Lecturas Matemáticas
Volumen **24** *(2003), páginas 123–136*

Teoremas de isomorfía en grupos diedros

Primitivo Belén Acosta Humánez
Universidad Sergio Arboleda, Bogotá

Dedicado a la memoria del Profesor Jairo Charris Castañeda

Abstract. In this paper we discuss the principal results obtained in my bachelor dissertation, supervised by Professor Jairo Charris Castañeda. We discuss only the so called (p, q) groups, in particular, the dihedral groups.

Key words and phrases. Dihedral group, cyclic groups, $(p.q)$ groups, Sylow theorems.

1991 Mathematics Subject Classification. 08A62.

Resumen. En este artículo discutimos los resultados principales alcanzados en mi trabajo de grado, el cual fue dirigido por el profesor Jairo Charris Castañeda. La discusión la limitaremos a los llamados (p, q) grupos, en particular a los grupos diedros.

1. Definiciones y Resultados Principales

El problema de la existencia de grupos con propiedades específicas se aborda usualmente mediante la teoría de los llamados grupos libres (y de los subgrupos y grupos cocientes de éstos determinados mediante generadores y relaciones). Esta teoría, bastante abstracta, conduce generalmente, para su concreción, a la llamada teoría de la representación de los grupos, un tema relativamente avanzado de la matemática, que hace buen uso del álgebra lineal y de la teoría de matrices, y que

no consideraremos aquí. Las demostraciones de los lemas, corolarios y teoremas omitidos en este artículo pueden verse en [1] y [2]. Las ideas principales de este trabajo surgieron de la lectura de [4]. Para ver el sentido geométrico de los grupos diedros véase al respecto [3].

Definición 1.1. Sean p, q enteros, $p \geq 1$, $q \geq 1$. Se dice que un grupo $(G, \cdot)$ es del tipo (p, q), si existen $a, b \in G$ y $1 < r < q$ tales que:

(i) $\mid a \mid = p$, $\mid b \mid = q$.
(ii) $ab = b^r a$.
(iii) Todo elemento $x \in G$ se escribe de manera única en la forma $x = a^i b^j$, donde $i, j \in \mathbb{Z}$, $0 \leq i < p$, $0 \leq j < q$.

Obsérvese que $q \geq 3$ y que G es no conmutativo, así que $p \geq 2$. De (iii) se deduce además que G es finito con

$$\circ(G) = pq. \tag{1}$$

Nota 1.2. Si $(G, \cdot)$ es como en la Definición 1.1, se dice, más precisamente, que $(G, \cdot)$ es del tipo (p, q) y generado por (a, b).

De la Definición 1.1 se deduce fácilmente que

(iv) $ab^{r^n} = b^{r^{n+1}} a$, $n = 0, 1, 2, ...$
(v) $a^n b = b^{r^n} a^n$, $n = 0, 1, 2, ...$
(vi) $a^n b^s = b^{sr^n} a^n$, $n \geq 0$, $s \in \mathbb{Z}$.

En efecto, la afirmación (iv) es cierta si $n = 0$, y para $n > 0$ resulta de que $ab^{r^n}a^{-1} = \left(aba^{-1}\right)^{r^n} = (b^r)^{r^n} = b^{r^{n+1}}$. La demostración de (v) resulta de un sencillo argumento por inducción basado en (iv), y la de (vi), de observar que $a^n b^s a^{-n} = (a^n b a^{-n})^s = \left(b^{r^n}\right)^s = b^{sr^n}$. Tal como se mostrará en detalle a continuación.

Además,

$$r^p \equiv 1 \,(\mathrm{mod}\, q)\,,\ \mathrm{mcd}(r, q) = 1. \tag{2}$$

En efecto, de (v), $a^p b = b^{r^p} a^p$, o sea, $b = b^{r^p}$. Entonces $b^{r^p - 1} = e$, de lo cual $q | r^p - 1$. Por otra parte, si fuera $\mathrm{mcd}(r, q) = d \neq 1$, sería $|b^r| = q/d$, lo cual es absurdo, pues de $b^r = aba^{-1}$ se deduce que $|b^r| = |b| = q$.

Como evidentemente $a^{-1} = a^{p-1}$, (2) y la validez de (vi) para $n \geq 0$ implican su validez para todo $n \in \mathbb{Z}$, así que

(vii) $a^n b^s = b^{sr^n} a^n$, $b^s a^n = a^n b^{sr^n}$, $n, s \in \mathbb{Z}$.

Teorema 1.3. *Sea $(G, \cdot)$ del tipo (p, q) y generado por (a, b). Sean $M = [a]$ y $N = [b]$. Entonces $G = MN$ y N es un subgrupo normal de G. Además, $M \cap N = \{e\}$.*

Demostración. Que $G = MN$ resulta inmediatamente de (iii). Por otra parte, de (ii) existe $1 < r < q$ tal que $aba^{-1} = b^r$, y de (vii) resulta que $a^n b^s a^{-n} = b^{sr^n} \in N$ cualesquiera que sean $s, n \in \mathbb{Z}$. Sean entonces $0 \leq i < p$, $0 \leq j < q$ y $x = a^i b^j \in G$. Entonces $xb^s x^{-1} = a^i \left(b^j b^s b^{-j}\right) a^{-i} = a^i b^s a^{-i} \in N$ cualquiera que sea $s \in \mathbb{Z}$, lo cual demuestra que N es normal. Finalmente, de $\circ\left(M \Big/ M \cap N\right) = \circ\left(MN \Big/ N\right) = \circ\left(G \Big/ N\right) = p$ se deduce que $\circ(M \cap N) = 1$, lo cual completa la demostración. ☑

Nota 1.4. Obsérvese que en el anterior teorema, la aplicación

$$\varphi : M \times N \to G,\ \varphi(x, y) = xy,$$

resulta ser biyectiva. Sin embargo, no puede ser un isomorfismo de grupos. En efecto, M no puede ser normal en G (pues sería $ab = ba$ y (ii) no podría ser válida), así que G no puede ser el producto directo de M y N.

Nota 1.5. Es claro que si $(G, \cdot)$ es finito y no conmutativo, y si $G = MN$ donde M y N son subgrupos cíclicos de G tales que $M \cap N = \{e\}$ y que N es normal en G, entonces G es del tipo (p, q) donde $p = \circ(M)$ y $q = \circ(N)$, y si $M = [a]$ y $N = [b]$, entonces (a, b) genera a G. En efecto, es claro que (i) y (iii) se satisfacen para (a, b) y que $aba^{-1} = b^r$, $0 \leq r < q$. Obviamente no puede ser $r = 0$, pues $b \neq e$, y tampoco puede ser $r = 1$, pues $(G, \cdot)$ no es conmutativo. Obsérvese que, bajo las hipótesis, $p \geq 2$ y $q \geq 3$.

Nota 1.6. Demostrar la existencia de grupos de un tipo (p, q) dado no es, en general, una tarea fácil. Nosotros no haremos esto sino en algunos casos muy especiales, pero, esperamos, muy significativos.

Definición 1.7 Se dice que un grupo G del tipo $(2,q)$ es diedro, si está generado por un par (a,b) tal que $\mid a \mid = 2, \mid b \mid = q$ y

$$aba^{-1} = b^{-1}. \tag{3}$$

Se escribe $G = D_q(a,b)$.

Nota 1.8. Obsérvese que $b^{-1} = b^{q-1}$.

Teorema 1.9. *Si $(G,\cdot)$ es un grupo de orden $2q$ con $q \geq 3$, $a \in G$ es tal que $\mid a \mid = 2$, y existe $b \in G$ con $\mid b \mid = q$ y $aba^{-1} = b^{-1}$, entonces G es diedro y generado por (a,b), así que $G = D_q(a,b)$.*

Es necesario demostrar que G es del tipo $(2,q)$, o sea, que (iii) de la Definición 1.1 se verifica. Esto será consecuencia del resultado más general siguiente.

Teorema 1.10. *Sea $(G,\cdot)$ un grupo de orden pq, donde p es primo. Si para algún $a \in G$ tal que $\mid a \mid = p$ existe $b \in G$ tal que $\mid b \mid = q$ y que*

$$aba^{-1} = b^r,\ 1 < r < q, \tag{4}$$

entonces G es del tipo (p,q) y generado por (a,b).

Demostración. Sean $M = [a]$ y $N = [b]$. Entonces $M \cap N = \{e\}$, ya que si $a^s \in N$, $1 \leq s < p$, entonces $M = [a^s] \subseteq N$, lo cual es absurdo, pues como N es conmutativo, (4) no podría tenerse con $r \neq 1$. Entonces $\#(MN) = pq$ y $G = MN$. Como (4) garantiza también que N es normal en G, el teorema resulta de lo dicho en la Nota 1.5. ☑

Demostraremos ahora la existencia de grupos diedros. El resultado es clásico.

Teorema 1.11. *Para todo $q \geq 3$ existen grupos diedros de orden $2q$. Uno de ellos es el subgrupo $D_q(\sigma,\rho)$ de S_q generado por el $q-$ciclo $\rho = (1,2,...,q)$ y la permutación σ dada por*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & \dfrac{q+1}{2} & \dfrac{q+3}{2} & \ldots & q \\ 1 & q & q-1 & \ldots & \dfrac{q+3}{2} & \dfrac{q+1}{2} & \ldots & 2 \end{pmatrix} \tag{5}$$

si q es impar y por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & \frac{q}{2} & \frac{q+2}{2} & \frac{q+4}{2} & ... & q \\ \\ 1 & q & q-1 & ... & \frac{q+4}{2} & \frac{q+2}{2} & \frac{q}{2} & ... & 2 \end{pmatrix} \tag{6}$$

si q es par.

Demostración. Nótese que σ es simplemente la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & q-1 & q \\ \\ 1 & q & q-1 & ... & 3 & 2 \end{pmatrix}.$$

Evidentemente $\sigma \neq e$ y, como se deduce de (5) y (6),

$$\sigma = (2, q)\,(3, q-1)\,...\left(\frac{q+1}{2}, \frac{q+3}{2}\right),\ q \text{ impar}, \tag{7}$$

y

$$\sigma = (2, q)\,(3, q-1)\,...\left(\frac{q}{2}, \frac{q+4}{2}\right),\ q \text{ par}. \tag{8}$$

Siendo producto de transposiciones disyuntas, $\sigma^2 = e$. Además, $\sigma\rho\sigma^{-1} = \sigma^{-1}\rho\sigma = (\sigma(1), \sigma(2), ..., \sigma(q)) = (1, q, q-1, ..., 2) = \rho^{-1}$, y se tiene que $\mid \rho \mid = l(\rho) = q$. Por lo tanto, si G es el subgrupo de S_q generado por $\{\sigma, \rho\}$, el Teorema 1.9 garantiza que $G = D_q(\sigma, \rho)$. ☑

Nota 1.12. Si σ es una permutación de S_q tal que $\sigma^{-1}\rho\sigma = \rho$, donde $\rho = (1, 2, ..., q)$, entonces $(\sigma(1), \sigma(2), ..., \sigma(q))$ es $(k+1, k+2, ..., q, 1, 2, ..., k)$ para algún $1 \leq k \leq q$, así que

$$\sigma\,(j) = \begin{cases} k + j,\ 1 \leq j \leq q - k \\ q - k + j,\ q - k < j \leq q \end{cases} \tag{9}$$

Entonces $\sigma = \rho^k$, $1 \leq k \leq q$. Se deduce que si σ, τ son tales que $\sigma\rho\sigma^{-1} = \rho^{-1}$ y $\tau\rho\tau^{-1} = \rho^{-1}$, en cuyo caso $\tau^{-1}(\sigma\rho\sigma^{-1})\tau = \rho$, necesariamente $\sigma^{-1}\tau = \rho^k$ para algún $0 \leq k < q$, de lo cual $\tau = \sigma\rho^k \in D_q(\sigma, \rho)$. Es decir, todas las permutaciones τ tales que $\tau\rho\tau^{-1} = \rho^{-1}$ están en el grupo $D_q(\sigma, \rho)$ del Teorema 1.10, y como además $\left(\sigma\rho^k\right)^2 =$

$\sigma\rho^k\sigma\rho^k = \rho^{-k}\rho^k$ para σ en tal teorema, necesariamente $\tau^2 = e$. Entonces $D_q(\sigma,\rho) = D_q(\tau,\rho)$, así que $D_q(\sigma,\rho)$ no depende de σ en tanto $\sigma\rho\sigma^{-1} = \rho^{-1}$. Tampoco depende de ρ en tanto ρ sea una potencia $k-$ésima de $(1,2,...,q)$ con $\text{mcd}(q,k) = 1$, pero, en general, ρ no puede sustituirse por un $q-$ciclo arbitrario. Obsérvese finalmente que

$$D_q(\sigma,\rho) = \{e,\sigma\} \cup \{\rho^k \mid 1 \leq k < q\} \cup \{\sigma\rho^k \mid 1 \leq k < q\} \qquad (10)$$

y que la reunión es disyunta. Si $(G,\cdot)$ es un grupo no conmutativo de orden $2q$ y N es un subgrupo de orden q de G, N es necesariamente normal en G. En efecto, si $a \in G$ y $a \notin N$ entonces $aN \cap N = N \cap Na = \phi$. Como $[G:N] = 2$ entonces $G = aN \cup N = N \cup Na$, lo cual implica que $aN = Na$. En virtud de lo dicho en la Nota 1.4, si existe $b \in N$ tal que $\mid b \mid = q$ (lo cual ocurre, por ejemplo, si q es primo), y $\mid a \mid = 2$, G es del tipo $(2,q)$ y generado por (a,b). Esto no garantiza que G sea diedro. Este es sin embargo el caso si $q \geq 3$ es primo, pues si $aba^{-1} = b^r$, $1 < r \leq q-1$, de $r^2 \equiv 1 (\text{mod}\, q)$ (relación (2)) se deduce que $q \mid (r-1)(r+1)$, así que $q = r+1$ y $r = q-1$. Entonces:

Teorema 1.13. *Si G es no conmutativo y de orden $2q$, donde $q \geq 3$ es primo, entonces G es diedro, y si $a,b \in G$ son tales que $\mid a \mid = 2$, $\mid b \mid = q$, G está generado por (a,b), y $aba^{-1} = b^{-1}$.*

Nota 1.14. Obsérvese que obviamente $2 \mid q-1$ en el teorema anterior.

Caracterizaremos ahora como grupos del tipo (p,q) a los grupos no conmutativos de orden pq donde $p < q$ son primos. Necesitaremos el siguiente lema.

Lema 1.15. *Si $(G,\cdot)$ es un grupo no conmutativo de orden pq, donde $p < q$ son primos, entonces $p \mid q-1$, y si $b \in G$ es tal que $\mid b \mid = q$, $N = [b]$ es un subgrupo normal de G.*

Demostración. Se utilizará la Teoría de Sylow. ☑

El siguiente lema es nuestro, y en cierta forma generaliza significativamente el anterior.

Lema 1.16. *Si G es un grupo no conmutativo de orden pq donde p es el menor primo que divide $\circ(G)$. No se supone que q sea primo, pero*

si que $p \nmid q$ y que existe $b \in G$ tal que $|b| = q$. Entonces $N = [b]$ es normal en G, $p \mid \varphi(q)$ y G es del tipo (p, q) y generado por (a, b) para todo $a \in G$ con $|a| = p$.

Demostración. Que N es normal resulta de la Teoría de Sylow. Entonces

$$aba^{-1} = b^r$$

y podemos suponer que $r < q$. También que $r > 1$, pues como antes, todo elemento $u \in G$ se escribe $u = a^i b^j$ y G no es conmutativo. Tal como en la relación (2) del artículo, se demuestra que $\text{mcd}(r, q) = 1$, así que la clase $\overline{r}$ módulo q está en $U(\mathbb{Z}_q)$. Por otra parte, también de (2) se deduce que $|\overline{r}| = p$. Entonces $p \mid \varphi(q)$. ☑

Teorema 1.17. *Si G es no conmutativo de orden pq^n donde $p < q$ son primos. Supóngase que existe $b \in G$ tal que $|b| = q^n$. Entonces $N = [b]$ es normal en G, $p \mid q - 1$ y G es del tipo (p, q^n) y generado por (a, b), donde $a \in G$ es tal que $|a| = p$.*

Demostración. $\varphi(q^n) = (q-1)q^{n-1}$. ☑

Corolario 1.18. *Si $(G, \cdot)$ es no conmutativo y de orden pq, donde $p < q$ son primos, entonces $p \mid q - 1$, y si $a, b \in G$ son tales que $\mid a \mid = p$ y $\mid b \mid = q$, G está generado por (a, b).*

Demostraremos ahora la existencia de algunos grupos del tipo (p, q). Son nuestros el Lema 1.19, el Corolario 1.20 y el Teorema 1.22.

Lema 1.19. *Sean $\rho = (1, 2, ..., q)$ un $q-$ciclo, $1 \leq k < q$, $m = mcd(q, k)$. Entonces ρ^k tiene orden $2/m$. Supóngase que $\rho^k = \rho_1 ... \rho_n$, $n \geq 1$, donde los ρ_i son ciclos disyuntos no triviales. Entonces $|\rho_i| = q/m$ y $n = m$. Es decir, ρ^k es el producto de $m-$ciclos de longitud q/m cada uno.*

Demostración. Como $|\rho| = q$, es claro que $|\rho^k|^{q/k} = e$, así que $|\rho^k| = q/m$. Si fuera $|\rho^k| < q/m$, sería $|\rho| < q$, lo cual es absurdo. Ahora, es claro que $|\rho_i| \leq q/m$ para $i = 1, 2, ..., n$, pues $|\rho| = \text{mcm}(|\rho_1|, ..., |\rho_n|)$, lo cual muestra también que no puede ser $|\rho_i| < q/m$. Entonces $|\rho_i| = q/m$,

$i = 1, 2, ..., n$, y como $l(\rho)^n = l(\rho_1) + ... + l(\rho_n) = n\dfrac{q}{m}$, necesariamente $n = m$. ☑

Corolario 1.20. *Si $mcd(q, k) = 1$, y $\rho = (1, ..., q)$, ρ^k es aún un ciclo de longitud q.*

Demostración. Consecuencia del Lema 1.19. ☑

Nota 1.21. Sea σ una permutación no trivial con $\sigma(1) = 1$, y sea $\rho = (1, 2, ..., q)$, si $\sigma = \rho^k$, donde $0 \leq k < q$, necesariamente $k = 0$. Esto es consecuencia de lo dicho en el Lema 1.19 (pues ρ^k no puede dejar de mover a 1).

Teorema 1.22. *Sean G un grupo no conmutativo de orden pq donde q es un entero y p es un primo que es menor que cualquier primo que divida a q. Supóngase además que $p \mid \varphi(q)$. Entonces existen $1 < r < q$ con $r^p \equiv 1 (\mathrm{mod}\, q)$ tal que $mcd(r, q) = 1$ y $\sigma, \rho \in S_q$ tales que*

$$|\sigma| = p, \ |\rho| = q \tag{11}$$

y que el subgrupo generado $D[p, q]$ de S_n generado por σ y ρ es del tipo (p, q) y generado por (σ, ρ). Además

$$\sigma\rho\sigma^{-1} = \rho^r. \tag{12}$$

Demostración. Podemos suponer que $p > 2$ (Teorema 1.13). Sea $1 < r < q$, mínimo, tal que $\overline{r}$ sea solución de la ecuación $x^p = \overline{1}$ en $\mathbb{Z}_q^*$. Sean $\rho = (1, 2, ..., q)$ y σ una permutación de S_q tales que $\sigma\rho\sigma^{-1} = \rho^r$ y que $\sigma(1) = 1$. Tal permutación existe pues ρ^r es también un $q-$ciclo, y la condición $\sigma(1) = 1$ la determina unívocamente. Sea $D[p, q]$ el subgrupo de S_q generado por $\{\sigma, \rho\}$. Claramente $\mid \rho \mid = q$. Demostraremos que $\sigma^p = e$, lo cual, dado que $\sigma \neq e$ (pues $\rho^r = (\sigma^{-1}(1), ..., \sigma^{-1}(q)) \neq \rho$), asegurará que $\mid \sigma \mid = p$, y completará, en virtud del Corolario 1.18, la demostración. Pero, tal como en la demostración de (v), se deduce, a partir de $\sigma\rho = \rho^r\sigma$, que $\sigma^p\rho = \rho^{r^p}\sigma^p$. Entonces $\sigma^p\rho = \rho\sigma^p$, pues $r^p \equiv 1 (\mathrm{mod}\, q)$. En virtud de lo dicho en la Nota 1.12, esto implica que

$\sigma^p = \rho^k$ es un producto de ciclos disyuntos no triviales, necesariamente $k = 0$ y $\sigma^p = e$. ☑

Corolario 1.23. *Sean G un grupo no abeliano de orden pq donde $p < q$ son primos tales que $p \mid q-1$. Sean $1 < r < q$ tal que $r^p \equiv 1 (\mathrm{mod}\, q)$, $mcd(r,q) = 1$. Sea $m \geq 1$. Entonces existen $\sigma, \rho \in S_{qm}$ tales que el subgrupo $D[p,q]$ generado por σ, ρ es del tipo (p,q) y*

$$\sigma\rho\sigma^{-1} = \rho^r. \tag{13}$$

Demostración. Consecuencia del Teorema 1.22. ☑

Nota 1.24. Si G tiene orden pq, donde $p < q$ son primos, y M y N son subgrupos respectivos de órdenes p y q de G, entonces G es cíclico si y sólo si M y N son normales en G (que es el caso si $p \nmid q-1$). En efecto, si $M = [a]$, $N = [b]$ y son normales, $ab = ba$, lo cual implica que $\mid ab \mid = \mid a \mid\mid b \mid = pq$. En tales circunstancias $G \approx \mathbb{Z}_{pq}$ (lo cual es aún posible si $p \mid q-1$).

2. Teoremas de isomorfía

Estudiaremos ahora el problema de la isomorfía de los grupos del tipo (p,q) y de los grupos diedros. Los resultados son en una u otra forma conocidos, pero nunca hemos visto una exploración tan detallada como la que sigue.

Teorema 2.1. *Sean $(G_1, \cdot)$ y $(G_2, \cdot)$ grupos del tipo (p,q), con generadores respectivos (a_1, b_1) y (a_2, b_2). Si $a_i b_i a_i^{-1} = b_i^r$, $1 < r < q$, $i = 1, 2$, entonces $G_1 \approx G_2$.*

Demostración. Sean $a = a_i$, $b = b_i$, $i = 1, 2$. Entonces $\left(a^i b^j\right)\left(a^h b^k\right) = a^i \left(b^j a^h\right) b^k$, donde $0 \leq i, h < p$, $0 \leq j, k < q$, de lo cual, mediante (vii), $\left(a^i b^j\right)\left(a^h b^k\right) = a^{i+h} b^{jr^h + k}$. Por lo tanto, si $f : G_1 \to G_2$ está

dada por $f\left(a_1^i b_1^j\right) = a_2^i b_2^j$, $i, j \in \mathbb{Z}$ (que f está bien definida resulta de (iii)), entonces

$$f\left(\left(a_1^i b_1^j\right)\left(a_1^h b_1^k\right)\right) = f\left(a_1^{i+h} b_1^{jr^h+k}\right) = a_2^{i+h} b_2^{jr^h+k} = \left(a_2^i b_2^j\right)\left(a_2^h b_2^k\right)$$
$$= f\left(a_1^i b_1^j\right) f\left(a_1^h b_1^k\right),$$

así que f es un homomorfismo; de hecho, un epimorfismo. Que f es inyectiva resulta de observar que si $f\left(a_1^i b_1^j\right) = a_2^i b_2^j = e$, donde $0 \leq i < p$, $0 \leq j < q$, necesariamente $i = j = 0$, de lo cual $a_1^i b_1^j = e$. Esto demuestra el teorema. ☑

Corolario 2.2. *Todo grupo diedro G de orden $2q$ es isomorfo al grupo $D_q(\sigma, \rho)$.*

Necesitaremos ahora el siguiente lema.

Lema 2.3. *Si G es del tipo (p, q) y está generado por (a, b) con $aba^{-1} = b^r$, $1 < r < q$, y si $1 \leq l < p$ es tal que $mcd(r^l, q) = 1$, entonces G está también generado por a y por $b_1 = b^{r^l}$. Además, $ab_1a^{-1} = b_1^r$.*

Demostración. Como $\text{mcd}(r^l, q) = 1$ entonces $\mid b_1 \mid = q$, y la relación $ab_1a^{-1} = b_1^r$ resulta fácilmente de (vii). Ahora, si $M = [a]$ y $N = [b]$ entonces $G = MN$ y $M \cap N = \{e\}$, y como $N = [b_1]$, (iii) es también válida para (a, b_1) (Nota 1.4). ☑

Teorema 2.4. *Si G_1 y G_2 son del tipo (p, q), donde $p < q$ son primos, entonces $G_1 \approx G_2$.*

Demostración. Supóngase que G_1 está generado por a_1 y b_1, con $a_1b_1a_1^{-1} = b_1^r$, $1 < r < q$, y que G_2 lo está a su vez por a_2 y b_2 con $a_2b_2a_2^{-1} = b_2^s$, $1 < s < q$. De (2), $r^p \equiv 1 (\mod q)$ y $s^p \equiv 1 (\mod q)$. En virtud del Teorema 1.3, esto implica que $s \equiv r^k (\mod q)$, $0 \leq k < p$. De hecho $k > 0$, pues $q \nmid s - 1$, y $q \nmid r^k$, ya que $q \nmid s$. Entonces $\text{mcd}(r^k, q) = 1$. Del Lema 2.3 se deduce entonces, reemplazando a b_2 por $b_2^{r^k}$, si es necesario, que podemos suponer $s = r$. En virtud de lo establecido en el Teorema 2.1, esto implica que $G_1 \approx G_2$. ☑

Nota 2.5. Se deduce que si G es del tipo (p, q), donde $p < q$ son primos, G está generado por (a, b) y (c, d), y $aba^{-1} = b^r$, $cdc^{-1} = d^s$, $1 < r$, $s < q$, entonces existe $0 < k < p$ tal que $s \equiv r^k (\mathrm{mod}\, q)$.

Corolario 2.6. *Si G_1 y G_2 son grupos no conmutativos de orden pq, donde $p < q$ son primos, entonces $G_1 \approx G_2$.*

Invocando los Corolarios 2.2 y 2.6, se tiene el resultado más preciso siguiente.

Corolario 2.7. *Si G es un grupo no conmutativo de orden pq donde $p < q$ son primos, entonces $p \mid q - 1$, y G es, de hecho, isomorfo al grupo $D[p, q]$.*

Nota 2.8. Se concluye que si G es un grupo de orden pq, donde $p < q$ son primos, se tiene la alternativa

1. $G \approx \mathbb{Z}pq$.
2. $G \approx D[p, q]$.

La primera posibilidad ocurre si y sólo si G es abeliano, lo cual se da automáticamente si $p \nmid q - 1$. La segunda posibilidad ocurre si y sólo si G es no abeliano, lo cual sólo es posible si $p \mid q - 1$.

Nota 2.9. El grupo diedro $D_q\,(\sigma, \rho)$ admite una interpretación simple y sugestiva que no deja de ser útil para calcular explícitamente tal grupo en casos especiales: como el grupo de las simetrías de un polígono regular de q lados.

Considérese el conjunto $S(q)$ de las simetrías de un polígono regular de q lados con respecto a sus "elementos de simetría". Estos últimos son:

1. Las bisectrices de los ángulos en los vértices, es decir, las rectas del plano que bisecan cada uno de estos ángulos.

2. El centro del polígono: punto de intersección de las bisectrices.

3. Las mediatrices, es decir, las rectas del plano que unen los puntos medios de lados opuestos.

Las mediatrices son elementos de simetría sólo cuando q es par, y son $\dfrac{q}{2}$ en número. Las correspondientes simetrías son:

a. Las reflexiones sobre una bisectriz.

b. Las rotaciones en un ángulo $\frac{2\pi}{q}k$, $k = 1, 2, ..., q$, alrededor del centro.

c. Las reflexiones sobre una mediatriz, cuando q es par.

Nótese que las bisectrices son q si q es impar y sólo $\frac{q}{2}$ si q es par, pues en este último caso cada una de ellas biseca simultáneamente dos ángulos.

Esto determina el número de posibles simetrías con respecto a cada uno de los elementos: $\frac{q}{2}$ reflexiones sobre las bisectrices si q es par; q, si q es impar; el número de rotaciones alrededor del centro es siempre q; cuando q es par habrá además $\frac{q}{2}$ reflexiones sobre las mediatrices. Esto da un total de $2q$ simetrías en cada caso. Así , $\#(S(q)) = 2q$. La ley de composición que hace de $S(q)$ un grupo se obtiene dando un sentido dinámico a las simetrías: reflejar sobre una recta, rotar en un cierto ángulo. La composición se obtiene entonces efectuando una de tales acciones, α, y seguidamente la otra, β. El resultado se escribe $\beta \circ \alpha$ o $\alpha\beta$, según el gusto. Nosotros preferiremos la segunda notación. Como es claro, cualquier sucesión de tales acciones deja invariante el polígono y debe ser por lo tanto una de las simetrías mencionadas. Es además claro que si α es una reflexión entonces $\mid \alpha \mid = 2$, y que si β es una rotación en un ángulo $\frac{2\pi}{q}$ entonces $\mid \beta \mid = q$.

Para interpretar $S(q)$ en términos de $D_q(\sigma, \rho)$, enumérense los vértices del polígono de 1 a q en el sentido positivo (el opuesto al del movimiento de las manecillas del reloj). Luego escójase un sistema de coordenadas $x - y$ en el plano de tal manera que el eje y sea la bisectriz al primer vértice del polígono, así que el centro de éste está también sobre el eje y. Colóquese finalmente el centro del polígono en el punto $(0, 0)$ del sistema $x - y$, y efectuando una rotación del polígono en un ángulo π, si es necesario, colóquese su primer vértice en el semiplano superior del sistema de coordenadas. Diremos en este caso que el polígono está en posición inicial canónica. Sea β la rotación en el sentido positivo

en un ángulo $\frac{2\pi}{q}$. Los vértices se permutarán en el orden $1 \to 2 \to 3 \to ... \to q-1 \to q \to 1$, y es natural describirla mediante el ciclo $(1, 2, 3, ..., q-1, q) = \rho$. A su vez, la reflexión α sobre el eje y (la bisectriz al primer vértice) permutará los vértices en la forma $1 \to 1$, $2 \to q$, $3 \to q-1$, $..., q-1 \to 3$, $q \to 2$, y puede entonces describirse mediante la permutación σ dada por (5) o (6) en el Teorema 1.11. Como es obvio, con estas identificaciones $\alpha\beta$ se identifica con $\sigma\rho$, y más generalmente, $\alpha^i\beta^j$, $i = 1, 2$, $j = 1, 2, ...q$, con $\sigma^i\rho^j$. Podemos entonces considerar que $S(q)$ es un subgrupo de $D_q(\sigma, \rho)$, así que $S(q) = D_q(\sigma, \rho)$. Como es claro, $\alpha^2 = e$ (todo queda quieto) y β^k, $1 \leq k \leq q$, es la rotación en un ángulo $\frac{2\pi}{q}k$, con $\beta^q = e$, así que si α_i denota la reflexión sobre la bisectriz al $i-$ésimo vértice ($\alpha_1 = \alpha$) y γ_j es la reflexión sobre la mediatriz por el punto medio del lado $[j, j+1]$, entonces

$$S(q) = \{\beta^k \mid 1 \leq k \leq q\} \cup \{\alpha_i \mid 1 \leq i \leq q\},\ q \text{ impar} \tag{14}$$

y

$$S(q) = \{\beta^k \mid 1 \leq k \leq q\} \cup \{\alpha_i \mid 1 \leq i \leq \frac{q}{2}\} \cup \{\gamma_j \mid 1 \leq j \leq \frac{q}{2}\},\ q \text{ par.} \tag{15}$$

La identificación de $S(q)$ con $D_q(\sigma, \rho)$ permite calcular rápidamente este último grupo en casos particulares. En cierta forma $S(q)$ establece, de manera intuitiva, la existencia de grupos diedros, suministrando un recurso adicional nada despreciable en la teoría de los grupos.

Referencias

[1] P. B. Acosta, *Grupos diedros y del tipo* (p, q). Trabajo de grado. Universidad Sergio Arboleda, Bogotá, DC, 2003.

[2] J. A. Charris, B. H. Aldana, P. B. Acosta, *Álgebra I. Fundamentos y teoría de los grupos*. Academia Colombiana de Ciencias Físicas, Exactas y Naturales en coedición con la Universidad Sergio Arboleda. de próxima aparición.

[3] J. B. Fraleigh, *A First Course in Abstract Algebra*, sixth edition. Addison Wesley Longman. New York. 2000.

[4] Hungerford, Thomas, *Algebra*, Graduate Texts in Mathematics, Springer Verlag. New York. 1973.

(Recibido en septiembre de 2003)

Primitivo Belén Acosta
e-mail: primitivo.acosta@usa.edu.co
Escuela de Matemáticas, Universidad Sergio Arboleda
Bogotá, Colombia