = g^t$$

donde s es el resto de dividir $k + r$ entre n. t es el resto de dividir s entre $\text{ord}(g)$.

$$\theta_g(x^k)\theta_g(x^r) = g^k g^r = g^u$$

donde u es el resto de dividir $k + r$ entre $\text{ord}(g)$.

Basta comprobar que $u = t$, que no es difícil usando propiedades de la división entera.

Sea $g \in G$ tal que $\text{ord}(g)|n$. Veamos que θ_g es monomorfismo si y solo si $\text{ord}(g) = n$.

Supongamos que θ_g es monomorfismo.

$$\ker(\theta_g) = \{1\}$$

Sea t el orden de g, entonces:

$$1 = g^t = \theta_g(x^t)$$

tenemos que

$$x^t \in \ker(\theta_g) = \{1\}$$

□