GRUPOS DE ORDEN pq

RESUMEN. Caracterizamos a menos de isomorfismo los grupos de orden pq donde p y q son dos primos positivos.

Fijamos a lo largo de esta nota dos primos $0 < p < q$. Comenzamos haciendo la siguiente observación:

Proposición 1. *Todo grupo de orden pq es isomorfo a un producto semidirecto $\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$.*

Demostración. Por el teorema de Cauchy existen $x, y \in G$ tales que $\operatorname{ord}(x) = p$ y $\operatorname{ord}(y) = q$. Notar que $\langle x\rangle \cap \langle y\rangle = 1$, ya que este subgrupo debe tener orden divisor de $p = |\langle x\rangle|$ y $q = |\langle y\rangle|$ simultáneamente. En particular $|\langle x\rangle\langle y\rangle| = |\langle x\rangle| \cdot |\langle y\rangle| = pq$ y entonces $G = \langle x\rangle\langle y\rangle$. Por otra parte, como $\langle y\rangle$ tiene índice p, y este es el menor primo que divide a $|G|$, entonces $\langle y\rangle$ resulta normal[1]. En consecuencia, se obtiene que G es un producto semidirecto interno de $\langle y\rangle$ y $\langle x\rangle$, de forma que

$$G \cong \langle y\rangle \rtimes_\psi \langle x\rangle \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$$

para algún $\phi\colon \mathbb{Z}/p\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$. □

Basta entonces, para caracterizar a los grupos de orden pq, caracterizar a los productos semidirectos entre $\mathbb{Z}/q\mathbb{Z}$ y $\mathbb{Z}/p\mathbb{Z}$.

1. AUTOMORFISMOS DE UN GRUPO CÍCLICO

Lema 1. *Sea $n \in \mathbb{N}_{\geq 2}$. Todo endomorfismo de grupos $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ es de la forma $g_{\overline{k}}(\overline{a}) = \overline{ka}$ para cierto $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, y $g_{\overline{k}}$ es un automorfismo si y sólo si k es coprimo con n.*

Demostración. Si $\overline{k} = f(\overline{1})$, entonces

$$f(\overline{a}) = \overbrace{f(\overline{1}) + \cdots + f(\overline{1})}^{a \text{ veces}} = \overbrace{\overline{k} + \cdots + \overline{k}}^{a \text{ veces}} = \overline{ka} = g_{\overline{k}}(\overline{a}).$$

Si $\overline{j}$ es tal que $(j : n) = 1$, entonces $\overline{jk} = \overline{1}$, y una verificación muestra que $g_{\overline{j}}$ es inversa de $g_{\overline{k}}$. Recíprocamente: si existe $\overline{j}$ tal que $g_{\overline{j}} \circ g_{\overline{k}} = \mathrm{id}$, evaluando en $\overline{1}$ es $\overline{jk} = \overline{1}$ y por lo tanto k es coprimo con n. □

Corolario 1. *Se tiene un automorfismo $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathcal{U}_n$ que envía f a $f(\overline{1})$.* □

2. PRODUCTOS SEMIDIRECTOS ENTRE $\mathbb{Z}/q\mathbb{Z}$ Y $\mathbb{Z}/p\mathbb{Z}$

Componiendo con el isomorfismo del Corolario 1, un morfismo $\phi\colon \mathbb{Z}/p\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$ se corresponde con un morfismo

$$\phi'\colon \mathbb{Z}/p\mathbb{Z} \to \mathcal{U}_q.$$

[1] Ver por ejemplo el Ejercicio 9 (III) de la práctica 3.

Si ϕ' no es el morfismo constantemente 1 –es decir, si $\phi \not\equiv \mathrm{id}$– entonces ϕ' está determinada por la elección de un elemento de orden p en $\mathcal{U}_q$. Por el teorema de Cauchy, existe un tal elemento si y sólo si $p \mid q-1$. De aquí tenemos una primera consecuencia:

Teorema 1. *Si $0 < p < q$ son dos primos tales que $p \not| q-1$, entonces todo grupo G de orden pq es isomorfo a $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.*

Demostración. Sabemos que $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$ para cierto $\phi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$, pero por consideraciones de orden ϕ necesariamente envía todo elemento del dominio a $\mathrm{id} \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. En consecuencia $\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Este útlimo es isomorfo a $\mathbb{Z}/pq\mathbb{Z}$ por el teorema chino del resto. □

Ahora consideremos el caso en el que $p \mid q-1$. En principio parecería haber muchos productos semidirectos distintos, pero veremos que hay sólo uno no abeliano a menos de isomorfismo. Recordemos que $\mathcal{U}_q$ es cíclico de orden $q-1$ y sea $\overline{\mu}$ un generador, de manera que $U_q = \{1, \overline{\mu}, \ldots, \overline{\mu^{q-2}}\}$. Por el Corolario 1, todo automorfismo de $\mathbb{Z}/q\mathbb{Z}$ es de la forma

$$g_{\overline{\mu^i}}\colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}, \qquad \overline{a} \mapsto \overline{\mu^i a}$$

para cierto $i \in \{0, \ldots, q-2\}$. Cada una de estas induce un morfismo

$$\phi_i\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}), \quad \phi_i(\overline{a}) = (g_{\overline{i}})^a, \quad (\phi_i(\overline{a}))(\overline{x}) = g_{\overline{i}}^a(\overline{x}) = \overline{\mu^{ai}x}.$$

Proposición 2. *Si $i \in \{1, \ldots, q-2\}$, entonces $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_i} \mathbb{Z}/p\mathbb{Z}$.*

Demostración. Proponemos la siguiente función

$$F\colon \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_i} \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}, \qquad F(\overline{x}, \overline{y}) = (\overline{x}, \overline{iy}) = (\overline{x}, g_{\overline{i}}(\overline{y})).$$

Notar que $g_{\overline{i}}$ es una biyección, por lo ya observado, así que F es biyectiva. Resta ver que es morfismo. En efecto, por un lado

$$F(\overline{x}, \overline{y})F(\overline{z}, \overline{w}) = (\overline{x}, \overline{iy})(\overline{z}, \overline{iw}) = (\overline{x} + \overline{\mu^{iy}z}, \overline{iy} + \overline{iw})$$

lo cual coincide con

$$F((\overline{x}, \overline{y})(\overline{z}, \overline{w})) = F(\overline{x} + \overline{\mu^{yi}z}, \overline{y+w}) = (\overline{x} + \overline{\mu^{yi}z}, \overline{i(y+w)})$$

□

Esto termina de caracterizar a nuestros grupos de interés.

Teorema 2. *Si $0 < p < q$ son dos primos tales que $p \mid q-1$, entonces todo grupo G de orden pq es o bien isomorfo a $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, si es abeliano, o bien isomorfo a $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}$ en caso contrario.*

Demostración. Ya observamos que todo grupo de orden pq es isomorfo un producto semidirecto de $\mathbb{Z}/q\mathbb{Z}$ por $\mathbb{Z}/p\mathbb{Z}$, determinado por cierto morfismo $\phi_i\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$, $i \in \{0, 1, \ldots, q-2\}$. La proposición anterior dice que si $i > 0$ entonces $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_i} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}$. Por otro lado $\phi_0 \equiv \mathrm{id}$ y entonces $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_0} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. A su vez, estos grupos no son isomorfos: el primero no es abeliano pero el segundo sí lo es. Estos son todos los posibles productos semidirectos a menos de isomorfismos, y por lo tanto todos los grupos de orden pq a menos de isomorfismo. □

Ejemplo 1. Si $p > 0$ es un primo impar, entonces a menos de isomorfismo todo grupo de orden $2p$ es $\mathbb{D}_p$ o $\mathbb{Z}/2p\mathbb{Z}$. En particular, para $p = 3$ esto recupera nuestra caracterización de los posibles grupos de orden 6.

3. ¿Y SI $p = q$?

Para concluir caracterizamos los grupos de orden p^2.

Lema 2. *Sea $p > 0$ un primo. Un grupo de orden p^2 es abeliano.*

Demostración. Sabemos, por la ecuación de clases, que $C(G) \triangleleft G$ es no trivial. Por lo tanto, tiene orden p o p^2. En consecuencia $G/C(G)$ tiene orden 1 o p, y en cualquiera de los dos casos debe ser cíclico. Esto último implica que G es abeliano, por el Ejercicio 13 de la práctica 2. □

Proposición 3. *Sea $p > 0$ un primo. Los grupos de orden p^2 a menos de isomorfismo son $\mathbb{Z}/p^2\mathbb{Z}$ y $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Demostración. Sea G un grupo de orden p^2. Si G es cíclico entonces $G \cong \mathbb{Z}/p^2\mathbb{Z}$; podemos suponer lo contrario y probar que $G \cong (\mathbb{Z}/p\mathbb{Z})^2$. Ya sabemos que G es abeliano y en particular todo subgrupo es normal. Resta entonces conseguir dos subgrupos H y K de orden p que tengan intersección trivial, ya que entonces $|H||K| = p^2$ y por lo tanto $G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Sean $x \in G \setminus \{1\}$ e $y \in G \setminus \langle x \rangle$ elementos de orden p. Veamos para terminar que $\langle x \rangle \cap \langle y \rangle$. Si $z \in \langle x \rangle \cap \langle y \rangle$, entonces existen $i, j \in \{0, \dots, p-1\}$ tales que

$$z = y^i = x^j.$$

Afirmamos que $i = 0$ y por lo tanto $z = y^0 = 1$. En efecto: de lo contrario existiría $k \in \mathbb{Z}$ tal que $ik \equiv 1 \pmod{p}$ y, elevando a la k, tenemos que

$$y = y^{ik} = (y^i)^k = (x^j)^k \in \langle x \rangle$$

lo cual es una contradicción. □