Apuntes de clase

José Antonio de la Rosa Cubero

Proposición 1. *Sea C_n el grupo cíclico de orden n. Existe un isomorfismo entre $\mathbb{Z}_n^\times \cong \mathrm{Aut}(G)$.*

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

Demostremos que para cada $g \in G$ tal que $\mathrm{ord}(g)|n$ 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 $\mathrm{ord}(g)$.

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

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

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

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

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

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

Sea $\mathrm{ord}(g) = n$ y $x^k \in \ker(\theta_g)$. Por tanto $n|k$ y entonces $k = 0$ y el núcleo es el trivial, luego θ_g es un monomorfismo.

Veamos que existe el isomorfismo del enunciado. Definamos $f_r(x) = x^r$. En particular $\mathrm{Aut}(C_n)$ es abeliano y tiene $\varphi(n)$ elementos.

$$U(\mathbb{Z}_n) = \{r : 1 \leq r < n \text{ y } \gcd(n, r) = 1\}$$

Entonces x^r es un generador de C_n pues $\mathrm{ord}(x^r) = \frac{n}{\gcd(n,r)} = n$.

Por lo que probamos antes, f_r es un monomorfismo. Como $\mathrm{Im}(f_r) = \langle f_r(x) \rangle = \langle x^r \rangle = C_n$ es también un epimorfismo.

Tenemos una aplicación f que aplica $r \mapsto f_r$. Veamos que es un homorfismo de grupos.

$$f(rs) = f_{rs} = f_r \circ f_s = f(r)f(s)$$

igualdad que se deduce de que $f_r \circ f_s(x) = f_r(x^s) = x^{rs} = f_{rs}(x)$.

Por lo visto anteriormente, es claro que f es un isomorfismo.

□

Proposición 2.

$$\mathrm{Aut}(C_8) \cong K$$

Demostración. Tenemos que $\mathrm{Aut}(C_8) \cong \mathbb{Z}_8^\times$. Es un grupo de orden 4, o es el cíclico o de orden 2.

Basta ver que $f_3^2 = f_5^2 = f_7^2 = 1$, es decir, todos tienen orden 2.

□

Proposición 3.

$$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$$

Demostración. Vamos a trabajar de forma abstracta, ya que $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ es isomorfo al de Klein.

Sea $\alpha \in S_3$, sea f_α que cumpla que $f_\alpha(1) = 1$ y $f_\alpha(a_i) = a_{\alpha(i)}$. Hay que ver que la aplicación es biyetiva y un isomorfismo.

□

Definición 1 (Producto directo de grupos)**.** Sean $G_1, \dots, G_n$ grupos. Definimos su producto directo como el grupo cuyos elementos son los del producto cartesiano $\prod_{i=1}^n G_i = G_1 \times \cdots \times G_n$ con la operación definida como sigue:

$$(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1y_1, \dots, x_ny_n)$$

Es fácil ver que es un grupo con uno la tupla $(1, \dots, 1)$ y donde $(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1})$.

Se tiene para cada $k = 1, \dots, n$ epimorfismos $p_k : \prod_i G_i \longrightarrow G_k$ definidos por $p_k(x_1, \dots, x_n) = x_k$ la proyección k-ésima.

Se tiene para cada $k = 1, \dots, n$ monomorfismos $\iota_k : G_k \longrightarrow \prod_i G_i$ definidos por $\iota_k(x_k) = (1, \dots, 1, x_k, 1, \dots, 1) = x_k$ la inyección k-ésima.

Es claro que

$$G_k \cong \mathrm{Im}(\iota_k)$$

y

$$\mathrm{Im}(\iota_k) \trianglelefteq \prod_i G_i$$

así que G_k es isomorfo a un subgrupo normal del producto directo.

Sea $H_k \in \mathrm{Sub}(G_k)$, entonces $\prod_i H_i$ es un subgrupo de $\prod_i G_i$.

Proposición 4. *Sean $G_1, \dots, G_n$ grupos finitos. El producto directo de los G_i es también finito y tiene como orden el producto de los órdenes.*

Sea $(x_1, \dots, x_n) \in \prod_i G_i$, tenemos que
$\mathrm{ord}((x_1, \dots, x_n)) = \mathrm{mcm}(\mathrm{ord}(x_1), \dots, \mathrm{ord}(x_n))$.

Supongamos que $\gcd(|G_i|, |G_j|) = 1$, entonces si cada G_i es cíclico, el producto es cíclico y si $L \leq \prod_i G_i$ entonces existen H_i tales que $L = \prod_i H_i$.

Demostración. El primer apartado se deduce de la teoría de conjuntos, del cardinal de un producto cartesiano.

$(x_1, \dots, x_r) \in \prod_i G_i$ y sea $t_i = \mathrm{ord}(x_i)$. Sea
$t = \mathrm{mcm}(t_1, \dots, t_n)$.

$$(x_1, \dots, x_n)^t = (x_1^t, \dots, x_n^t) = (1, \dots, 1)$$

Supongamos que $m \geq 1$:

$$(x_1, \dots, x_n)^m = (x_1^m, \dots, x_n^m) = (1, \dots, 1)$$

Entonces $t_i | m$ y por tanto $t | m$, donde $t_i = \mathrm{ord}(x_i)$.

Para el último apartado, suponemos que $G_i = \langle a_i \rangle$ y consideramos $a = (a_1, \dots, a_n)$. Por lo visto anteriormente,

$$\mathrm{ord}(a) = \mathrm{mcm}(\mathrm{ord}(a_1), \dots, \mathrm{ord}(a_n)) = \mathrm{mcm}(|G_1|, \dots, |G_n|) = \prod_i |G_i|$$

Hacemos inducción en n. Caso $n = 2$. $L \leq G_1 \times G_2$, consideramos p_1, p_2 las proyecciones canónicas.

Sea $H_1 = p_1\{L\}$ y $H_2 = p_2\{L\}$. Veamos que son los que cumplen la hipótesis. Sea $(x_1, x_2) \in L$, entonces $p_1(x_1, x_2) = x_1 \in H_1$, y $p_2(x_1, x_2) = x_2 \in H_2$. Por tanto, $L \leq H_1 \times H_2$.

Recíprocamente, $r = |G_1|$, $s = |G_2|$. Por el teorema de Bezout, elegimos $a, b \in \mathbb{Z}$ tales que:

$$1 = ar + bs$$

Sea $x_1 \in H_1$ entonces, existe un $y_2 \in G_2$ tal que $(x_1, y_2) \in L$.

$$(x_1, y_2) \in L \implies (x_1, y_2)^{bs} \in L$$

$$(x_1, y_2)^{bs} = (x_1^{bs}, y_2^{bs}) = (x_1^{1-ar}, 1) = (x_1, 1)$$

Por tanto, si $x_1 \in H_1$, $(x_1, 1) \in L$. Análogamente, si $x_2 \in H_2$, $(1, x_2) \in L$.

Sea $(x_1, x_2) \in H_1 \times H_2$, tenemos que $(x_1, x_2) = (x_1, 1)(1, x_2) = (x_1, x_2) \in L$. Así, $L = H_1 \times H_2$.

Sea $L \leq \prod_i^n G_i = \left(\prod_i^{n-1} G_i\right) \times G_n$, como el mcd de sus órdenes es 1, por el caso anterior:

$$L = K \times H_n$$

Pero aplicando la hipótesis de inducción sobre K obtenemos lo que se pide.

□

Corolario 1. Sean $n, m \geq 1$, entonces

$$C_n \times C_m \cong C_{nm} \iff \gcd(n, m) = 1$$

Proposición 5. *Supongamos un grupo G y $H_i \in \mathrm{Sub}(G)$. Consideramos su producto directo. Tenemos una aplicación $\phi : \prod_i H_i \longrightarrow G$ dada por $\phi(x_1, \ldots, x_n) = x_1 \cdots x_n$.*

Se verifica que ϕ es un isomorfismo si:

1. *$H_i \trianglelefteq G$ para todo i.*
2. *$H_1 H_2 \cdots H_n = G$.*
3. *$(H_1 \cdots H_{i-1}) \cap H_i = \{1\}$ para todo $i \in \{1, \ldots, n\}$*

En estas condiciones se dice que el grupo es producto directo interno de los subgrupos $H_1, \ldots, H_n$.

Demostración. $\phi(x_1, \ldots, x_n) = x_1 \cdots x_n$ es isomorfismo. En particular es epimorfismo y se tiene:

$$\mathrm{Im}(\phi) = H_1 \cdots H_n = G$$

y se tiene el segundo resultado.

Como para cada $k = 1, \ldots, n$ tenemos que:

$$\mathrm{Im}(\iota_k) \trianglelefteq \prod_i H_i$$

entonces $\phi(\mathrm{Im}(\iota_k)) = H_k \trianglelefteq \mathrm{Im}(\phi) = G$.

$\square$