Álgebra III
Semana 6

Alejandro García Montoro
agarciamontoro@correo.ugr.es

11 de noviembre de 2015

Ejercicio 1. *Se considera el grupo $C_p \times C_p$, siendo p un entero primo positivo.*

Apartado 1.1. Prueba que $Aut(C_p \times C_p)$ es el grupo lineal general $GL(p, 2)$.

Solución. *Nota:* $GL(p, 2)$ = matrices invertibles de orden 2 con sus elementos en C_p.

En general, sabemos que si K es un cuerpo y V un espacio vectorial de dimensión n sobre K, se tiene que:

$$End_K(V) \cong \mathbb{M}_n(K)$$

Además, si un endomorfismo es invertible —es un automorfismo—, su matriz asociada es también invertible, con su inversa la matriz asociada al endomorfismo inverso. Esto es:

$$Aut_K(V) \cong GL(p, n)$$

En nuestro caso, tomando $K = C_p$ y $V = C_p \times C_p$ —espacio vectorial de dimensión 2 sobre C_p—, se tiene el resultado pedido.

Podemos demostrar el resultado general para espacios vectoriales de dimensión 2, como $C_p \times C_p$. Es decir, dado K un cuerpo, veamos la biyección existente entre automorfismos de $K \times K$ y las matrices de dimensión 2 sobre el cuerpo K:

Sea $f \in End(K \times K)$ y $B = \{e_1, e_2\}$ una base de $K \times K$, con $e_1 = (1, 0)$ y $e_2 = (0, 1)$. Si denotamos

$$f(e_1) = \begin{pmatrix} a_{1,1} \\ a_{2,1} \end{pmatrix},\ f(e_2) = \begin{pmatrix} a_{1,2} \\ a_{2,2} \end{pmatrix} \in K \times K$$

podemos escribir la imagen de cualquier elemento $x = (x_1, x_2) \in K \times K$

como sigue:

$$f(x) = f\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = f\begin{pmatrix} x_1 \\ 0 \end{pmatrix} + f\begin{pmatrix} 0 \\ x_2 \end{pmatrix} = x_1 f(e_1) + x_2 f(e_2) =$$
$$= x_1 \begin{pmatrix} a_{1,1} \\ a_{1,2} \end{pmatrix} x_2 \begin{pmatrix} a_{1,2} \\ a_{2,2} \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Por tanto, podemos asociar cualquier endomorfismo de $K \times K$ con una matriz de dimensión 2 sobre K —y viceversa, pues el camino es biyectivo—, donde las columnas son las imágenes por el endomorfismo de la base de $K \times K$:

$$f \longleftrightarrow \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

Además, si f tiene inversa, la matriz asociada es invertible y su inversa es la asociada a f^{-1}.

Por tanto, concluimos que $Aut(C_p \times C_p) \cong GL(p, 2)$.

Apartado 1.2. Para $p = 2$ prueba que $Aut(C_2 \times C_2) \cong S_3$.

Solución. Es claro que cualquier $f \in Aut(C_2 \times C_2)$ tiene que dejar fijo al uno del cuerpo. Por tanto, si notamos $C_2 \times C_2 = \langle 1, a, b \mid a^2 = b^2 = 1, ab = ba \rangle = \{1, a, b, ab\}$, tenemos que todos los automorfismos que buscamos están determinados por las imágenes de los elementos a, b, ab. Estas pueden ser las siguientes:

$$a, b, ab \xrightarrow{id} a, b, ab$$
$$a, b, ab \xrightarrow{f_1} a, ab, b$$
$$a, b, ab \xrightarrow{f_2} b, a, ab$$
$$a, b, ab \xrightarrow{f_3} b, ab, a$$
$$a, b, ab \xrightarrow{f_4} ab, a, b$$
$$a, b, ab \xrightarrow{f_5} ab, b, a$$

Que los anteriores son automorfismos es claro por la construcción del cuerpo; como no hay más posibilidades, concluimos que

$$Aut(C_2 \times C_2) = \{1, f_1, f_2, f_3, f_4, f_5\}$$

Sabemos, por otro lado, que S_3 es el grupo de permutaciones de un conjunto de tres elementos; esto es, el conjunto visto anteriormente. Es evidente entonces que

$$Aut(C_2 \times C_2) \cong S_3$$

Una forma quizás más sencilla de ver este resultado es el siguiente: por el apartado anterior, sabemos que $Aut(C_2 \times C_2) \cong GL(2,2)$; es decir, los automorfismos de $C_2 \times C_2$ son las matrices de orden 2 con elementos en C_2 que son invertibles; esto es, tales que su determinante es distinto de cero.

Dada una matriz general

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

sabemos que es invertible si, y sólo si, $ad - bc \neq 0$. En nuestro caso, en el que los elementos están en $C_2 = \mathbb{Z}_2$, las posibles matrices son las siguientes:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \beta = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \delta = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \delta^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Estamos entonces ante un grupo de orden 6, luego es C_6 ó S_3. Como hay más de un elemento de orden 2 —de hecho, $\alpha^2 = \beta^2 = \gamma^2 = 1$—, el grupo tiene que ser S_3.

Apartado 1.3. Determina el grupo $(C_2 \times C_2) \rtimes C_2$.

Solución. Para definir el grupo, lo único que necesitamos es la definición de la operación producto. En un producto semidirecto de grupos $N \rtimes H$, el producto se define como sigue:

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2)$$

donde $\varphi : H \to Aut(N)$ es un homomorfismo de grupos.

En nuestro caso, $N = C_2 \times C_2$ y $H = C_2$. Como $Aut(N) = Aut(C_2 \times C_2) \cong S_3$, basta encontrar el homomorfismo de grupos $\varphi : C_2 \to S_3$. Como $C_2 = \langle c | c^2 = 1 \rangle = \{1, c\}$ sólo tiene un elemento distinto a la identidad, c, y este es de orden 2, los homomorfismos que buscamos —además del trivial, que lleva todos los elementos a la identidad y en cuyo caso el producto semidirecto no es más que el producto directo— serán aquellos que lleven c a un elemento de orden 2 en S_3.

Los elementos de orden 2 de S_3 son exactamente los ciclos de longitud 2; esto es: $(23), (12)$ y (13). Con la notación del apartado anterior, estos ciclos son $f_1 = (b \ \ ab), f_2 = (a \ \ b)$ y $f_5 = (a \ \ ab)$.

Tenemos entonces las siguientes posibilidades:

$$\begin{aligned} \varphi_0 : C_2 &\longrightarrow Aut(C_2 \times C_2) \\ 1 &\longmapsto id \\ c &\longmapsto id \end{aligned}$$

$$\begin{aligned}\varphi_1 : C_2 &\longrightarrow Aut(C_2 \times C_2)\\ 1 &\longmapsto id\\ c &\longmapsto (b\ \ ab)\end{aligned}$$

$$\begin{aligned}\varphi_2 : C_2 &\longrightarrow Aut(C_2 \times C_2)\\ 1 &\longmapsto id\\ c &\longmapsto (a\ \ b)\end{aligned}$$

$$\begin{aligned}\varphi_3 : C_2 &\longrightarrow Aut(C_2 \times C_2)\\ 1 &\longmapsto id\\ c &\longmapsto (a\ \ ab)\end{aligned}$$

Cabría esperar que los productos semidirectos asociados a cada φ_i fueran diferentes pero, como veremos, tenemos esencialmente dos:

$$(C_2 \times C_2) \rtimes_{\varphi_0} C_2 = C_2 \times C_2 \times C_2$$
$$(C_2 \times C_2) \rtimes_{\varphi_1} C_2 = (C_2 \times C_2) \rtimes_{\varphi_2} C_2 = (C_2 \times C_2) \rtimes_{\varphi_3} C_2 = D_4$$

El primero es claro: φ_0 es el homomorfismo trivial que lleva todos los elementos a la identidad, luego el producto se define como

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi_0(h_1)(n_2), h_1h_2) = (n_1n_2, h_1h_2)$$

es decir, es el producto directo de los dos grupos con la operación usual.

Que todos los demás homomorfismos generan el mismo grupo tampoco es difícil: en S_3, los elementos de orden 2 son todos conjugados los unos de los otros:

$$\begin{aligned}(12) &= (23)(13)(23) = (13)(23)(13)\\ (13) &= (23)(12)(23) = (12)(23)(12)\\ (23) &= (13)(12)(13) = (12)(13)(12)\end{aligned}$$

Por tanto, al aplicarse sobre todos los elementos de C_2 generan el mismo grupo.

Lo único que nos falta por ver es que el grupo es, de hecho, D_4. Estudiemos, por ejemplo, $(C_2 \times C_2) \rtimes_{\varphi_1} C_2$ —como hemos visto, da igual estudiar este que cualquier de los otros dos—.

Evidentemente, es un grupo de 8 elementos —los elementos son todas las posibles parejas de un grupo de 4 elementos y otro de 2— no abeliano. Para ver que no es abeliano basta dar dos elementos que no conmuten; consideramos, por ejemplo, (a, c) y $(b, 1)$:

$$\begin{aligned}(a, c)(b, 1) &= (a\varphi_1(c)(b), c1) = (aab, c) = (b, c)\\ (b, 1)(a, c) &= (a\varphi_1(1)(a), 1c) = (aa, c) = (1, c)\end{aligned}$$

Esto nos acota la búsqueda, pues grupos con esas características sólo hay dos: el diédrico, $D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$, y el grupo de los cuaternios, $Q = \{1, -1, i, -i, j, -j, k, -k\}$.

Sabemos que en el grupo de los cuaternios sólo hay un elemento de orden 2: el -1 —todos los demás son de orden 4—. Pero en nuestro producto $(C_2 \times C_2) \rtimes_{\varphi_1} C_2$ podemos encontrar más de un elemento de orden 2; por ejemplo, $(1, c)$ y $(a, 1)$:

$$(1, c)(1, c) = (1\varphi_1(c)(1), c^2) = (1, 1)$$
$$(a, 1)(a, 1) = (a\varphi_1(1)(a), 1 \cdot 1) = (a^2, 1) = (1, 1)$$

Por tanto, concluimos que:

$$(C_2 \times C_2) \rtimes_{\varphi} C_2 = \begin{cases} C_2 \times C_2 \times C_2 & \text{si } \varphi = \text{trivial} \\ D4 & \text{en otro caso} \end{cases}$$

Apartado 1.4. Para $p = 3$ calcular el grupo $Aut(C_3 \times C_3)$ y su estructura.

Solución. Por el segundo apartado del ejercicio, sabemos que $Aut(C_3 \times C_3) = GL(3, 2)$; esto es, el grupo de las matrices invertibles de orden 2 con sus elementos en C_3.

Un cálculo rápido en GAP nos permite ver el número de elementos que tiene este grupo:

```
1  gap> C3:=CyclicGroup(3);
2  <pc group of size 3 with 1 generators>
3
4  gap> C3xC3:=DirectProduct(C3,C3);
5  <pc group of size 9 with 2 generators>
6
7  gap> Size(Elements(AutomorphismGroup(C3xC3)));
8  48
```

Esto nos da bastante información del grupo. Como $48 = 2^4 * 3 = 16 * 3$, el teorema de Sylow nos dice que el número n de 3-subgrupos de Sylow —que son de orden $3^1 = 3$— debe cumplir:

- $n|16$
- $n \equiv 1(mod 3)$

Por tanto, podemos tener 1, 4, ó 16 3-subgrupos de Sylow. Resulta que hay 4 3-subgrupos de Sylow, pero lo que nos interesa es realmente otro aspecto:

Sabemos que para un p fijo, los p-subgrupos de Sylow son todos conjugados entre sí. Por tanto, tenemos que todos los 3-subgrupos de Sylow de $Aut(C_3 \times C_3)$ son conjugados. Como todos estos subgrupos son de orden 3, y todos los grupos de orden 3 son isomorfos al cíclico de orden 3 —esto es, generados

por un elemento de orden 3—, tenemos que *todos* los elementos de orden 3 de $Aut(C_3 \times C_3)$ son conjugados entre sí. Esta propiedad nos ayudará a definir el producto semidirecto del último apartado con comodidad.

Apartado 1.5. Determina un elemento de orden 3 de $Aut(C_3 \times C_3)$.

Solución. Para encontrar un elemento de orden 3 de $Aut(C_3 \times C_3)$ hay que buscar una matriz 2×2 en C_3 —de aquí en adelante consideramos $C_3 = \mathbb{Z}_3$— cuyo cubo sea la matriz identidad.

Una opción para hacer esto es tomar una matriz 2×2 general

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

y calcular su cubo:

$$A^3 = \begin{pmatrix} b(ac+cd)+a(a^2+bc) & b(bc+d^2)+a(ab+bd) \\ d(ac+cd)+c(a^2+bc) & d(bc+d^2)+c(ab+bd) \end{pmatrix}$$

Imponemos entonces $A^3 = I_2$ y tenemos un sistema no lineal de cuatro ecuaciones con cuatro incógnitas:

$$\begin{cases} b(ac+cd)+a(a^2+bc) = 1 \\ b(bc+d^2)+a(ab+bd) = 0 \\ d(ac+cd)+c(a^2+bc) = 1 \\ d(bc+d^2)+c(ab+bd) = 0 \end{cases}$$

Las soluciones para a, b, c, d determinan todos los posibles elementos de orden 3.

Podemos también buscar el elemento con un sistema de cálculo como GAP

```
gap> C3:=CyclicGroup(3);
<pc group of size 3 with 1 generators>

gap> C3xC3:=DirectProduct(C3,C3);
<pc group of size 9 with 2 generators>

gap> A:=AutomorphismGroup(C3xC3);
<group with 4 generators>

gap> Aut:=Elements(A);;

gap> Filtered(Aut,x->Order(x)=3)[1];
[ f1, f2 ] -> [ f1*f2^2, f2 ]
```

El último comando simplemente filtra, de entre todos los elementos de $Aut(C_3 \times C_3)$, aquellos de orden 3 y devuelve el primero que se encuentra. La salida de este comando se interpreta como sigue: f1 y f2 son los dos generadores de $C_3 \times C_3$. Si lo vemos como $\mathbb{Z}_3 \times \mathbb{Z}_3$, podemos considerar $f1 = (1,0)$ y $f2 = (0,1)$.

Entonces, el elemento que muestra la línea 13 del código anterior es el que lleva el $(1,0)$ en $(1,0)+(0,1)+(0,1) = (1,2)$ —estamos escribiendo aquí en notación aditiva lo que GAP nos proporciona con notación multiplicativa— y el $(0,1)$ en $(0,1)$; es decir, es la matriz

$$B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

que es un elemento de orden 3:

$$B^3 = \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Apartado 1.6. Determina el grupo $(C_3 \times C_3) \rtimes C_3$.

Solución. Como en el apartado 1.3, basta definir el homomorfismo $\varphi : C_3 \to Aut(C_3 \times C_3)$.

Pero para determinar este homomorfismo basta determinar la imagen del generador de $C_3 = \mathbb{Z}_3$, al que llamamos 1 —usamos notación aditiva—. Como 1 es de orden 3 —$1+1+1 = 3 \equiv 0(mod 3)$—, su imagen por φ tiene que ser un elemento de orden 3.

Pero en el apartado 1.4 probamos que todos los elementos de orden 3 de $Aut(C_3 \times C_3)$ son conjugados, lo que nos permite afirmar que el producto semidirecto es independiente del elemento de orden 3 que tomemos como imagen del 1.

Por tanto, construimos el homomorfismo con el elemento de orden 3 que obtuvimos en el apartado anterior:

$$\begin{aligned} \varphi : C_3 &\longrightarrow Aut(C_3 \times C_3) \\ 0 &\longmapsto id \\ 1 &\longmapsto B \end{aligned}$$

donde B es la matriz definida anteriormente.

Tenemos entonces que $(C_3 \times C_3) \rtimes_\varphi C_3$ es un grupo no abeliano de orden 27 —parejas de un grupo de orden 9 y de un grupo de orden 3— con producto

como sigue:

$$\begin{aligned}((x_1,y_1),z_1)((x_2,y_2),z_2) &= ((x_1,y_1)\varphi(z_1)(x_2,y_2),z_1z_2) = \\ &= \begin{cases}((x_1x_2,y_1y_2),0) & \text{si } z_1=0\\ ((x_1,y_1)B(x_2,y_2),z_2) & \text{si } z_1=1\\ ((x_1,y_1)B^2(x_2,y_2),2z_2) & \text{si } z_1=2\end{cases}\\ &= \begin{cases}((x_1x_2,y_1y_2),0) & \text{si } z_1=0\\ ((x_1,y_1)(x_2,2x_2+y_2),z_2) & \text{si } z_1=1\\ ((x_1,y_1)(x_2,x_2+y_2),2z_2) & \text{si } z_1=2\end{cases}\\ &= \begin{cases}((x_1x_2,y_1y_2),0) & \text{si } z_1=0\\ ((x_1x_2,y_1(2x_2+y_2)),z_2) & \text{si } z_1=1\\ ((x_1x_2,y_1(x_2+y_2)),2z_2) & \text{si } z_1=2\end{cases}\end{aligned}$$

donde el producto de B —resp. B^2— con el elemento (x_2, y_2) es el producto matricial usual:

$$B(x_2,y_2) = \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}\begin{pmatrix}x_2\\ y_2\end{pmatrix} = \begin{pmatrix}x_2\\ 2x_2+y_2\end{pmatrix}$$
$$B^2(x_2,y_2) = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}x_2\\ y_2\end{pmatrix} = \begin{pmatrix}x_2\\ x_2+y_2\end{pmatrix}$$

Que es no abeliano es claro; basta tomar, por ejemplo, los elementos $((0,1),2)$ y $((1,1),2)$, que no conmutan:

$$((0,1),2)((1,1),2) = ((0,1(1+1)),2\cdot 2) = ((0,2),1)$$
$$((1,1),2)((0,1),2) = ((0,1(0+1)),2\cdot 2) = ((0,1),1)$$

Una búsqueda rápida en la wiki de GroupProps[1] nos permite saber que hay sólo dos grupos no abelianos de orden 27: $M_{27} = C_9 \rtimes C_3$, el producto semidirecto del cíclico de orden nueve y del cíclico de orden tres[2], y $UT(3,3)$, el grupo de matrices sobre $\mathbb{Z}_3$ unitriangulares[3] —es decir, matrices con todos los elementos de su diagonal igual a 1, todos los elementos debajo de la diagonal igual a 0 y elementos arbitrarios encima—, de dimensión 3.

Como $C_3 \times C_3 \ncong C_9$, entonces $(C_3 \times C_3) \rtimes C_3 \ncong M_{27}$. Por tanto, podemos concluir que el grupo que buscamos es isomorfo al grupo de matrices unitriangulares de dimensión 3.

[1] `http://groupprops.subwiki.org/wiki/Groups_of_order_27`
[2] `http://groupprops.subwiki.org/wiki/M27`
[3] `http://groupprops.subwiki.org/wiki/Prime-cube_order_group:U(3,3)`

Además, como antes, si consideramos el homomorfismo trivial

$$\begin{aligned} \psi : C_3 &\longrightarrow Aut(C_3 \times C_3) \\ 0 &\longmapsto id \\ 1 &\longmapsto id \end{aligned}$$

tenemos el producto directo:

$$(C_3 \times C_3) \rtimes_\psi C_3 = C_3 \times C_3 \times C_3$$

Por tanto, el producto semidirecto que buscamos queda totalmente determinado:

$$(C_3 \times C_3) \rtimes_\varphi C_3 = \begin{cases} C_3 \times C_3 \times C_3 & \text{si } \varphi = \text{trivial} \\ UT(3,3) & \text{en otro caso} \end{cases}$$