Algebra II (Doble grado Informática-Matemáticas)

24 de marzo de 2020

1. Tema 4: Grupos cocientes. Teoremas de isomorfía.

Continuamos en esta clase con el Tema 4 del programa. Definiremos en esta clase el concepto de producto directo de una familia finita de grupos y estudiaremos sus propiedades.

Previamente, recordemos que en la clase anterior (del 23 de marzo) terminamos con el grupo de automorfismos de un grupo G y realizamos el Ejercicio 18 de la Relación 3 por el que obteníamos una descripción completa de $Aut(C_n)$, el grupo de automorfismos del grupo cíclico finito de orden n. Concretamente obteníamos que

$$Aut(C_n) = \{f_r / 1 \leq r \leq n-1, \text{ y } \text{m. c. d.}(r,n) = 1\},$$

siendo

$$f_r : C_n \to C_n, \text{ dado por } f_r(x) = x^r.$$

En particular $|Aut(C_n)| = \varphi(n)$.

Veamos un ejemplo

Ejercicio. (Ejercicio 19. Relación 3).

1. Describir explícitamente el grupo de automorfismos $Aut(C_8) = \langle x / x^8 = 1 \rangle$.
2. Demostrar que $Aut(C_8)$ es isomorfo al grupo de Klein.

Resolución. 1.- Según la descripción anterior tenemos que

$$Aut(C_8) = \{f_1 = id, f_3, f_5, f_7\},$$

siendo

$$f_r : C_8 \to C_8 \text{ dado por } f_r(x) = x^r \ r = 1, 3, 5, 7.$$

2.- Puesto que $Aut(C_8)$ es un grupo con 4 elementos entonces es isomorfo al cíclico de orden 4 ó al grupo de Klein (véase Ejercicio 23 de la relación 2). Para ver que es isomorfo al grupo de Klein, basta ver que todos los elementos de $Aut(C_8)$ distintos de id, tienen orden 2 . En efecto (recordemos que la operación de $Aut(C_8)$ es la composición)

$(f_3)^2(x) f = f_3(f_3(x)) = f_3(x^3) = (f_3(x))^3 = (x^3)^3 = x^9 = x \implies f_3 = id$

De igual forma se demuestra que $(f_5)^2 = id = (f_7)^2$, y se tiene lo pedido.

Cuando consideramos grupos diferentes a los cíclicos, el cálculo de su grupo de automorfismos no es tan inmediato y depende de cada caso particular

Veamos un ejemplo:

Ejercicio. (Ejercicio 20. Relación 3) Demostrar que el grupo $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ es isomorfo a S_3.

Resolución. Puesto que $\mathbb{Z}_2 \times \mathbb{Z}_2$ es isomorfo al grupo de Klein. Veamos que el grupo de automorfismos del grupo de Klein es isomorfo a S_3.

Recordemos (vease Ejercicio 20 de la relación 2 resuelto en la clase del 16 de marzo) que el grupo de Klein es dado por

$$K = \{1, a_1, a_2, a_3\}$$

y su tabla es

	1	a_1	a_2	a_3
1	1	a_1	a_2	a_3
a_1	a_1	1	a_3	a_2
a_2	a_2	a_3	1	a_1
a_3	a_3	a_2	a_1	1

Esto es

$$a_1^2 = a_2^2 = a_3^2 = 1, \text{ y para } \ i \neq j \text{ es } a_i a_j = a_k \text{ con } k \neq i, j.$$

Sea $\alpha \in S_3$, definimos $f_\alpha : K \to K$ por

$$f_\alpha(1) = 1,$$
$$f_\alpha(a_i) = a_{\alpha(i)}, i = 1, 2, 3.$$

Es fácil ver (hacedlo!!) que f_α es un homomorfismo de grupos y entonces un automorfismo pues claramente es biyectiva. Tenemos pues una aplicación

$$f : S_3 \to Aut(K), \ \alpha \mapsto f_\alpha$$

Veamos que es un homomorfismo: Sean $\alpha, \beta \in S_3$ entonces

$$f_{\alpha\beta}(1) = 1 = (f_\alpha f_\beta)(1)$$
$$f_{\alpha\beta}(a_i) = a_{(\alpha\beta)(i)} = a_{\alpha(\beta(i))} = f_\alpha(a_{\beta(i)}) = (f_\alpha f_\beta)(a_i), \ i = 1, 2, 3$$

Así pues $f(\alpha\beta) = f(\alpha)f(\beta)$ y f es un homomorfismo. Sea $\alpha \in S_3$ tal que $f(\alpha) = f_\alpha = id_K$, entonces $f_\alpha(a_i) = a_{\alpha(i)} = a_i$, con lo que $\alpha(i) = i$, para todo $i = 1, 2, 3$ y $\alpha = id$. Concluimos entonces con que $Ker(f) = \{id\}$ y por tanto f es un monomorfismo.

Finalmente, sea $t : K \to K$ un automorfismo de K. Definimos $\alpha \in S_3$ por la regla

$$\alpha(i) = k \iff t(a_i) = a_k,$$

para todo $i \in \{1, 2, 3\}$. Puesto que t es un automorfismo (y entonces biyectiva) α es en efecto una permutación de S_3. Por definición es claro que $f(\alpha) = t$ con lo que f es también un epimorfismo.

Como f es monomorfismo y epimorfismo entonces es un isomorfismo, como queríamos demostrar.

Pasemos ya a estudiar el producto directo de grupos:

Definición 1.1. *Sean $G_1, G_2, \ldots, G_n$ una familia de n grupos, $n \geq 2$. Definimos su* **producto directo** *como el grupo cuyos elementos son los del producto cartesiano*

$$G_1 \times G_2 \times \cdots \times G_n = \{(x_1, x_2, \ldots, x_n)/x_i \in G_i,\ i = 1, 2, \ldots, n\},$$

con producto definido por

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) := (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

Es fácil ver que con esta operación $G_1 \times G_2 \times \cdots \times G_n$ es un grupo, con elementoe unidad dado por la n-tupla $(1, 1, \ldots, 1)$ y donde, para cada $(x_1, x_2, \ldots, x_n) \in G_1 \times G_2 \times \cdots \times G_n$, su inverso es dado por $(x_1, x_2, \ldots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$.

Usaremos también la notación $\prod_{i=1}^n G_1$ para denotar al producto directo.

Para cada $k = 1, 2, \ldots, n$ se tienen homomorfismos

$$p_k : \prod_{i=1}^{n} G_i \to G_k,\ \textit{definidos por } p_k(x_1, x_2, \ldots, x_n) := x_k,$$

que claramente son epimorfismos y que llamaremos las **proyecciones canónicas.**

Así mismo, para cada $k = 1, 2, \ldots, n$ se tienen homomorfismos

$$j_k : G_k \to \prod_{i=1}^{n} G_i \ \textit{ definidos por } j_k(x_k) := (1, , \ldots, x_k, \ldots, 1)$$

que claramente son monomorfismos y que llameremos las **inyecciones canónicas.**

Notemos que

- $G_k \cong Img(j_k)$ para todo $k = 1, 2, \ldots, n$.
- $Img(j_k) \trianglelefteq \prod_{i=1}^n G_i$ para cada $k = 1, 2, \ldots n$. Por tanto cada G_k es isomorfo a un subgrupo normal del producto directo.

  En efecto, para cada $(y_1, y_2, \ldots, y_n) \in \prod_{i=1}^n G_i$ y $(1, \ldots, x_k, \ldots, 1) = j_k(x_k) \in Img(j_k)$, se tiene

  $$\begin{aligned}(y_1, y_2, \ldots, y_n)(1, \ldots, x_k, \ldots, 1)(y_1, y_2, \ldots, y_n)^{-1} & \\ &= (1, \ldots, y_kx_ky_k^{-1}, \ldots, 1) \\ &= j_k(y_kx_ky_k^{-1}) \in Img(j_k).\end{aligned}$$

- Si H_i es un subgrupo de G_i, para cada $i = 1, 2, \ldots, n$, entonces $\prod_{i=1}^n H_i \leq \prod_{i=1}^n G_i$.

Sin embargo no es en general cierto que todos los subgrupos de $\prod_{i=1}^n G_i$ sean producto directo de subgrupos, como vemos en el siguiente ejemplo:

Ejercicio. (Ejercicio 26. Relación 3) Demostrar que no todo subgrupo de un producto directo $H \times K$ es de la forma $H_1 \times K_1$, con H_1 subgrupo de H y K_1 subgrupo de K.

Resolución. Tomemos $H = K = \mu_2$, el grupo de las raíces cuadradas de la unidad. Entonces $L = \{(1,1),(-1,-1)\}$ es un subgrupo de $H \times K = \mu_2 \times \mu_2$ y no es de la forma $H_1 \times K_1$ para $H_1, K_1 \leq \mu_2$:

Para el caso de grupos finitos tenemos

Proposición 1.2. *Sean $G_1, G_2, \ldots, G_n$ grupos finitos, $n \geq 2$. Entonces*

(1) $|G_1 \times G_2 \times \cdots \times G_n| = |G_1||G_2| \ldots |G_n|$.

(2) *Para cada $(x_1, x_2, \ldots, x_n) \in \prod_{i=1}^n G_i$ se tiene que*

$$ord(x_1, x_2, \ldots, x_n) = \text{m. c. m.}(ord(x_1), ord(x_2), \ldots, ord(x_n)).$$

Supongamos ahora que $\text{m. c. d.}(|G_i|, |G_j|) = 1$*, para todo $i \neq j$, entonces*

(3) *Si G_i es un grupo cíclico, para todo $i = 1, 2, \ldots, n$, entonces $\prod_{i=1}^n G_i$ es también un grupo cíclico.*

(4) *Supongamos dado un subgrupo $L \leq \prod_{i=1}^n G_i$, entonces existen subgrupos $H_i \leq G_i$, $i = 1, 2, \ldots, n$ tal que $L = \prod_{i=1}^n H_I$.*

Demostración. (1) Es claro.

(2) Sea $t_i = ord(x_i)$, $i = 1, 2, \ldots, n$, y sea $t = \text{m. c. m.}(t_1, t_2, \ldots, t_n)$. Puesto que t es un múltiplo de cada t_i será

$$(x_1, x_2, \ldots, x_n)^t = (x_1^t, x_2^t, \ldots, x_n^t) = (1, 1, \ldots, 1).$$

Sea $m \geq 1$ tal que $(x_1, x_2, \ldots, x_n)^m = (x_1^m, x_2^m, \ldots, x_n^m) = (1, 1, \ldots, 1)$, entonces $x_i^m = 1$ para todo $i = 1, 2, \ldots, n$, y como $ord(x_i) = t_i$, será $t_i | m$ para todo $i = 1, 2, \ldots, n$ y por tanto $t | m$ (por ser t el mínimo común múltiplo). Consecuentemente $t = ord(x_1, x_2, \ldots, x_n)$.

Para los dos siguientes apartados, suponemos ahora que $\text{m. c. d.}(|G_i|, |G_j|) = 1$, para todo $i \neq j$

(3) Sea $G_i = \langle a_i \rangle$, $i = 1, 2, \ldots, n$, tendremos entonces que $ord(a_i) = |G_i|$ y por tanto $\text{m. c. d.}(ord(a_i), ord(a_j)) = 1$, para todo $i \neq j$. Consideramos el elemento $a = (a_1, a_2, \ldots, a_n) \in \prod_{i=1}^n G_i$, por el apartado anterior será

$$\begin{aligned} ord(a) = \text{m. c. m.}(ord(a_1), ord(a_2), \ldots, ord(a_n)) & \\ &= ord(a_1) ord(a_2) \ldots ord(a_n) \\ &= |G_i||G_2| \ldots |G_n| \\ &= |\prod_{i=1}^n G_i|, \end{aligned}$$

consecuentemente $\langle a \rangle = \prod_{i=1}^n G_i$ y entonces es cíclico.

(3) Hacemos inducción en n.

El primer caso es $n = 2$: Supongamos que $|G_1| = r$ y $|G_2| = s$. Como $\text{m. c. d.}(r, s) = 1$, por el teorema de Bezout, existirán $a, b \in \mathbb{Z}$ tal que $1 = ar + bs$.

Sea $L \leq G_1 \times G_2$ y consideremos las proyecciones canónicas

$p_1 : G_1 \times G_2 \to G_1,\ p_1(x_1, x_2) = x_1$

$p_2 : G_1 \times G_2 \to G_2,\ p_2(x_1, x_2) = x_2$

Sean $H_1 := (p_1)_*(L) \leq G_1$ y $H_2 := (p_2)_*(L) \leq G_2$. Veamos que $L = H_1 \times H_2$:

En efecto, ses $x = (x_1, x_2) \in L$ entonces $x_i = p_i(x) \in (p_i)_*(L) = H_i$, para $i = 1, 2$ y por tanto $x = (x_1, x_2) \in H_1 \times H_2$. Esto es, $L \leq H_1 \times H_2$.

Para la otra inclusión, en primer lugar observamos que si $x_1 \in H_1$ entonces $x_1 = p_1(x_1, y_2)$, para algún $(x_1, y_2) \in L$, entonces, como el orden de cualquier elemento de un grupo es un divisor del orden del grupo al que pertenece y $|G_1| = r, |G_2| = s$, tendremos

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

con lo que el elemento $(x_1, 1) \in L$. De forma análoga se demuestra que si $x_2 \in H_2$ entonces $(1, x_2) \in L$

Sea pues, $(x_1, x_2) \in H_1 \times H_2$, entonces $x_1 \in H_1 \Rightarrow (x_1, 1) \in L$ y $x_2 \in H_2 \Rightarrow (1, x_2) \in L$ con lo que $(x_1, x_2) = (x_1, 1)(1, x_2) \in L$. Esto es $H_1 \times H_2 \leq L$ y de la doble inclusión deducimos la igualdad es decir, $L = H_1 \times H_2$. Por tanto la afirmación es cierta para el caso $n = 2$.

Supuesto cierto para n véamoslo para $n + 1$:

Sea $L \leq \prod_{i=1}^{n+1} G_i$, como $G_1 \times \cdots \times G_n \times G_{n+1} = (G_1 \times \cdots \times G_n) \times G_{n+1}$ y $\mathrm{m.\,c.\,d.}(|G_1 \times \cdots \times G_n|, |G_{n+1}|) = 1$ entonces, por el caso 2 anteriormente visto, existirá $K \leq \prod_{i=1}^{n} G_i$ y $H_{n+1} \leq G_{n+1}$ tal que $L = K \times G_{n+1}$. Para $K \leq \prod_{i=1}^{n} G_i$, por hipótesis de inducción, , existirán $H_i \in G_i$, $i = 1, 2, \ldots, n$ tal que $K = H_1 \times H_2 \times \cdots \times H_n$. Entonces

$$L = K \times H_{n+1} = H_1 \times H_2 \times \cdots \times H_n \times H_{n+1},$$

lo que acaba la demostración.

□

Como corolario de la proposición anterior, deducimos un hecho bien concido por vosotros:

Corolario 1.3. *Sean $n, m \geq 1$, entonces*

$$C_n \times C_m \cong C_{nm} \iff \mathrm{m.\,c.\,d.}(n, m) = 1.$$

Demostración. Es consecuencia directa del apartado (3) de la proposición anterior. □