Divulgaciones Matemáticas Vol. 11 No. 1(2003), pp. 61–70

Un Estudio Elemental de los Grupos cuyo Orden es Producto de dos Primos

An Elemental Study of Groups whose Order is a Product of two Primes

Alfonso Ríder Moyano (ma1rurur@uco.es)
Rafael María Rubio Ruiz (ma1rimoa@uco.es)
Departamento de Matemáticas, Universidad de Córdoba
Campus de Rabanales, Edificio C2
Córdoba, 14071, España.

Resumen

En este trabajo se estudia la cantidad de grupos finitos, distintos salvo isomorfismo, que tienen como orden el producto de dos primos absolutos. Se utilizan para ello métodos elementales, basados en la acción sobre el propio grupo, de los automorfismos internos.
Palabras y frases clave: Grupos finitos, acción, teoremas de Sylow, orden, conjugación.

Abstract

In this paper we study the number of finite abstract groups whose order is the product of two primes. We use elementary methods based in the action of the group on itself by conjugation.
Key words and phrases: Finite groups, action, Sylow's theorems, order, conjugation.

1 Introducción

Consideremos un grupo G de orden $n = pq$, con $2 \leq p < q$, donde p y q son primos absolutos, a continuación analizaremos cuantos grupos existen de orden n.

Recibido 2003/03/26. Aceptado 2003/06/01.
MSC (2000): 20D20, 20D45, 20E34.

Con este propósito haremos que el grupo G actúe sobre si mismo mediante los automorfismos internos y estudiaremos sus órbitas de conjugación. Se denotará en lo que sigue por $\mathcal{Z}$ al centro de G, por $\mathcal{C}_n$ al grupo cíclico de orden n y escribiremos $H \odot K$ para referirnos al producto directo interno de dos subgrupos H y K .

Probaremos finalmente los siguientes resultados:

Teorema 1: Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si existe un grupo G de orden n para el cual $\mathcal{Z} = \{e\}$, necesariamente se cumple

$$q \equiv 1 \text{ mód } p.$$

Teorema 2: Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si $q \not\equiv 1$ mód p, el único grupo de orden n es el $\mathcal{C}_n$.

Además en el caso en que $q \equiv 1$ mód p probaremos la existencia y unicidad de un grupo no comnutativo.

2 Preliminares

Recordemos que un grupo G es *producto semidirecto interior* del subgrupo H por el subgrupo K, y se denota $G = H[K]$, cuando

1) Para todo $g \in G$ existen $x \in H, u \in K$, únicos, de manera que

$$g = xu.$$

2) Cualesquiera que sean $x \in H, u \in K, se$ cumple

$$x^{-1}ux \in \text{ K.}$$

Por otra parte dado un grupo K, si H es un grupo de operadores de K mediante un morfismo

$$\rho : H \mapsto \text{Aut}(K),$$

la operación del conjunto $H \times K$ definida por la ley

$$(x, u)(y, v) = (xy, \rho(y)(u)v)$$

dota al conjunto $H \times K$ de la estructura de grupo.

El grupo así construido se conoce como *producto semidirecto (exterior)* de H por K mediante el morfismo $\rho : H \mapsto \text{Aut}(K)$, y se denota $H_\rho \times K$.

3 Estudio de las órbitas de conjugación

Haciendo que G actúe sobre sí mismo mediante los automorfismos internos, tendremos las correspondientes órbitas de conjugación. Cada una de ellas tiene cardinal divisor de n. Las de cardinal 1 corresponden a elementos centrales de G. Si denotamos por $\mathcal{Z}(b)$ al centralizador de un elemento $b \in G$, Z al centro del grupo y $\alpha = Ord(\mathcal{Z})$ la cantidad de órbitas de cardinal 1, caben tres posibilidades:

1) $\alpha = n$.

En este caso G es abeliano. Como p y q son primos entre sí, existen subgrupos H y K tales que

$$G = H \odot K \simeq \mathcal{C}_p \times \mathcal{C}_q \simeq \mathcal{C}_{pq} = \mathcal{C}_n.$$

2) $1 < \alpha < n$.

Supongamos que hay al menos una órbita de cardinal p. Siendo b un elemento de la misma, su estabilizador, coincidente con su centralizador, tiene índice p, luego es de orden q. Será cíclico y como $b \in \mathcal{Z}(b)$, se tiene $\mathcal{Z}(b) =< b >$. Más, como $\mathcal{Z} \subseteq \mathcal{Z}(b)$ y $\mathcal{Z} \neq \{e\}$,se tiene $\mathcal{Z} =< b >$. El cociente $G/\mathcal{Z}$ será cíclico, de orden p, luego existe un $a \in G$ tal que

$$G/\mathcal{Z} = \{\mathcal{Z}, a\mathcal{Z}, a^2\mathcal{Z}, \ldots, a^{p-1}\mathcal{Z}\}.$$

Entonces,

$$p = Ord(a\mathcal{Z}) = Ord(\pi(a)) \mid Ord(a) \Rightarrow Ord(a) = p$$

(También podría ser el orden de a igual a n, pero ello contradice la hipótesis $\alpha < n$). Como b es central, se tiene $ab = ba$, luego ab es de orden n. Esto contradice de nuevo la hipótesis $\alpha < n$, luego en este supuesto es imposible la existencia de órbitas de cardinal p.

Puesto que no se ha usado para nada el hecho de que $p < q$, cambiando el papel de ambos números, se concluye también que no pueden existir órbitas de cardinal q.

De ambas exclusiones, lo que deducinos es que la posibilidad $1 < \alpha < n$ es inconsistente.

3) $\alpha = 1$.

Si hay β de cardinal p y γ de cardinal q, se tiene

$$1 + \beta p + \gamma q = pq \Rightarrow \beta p \equiv q - 1 \text{ mód } q.$$

Como $q > 1$ y $\mathbb{Z}/q\mathbb{Z}$ es un cuerpo, se deduce que β no puede ser nulo. Existiendo, pues, al menos una órbita de cardinal p, deducimos como en la parte anterior la existencia de un elemento b de orden q, tal que

$$\mathcal{Z}(b) =< b >,$$

si bien ahora no se trata del centro porque éste lo estamos suponiendo neutro. Sea $a \notin < b >$ y pongamos $H =< a >, K =< b >$. Probaremos varios lemas:

3.1) $H \cap K = \{e\}$.

Sea $0 \leq x < Ord(a)$. Como este orden es p o q, ambos primos, a^x genera aH, luego existe un exponente y tal que $(a^x)^y = a^{xy} =$ a. Entonces,

$$a^x \in K \Rightarrow a \in K,$$

en contra de su elección. Por tanto, $x = 0$. Esto prueba que $H \cap K = \{e\}$.

3.2) Supongamos dos exponentes $0 \leq x < y < Ord(a)$. Entonces,

$$a^x K \neq a^y \text{K}.$$

Si se diera la igualdad, tendríamos

$$a^x K = a^y K \Leftrightarrow a^x \equiv a^y, \text{ mód } K(\text{por la izquierda}) \Leftrightarrow (a^x)^{-1} a^y = a^{-x} a^y = a^{y-x} \in K$$

$$\Rightarrow a^{y-x} \in H \cap K \Rightarrow a^{y-x} = e \Rightarrow y - x = 0 \Rightarrow x = \text{ y}.$$

3.3) $Ord(a) = p$.

Si a tuviese orden q, según lo anterior, habría al menos q clases laterales. Esto es imposible porque, al ser K de orden q, su índice es

$$n/q = p < \text{ q}.$$

(Como la única condición para a es la a $\notin K$, se tiene que todos los elementos del complemento conjuntista de K son de orden p).

3.4) $G = HK$.

Puesto que

$$G = K \cup aK \cup a^2K \cup \ldots \cup a^{p-1}K,$$

todo elemento $g \in G$ es de la forma

$$g = a^x b^u, \text{ con } 0 \leq x < p, 0 \leq u < \text{ q}.$$

3.5) K es normal en G.

Sea $0 \leq u < q-1$. Si $u = 0$, trivialmente $g^{-1}b^u g = e \in K$, cualquiera que sea $g \in G$. En caso contrario, se tiene

$$Ord(g^{-1}b^u g) = Ord(b^u) = q \Rightarrow g^{-1}b^u g \in K,$$

porque de $g^{-1}b^u g \notin K$ se seguiría que su orden es $p < q$.

3.6) Existe un exponente μ tal que $2 \leq \mu \leq q-1$ para el cual

$$a^{-1}ba = b^{\mu}.$$

Por la normalidad de K, este exponente existe y no supera a $q-1$. No puede valer 0 porque ello implicaría $b = e$. No puede valer 1 porque ello nos conduciría al caso abeliano.

3.7) Para todo $v \in [0, q-1]$ se cumple

$$a^{-1}b^v a = b^{\mu v}.$$

Basta ver que

$$a^{-1}b^v a = (a^{-1}ba)^v = (b^{\mu})^v = b^{\mu v}.$$

3.8) Para todo $x \in [0, p-1]$ se cumple

$$a^{-x}ba^x = b^{\mu^x}.$$

Se razona por recurrencia: Para $x = 0, 1$ es de inmediata comprobación. En general,

$$a^{-(x+1)}ba^{x+1} = a^{-1}(a^{-x}ba^x)a = a^{-1}b^{\mu^x}a = b^{\mu\mu^x} = b^{\mu^{x+1}}$$

3.9) Para todo x tal que $1 \leq x \leq p$, se cumple

$$(ab)^x = a^x b^{(\mu^{x-1}+\ldots+\mu^2+\mu+1)}.$$

Se razona por recurrencia: Para $x = 1$ es trivial. En general, usando la igualdad $ba^x = a^x b^{\mu^x}$, equivalente a la 3.8, se tiene

$$(ab)^{x+1} = (ab)(ab)^x = (ab)(a^x b^{(\mu^{x-1}+\ldots+\mu^2+\mu+1)}) =$$

$$= a(ba^x)b^{(\mu^{x-1}+\ldots+\mu^2+\mu+1)} = a(a^x b^{\mu^x})b^{(\mu^{x-1}+\ldots+\mu^2+\mu+1)} =$$

$$= a^{x+1}b^{(\mu^x+\mu^{x-1}+\ldots+\mu^2+\mu+1)}$$

3.10) Siendo μ el exponente tal que $a^{-1}ba = b^{\mu}$, se cumple

$$\mu^{p-1} + \ldots + \mu^2 + \mu + 1 \equiv 0 \text{ mód } q.$$

Aplicando la fórmula anterior para $x = p$, y teniendo en cuenta que tanto a como ab son de orden p, se tiene

$$e = (ab)^p = a^p b^{(\mu^{p-1}+\ldots+\mu^2+\mu+1)} = b^{(\mu^{p-1}+\ldots+\mu^2+\mu+1)}$$

igualdad que equivale a la relación propuesta.

3.11) Siendo μ el exponente tal que $a^{-1}ba = b^{\mu}$, se cumple

$$\mu^p - 1 \equiv 0 \text{ mód } q.$$

Usando la igualdad

$$\mu^p - 1 = (\mu^{p-1} + \ldots + \mu^2 + \mu + 1)(\mu - 1),$$

por ser $\mu \geq 2$ y por ser $\mathbb{Z}/q\mathbb{Z}$ un cuerpo, la relación propuesta es equivalente a la de 3.10.

Asíllegamos a los siguientes enunciados:

Teorema 1: Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si existe un grupo G de orden n para el cual $\mathcal{Z} = \{e\}$, necesariamente se cumple $q \equiv 1$ mód p.

Demostración: La última fórmula indica que μ, como elemento del grupo multiplicativo $\Phi(q)$, debe ser de orden divisor de p. En realidad, es de orden p, porque $\mu > 1$ no puede ser de orden 1. Entonces,

$$p \mid (q-1) \Leftrightarrow (q-1) = pc \Leftrightarrow q = pc + 1 \Leftrightarrow q \equiv 1 \text{ mód } p.$$

Teorema 2: Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si $q \not\equiv 1$ mód p, el único grupo de orden n es el $\mathcal{C}_n$.

Demostración: La posibilidad $\mathcal{Z} = \{e\}$ es inconsistente, con lo cual la única de las planteadas para $\alpha = Ord(\mathcal{Z})$ es la $\alpha = n$, que nos condujo a esta única solución.

4 Simplificación con los teoremas de Sylow

El anterior estudio es elemental y por ello ha resultado prolijo. Si se recurre a los teoremas de Sylow, tenemos significativas simplificaciones

Proposición 01: Sea G un grupo de orden $n = pq$, donde p y q son primos tales que $2 \leq p < q$. Entonces, G admite un único subgrupo K de orden q, el cual es cíclico y normal.

Demostración: Siendo s_q la cantidad de subgrupos de orden q, los Teoremas de Sylow aseguran que

$$s_q \neq 0, \quad s_q \equiv 1 \text{ mód } q, \quad s_q \mid n.$$

Como los divisores de $n = pq$ son 1, p, q, pq, y los dos últimos son nulos, módulo q, se tendrá $s_q = 1$ o $s_q = p$. Pero, siendo $1 < p < q$, el valor $s_q = p$ no puede verificar la condición $s_q \equiv 1$, mód q, luego necesariamente es $s_q = 1$. Si K es tal subgrupo, será cíclico por tener orden primo y será normal por ser el único q-subgrupo de Sylow que admite G.

Proposición 02: Si $q \not\equiv 1$ mód p, G admite un único subgrupo H de orden p, el cual será cíclico y normal en G. En caso contrario, o bien G admite un único subgrupo H de orden p, cíclico y normal, o bien admite q subgrupos $H_1, H_2, \ldots, H_q$, de orden p, cíclicos y conjugados entre sí.

Demostración: Siendo s_p la cantidad de subgrupos de orden p, los Teoremas de Sylow aseguran que

$$s_p \neq 0, \quad s_p \equiv 1 \text{ mód } p, \quad s_p \mid n.$$

De los cuatro divisores $1, p, q, pq$, quedan descartados los valores segundo y cuarto por ser nulos, módulo p. Si, además, $q \not\equiv 1$ mód p, necesariamente debe ser $s_p = 1$. En este caso, el subgrupo H de orden p será cíclico por tener orden primo y será normal por ser el único p- subgrupo de Sylow en G. En cambio, si $q \equiv 1$ mód p, pueden darse las dos posibilidades $s_p = 1$ o $s_p = q$. En la segunda de ellas, los correspondientes subgrupos $H_1, H_2, \ldots, H_q$ de orden p serán cíclicos por tener orden primo y conjugados unos con otros por ser todos ellos p- subgrupos de Sylow de G.

Proposición 03: Siendo H uno de los p-subgrupos (haya uno o haya varios) y siendo K el q-subgrupo (normal), se prueba que

$$G = H[K].$$

Demostración: Como el orden de cualquier elemento de $H \cap K$ es divisor común de p y q, y estos números son primos entre sí, queda que el subgrupo intersección está formado por los elementos de orden 1, o sea, se reduce a $\{e\}$. Por otra parte, la normalidad de K implica que HK sea un subgrupo de G. Al ser trivial la intersección, se cumple

$$Ord(HK) = Ord(H)Ord(K) = pq = n = Ord(G) \Rightarrow HK = \text{ G.}$$

Con estas condiciones, G es efectivamente producto semidirecto de H y K.

Proposición 04: Si G admite un único subgrupo H de orden p, necesariamente $G \simeq \mathcal{C}_n$.

Demostración: En este caso, además de la condiciones

$$H \cap K = \{e\}, K \text{ mormal en } G, HK = G,$$

se tiene que también H es normal. Entonces,

$$G = H \odot K \simeq \mathcal{C}_p \times \mathcal{C}_q \simeq \mathcal{C}_{pq} = \mathcal{C}_n.$$

Proposición 05: Siendo $n = pq$, con $2 \leq p < q$, donde p y q son números primos absolutos, si $q \not\equiv 1$ mód p, el único grupo de orden n es el $\mathcal{C}_n$.

Demostración: Según 02, la condición $q \not\equiv 1$ mód p, nos conduce a que H sea único. Ahora basta aplicar 04.

5 Existencia de un grupo no conmutativo en el caso $q \equiv 1$ mód p

Si $p = 2$, al ser $q > p$ primo, es un número impar y siempre cumple la condición $q \equiv 1$ mód 2. En este caso sabemos que existe un grupo no conmutativo (único, además) de orden $n = 2q$, tratándose del $\mathcal{D}_q$. Tratamos ahora de generalizar esta existencia y unicidad. Situémonos en el grupo multiplicativo $\Phi(q)$, cíclico

y de orden $q - 1$ ya que q es primo. Sea γ una raíz primitiva mód q, esto es, un generador de $\Phi(q)$. Como ya hemos tenido ocasión de mostrar (Teorema 1 de nuestro estudio) se tiene

$$p \mid (q-1) \Leftrightarrow (q-1) = pc \Leftrightarrow q = pc + 1 \Leftrightarrow q \equiv 1 \text{ mód } p.$$

Luego en $\Phi(q)$ existe un subgrupo de orden p. Será el generado por

$$\gamma^{(q-1)/p},$$

y todos sus elementos, salvo el 1, serán de orden p, ya que p es primo. Sea $\mu \neq 1$ uno de ellos.

Tomemos los grupos $H = \mathcal{C}_p =< a >$ y $K = \mathcal{C}_q =< b >$. Puesto que $\mu < q$, será primo con él. Esto asegura que la aplicación

$$\alpha : K \to K, \text{ de ley } \alpha(b^v) = b^{v\mu}$$

es un automorfismo de K. Para cada $x \in [1,p], \alpha^x$será otro automorfismo. Cumplirá

$$\alpha^x(b) = b^{\mu^x}, \alpha^x(b^v) = b^{v\mu^x}.$$

La aplicación

$$\rho : H \to \mathrm{Aut}(K), \text{ de ley } \rho(a^x) = \alpha^x$$

$$\rho(a^x a^y)(b^v) = \rho(a^{x+y})(b^v) = b^{v\mu^{x+y}}$$

$$\rho(a^y)(\rho(a^x)(b^v)) = \rho(a^y)(b^{v\mu^x}) = b^{(v\mu^x)\mu^y}$$

$$\rho(a^x)(b^v) = b^{v\mu^x} = b^v \Rightarrow v(\mu^x - 1) \equiv 0 \text{ mód } q \Rightarrow \mu^x - 1 \equiv 0 \Rightarrow x = 0$$

es un monomorfismo que aplica H sobre un subgrupo de $\mathrm{Aut}(K)$, el cual subgrupo es, a su vez, isomorfo al subgrupo $< \mu >$ de $\Phi(q)$.

Esto permite construir el grupo

$$G = H_\rho \times K,$$

que es un producto semidirecto exterior de H por K.
La operación será
$(a^x, b^u)(a^y, b^v) = (a^x a^y, \rho(a^y)(b^u)b^v) = (a^{x+y}, b^{u\mu^y + v})$

Este grupo es de orden $n = pq$. No es conmutativo:

$$(e,b)(a,e) = (a,b^\mu) \neq (a,e)(e,b) = (a,b) \text{ porque } \mu > 1.$$

Hay un subgrupo $K^* = \{(e,b^u)\}$ de orden q, isomorfo a K
Hay un subgrupo , etc.
Este modelo responde a la propuesta.

Supongamos otro G' que también lo haga. Debo ver que son isomorfos

Tomo d, c en G' cumpliendo todos los requisitos del estudio.
$c^{-1}dc = d^{\mu^h}$
Se tiene

$$\varphi : H_\rho \times K \to G', \text{ de ley}$$

$$\varphi(a^x, b^u) = c^{kx} d^u$$

Si $\mu^h = \mu'$, debe ser $hk \equiv 1$ mód p

a) Veamos que φ es un morfismo de grupos:

$$\varphi((a^x, b^u)(a^y, b^v)) = c^{kx+ky} d^{\mu^y + v}$$

$$\varphi(a^x, b^u)\varphi(a^y, b^v) = (c^{kx}d^u)(c^{ky}d^v) =$$
$$= c^{kx}c^{ky}(c^{-ky}d^u c^{ky})d^v =$$
$$= c^{kx+ky}(c^{-ky}dc^{ky})^u d^v =$$
$$= c^{kx+ky}(d^{(\mu^h)^{ky}})^u d^v = c^{kx+ky}d^{u\mu^{hky+v}}$$

Hay que comprobar que

$$c^{kx}d^u = e \Rightarrow x = u = 0, \text{ luego es inyectiva.}$$

Como ambos son de igual orden, es biyectiva.

Referencias

[1] Alperin, J. L., *Centralizers of abelian normal subgroups of p-groups*, Jour. Alg., **1** (1964), 110–113.

[2] Bender, H., *A group theoretic proof of Burnside's p^aq^b-theorem*, Math. Z. **126** (1972), 327–338.

[3] Burnside, W., *Theory of Groups of Finite Order*, 2nd edition, Dover, New York, 1955.

[4] Robinson, Derek J. S., *A Course in the Theory of Groups*, Springer, New York, 1995.

[5] Fraleigh, J. B., *lgebra Abstracta*, Addison-Wesley Iberoamericana, 1987.

[6] Gorenstein, D. *Finite Groups*, Chelsea, New York, 1980.

[7] Jacobson, N. *Basic Algebra*, 2nd edition. Freeman and Company, New York, 1985.

[8] Kerber, A. *Aplied Finite Group Actions*, 2nd edition, Springer 1999.

[9] Kurosh, A., *Group Theory*, Chelsea, New York, 1979.