Lecturas Matemáticas
Volumen **23** *(2002), páginas 99–106*

Wedderburn decomposition of some special rational group algebras

Carmen Rosa Giraldo Vergara*
Universidade Federal do Rio de Janeiro, Brazil
Fabio Enrique Brochero Martínez
Universidade Federal de Minas Gerais, Brazil

Abstract. In this note we give an elementary proof of the Wedderburn decomposition of rational quaternion and rational dihedral group algebras.

Key words and phrases. Rational group algebras, Wedderburn.

2000 Mathematics Subject Classification. Primary 20C05. Secondary 16S34 .

Resumen. En esta nota se da una demostración elemental de la descomposición de Wedderburn de las álgebras de grupo racionales diedras y cuaterniónicas.

Let K be a field and G be a finite group. A group algebra KG over K is a free K-module with a basis consisting of the elements of G, and with multiplication induced by the given multiplication in G. We say that KG is a semisimple algebra if $KG = \bigoplus_{i\in J} N_i$ where each N_i is a simple

* Partially supported by CNPq, Brasil

right KG-module. It is well known by the theorem of MASCHKE (see [4]) that KG is a semisimple algebra if and only if the characteristic of K does not divide the order of G. In this case, by the WEDDERBURN's structure theorem we have

$$KG \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r).$$

where $n_1, \ldots, n_r \in \mathbb{N}$ and $D_1, \ldots, D_r$ are division algebras over K.

However, for an arbitrary finite group it is not easy to find explicitly its WEDDERBURN decomposition. In the case $K = \mathbb{Q}$ this decomposition is known for groups whose orders are less or equal than 32 (see [1]), or for some especial families of groups.

In this note we obtain explicitly the Wedderburn decomposition for the rational dihedral algebras, and, as a consequence, the decomposition for the rational quaternion algebras.

Our first result is the following:

Theorem 1. *Let G be the dihedral group of order $2n$, i.e.,*

$$G = D_n = \langle x, y : x^n = 1, y^2 = 1, xy = yx^{-1} \rangle.$$

Then

$$\mathbb{Q}G \cong \bigoplus_{d|n} A_d$$

where $A_d \cong \mathbb{Q} \oplus \mathbb{Q}$ if $d = 1, 2$, and $A_d \cong M_2(\mathbb{Q}[\zeta_d + \zeta_d^{-1}])$ if $d > 2$, where ζ_q denotes a q^{th} primitive root of the unit.

Proof. Let d be a positive divisor of n and ζ_d be a primitive d-th root of unity. Let

$$\tau_d : \mathbb{Q}G \longrightarrow \mathbb{Q} \oplus \mathbb{Q},$$

for d=1,2, the homomorphisms defined by $\tau_1(x) = (1, 1)$ and $\tau_1(y) = (1, -1)$; $\tau_2(x) = (-1, -1)$ and $\tau_2(y) = (1, -1)$. If $d > 2$, let

$$\tau_d : \mathbb{Q}G \longrightarrow M_2(\mathbb{Q}[\zeta_d]), \quad \text{if } (d > 2),$$

be defined by

$$\tau_d(x) = \begin{bmatrix} \zeta_d & 0 \\ 0 & \zeta_d^{-1} \end{bmatrix}, \quad \tau_d(y) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

It is clear that $(\tau_d(x))^n = 1$, $(\tau_d(y))^2 = 1$ and $\tau_d(y)^{-1}\tau_d(x)\tau_d(y)^{-1} = \tau_d(x)^{-1}$. Thus τ_d is a well defined homomorphism for every $d \mid n$.

Let us remark that $\tau_d(\mathbb{Q}G)$ has dimension less than or equal to $2\phi(d)$. In fact, for $d = 1, 2$ the result is trivial. For $d > 2$, we consider the matrix

$$Z_d = \begin{bmatrix} 1 & -\zeta_d \\ 1 & -\zeta_d{-}1 \end{bmatrix}$$

and define

$$\sigma : M_2(\mathbb{Q}[\zeta_d]) \longrightarrow M_2(\mathbb{Q}[\zeta_d])$$

by

$$\sigma(A) = Z_d{-}1AZ_d \ , \quad A \in M_2(\mathbb{Q}[\zeta_d]).$$

It is not difficult to see that σ is an automorphism. Thus, both

$$\begin{aligned} \sigma\tau_d(x) &= Z_d^{-1}\tau_d(x)Z_d = \left[\begin{array}{cc} 0 & 1 \\ -1 & \zeta_d + \zeta_d^{-1} \end{array}\right] \\ ,\sigma\tau_d(y) &= Z_d^{-1}\tau_d(y)Z_d = \left[\begin{array}{cc} 1 & -(\zeta_d + \zeta_d^{-1}) \\ 0 & -1 \end{array}\right] , \end{aligned}$$

belong to $M_2(\mathbb{Q}[\zeta_d + \zeta_d^{-1}])$. Then, the dimension of the image of τ_d is less than or equal to

$$\dim(M_2(\mathbb{Q}[\zeta_d + \zeta_d^{-1}])) = 4\frac{\phi(d)}{2} = 2\phi(d).$$

If $E_d \cong \mathbb{Q} \oplus \mathbb{Q}$ for $d = 1, 2$, and $E_d \cong M_2(\mathbb{Q}[\zeta_d])$ for $d > 2$, we define $\tau : \mathbb{Q}G \longrightarrow \bigoplus_{d|n} E_d$ as $\tau = \bigoplus \tau_d$. We claim that τ is a injective homomorphism. Indeed, suppose that u is in the kernel of τ. If we rewrite u as

$$u = (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) + (b_0 + b_1x + \cdots + b_{n-1}x^{n-1})y \ ,$$

and define $F_1(z) = a_0 + a_1z + \cdots + a_{n-1}z^{n-1}$ and $F_2(z) = b_0 + b_1z + \cdots + b_{n-1}z^{n-1}$, then for each $d \mid n$, $d > 2$, we have

$$\tau_d(u) = \left[\begin{array}{cc} F_1(\zeta_d) & F_2(\zeta_d) \\ F_2(\zeta_d^{-1}) & F_1(\zeta_d^{-1}) \end{array}\right] = \left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array}\right]$$

Thus, $F_1(\zeta_d) = 0$ and $F_2(\zeta_d) = 0$. For $d = 1$, we have

$$\tau_1(u) = (F_1(1) + F_2(1), F_1(1) - F_2(1)) = 0,$$

and for $d = 2$ have

$$\tau_2(u) = (F_1(-1) + F_2(-1), F_1(-1) - F_2(-1)) = 0.$$

Then the roots of F_1 and F_2 are roots of the polynomial $z^n - 1$. So F_1 and F_2 are null polynomials, and $a_i = b_i = 0$ for every i, which shows that $u = 0$.

Let now

$$\theta : \mathbb{Q}G \longrightarrow \bigoplus_{d|n} A_d \ ,$$

be the homomorphism defined by $\theta = \bigoplus_{d|n} \theta_d$, where θ_d is obtained from τ_d for conjugating by Z_d if $d > 2$, and $\theta_d = \tau_d$ if $d = 1, 2$ and $A_d \cong \mathbb{Q} \oplus \mathbb{Q}$ if $d = 1, 2$, and $A_d \cong M_2(\mathbb{Q}[\zeta_d + \zeta_d^{-1}])$ if $d > 2$. Let us remark that that θ is injective. Furthermore, the dimension of $\bigoplus\limits_{d|n} A_d$ equals $2\sum_{d|n} \phi(d) = 2n$. Since the dimension of $\mathbb{Q}G$ is $2n$, the above implies that θ is the isomorphism. ☑

Using theorem 1, we find the Wedderburn decomposition of rational quaternion algebras, i.e.

Theorem 2. *If G is the quaternion group of order $4n$, i.e.,*

$$G = Q_n = \langle x, y : x^{2n} = 1, y^2 = x^n, xy = yx^{-1} \rangle \ .$$

Then

$$\mathbb{Q}G \cong \mathbb{Q}D_n \bigoplus_{\substack{d=2^k r \\ r|m}} \mathbb{Q}[\zeta_{2d}, j],$$

where k and m are non negative integers with m odd, such that $n = 2^k m$, $j^2 = -1$ and $\alpha j = j\overline{\alpha}$ for all $\alpha \in \mathbb{Q}[\zeta_{2d}]$.

Before proving this theorem, we make the following remark:

Remark. Denote by $\left(\dfrac{a, b}{K}\right)$ the quaternion algebra over the field K, generated for i, j, where $i^2 = a$, $j^2 = b$ and $ij = -ji$. Then, if $d = 1$,

$\mathbb{Q}[\zeta_{2d}, j] \cong \mathbb{Q}(i)$, and if $d \neq 1$ and writing $w_{2d} = \zeta_{2d} + \zeta_{2d}^{-1}$, we have

$$\begin{aligned}\mathbb{Q}[\zeta_{2d}, j] &\cong \mathbb{Q}[w_{2d}][\zeta_{2d} - \zeta_{2d}^{-1}, j] \\ &\cong \left(\frac{(\zeta_{2d} - \zeta_{2d}^{-1})^2, -1}{\mathbb{Q}[w_{2d}]}\right) = \left(\frac{w_{2d}^2 - 4, -1}{\mathbb{Q}[w_{2d}]}\right).\end{aligned}$$

Proof. Since $\langle x^n \rangle$ is a normal subgroup of G, then $\dfrac{1+x^n}{2}$ and $\dfrac{1-x^n}{2}$ are idempotent orthogonal elements of $\mathbb{Q}G$. Thus,

$$\mathbb{Q}G \cong \mathbb{Q}G\left(\frac{1+x^n}{2}\right) \oplus \mathbb{Q}G\left(\frac{1-x^n}{2}\right),$$

and x^n plays the role of identity in $\mathbb{Q}G\left(\dfrac{1+x^n}{2}\right)$, so

$$\mathbb{Q}G\left(\frac{1+x^n}{2}\right) \cong \mathbb{Q}D_n\ ,$$

where D_n is the dihedral group of order $2n$.

Let us suppose now that $n = 2^k m$ where m is odd. We intend to show that

$$\mathbb{Q}G\left(\frac{1-x^n}{2}\right) \cong \bigoplus_{\substack{d=2^k r \\ r \mid m}} \mathbb{Q}[\zeta_{2d}, j],$$

where $j^2 = -1$ and $\alpha j = j\overline{\alpha}$ for all $\alpha \in \mathbb{Q}[\zeta_{2d}]$.

Let us consider the homomorphism

$$\tau_{2d} : \mathbb{Q}G\left(\frac{1-x^n}{2}\right) \longrightarrow \mathbb{Q}[\zeta_{2d}, j] \quad ,$$

where $d = 2^k r$ with $r \mid m$, defined by $\tau_{2d}(x) = \zeta_{2d}$ and $\tau_{2d}(y) = j$. It is clear that, $(\tau_{2d}(x))^n = \zeta_{2d}^n = \zeta_{2d}^{2^k m} = -1 = j^2 = (\tau_{2d}(y))^2$, $\tau_{2d}(y^{-1}xyx) = 1$ and $\tau_{2d}\left(\dfrac{1-x^n}{2}\right) = 1$. Thus τ_{2d} is a well defined homomorphism. Furthermore, the dimension of $\mathbb{Q}[\zeta_{2d}, j]$ over $\mathbb{Q}$ equals $2\phi(2d)$.

Let now

$$\tau : \mathbb{Q}G\left(\frac{1-x^n}{2}\right) \longrightarrow \bigoplus_{\substack{d=2^k r\\ r|m}} \mathbb{Q}[\zeta_{2d}, j],$$

where $\tau = \bigoplus_d \tau_{2d}$. Now we claim that τ is an injective homomorphism. Indeed, suppose that u is in the kernel of τ. If now we rewrite u as

$$\begin{aligned}
&\left(\sum_{i=0}^{2n-1} a_i x^i + \sum_{i=0}^{2n-1} b_i x^i y\right)\left(\frac{1-x^n}{2}\right) = \\
&\frac{1}{2}\left(\sum_{i=0}^{n-1}(a_i - a_{i+n})(x^n - x^{i+n}) + \sum_{i=0}^{n-1}(b_i - b_{i+n})(x^n - x^{i+n})y\right) = \\
&\qquad\left(\sum_{i=0}^{n-1}(a_i - a_{i+n})x^i + \sum_{i=0}^{n-1}(b_i - b_{i+n})x^i y\right)\left(\frac{1-x^n}{2}\right),
\end{aligned}$$

and define $F_1(z) = c_0 + c_1 z + \cdots + c_{n-1}z^{n-1}$ and $F_2(z) = d_0 + d_1 z + \cdots + d_{n-1}z^{n-1}$, where $c_i = a_i - a_{i+n}$ and $d_i = b_i - b_{i+n}$ with $i = 0, \ldots, n-1$, then for each d we get

$$\tau_{2d}(u) = F_1(\zeta_{2d}) + F_2(\zeta_{2d})j = 0.$$

Thus, $F_1(\zeta_{2d}) = 0$ and $F_2(\zeta_{2d}) = 0$. Then F_1 and F_2 have all the roots of the polynomial $z^n + 1$ as roots. Therefore, F_1 and F_2 are null polynomials. Thus, $c_i = d_i = 0$ for every $i = 0, \ldots, n-1$, implies $u = 0$, i.e., τ is injective. Moreover, the dimension of

$$\bigoplus_{\substack{d=2^k r\\ r|m}} \mathbb{Q}[\zeta_{2d}, j]$$

equals

$$2\sum_{r|m}\phi(2^{k+1}r) = 2^{k+1}\sum_{r|m}\phi(r) = 2^{k+1}m = 2n.$$

Since the dimension of $\mathbb{Q}G\left(\frac{1-x^n}{2}\right)$ is $2n$, we conclude that τ is an isomorphism. ☑

In the following tables we exhibit the Wedderburn decomposition of the rational quaternion and dihedral algebras of dimensions in the range comprised between 16 and 32.

Group	WEDDERBURN **Decomposition**
D_8	$\mathbb{Q}D_8 \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}[\sqrt{2}])$
D_9	$\mathbb{Q}D_9 \cong 2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}[\zeta_9 + \zeta_9^{-1}])$
D_{10}	$\mathbb{Q}D_{10} \cong 4\mathbb{Q} \oplus 2M_2(\mathbb{Q}[\sqrt{5}])$
D_{11}	$\mathbb{Q}D_{11} \cong \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}[\zeta_{11} + \zeta_{11}^{-1}])$
D_{12}	$\mathbb{Q}D_{12} \cong 4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}[\sqrt{3}])$
D_{13}	$\mathbb{Q}D_{13} \cong \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}[\zeta_{13} + \zeta_{13}^{-1}])$
D_{14}	$\mathbb{Q}D_{14} \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}[\zeta_7 + \zeta_7^{-1}]) \oplus M_2(\mathbb{Q}[\zeta_{14} + \zeta_{14}^{-1}])$
D_{15}	$\mathbb{Q}D_{15} \cong 2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}[\sqrt{5}]) \oplus M_2(\mathbb{Q}[\zeta_{15} + \zeta_{15}^{-1}])$
D_{16}	$\mathbb{Q}D_{16} \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}[\sqrt{2}]) \oplus M_2(\mathbb{Q}[\sqrt{2+\sqrt{2}}])$

Group	WEDDERBURN **Decomposition**
Q_4	$\mathbb{Q}Q_4 \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus \left(\frac{-1,-1}{\mathbb{Q}[\sqrt{2}]}\right)$
Q_5	$\mathbb{Q}Q_5 \cong 2\mathbb{Q} \oplus 2\mathbb{Q} \oplus \mathbb{Q}(i) \oplus M_2(\sqrt{5}]) \oplus \left(\frac{\frac{-5+\sqrt{5}}{2},-1}{\mathbb{Q}[\sqrt{5}]}\right)$
Q_6	$\mathbb{Q}Q_6 \cong 4\mathbb{Q} \oplus 2M_2(\mathbb{Q}) \oplus \left(\frac{-2,-1}{\mathbb{Q}}\right) \oplus \left(\frac{-1,-1}{\mathbb{Q}[\sqrt{3}]}\right)$
Q_7	$\mathbb{Q}Q_7 \cong 2\mathbb{Q} \oplus \mathbb{Q}(i) \oplus M_2(\mathbb{Q}[\zeta_7 + \zeta_7^{-1}]) \oplus \left(\frac{(\zeta_{14}-\zeta_{14}^{-1})^2,-1}{\mathbb{Q}[\zeta_{14}+\zeta_{14}^{-1}]}\right)$
Q_8	$\mathbb{Q}Q_8 \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}[\sqrt{2}]) \oplus \left(\frac{2-\sqrt{2},-1}{\mathbb{Q}[\sqrt{2+\sqrt{2+\sqrt{2}}}]}\right)$

Acknowledgments. The authors wish to thank an unknown referee for helpful suggestions that improved the presentation of this note.

Bibliography

[1] Giraldo, Carmen Rosa. *Algebras de grupos racionais* Tesis de Mestre UFRJ, Rio de Janeiro, 1997.
[2] Jacobson, Nathan. *Basic Algebra II.* W.H Freman and Company. New York, 1989.
[3] Passman, Donald S. *The Algebraic Structure of Group Rings.* Wiley Interscience. New York, 1977.
[4] Pierce, Richard. *Associative Algebras.* Springer–Verlag. New York, 1980.
[5] Polcino Miles, César. *Anéis de Grupos.* SBM. São Paulo, 1976.

(Recibido en diciembre de 2001; la versión revisada en noviembre de 2002)

Fabio Enrique Brochero Martínez, Departamento de Matemática ICEx
Universidade Federal de Minas Gerais
CEP 30123-970, Belo Horizonte, MG, Brazil
e-mail: fbrocher@mat.ufmg.br
Carmen Rosa Giraldo Vergara, Instituto de Matemática
Universidade Federal de Rio de Janeiro
CEP 21945-970, Rio de Janeiro, Brazil
e-mail: carmitagv@yahoo.com.br