Boletín de Matemáticas
Nueva Serie Vol.I No.1 (1994) (9-15)

LOS CUATERNIONES Y SU GRUPO DE AUTOMORFISMOS

CLAUDIA GÓMEZ Y
VÍCTOR ARDILA DE LA P.

Universidad de Nariño
Universidad Nacional de Colombia

ABSTRACT. Se calcula el grupo de automorfismos del grupo de los cuaterniones Q_8, y se da una demostración de su isomorfismo con el grupo simétrico S_4.

1. PRELIMINARES

Una presentación para el grupo de los cuaterniones es la siguiente:

$$Q_8 = \langle \ \text{a,b} : a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle.$$

(Ver también [6], o [4], o [2] pag. 291). Nótese que cada elemento de Q_8 es de la forma $(a^k)(b^r)$ donde k y r son enteros con $0 \leq k \leq 3$ y $0 \leq r \leq 1$. Además la regla de multiplicación para elementos $a^k b^r$ y $a^{k'} b^{r'}$ de este grupo está dada por:

$$(a^k b^r)(a^{k'} b^{r'}) = \begin{cases} a^{k+k'} b^{r'}, & \text{si } r = 0 \\ a^{k-k'} b^{r+r'}, & \text{si } r = 1 \end{cases}$$

Antes de entrar a determinar los automorfismos del grupo de los cuaterniones, es importante que recordemos algunas definiciones y propiedades necesarias para tal efecto.

-. Un *isomorfismo* entre un grupo G y un grupo H es una función $f : G \longrightarrow H$, tal que:

i) f es biyectiva.

ii) $f(x.y) = f(x).f(y)$ para todo $x, y \in G$.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

-. Un *automorfismo* de un grupo G es un isomorfismo entre G y él mismo.
-. Designamos con $Aut(G)$ al conjunto de todos los automorfismos del grupo G.

Son de fácil demostración las siguientes propiedades de los automorfismos:

-. Sea G un grupo, $a \in G$ y $f \in Aut(G)$, entonces $G = \langle a \rangle$ si y sólo si $G = \langle f(a) \rangle$. (Ver [1], Capítulo 7).
-. Sea G un grupo, $a \in G$ y $f \in Aut(G)$; si $|a|$ (= orden de a) $= n$ entonces $|f(a)| = n$. (Ver [3]).

Para demostrar que Aut(Q_8) es isomorfo a S_4, nos basaremos en el teorema que enunciamos a continuación (cuya prueba puede verse en [5], pag. 66):

(I) Teorema. *Sea $k \geq 2$. Sea G un grupo con generadores $x_1, x_2, ..., x_{k-1}$ que satisfacen las relaciones:*

i) $x_i^2 = 1 (1 \leq i \leq k-1)$.
ii) $x_i.x_j = x_j.x_i$ $(1 \leq i, j \leq k-1, j \neq i+1)$.
iii) $x_j.x_{j+1}.x_j = x_{j+1}.x_j.x_{j+1}$ $(1 \leq j \leq k-2)$.

Entonces G es isomorfo al grupo simétrico S_k.

2.- Construcción de los Automorfismos de Q_8

Para construir los automorfismos de Q_8, es necesario observar que:

-. Q_8 tiene seis elementos de orden 4, a saber: a, a^3, b, ab, a^2b y a^3b; mientras que tiene un solo elemento de orden 2 el cual es a^2.
-. Si $f \in Aut(Q_8)$, tenemos que $f(Q_8) = Q_8$, $f(1) = 1$ y $f(a^2) = a^2$, por ser a^2 el único elemento de orden 2.
-. Si $f \in Aut(Q_8)$, f está plena y unívocamente determinada por $f(a)$ y $f(b)$ debido a que a y b generan Q_8.

De lo dicho anteriormente tenemos que las posibilidades para $f(a)$ son a, a^3, b, ab, a^2b y a^3b; examinemos cada una de ellas, determinando en cada caso $f(b)$.
Caso 1.
Si $f(a) = a$, entonces:

$$f(a^3) = [f(a)]^3 = a^3,$$
$$f(ab) = f(a).f(b) = af(b),$$
$$f(a^2b) = [f(a)]^2.f(b) = a^2f(b),$$
$$f(a^3b) = [f(a)]^3.f(b) = a^3f(b).$$

De lo cual deducimos que $f(b) \notin \{1, a, a^3\}$ y que $f(b) \neq a^2$, pues $|b| = 4$. Por lo tanto $f(b) \in \{b, ab, a^2b, a^3b\}$.

i) Si $f(b) = b$, entonces $f(a^jb) = a^jb$ para todo $j = 1, 2, 3$, y así $f = id_{Q_8}$.

ii) Si $f(b) = ab$, entonces:

$$
\begin{aligned}
f(ab) &= a.ab = a^2b,\\
f(a^2b) &= a^2.ab = a^3b,\\
f(a^3b) &= a^3.ab = b.
\end{aligned}
$$

iii) Si $f(b) = a^2b$, entonces:

$$
\begin{aligned}
f(ab) &= a.a^2b = a^3b,\\
f(a^2b) &= a^2.a^2b = b,\\
f(a^3b) &= a^3.a^2b = ab.
\end{aligned}
$$

iv) Si $f(b) = a^3b$, entonces:

$$
\begin{aligned}
f(ab) &= a.a^3b = b,\\
f(a^2b) &= a^2.a^3b = ab,\\
f(a^3b) &= a^3.a^3b = a^2b.
\end{aligned}
$$

Caso 2.
Si $f(a) = a^3$, entonces $f(b) \in \{b, ab, a^2b, a^3b\}$ puesto que $f(b) \notin \{1, a^2, a^3\}$ y $f(b) \neq a$ ya que $f(a^3) = a^9 = a$. Fácilmente el lector puede determinar $f(a^j b)$ con $0 \leq j \leq 3$, en cada una de las posibilidades de $f(b)$.
Caso 3.
Si $f(a) = b$, entonces $f(b) \in \{a, a^3, ab, a^3b\}$, ya que $f(b) \notin \{1, a^2, b, a^2b\}$.
Caso 4.
Si $f(a) = a^2b$, entonces $f(b) \in \{a, a^3, ab, a^3b\}$, ya que $f(b) \notin \{1, a^2, b, a^2b\}$.

Caso 5.
Si $f(a) = ab$, entonces $f(b) \in \{a, a^3, b, a^2b\}$, ya que $f(b) \notin \{1, a^2, ab, a^3b\}$.
Caso 6.
Si $f(a) = a^3b$, entonces $f(b) \in \{a, a^3, b, a^2b\}$, ya que $f(b) \notin \{1, a^2, ab, a^3b\}$.

Teniendo en cuenta los casos anteriores y calculando $f(a^j b^r)$ con $0 \leq j \leq 3$ y $0 \leq r \leq 1$ para los casos desde el 2 hasta el 6, presentamos el siguiente conjunto de biyecciones σ_i de Q_8, donde $i = 1, 2, ..., 24$:

.	1	a	a^2	a^3	b	ab	a^2b	a^3b
σ_1	1	a	a^2	a^3	b	ab	a^2b	a^3b
σ_2	1	a	a^2	a^3	ab	a^2b	a^3b	b
σ_3	1	a	a^2	a^3	a^2b	a^3b	b	ab
σ_4	1	a	a^2	a^3	a^3b	b	ab	a^2b
σ_5	1	a^3	a^2	a	b	a^3b	a^2b	ab
σ_6	1	a^3	a^2	a	ab	b	a^3b	a^2b
σ_7	1	a^3	a^2	a	a^2b	ab	b	a^3b
σ_8	1	a^3	a^2	a	a^3b	a^2b	ab	b
σ_9	1	b	a^2	a^2b	a	a^3b	a^3	ab
σ_{10}	1	b	a^2	a^2b	a^3	ab	a	a^3b
σ_{11}	1	b	a^2	a^2b	ab	a	a^3b	a^3
σ_{12}	1	b	a^2	a^2b	a^3b	a^3	ab	a
σ_{13}	1	a^2b	a^2	b	a	ab	a^3	a^3b
σ_{14}	1	a^2b	a^2	b	a^3	a^3b	a	ab
σ_{15}	1	a^2b	a^2	b	ab	a^3	a^3b	a
σ_{16}	1	a^2b	a^2	b	a^3b	a	ab	a^3
σ_{17}	1	ab	a^2	a^3b	b	a^3	a^2b	a
σ_{18}	1	ab	a^2	a^3b	a	b	a^3	a^2b
σ_{19}	1	ab	a^2	a^3b	a^3	a^2b	a	b
σ_{20}	1	ab	a^2	a^3b	a^2b	a	b	a^3
σ_{21}	1	a^3b	a^2	ab	b	a	a^2b	a^3
σ_{22}	1	a^3b	a^2	ab	a	a^2b	a^3	b
σ_{23}	1	a^3b	a^2	ab	a^3	b	a	a^2b
σ_{24}	1	a^3b	a^2	ab	a^2b	a^3	b	a

Sea $L = \{ \sigma_i$: i=1,2,...,24$\}$. Es fácil observar que cada una de las σ_i es una biyección de Q_8 en él mismo. Además, debido al análisis previo a la construcción de la tabla anterior, es claro que $Aut(Q_8) \subseteq L$. Veamos ahora que $L \subseteq Aut(Q_8)$ (es decir, que cada una de las σ_i es un automorfismo de Q_8).

Obsérvese que si $x = a^s b^t \in Q_8$ con $0 \leq s \leq 3$ y $0 \leq t \leq 1$, y si $\sigma \in L$, entonces:

$$\sigma(x) = \sigma(a^s b^t) = (\sigma(a))^s (\sigma(b))^t; \tag{1}$$

Esto debido a la forma misma como ha sido obtenida cada una de las σ_i.

Sean ahora $\sigma \in L$, $x, z \in Q_8$ arbitrarias; entonces $x = a^s b^t$, y $z = a^{s'} b^{t'}$, donde $0 \leq s, s' \leq 3$ y $0 \leq t, t' \leq 1$.. Consideremos los dos casos para el exponente de b y utilicemos (1) donde sea necesario.

<u>Caso A:</u>

Si $t = 0$, $x = a^s$, y $z = a^{s'} b^{t'}$.

-. Si $s = 0$, $x = 1$, luego $\sigma(xz) = \sigma(z) = 1\sigma(z) = \sigma(1)\sigma(z)$.

-. Si $s' = 0$, $x = a^s$, $z = b^{t'}$, luego $\sigma(xz) = \sigma(a^s b^{t'}) = (\sigma(a))^s(\sigma(b))^{t'}$. Por otro lado, $\sigma(x)\ \sigma(z) = \sigma(a^s)\ \sigma(b^{t'}) = (\sigma(a))^s(\sigma(b))^{t'}$. Por lo tanto, $\sigma(xz) = \sigma(x)\ \sigma(z)$.

-. Si $1 \leq s, s' \leq 3$, tenemos que $2 \leq s + s' \leq 6$, y entonces:

$$\sigma(xz) = \sigma(a^{s+s'}b^{t'}) = \begin{cases} \sigma(a^2b^{t'}) = (\sigma(a))^2(\sigma(b))^{t'} & \text{si } s+s' = 2, \text{o}, \ 6, \\ \sigma(a^3b^{t'}) = (\sigma(a))^3(\sigma(b))^{t'} & \text{si } s+s' = 3, \\ \sigma(b^{t'}) = (\sigma(b))^{t'} & \text{si } s+s' = 4, \\ \sigma(\ ab^{t'}) = \sigma(a)(\sigma(b))^{t'} & \text{si } s+s' = 5. \end{cases}$$

Por otro lado, tenemos que:
$\sigma(x))(\sigma(z)) = (\sigma(a))^s(\sigma(a))^{s'}(\sigma(b))^{t'} = (\sigma(a))^{s+s'}(\sigma(b))^{t'} =$

$$\begin{cases} (\sigma(a))^2(\sigma(b))^{t'} & \text{si } s+s' = 2, \text{o}, \ 6, \ (*) \\ (\sigma(a))^3(\sigma(b))^{t'} & \text{si } s+s' = 3, \\ (\sigma(b))^{t'} & \text{si } s+s' = 4, \ (**) \\ \sigma(a)(\sigma(b))^{t'} & \text{si } s+s' = 5, \ (**) \end{cases}$$

(*) se tiene gracias a que para todo $x \in Q_8$, $x^6 = x^4.x^2 = 1.x^2 = x^2$.
(**) se tiene debido a que para todo $x \in Q_8$, $x^4 = 1$.

Caso B:

Si $t = 1$, $x = a^s b^t = a^s b$ y $z = a^{s'} b^{t'}$; luego $xz = a^{s-s'} b^{1+t'}$.
-. Si $s' = 0$, tenemos que:

$$\sigma(xz) = \sigma(a^s b^{1+t'}) = (\sigma(a))^s(\sigma(b))^{1+t'}.$$

Por otro lado,

$$\sigma(x)\sigma(z) = \sigma(a^s b)\sigma(b^{t'}) =$$
$$(\sigma(a))^s(\sigma(b))(\sigma(b))^{t'} = (\sigma(a))^s(\sigma(b))^{1+t'}.$$

-. Si $s' = 1$, tenemos que:

$$\sigma(xz) = \sigma(a^{s-1}b^{1+t'}) = (\sigma(a))^{s-1}(\sigma(b))^{1+t'} =$$
$$(\sigma(a))^{s+3}(\sigma(b))^{1+t'}, \text{pues } (\sigma(a))^{s-1} = (\sigma(a))^{s+3}.$$

Por otro lado, $\sigma(x)\sigma(z) = \sigma(a^s b)\sigma(a^{s'} b^{t'}) =$

$$\sigma(a^s b)\sigma(ab^{t'}) = (\sigma(a))^s(\sigma(b))\sigma(a)(\sigma(b))^{t'} =$$
$$(\sigma(a))^s(\sigma(ba))(\sigma(b))^{t'} = (\sigma(a))^s\sigma(a^3 b)(\sigma(b))^{t'} =$$
$$(\sigma(a))^s\sigma(a^3 b)(\sigma(b))^{t'} = (\sigma(a))^s(\sigma(a))^3(\sigma(b))(\sigma(b))^{t'} =$$

$$(\sigma(a))^{s+3}(\sigma(b))^{1+t'}.$$

En el paso de que $\sigma(b)\sigma(a) = \sigma(ba)$ se ha utilizado que:
Para todo $x \in Q_8 - \{1, a^2\}$, y para toda $\sigma \in L$, $(\sigma(x))^2 = a^2$; $a^2 \in Z(Q_8)$, $(**)$, (1) y el hecho de que $ba = a^{-1}b$.

-. Si $s' = 2$, tenemos que:

$$\sigma(xz) = \sigma(a^{s-2}b^{1+t'}) = \sigma(a^{s+2}b^{1+t'}) =$$

$$(\sigma(a))^{s+2}(\sigma(b))^{1+t'}.$$

Por otro lado, $\sigma(x)\sigma(z) = \sigma(a^s b)\sigma(a^{s'}b^{t'}) =$

$$\sigma(a^s b)\sigma(a^2 b^{t'}) = (\sigma(a))^s(\sigma(b))(\sigma(a))^2(\sigma(b))^{t'} =$$

$$(\sigma(a))^s(\sigma(b))a^2(\sigma(b))^{t'} = (\sigma(a))^s a^2\sigma(b)(\sigma(b))^{t'} =$$

$$(\sigma(a))^s(\sigma(a))^2(\sigma(b))^{1+t'} = (\sigma(a))^{s+2}(\sigma(b))^{1+t'}.$$

-. Si $s' = 3$, tenemos que:

$$\sigma(xz) = \sigma(a^{s-3}b^{1+t'}) = \sigma(a^{s+1}b^{1+t'}) =$$

$$(\sigma(a))^{s+1}(\sigma(b))^{1+t'}.$$

Por otro lado,

$$\sigma(x)\sigma(z) = \sigma(a^s b)\sigma(a^{s'}b^{t'}) = \sigma(a^s b)\sigma(a^3 b^{t'}) =$$

$$(\sigma(a))^s(\sigma(b))(\sigma(a))^3(\sigma(b))^{t'} = (\sigma(a))^s(\sigma(b))\sigma(a^3)(\sigma(b))^{t'} =$$

$$(\sigma(a))^s\sigma(ba^3)(\sigma(b))^{t'} = (\sigma(a))^s\sigma(ab)(\sigma(b))^{t'} =$$

$$(\sigma(a))^s\sigma(a)\sigma(b)(\sigma(b))^{t'} = (\sigma(a))^{s+1}(\sigma(b))^{1+t'}.$$

En el paso de que $\sigma(b)\sigma(a^3) = \sigma(ba^3)$ se ha utilizado que:
Para todo $x \in Q_8 - \{1, a^2\}$, $(\sigma(x))^2 = a^2; a^2 \in Z(Q_8)$, $(**)$, (1), el hecho de que $ba = a^{-1}b$, el caso A, y el resultado ya demostrado de que $\sigma(b)\sigma(a) = \sigma(ba)$.

Por lo tanto, de los casos A y B, tenemos que para todo $\sigma \in L$, y para todo $x, z \in Q_8$, $\sigma(xz) = \sigma(x)\sigma(z)$.
Luego en total, cada $\sigma \in L$ es un automorfismo de Q_8, y así se ha probado que:

$$L = Aut(Q_8). \tag{2}$$

Proposición. *$Aut(Q_8) = \langle\sigma_{24}, \sigma_{20}, \sigma_9\rangle$.*

Demostración:. Partiendo de (2), son de sencilla verificación las siguientes igualdades:

$\sigma_9^2 = \sigma_{20}^2 = \sigma_{24}^2 = \sigma_1 = id_{Q_8}$.

$\sigma_2 = \sigma_{24}.\sigma_9.\sigma_{20}$	$\sigma_{12} = \sigma_9.\sigma_{24}.\sigma_9.\sigma_{20}$	$\sigma_{22} = \sigma_{20}.\sigma_{24}.\sigma_9.\sigma_{24}$
$\sigma_3 = \sigma_9.\sigma_{20}.\sigma_{24}.\sigma_9$	$\sigma_{13} = \sigma_9.\sigma_{24}.\sigma_{20}$	$\sigma_{23} = \sigma_9.\sigma_{20}$
$\sigma_4 = \sigma_{20}.\sigma_9.\sigma_{24}$	$\sigma_{14} = \sigma_{24}.\sigma_9.\sigma_{20}.\sigma_9.\sigma_{24}$	$\sigma_{24} = \sigma_{24}$
$\sigma_5 = \sigma_{20}.\sigma_{24}$	$\sigma_{15} = \sigma_{20}.\sigma_9$	
$\sigma_6 = \sigma_9.\sigma_{24}.\sigma_9$	$\sigma_{16} = \sigma_{24}.\sigma_9$	
$\sigma_7 = \sigma_9.\sigma_{20}.\sigma_{24}.\sigma_{20}$	$\sigma_{17} = \sigma_9.\sigma_{20}.\sigma_{24}.\sigma_9.\sigma_{24}$	
$\sigma_8 = \sigma_9.\sigma_{20}.\sigma_9$	$\sigma_{18} = \sigma_{24}.\sigma_9.\sigma_{20}.\sigma_9$	
$\sigma_9 = \sigma_9$	$\sigma_{19} = \sigma_9.\sigma_{24}$	
$\sigma_{10} = \sigma_{20}.\sigma_{24}.\sigma_9$	$\sigma_{20} = \sigma_{20}$	
$\sigma_{11} = \sigma_{20}.\sigma_9.\sigma_{24}.\sigma_{20}$	$\sigma_{21} = \sigma_9.\sigma_{20}.\sigma_{24}.\sigma_9.\sigma_{20}$	

(El punto indica la composición usual).

Teorema. *$Aut(Q_8)$ es isomorfo a S_4.*

Demostración. Veamos que los generadores de Q_8 enunciados en la Proposición anterior satisfacen el Teorema mencionado en **(*I*)** del numeral 1.-.
$\sigma_9^2 = \sigma_{20}^2 = \sigma_{24}^2 = \sigma_1 = id_{Q_8}$.
Sean $x_1 = \sigma_{20}$, $x_2 = \sigma_9$ y $x_3 = \sigma_{24}$.
Entonces:

$$x_1.x_3 = \sigma_{20}.\sigma_{24} = \sigma_{24}.\sigma_{20} = x_3.x_1.$$

$$x_2.x_3.x_2 = \sigma_9.\sigma_{24}.\sigma_9 = \sigma_6.$$

$$x_3.x_2.x_3 = \sigma_{24}.\sigma_9.\sigma_{24} = \sigma_6.$$

Luego $x_2.x_3.x_2 = x_3.x_2.x_3$.
Además:

$$x_1.x_2.x_1 = \sigma_{20}.\sigma_9.\sigma_{20} = \sigma_8.$$

$$x_2.x_1.x_2 = \sigma_9.\sigma_{20}.\sigma_9 = \sigma_8$$

Luego $x_1.x_2.x_1 = x_2.x_1.x_2$.
Así, por **(*I*)**, tenemos que:

$$Aut(Q_8) \text{ es isomorfo a } S_4.$$

3.- BIBLIOGRAFÍA

[1]. Fraleigh, J., *Algebra Abstracta*, Addison-Wesley Iberoamericana, S. A., Wilmington, Delaware, E.U.A., 1988.

[2]. Kostrikin, A. I., *Introducción al Algebra*, Editorial Mir., Moscú., 1983.

[3]. Hall, M. J. (Jr)., *The Theory of Groups*, MacMillan, New York, 1959.

[4]. Hall, M. J. (Jr)., *The groups of order* $2^n (n \leq 6)$, Mac Millan, New York, 1964.

[5]. O'Brein, Horacio, *Estructuras Algebraicas III. (Grupos Finitos)*, Organización de Estados Americanos, Washington, D.C, 1973.

[6]. Coxeter, *Generators and relations for discrete groups.*, Springer-Verlag, New York, 1965.