International Electronic Journal of Algebra
Volume 31 (2022) 143-160
DOI: 10.24330/ieja.1058426

COUNTING NON-ISOMORPHIC GENERALIZED HAMILTON QUATERNIONS

José María Grau, Celino Miguel and Antonio M. Oller-Marcén

Received: 7 January 2021; Revised: 22 March 2021; Accepted: 5 June 2021
Communicated by Meltem Altun Özarslan

Abstract. In this paper we study the isomorphisms of generalized Hamilton quaternions $\left(\frac{a,b}{R}\right)$ where R is a finite unital commutative ring of odd characteristic and $a, b \in R$. We obtain the number of non-isomorphic classes of generalized Hamilton quaternions in the case where R is a principal ideal ring. This extends the case $R = \mathbb{Z}/n\mathbb{Z}$ where n is an odd integer.

Mathematics Subject Classification (2020): 16H05, 11R52, 13M99
Keywords: Finite local ring, quaternion algebra, Hensel lemma

1. Introduction

The origin of quaternions dates back to 1843, when William Rowan Hamilton considered a 4-dimensional vector space over $\mathbb{R}$ with basis $\{1, i, j, k\}$ and defined an associative product given by the now classical rules $i^2 = j^2 = -1$ and $ij = -ji = k$.

This construction admits a very natural extension like the following. Let R be a commutative and associative ring with identity and let $H(R)$ denote the free R-module of rank 4 with basis $\{1, i, j, k\}$. That is,

$$H(R) = \{x_0 + x_1 i + x_2 j + x_3 k \ : \ x_0, x_1, x_2, x_3 \in R\}.$$

Now, let $a, b \in R$ and define an associative multiplication in $H(R)$ according to the following rules:

$$\begin{aligned} i^2 &= a, \\ j^2 &= b, \\ ij &= -ji = k. \end{aligned} \tag{1}$$

Thus, we obtain an associative unital ring that will be denoted by $\left(\frac{a,b}{R}\right)$ and that we call ring of *generalized Hamilton quaternions over* R. If both a and b are units and the underlying ring R is a field $\mathbb{F}$ of characteristic different from 2, the structure of the corresponding quaternion algebra is well-known[1]. Indeed, such a quaternion algebra is either a division ring or isomorphic to the full matrix ring $\mathbb{M}_2(\mathbb{F})$ [11, p.

[1]The analogues of the quaternion algebras over fields of characteristic 2 requires a slight modification in the definition of multiplication. See [11, p. 16], for example.

19]. Thus, if $\mathbb{F}$ is finite, it follows from Wedderburn's little theorem [17, p. 1] that $\mathbb{M}_2(\mathbb{F})$ is the only quaternion algebra over $\mathbb{F}$.

The structure of quaternion algebras over a commutative base ring R has been considered by Kanzaki [6], Knus [7], Tuganbaev [14], Hahn [5], Gross and Lucianovic [4], and most recently by Voight [15,16], Miguel and Serodio [9], Grau et al. [2] or Savin [12].

In this paper we study the isomorphism classes of generalized Hamilton quaternions $\left(\frac{a,b}{R}\right)$ where R is a finite unital commutative ring of odd characteristic with $a, b \in R$. In particular, we obtain the number of non-isomorphic Hamilton quaternions in the case where R is a principal ideal ring. As we will see, this number depends only on the degree of nilpotence of the radical and our results extend the case $R = \mathbb{Z}/n\mathbb{Z}$ (odd n) which was considered in [3].

2. Ring-theoretical preliminaries

In this section we present some ring-theoretical tools that will be useful in order to prove our results.

The first tool is the well-known structure of finite commutative rings with identity. Let R be a a finite commutative ring with identity $1 \neq 0$. It is well known that R can be uniquely expressed as a direct sum of local rings [8, p. 95]. That is,

$$R \cong R_1 \oplus \cdots \oplus R_l, \tag{2}$$

where each R_i is a local ring. If $\mathfrak{m}_i$ is the maximal ideal of R_i, and the residue field $R_i/\mathfrak{m}_i$ has order $p_i^{s_i}$, then the ring R is said to be of type

$$((R_1, \mathfrak{m}_1, p_1^{s_1}), (R_2, \mathfrak{m}_2, p_2^{s_2}), \ldots, (R_l, \mathfrak{m}_l, p_l^{s_l}))\,.$$

In this paper we assume that the primes p_i are odd for every $i = 1, \ldots, l$. In other words, that the ring R has odd characteristic.

From decomposition (2) it follows that each element of R can be identified with an l-tuple $(r_1, \ldots, r_l)$, where $r_i \in R_i$. With this notation it is easy to see that decomposition (2) induces a natural isomorphism

$$\left(\frac{a,b}{R}\right) \cong \left(\frac{a_1,b_1}{R_1}\right) \oplus \cdots \oplus \left(\frac{a_l,b_l}{R_l}\right). \tag{3}$$

Consequently, we may restrict ourselves to the case where the base ring is a local ring.

The second tool is a simple yet powerful result. Assume that R is a finite local ring and let $\mathfrak{m}$ be its maximal ideal. Then $\mathfrak{m}$ is precisely the nilradical of R and, since for every finite ring the nilradical is nilpotent, it follows that $\mathfrak{m}$ is a nilpotent

ideal. Moreover, if k is the index of nilpotence of $\mathfrak{m}$, we have the following filtration

$$0 = \mathfrak{m}^k \subset \mathfrak{m}^{k-1} \subset \mathfrak{m}^{k-2} \subset \ldots \subset \mathfrak{m} \subset \mathfrak{m}^0 = R. \tag{4}$$

Now, consider the following sequence of epimorphisms

$$R \xrightarrow{\varphi_{k-1}} R/\mathfrak{m}^{k-1} \xrightarrow{\varphi_{k-2}} R/\mathfrak{m}^{k-2} \xrightarrow{\varphi_{k-3}} \ldots \xrightarrow{\varphi_2} R/\mathfrak{m}^2 \xrightarrow{\varphi_1} R/\mathfrak{m}, \tag{5}$$

where $\varphi_i(a + \mathfrak{m}^{i+1}) = a + \mathfrak{m}^i$. For each $1 \leq s \leq k-1$, we can use sequence (5) to define an epimorphism $\gamma_s : R \longrightarrow R/\mathfrak{m}^s$ by $\gamma_s = \varphi_s \circ \varphi_{s+1} \circ \ldots \circ \varphi_{k-1}$.

Moreover, for every $a \in R$, let us denote by $w(a)$ the largest integer $i \in \{0, 1, \ldots, k\}$ such that $a \in \mathfrak{m}^i$. Then $\ker(\gamma_s) = \mathfrak{m}^s = \{x \in R : w(x) \geq s\}$ and it is clear that γ_s induces an epimorphism

$$\overline{\gamma}_s : \left(\frac{a,b}{R}\right) \longrightarrow \left(\frac{\gamma_s(a), \gamma_s(b)}{R/\mathfrak{m}^s}\right). \tag{6}$$

The third tool is an extension to finite local rings of the following well-known result [13, p. 103].

Lemma 2.1. *Let $\mathbb{F}$ be a field of odd characteristic and let a and b be nonzero elements of $\mathbb{F}$. Then, for every $c \in \mathbb{F}$, there exist $x, y \in \mathbb{F}$ such that $c = ax^2 + by^2$.*

In order to extend this result to finite local rings we first need to introduce the following result, which is a particular case of an extension of Hensel's lemma to polynomials in several variables that was proved in [10, Theorem 3].

Lemma 2.2. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$, $n \geq 1$ and $f \in R[X_1, \ldots, X_n]^n$. If there exists $a \in R^n$ such that $det(Jac\ f(a))$ is a unit in R and $f(a) \in \mathfrak{m}^n$, then there exists a unique $b \in R^n$ such that $b - a \in \mathfrak{m}^n$ and $f(b) = 0$.*

We can now provide the required extension of Lemma 2.1 to finite local rings that will be used in the sequel.

Lemma 2.3. *Let R be a finite local ring of odd characteristic. Let a, b, c be units in R. Then, the equation*

$$ax^2 + by^2 = c, \tag{7}$$

has a solution in R, with either x or y a unit in R.

Proof. Let $\psi : R \to R/\mathfrak{m}$ be the canonical epimorphism. Let $(z_1, z_2) \in (R/\mathfrak{m})^2$ be a solution of equation $\psi(a)x^2 + \psi(b)y^2 = \psi(c)$ in the field $R/\mathfrak{m}$. Since $\ker(\psi) = \mathfrak{m}$ and $\mathfrak{m}$ is the set of all non units of R it follows that $\psi(c) \neq 0$. Consequently, $z_1 \neq 0$ or $z_2 \neq 0$. Assume without loss of generality that $z_1 \neq 0$. Let us choose elements $w_1, w_2 \in R$ such that $\psi(w_1) = z_1$ and $\psi(w_2) = z_2$ and consider

$$f = (ax^2 + by^2 - c, y - w_2) \in R[x, y]^2.$$

Note that, $f(w_1, w_2) \in \mathfrak{m}^2$ and $\det(\mathrm{Jac} f(w_1, w_2)) = 2aw_1$ is a unit. Hence, the result follows immediately from Lemma 2.2. □

3. Basic results about generalized Hamilton quaternions

In this section, for the sake of completeness, we present some basic definitions and results regarding generalized Hamilton quaternions that will be used in the sequel. The proofs of these results can be found in [3].

The basis $\{1, i, j, k\}$ of the R-module $H(R)$ that satisfies relations (1) is not unique. For example $\{1, -i, -j, k\}$ is also a basis of the R-module $H(R)$ that satisfies the same relations (1). Thus, we make the following definition.

Definition 3.1. A *quaternionic basis* of $\left(\frac{a,b}{R}\right)$ is any basis $\mathcal{B} = \{1, I, J, K\}$ of the free R-module $H(R)$ such that

$$I^2 = a,$$
$$J^2 = b,$$
$$IJ = -JI = K.$$

Given a quaternionic basis $\{1, i, j, k\}$, the elements of the submodule $\langle i, j, k\rangle$, generated by i, j, k, are called *pure quaternions*. Note that the square of any pure quaternion is an element of R.

Remark 3.2. Given $q \in \left(\frac{a,b}{R}\right)$ and a fixed quaternionic basis, there exist $x_0 \in R$ and a pure quaternion q_0 such that $q = x_0 + q_0$. Observe that both x_0 and q_0 are uniquely determined and also that the only pure quaternion in R is 0.

The following classical concepts are not altered by the fact that a and b are not necessarily units.

Definition 3.3. Consider the quaternionic basis $\{1, i, j, k\}$ and let $q \in \left(\frac{a,b}{R}\right)$. Put $q = x_0 + q_0$ with $x_0 \in R$ and $q_0 = x_1 i + x_2 j + x_3 k$ a pure quaternion. Then,

(i) The conjugate of q is: $\overline{q} = x_0 - q_0 = x_0 - x_1 i - x_2 j - x_3 k$.
(ii) The trace of q is $\mathrm{tr}(q) = q + \overline{q} = 2x_0$.
(iii) The norm of q is $\mathrm{n}(q) = q\overline{q} = x_0^2 - q_0^2 = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$.

Note that $\mathrm{n}(q), \mathrm{tr}(q) \in R$ and $\mathrm{n}(q_1 q_2) = \mathrm{n}(q_1)\mathrm{n}(q_2)$.

Remark 3.4. Observe that, if q is a pure quaternion, then $\overline{q} = -q$ and $\mathrm{tr(q)} = 0$. The converse also holds if R has odd characteristic.

In what follows, we assume that a homomorphism f between two quaternion rings is also an R-module homomorphism. Hence, $f(1) = 1$ and it fixes every element of the base ring R. For the sake of simplicity we will call them

R-homomorphisms and an R-isomorphism is just a bijective R-homomorphism. Now, let $f : \left(\frac{a,b}{R}\right) \to \left(\frac{c,d}{R}\right)$ be a linear map and let us consider quaternionic bases $\{1, i, j, k\}$ and $\{1, I, J, K\}$ of $\left(\frac{a,b}{R}\right)$ and $\left(\frac{c,d}{R}\right)$, respectively. It is clear that if $f(1) = 1$, $f(i^2) = a$, $f(j^2) = b$ and $f(ij) = -f(ji) = f(k)$, then f induces a well-defined R-homomorphism between both quaternion rings. We will make extensive use of this fact in the next section.

The next result [3, Th. 2, Cor. 1] shows that isomorphisms preserve conjugation and, consequently, also traces and norms.

Theorem 3.5. *Let $f : \left(\frac{a,b}{R}\right) \to \left(\frac{c,d}{R}\right)$ be an algebra isomorphism. Then, for every $q \in \left(\frac{a,b}{R}\right)$ the following hold.*

(i) $f(\overline{q}) = \overline{f(q)}$.
(ii) $\mathrm{tr}\,(f(q)) = \mathrm{tr}(q)$.
(iii) $\mathrm{n}\,(f(q)) = \mathrm{n}(q)$.

Remark 3.6. Theorem 3.5 implies in particular that the conjugate, the trace and the norm of an element are independent from the quaternionic basis of $\left(\frac{a,b}{R}\right)$ used to compute them. Moreover, according to Remark 3.4, Theorem 3.5 implies that, in the odd characteristic case, every isomorphism preserves pure quaternions.

Finally, the following proposition [3, Prop. 1] provides information about the isomorphisms between quaternion rings of a specific kind.

Proposition 3.7. *Let R be a ring with odd characteristic and let $f : \left(\frac{a,b}{R}\right) \to \left(\frac{a,c}{R}\right)$ be an algebra isomorphism. Then, for some pair of quaternionic bases the matrix of f has the form*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha_1 & \alpha_2 \\ 0 & 0 & \beta_1 & \beta_2 \\ 0 & 0 & \gamma_1 & \gamma_2 \end{pmatrix},$$

with $\alpha_1 a = \alpha_2 a = 0$.

4. Isomorphisms of generalized Hamilton quaternions over finite local rings

For any ring R the matrix ring $\mathbb{M}_2(R)$ is isomorphic to $\left(\frac{-1,1}{R}\right)$. Any quaternion algebra isomorphic to $\mathbb{M}_2(R)$ is called a *split quaternion algebra over R*. It is well-known [11, p. 19] that every quaternion algebra $\left(\frac{a,b}{\mathbb{F}}\right)$ over a finite field $\mathbb{F}$ of odd characteristic with $ab \neq 0$ is split. In the following lemma we extend this result to finite local rings and, due to decomposition (3), also to finite rings.

Lemma 4.1. *Let R be a finite local ring of odd characteristic. If $a, b \in R$ are units, then*

$$\left(\frac{a,b}{R}\right) \cong \mathbb{M}_2(R).$$

Proof. Let a, b be units in R. Due to Lemma 2.3 we can find $u, v \in R$ such that $b = u^2 - av^2$.

Now, let us consider the matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} u & -av \\ v & -u \end{pmatrix}.$$

Clearly we have that $A^2 = aI$, $B^2 = bI$ and $AB = -BA$.

Moreover, if $\alpha, \beta, \gamma, \delta \in R$ and we solve the linear system of equations associated to

$$x_0 I + x_1 A + x_2 B + x_3 AB = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

we get that it has a unique solution which is given by:

$$\begin{aligned} x_0 &= \frac{\alpha + \delta}{2}, \\ x_1 &= \frac{\beta + a\gamma}{2a}, \\ x_2 &= \frac{\alpha\ u - \delta u + \beta v - a\gamma v}{2b}, \\ x_3 &= \frac{-\beta u + a\gamma u - a\alpha v + a\delta v}{2ab}. \end{aligned}$$

Consequently, the set $\{I, A, B, AB\}$ is a basis of $\mathbb{M}_2(R)$ and the result follows. □

The rest of this section is devoted to the study of isomorphisms between generalized Hamilton quaternions over finite local rings.

The following result gives us a technique to prove that two rings of generalized Hamilton quaternions over a ring R are not isomorphic. Roughly speaking, we replace the ring R by one of its quotients.

Lemma 4.2. *Let R be a finite local ring with odd characteristic with maximal ideal $\mathfrak{m}$ with index of nilpotence k. Let a_i, for $i = 1, ..., 4$, be elements of R such that*

$$\left(\frac{a_1, a_2}{R}\right) \cong \left(\frac{a_3, a_4}{R}\right).$$

Then, for $s = 1, \ldots, k$ we have

$$\left(\frac{\gamma_s(a_1), \gamma_s(a_2)}{R/\mathfrak{m}^s}\right) \cong \left(\frac{\gamma_s(a_2), \gamma_s(a_3)}{R/\mathfrak{m}^s}\right).$$

Proof. Let f be an isomorphism from $\left(\frac{a_1,a_2}{R}\right)$ to $\left(\frac{a_3,a_4}{R}\right)$, and let $A = [a_{ij}]$ be the coordinate matrix of f with respect to some quaternionic bases. Consider the matrix $\gamma_s(A) = [\gamma_s(a_{ij})]$ over $R/\mathfrak{m}^s$. Since γ_s preserves isomorphisms of R, it follows that

$$\det\left(\gamma_s(A)\right) = \gamma_s\left[\det(A)\right]. \tag{8}$$

If x is a unit in R, then $\gamma_s(x)$ is a unit in $R/\mathfrak{m}^s$. Then, it follows from (8) that $\det\left(\gamma_s(A)\right)$ is a unit. Consequently, the homomorphism from $\left(\frac{\gamma_s(a_1),\gamma_s(a_2)}{R/\mathfrak{m}^s}\right)$ to $\left(\frac{\gamma_s(a_3),\gamma_s(a_4)}{R/\mathfrak{m}^s}\right)$ defined by the matrix $\gamma_s(A)$ is an isomorphism, which proves the result. □

Lemma 4.3. *Let R be a finite local ring of odd characteristic and let $0 \neq a, b \in R$. Then, the quaternion algebras R_1, R_2, R_3 defined by*

$$R_1 = \left(\frac{a,b}{R}\right), \quad R_2 = \left(\frac{a,0}{R}\right), \quad R_3 = \left(\frac{0,0}{R}\right)$$

are pairwise non-isomorphic.

Proof. For each $i \in \{1,2\}$ let us define the set $\mathbb{P}_i := \{q \in R_i : \mathrm{tr}(q) = 0\}$. Note that, $\mathbb{P}_i$ is precisely the set of pure quaternions and is hence preserved by isomorphisms. Now, for every element $q \in \mathbb{P}_3$ it holds that $q^2 = 0$, while $\mathbb{P}_1$ and $\mathbb{P}_2$ contain elements whose square is non-zero. This implies that R_3 is not isomorphic to R_1 or R_2.

Assume that $R_1 \cong R_2$. We apply Proposition 3.7 and thus we can consider $\{1, i, j, k\}$ and $\{1, I, J, K\}$ quaternionic bases of R_1 and R_2, respectively, such that the matrix of the isomorphism f with respect to these bases is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha_1 & \alpha_2 \\ 0 & 0 & \beta_1 & \beta_2 \\ 0 & 0 & \gamma_1 & \gamma_2 \end{pmatrix}.$$

with $\alpha_1 a = \alpha_2 a = 0$. Then

$$b = j^2 = f(j^2) = f(j)^2 = (\alpha_1 I + \beta_1 J + \gamma_1 K)^2 = \alpha_1 I^2 + \beta_1^2 J^2 + \gamma_1^2 K^2 = 0,$$

a contradiction. □

Lemma 4.4. *Let R be a finite local ring of odd characteristic with maximal ideal $\mathfrak{m}$, and let $a_1, a_2, a_3 \in R$ such that $w(a_2) \neq w(a_3)$. Then*

$$\left(\frac{a_1, a_2}{R}\right) \ncong \left(\frac{a_1, a_3}{R}\right).$$

Proof. The main idea behind the proof is to exploit the epimorphism defined in (6) and then apply Lemma 4.3. Recall that $\ker(\gamma_s) = \mathfrak{m}^s = \{x \in R : w(x) \geq s\}$. Let us assume that both rings are isomorphic. Without loss of generality we can assume that $w(a_2) < w(a_3)$ and three different situations arise:

(i) $w(a_1) \leq w(a_2) < w(a_3)$. In this case, if we consider the isomorphism $\gamma_{w(a_3)} : R \longrightarrow R/\mathfrak{m}^{w(a_3)}$ given by Lemma 4.2:

$$\left(\frac{\gamma_{w(a_3)}(a_1), \gamma_{w(a_3)}(a_2)}{R/\mathfrak{m}^{w(a_3)}}\right) \cong \left(\frac{\gamma_{w(a_3)}(a_1), \gamma_{w(a_3)}(a_3)}{R/\mathfrak{m}^{w(a_3)}}\right).$$

Now, $\gamma_{w(a_3)}(a_i)$ is nonzero for $i = 1, 2$ but $\gamma_{w(a_3)}(a_3) = 0$, which contradicts Lemma 4.3.

(ii) $w(a_2) < w(a_1) < w(a_3)$. In this case, we consider again the isomorphism $\gamma_{w(a_3)} : R \longrightarrow R/\mathfrak{m}^{w(a_3)}$ given by Lemma 4.2:

$$\left(\frac{\gamma_{w(a_3)}(a_1), \gamma_{w(a_3)}(a_2)}{R/\mathfrak{m}^{w(a_3)}}\right) \cong \left(\frac{\gamma_{w(a_3)}(a_1), \gamma_{w(a_3)}(a_3)}{R/\mathfrak{m}^{w(a_3)}}\right).$$

Now, $\gamma_{w(a_3)}(a_i)$ is nonzero for $i = 1, 2$ while $\gamma_{w(a_3)}(a_3) = 0$, which contradicts Lemma 4.3.

(iii) $w(a_2) < w(a_3) \leq w(a_1)$. In this case, if we consider the isomorphism $\gamma_{w(a_3)} : R \longrightarrow R/\mathfrak{m}^{w(a_3)}$ given by Lemma 4.2:

$$\left(\frac{\gamma_{w(a_3)}(a_1), \gamma_{w(a_3)}(a_2)}{R/\mathfrak{m}^{w(a_3)}}\right) \cong \left(\frac{\gamma_{w(a_3)}(a_1), \gamma_{w(a_3)}(a_3)}{R/\mathfrak{m}^{w(a_3)}}\right).$$

Now, $\gamma_{w(a_3)}(a_2)$ is nonzero, while $\gamma_{w(a_3)}(a_i) = 0$ for $i = 1, 3$; which contradicts Lemma 4.3.

So, in every case we reach a contradiction, and the result follows. □

Lemma 4.5. *Let R be a finite local ring of odd characteristic with maximal ideal $\mathfrak{m}$, and let $\psi : R \to R/\mathfrak{m}$ be the canonical epimorphism. Let s and t be units of R such that $\psi(st)$ is a quadratic residue in the field $R/\mathfrak{m}$. Then, for every $a, b \in R$ we have that*

$$L = \left(\frac{ta, b}{R}\right) \cong \left(\frac{sa, b}{R}\right) = S.$$

Proof. Let $y \in R/\mathfrak{m}$ be such that $y^2 = \psi(st)$. By Hensel's lemma [1, p. 115], there is an element $z \in R$ such that $z^2 = st$. Now if $w = zs^{-1}$ we have $w^2 = s^{-1}t$. Let us consider $\{1, i, j, k\}$ and $\{1, I, J, K\}$ quaternionic bases of L and S, respectively. Then, the linear map $L \longrightarrow S$ whose matrix with respect to these bases is

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & w & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & w \end{pmatrix}$$

induces an isomorphism because $(wI)^2 = w^2I^2 = ts^{-1}sa = at$ and A is invertible over R. □

Lemma 4.6. *Let R be a finite local ring of odd characteristic with maximal ideal $\mathfrak{m}$, and let $\psi : R \to R/\mathfrak{m}$ be the canonical epimorphism. Let $s \in R$ be a unit. Then, for any $r \in R$ we have*

$$L = \left(\frac{r, r}{R}\right) \cong \left(\frac{sr, sr}{R}\right) = S.$$

Proof. From Lemma 2.3 it follows that any unit of R can be written as a sum of two squares. So, let $x, y \in R$ be such that $x^2 + y^2 = s^{-1}$. Now let us consider $\{1, i, j, k\}$ and $\{1, I, J, K\}$ quaternionic bases of L and S, respectively. Then, the linear map $L \longrightarrow S$ whose matrix with respect to these bases is

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x & -y & 0 \\ 0 & y & x & 0 \\ 0 & 0 & 0 & s^{-1} \end{pmatrix}$$

induces an isomorphism because

$$(xI + yJ)^2 = (x^2 + y^2)sr = r,$$

$$(-yI + xJ)^2 = (x^2 + y^2)sr = r,$$

$$(xI + yJ)(-yI + xJ) = (x^2 + y^2)K = s^{-1}K$$

and A is invertible over R. □

Lemma 4.7. *Let R be a finite local ring of odd characteristic with maximal ideal $\mathfrak{m}$ and let $\psi : R \to R/\mathfrak{m}$ be the canonical epimorphism. Let $s, t, u \in R$ be units. Then,*

(i) *For every $m \in R$:*

$$\left(\frac{1, sm}{R}\right) \cong \left(\frac{1, m}{R}\right) \text{ and } \left(\frac{u, m}{R}\right) \cong \left(\frac{u, tm}{R}\right).$$

(ii) *If m is a zero divisor and $\psi(u)$ is a quadratic nonresidue in the field $R/\mathfrak{m}$:*

$$\left(\frac{1, m}{R}\right) \ncong \left(\frac{u, m}{R}\right).$$

Proof. We proceed case by case:

(i) To see that $L = \left(\frac{1, m}{R}\right) \cong \left(\frac{1, sm}{R}\right) = S$, let us consider $\{1, i, j, k\}$ and $\{1, I, J, K\}$ quaternionic bases of L and S, respectively. Using Lemma 2.3

there are $x, y \in R$, such that $x^2 - y^2 = s^{-1}$. Then, the linear map $L \longrightarrow S$ whose matrix with respect to these bases is

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x & y \\ 0 & 0 & y & x \end{pmatrix}$$

induces an isomorphism because

$$(xJ + yK)^2 = x^2J^2 + y^2K^2 = x^2sm - y^2sm = sm(x^2 - y^2) = m$$

and A is invertible over R.

The other isomorphism can be proved in a similar way.

(ii) To see that $\left(\frac{1,m}{R}\right) \ncong \left(\frac{u,m}{R}\right)$ it is enough to observe that $\left(\frac{1,m}{R}\right)$ does not contain any pure quaternion q with $q^2 = u$. In fact, if $\{1, i, j, k\}$ is a quaternionic basis, $q = ai + bj + ck$ and $q^2 = a^2 + (b^2 - c^2)m$. Hence, $\psi(u) = \psi(a)^2$ in the field $R/\mathfrak{m}$, which is a contradiction. □

Lemma 4.8. *Let R be a finite local ring of odd characteristic with maximal ideal $\mathfrak{m}$. Let $\psi : R \to R/\mathfrak{m}$ be the canonical epimorphism. Let $u \in R$ be a unit such that $\psi(u)$ is a quadratic nonresidue in $R/\mathfrak{m}$ and let $m \in R$ be a nonzero zero divisor. Then,*

(i) $R_1 = \left(\frac{um,m}{R}\right) \ncong \left(\frac{m,m}{R}\right) = R_2$.

(ii) $S_1 = \left(\frac{um,0}{R}\right) \ncong \left(\frac{m,0}{R}\right) = S_2$.

Proof. We proceed case by case:

(i) Let $\{1, i, j, k\}$ and $\{1, I, J, K\}$ be quaternionic bases of R_1 and R_2, respectively. Let us consider the following sets:

$$N_1 := \{q = x_1i + x_2j + x_3k \in R_1 : \mathrm{n}(q) = 0, \text{ and } x_l \text{ is a unit for } l = 1, 2, 3\},$$

$$N_2 := \{q = y_1I + y_2J + y_3K \in R_2 : \mathrm{n}(q) = 0, \text{ and } y_l \text{ is a unit for } l = 1, 2, 3\}.$$

Note that $q = x_1i + x_2j + x_3k \in N_1$ if and only if

$$x_1^2um + x_2^2m - x_3^2um^2 = 0, \tag{9}$$

and x_l is a unit for $l = 1, 2, 3$.

On the other hand, $q = y_1I + y_2J + y_3K \in N_2$ if and only if

$$y_1^2m + y_2^2m - y_3^2m^2 = 0, \tag{10}$$

and y_l is a unit for $l = 1, 2, 3$.

Equation (9) is equivalent to $(x_1^2u + x_2^2 - x_3^2um)m = 0$. Since m is nonzero it follows that $x_1^2u + x_2^2 - x_3^2um$ is a zero divisor. Hence,

$$\psi(x_1)^2\psi(u) + \psi(x_2)^2 = 0. \tag{11}$$

Similarly we have

$$\psi(y_1)^2 + \psi(y_2)^2 = 0. \tag{12}$$

Moreover, we can see that:

(a) If -1 is a quadratic residue in $R/\mathfrak{m}$ (i.e., if $\text{char}(R/\mathfrak{m}) \equiv 1 \pmod 4$), then equation (12) has non-zero solutions while equation (11) has not.

(b) If -1 is a quadratic nonresidue in $R/\mathfrak{m}$ (i.e., if $\text{char}(R/\mathfrak{m}) \equiv 3 \pmod 4$), then equation (11) has non-zero solutions while equation (12) has not.

Now, if there was an isomorphism $\phi : R_1 \longrightarrow R_2$, then we would have $\phi(N_1) = N_2$ which we just saw is not possible by comparing their non-zero elements.

(ii) For this case, it is enough to observe that S_2 does not contain pure quaternions q such that $q^2 = um$, while S_1 obviously does contain such type of elements. To do so, just note that the equation $x^2m = um$ implies that $x^2 - u$ is a zero divisor, and hence

$$\psi(x)^2 = \psi(u). \tag{13}$$

But equation (13) has no solutions because $\psi(u)$ is a quadratic nonresidue in the field $R/\mathfrak{m}$. □

Lemma 4.9. *Let R be a finite local ring of odd characteristic with maximal ideal $\mathfrak{m}$. Let $\psi : R \to R/\mathfrak{m}$ be the canonical epimorphism. Let $u \in R$ be a unit such that $\psi(u)$ is a quadratic nonresidue in $R/\mathfrak{m}$. Let $m_1, m_2 \in R$ be two nonzero zero divisors such that $w(m_1) < w(m_2)$. Then, the quaternion rings $R_1 = \left(\frac{um_1, um_2}{R}\right)$, $R_2 = \left(\frac{m_1, um_2}{R}\right)$, $R_3 = \left(\frac{um_1, m_2}{R}\right)$ and $R_4 = \left(\frac{m_1, m_2}{R}\right)$ are pairwise non-isomorphic.*

Proof. Let us see that $R_1 \ncong R_2$, $R_1 \ncong R_4$, $R_2 \ncong R_3$ and $R_3 \ncong R_4$. If they were isomorphic, then due to Lemma 4.2 and considering the homomorphism $\gamma_{w(m_2)} : R \longrightarrow R/\mathfrak{m}^{w(m_2)}$ we would have that $\left(\frac{\gamma_{w(m_2)}(um_1), 0}{R/\mathfrak{m}^{w(m_2)}}\right) \cong \left(\frac{\gamma_{w(m_2)}(m_1), 0}{R/\mathfrak{m}^{w(m_2)}}\right)$, which contradicts Lemma 4.8.

Now, let us see that $R_1 \ncong R_3$. Assume that $R_1 \cong R_3$. Then, due to Proposition 3.7, we can consider $\{1, i, j, k\}$ and $\{1, I, J, K\}$ quaternionic bases of R_1 and R_3, respectively such that the matrix of the isomorphism f with respect to these bases

is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha_1 & \alpha_2 \\ 0 & 0 & \beta_1 & \beta_2 \\ 0 & 0 & \gamma_1 & \gamma_2 \end{pmatrix},$$

with $\alpha_1 u m_1 = 0$. In particular,

$$um_2 = j^2 = f(j^2) = f(j)^2 = (\alpha_1 I + \beta_1 J + \gamma_1 K)^2 = \alpha_1^2 u m_1 + \beta_1^2 m_2 - \gamma_1^2 u m_1 m_2 = \\ = \beta_1^2 m_2 - \gamma_1^2 u m_1 m_2.$$

In other words, $\beta_1^2 m_2 - \gamma_1^2 u m_1 m_2 = u m_2$. Therefore, $(\beta_1^2 - \gamma_1^2 u m_1 - u) m_2 = 0$, and hence $\beta_1^2 - \gamma_1^2 u m_1 - u$ is a zero divisor. Thus $\psi(\beta_1)^2 = \psi(u)$ in the residue field $R/\mathfrak{m}$, which is a contradiction because $\psi(u)$ is a quadratic nonresidue.

The remaining case, namely $R_2 \ncong R_4$, can be proved in the exact same way. □

Now, we close this section with the main result that summarizes all the previous work.

Theorem 4.10. *Let R be a finite local ring of odd characteristic with maximal ideal $\mathfrak{m}$. Let $\psi : R \to R/\mathfrak{m}$ be the canonical epimorphism. Let $u \in R$ be a unit such that $\psi(u)$ is a quadratic nonresidue in $R/\mathfrak{m}$. Let $s, t \in R$ be units and let $m, m_1, m_2 \in R$ be nonzero zero divisors such that $w(m_1) < w(m_2)$. Then, the following hold*

(i) $\left(\frac{s,t}{R}\right) \cong \left(\frac{1,1}{R}\right)$.

(ii) $\left(\frac{s,tm}{R}\right) \cong \begin{cases} \left(\frac{u,m}{R}\right), & \text{if } \psi(s) \text{ is a quadratic nonresidue ;} \\ \left(\frac{1,m}{R}\right), & \text{if } \psi(s) \text{ is a quadratic residue .} \end{cases}$

(iii) $\left(\frac{sm,tm}{R}\right) \cong \begin{cases} \left(\frac{um,m}{R}\right), & \text{if } \psi(st) \text{ is a quadratic nonresidue ;} \\ \left(\frac{m,m}{R}\right), & \text{if } \psi(st) \text{ is a quadratic residue .} \end{cases}$

(iv) $\left(\frac{sm_1,tm_2}{R}\right) \cong \begin{cases} \left(\frac{um_1,m_2}{R}\right), & \text{if only } \psi(t) \text{ is a quadratic residue;} \\ \left(\frac{m_1,um_2}{R}\right), & \text{if only } \psi(s) \text{ is a quadratic residue.} \\ \left(\frac{m_1,m_2}{R}\right), & \text{if both } \psi(s) \text{ and } \psi(t) \text{ are quadratic residues.} \\ \left(\frac{um_1,um_2}{R}\right), & \text{if both } \psi(s) \text{ and } \psi(t) \text{ are quadratic nonresidues.} \end{cases}$

Proof. (i) Just apply Lemma 4.1.

(ii) We make use of the well known fact that in a finite field the product of two non-square elements is a square. If $\psi(s)$ is a quadratic nonresidue:

$$\left(\frac{s,tm}{R}\right) \overset{\text{Lem. 4.7}}{\cong} \left(\frac{s,m}{R}\right) \overset{\text{Lem. 4.5}}{\cong} \left(\frac{u,m}{R}\right).$$

Now, if $\psi(s)$ is a quadratic residue:

$$\left(\frac{s,tm}{R}\right) \underset{\text{Lem. } 4.5}{\cong} \left(\frac{1,tm}{R}\right) \underset{\text{Lem. } 4.7}{\cong} \left(\frac{1,m}{R}\right).$$

Finally, $\left(\frac{u,m}{R}\right)$ and $\left(\frac{1,m}{R}\right)$ are not isomorphic due to Lemma 4.7.

(iii) If $\psi(st)$ is a quadratic nonresidue, only one among $\psi(s)$ and $\psi(t)$ is a quadratic residue. We can assume without loss of generality that $\psi(s)$ is a quadratic residue and that $\psi(t)$ is a quadratic nonresidue (so $\psi(ut)$ is a quadratic residue) and then:

$$\left(\frac{sm,tm}{R}\right) \underset{\text{Lem. } 4.5}{\cong} \left(\frac{sm,um}{R}\right) \underset{\text{Lem. } 4.5}{\cong} \left(\frac{m,um}{R}\right).$$

Now, if $\psi(st)$ is a quadratic residue:

$$\left(\frac{sm,tm}{R}\right) \underset{\text{Lem. } 4.5}{\cong} \left(\frac{tm,tm}{R}\right) \underset{\text{Lem. } 4.6}{\cong} \left(\frac{m,m}{R}\right).$$

Finally, $\left(\frac{m,m}{R}\right)$ and $\left(\frac{um,m}{R}\right)$ are not isomorphic due to Lemma 4.8.

(iv) Like in the previous points, it is enough to apply Lemma 4.5 repeatedly. The four different cases that arise are non-isomorphic due to Lemma 4.9.

□

5. Counting non-isomorphic generalized Hamilton quaternions over principal ideal rings of odd characteristic

When the maximal ideal $\mathfrak{m}$ is principal, we will be able to count the total number of generalized Hamilton quaternion rings over R. This number depends only on the degree of nilpotence of $\mathfrak{m}$. Assume that the degree of nilpotence of $\mathfrak{m}$ is k and let g be a fixed generator of $\mathfrak{m}$. Then, every element x of R can be represented in the form

$$x = ag^{w(x)},$$

where $a \in R$ is a unit. Moreover, we have the following partition of the ring R

$$R = \{0\} \cup \mathcal{U}(R) \cup \mathcal{U}(R)g \cup \mathcal{U}(R)g^2 \cup \ldots \cup \mathcal{U}(R)g^{k-1}.$$

Note that this partition corresponds to the equivalence relation in R defined by $x \sim y$ if and only if $w(x) = w(y)$.

In order to count the total number of generalized Hamilton quaternion rings $\left(\frac{x,y}{R}\right)$, we divide the problem into four cases. We will repeatedly make use of the well-known fact that

$$\left(\frac{a,b}{R}\right) \cong \left(\frac{b,a}{R}\right). \tag{14}$$

(1) Both x and y are units.

In this case, it follows from Lemma 4.1 that there is only one generalized Hamilton quaternion ring.

(2) Both x and y are nonzero zero divisors.

Let g be as above. Then,

$$x = ag^{w(x)} \quad \text{and} \quad y = bg^{w(y)},$$

where a and b are units in R.

We subdivide into two subcases:

(a) $w(x) = w(y)$.

In this subcase, it follows from Theorem 4.10 (iii) that for any unit $u \in R$,

$$\left(\frac{x,y}{R}\right) \cong \begin{cases} \left(\frac{ug^{w(x)},g^{w(y)}}{R}\right), & \text{if } \psi(ab) \text{ is a quadratic nonresidue ;} \\ \left(\frac{g^{w(x)},g^{w(y)}}{R}\right), & \text{if } \psi(ab) \text{ is a quadratic residue.} \end{cases}$$

Therefore, as the degree of nilpotence of $\mathfrak{m}$ is k, we have $2(k-1)$ different non isomorphic generalized Hamilton quaternion rings, one for each value of $w(x)$.

(b) $w(x) < w(y)$.

In this subcase, it follows from Theorem 4.10 (iv) that for any unit $u \in R$,

$$\left(\frac{x,y}{R}\right) \cong \begin{cases} \left(\frac{ug^{w(x)},g^{w(y)}}{R}\right), & \text{if only } \psi(b) \text{ is a quadratic residue;} \\ \left(\frac{g^{w(x)},ug^{w(y)}}{R}\right), & \text{if only } \psi(a) \text{ is a quadratic residue;} \\ \left(\frac{g^{w(x)},g^{w(y)}}{R}\right), & \text{if both } \psi(a) \text{ and } \psi(b) \text{ are quadratic residues;} \\ \left(\frac{ug^{w(x)},ug^{w(y)}}{R}\right), & \text{if both } \psi(a) \text{ and } \psi(b) \text{ are quadratic nonresidues.} \end{cases}$$

Therefore, as the degree of nilpotence of $\mathfrak{m}$ is k, and taking (14) into account, we have $2(k-2)(k-1)$ different non isomorphic generalized Hamilton quaternion rings, one for each value of $w(x)$.

(3) x is a unit and y is a nonzero zero divisor.

We subdivide into two subcases:

(a) $\psi(x)$ is a quadratic residue in $R/\mathfrak{m}$.

From Theorem 4.10 (ii) it follows that

$$\left(\frac{x,y}{R}\right) \cong \left(\frac{1,y}{R}\right).$$

Note that $\left(\frac{1,y}{R}\right) \cong \left(\frac{1,y'}{R}\right)$ if and only if $w(y) = w(y')$. The "only if" part follows from Lemma 4.4. On the other hand, if $w(y) = w(y')$ then

there is a unit $e \in R$ such that $y = ey'$. Therefore, the result follows from Lemma 4.7.

Thus, as the degree of nilpotence of $\mathfrak{m}$ is k, and taking (14) into account, we have $k-1$ different non isomorphic generalized Hamilton quaternion rings, one for each value of $w(x)$.

(b) $\psi(x)$ is a quadratic nonresidue in $R/\mathfrak{m}$.

As in the previous subcase, from Theorem 4.10 (ii) it follows that

$$\left(\frac{x,y}{R}\right) \cong \left(\frac{u,y}{R}\right),$$

where $u \in R$ is a unit such that $\psi(u)$ is a quadratic non-residue in $R/\mathfrak{m}$.

As in the previous subcase we have that $\left(\frac{u,y}{R}\right) \cong \left(\frac{u,y'}{R}\right)$ if and only if $w(y) = w(y')$.

So, as the degree of nilpotence of $\mathfrak{m}$ is k, and taking (14) into account, we have $k-1$ non isomorphic generalized Hamilton quaternion rings, one for each value of $w(x)$.

(4) $x = 0$ or $y = 0$.

In this case we have the ring $\left(\frac{0,0}{R}\right)$ and for $y \neq 0$ it follows from Lemma 4.4 that $\left(\frac{0,y}{R}\right) \ncong \left(\frac{0,y'}{R}\right)$ if $w(y) \neq w(y')$. Now, if $w(y) = w(y')$ we have $y = uy'$, for a unit u. If $\psi(u)$ is a quadratic residue, then it follows from Lemma 4.5 that $\left(\frac{0,y}{R}\right) \cong \left(\frac{0,y'}{R}\right)$. On the other hand, if $\psi(u)$ is a quadratic non-residue, then it follows from Lemma 4.8 that $\left(\frac{0,y}{R}\right) \ncong \left(\frac{0,y'}{R}\right)$.

Hence, as the degree of nilpotence of $\mathfrak{m}$ is k, we have $2k+1$ different non isomorphic generalized Hamilton quaternion rings, one for each value of $w(x)$.

Finally, taking into consideration all the previous information, we conclude that there exist

$$2(k-1) + 2(k-2)(k-1) + (k-1) + (k-1) + 2k + 1 + 1 = 2k^2 + 2$$

non-isomorphic generalized Hamilton quaternions over R.

As a consequence of all the previous computations we obtain the following result.

Theorem 5.1. *Let R be a finite unital principal ideal ring of odd characteristic of type*

$$((R_1, \mathfrak{m}_1, p_1^{s_1}), (R_2, \mathfrak{m}_2, p_2^{s_2}), \ldots, (R_l, \mathfrak{m}_l, p_l^{s_l}))$$

and let k_i be the index of nilpotence of $\mathfrak{m}_i$. Then, the number of non-isomorphic generalized Hamilton quaternions over R is

$$2^l \prod_{i=1}^{l} (k_i^2 + 1).$$

Finally, we close this section, giving two applications of the previous result. The first one is the case $R = \mathbb{Z}/n\mathbb{Z}$ for an odd n, which was given in [3, Corollary 5].

Corollary 5.2. *Let n be an odd integer. Let us denote by $P(n)$ the number of different primes dividing n and by $w_p(n)$ the p-adic order of n. Then, the number of non-isomorphic generalized Hamilton quaternions over $\mathbb{Z}/n\mathbb{Z}$ is*

$$2^{P(n)} \prod_{p|n} (w_p(n)^2 + 1).$$

Finally, if $R = \mathbb{F}$ is a finite field of odd characteristic we get the following corollary.

Corollary 5.3. *Let $\mathbb{F}$ be a finite field of odd characteristic and let $a \in \mathbb{F}$ be a quadratic nonresidue. Then, up to isomorphism, there exist exactly four generalized Hamilton quaternions over $\mathbb{F}$. Namely,*

$$\left(\frac{1,1}{\mathbb{F}}\right), \left(\frac{a,0}{\mathbb{F}}\right), \left(\frac{1,0}{\mathbb{F}}\right) \text{ and } \left(\frac{0,0}{\mathbb{F}}\right).$$

Acknowledgement. The authors would like to thank the referees for their valuable suggestions and comments.

References

[1] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass.-London-Don Mills, 1969.

[2] J. M. Grau, C. Miguel and A. M. Oller-Marcén, *On the structure of quaternion rings over $\mathbb{Z}/n\mathbb{Z}$*, Adv. Appl. Clifford Algebr., 25(4) (2015), 875-887.

[3] J. M. Grau, C. Miguel and A. M. Oller-Marcén, *Quaternion rings over $\mathbb{Z}/n\mathbb{Z}$ for an odd n*, Adv. Appl. Clifford Algebr., 28(1) (2018), 17 (14 pp).

[4] B. H. Gross and M. W. Lucianovic, *On cubic rings and quaternion rings*, J. Number Theory, 129(6) (2009), 1468-1478.

[5] A. J. Hahn, Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups, Springer-Verlag, New York, 1994.

[6] T. Kanzaki, *On non-commutative quadratic extensions of a commutative ring*, Osaka Math. J., 10 (1973), 597-605.

[7] M. A. Knus, Quadratic and Hermitian Forms Over Rings, Grundlehren der Mathematischen Wissenschaften (no. 294), Springer-Verlag, Berlin, 1991.

[8] B. R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics (Vol. 28), Marcel Dekker, New York, 1974.

[9] C. Miguel and R. Serôdio, *On the structure of quaternion rings over* $\mathbb{Z}_p$, Int. J. Algebra, 5(27) (2011), 1313-1325.

[10] S. Priess-Crampe and P. Ribenboim, *A general Hensel's lemma*, J. Algebra, 232(1) (2000), 269-281.

[11] R. S. Pierce, Associative Algebras, Springer-Verlag, New York-Berlin, 1982.

[12] D. Savin, *About Special Elements in Quaternion Algebras Over Finite Fields*, Adv. Appl. Clifford Algebr., 27(2) (2017), 1801-1813.

[13] C. Small, Arithmetic of Finite Fields, Marcel Dekker, New York, 1991.

[14] A. A. Tuganbaev, *Quaternion algebras over commutative rings*, Math. Notes, 53(1-2) (1993), 204-207.

[15] J. Voight, *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math., 657 (2011), 113-134.

[16] J. Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, Quadratic and Higher Degree Forms, Dev. Math., vol. 31, Springer, New York, 2013, 255-298.

[17] A. Weil, Basic Number Theory, Die Grundlehren der Mathematischen Wissenschaften (Band 144), Springer-Verlag, New York-Berlin, 1974.

José María Grau
Departamento de Matemáticas
Universidad de Oviedo
33007 Oviedo, Spain
e-mail: grau@uniovi.es

Celino Miguel
Departamento de Matemática
Universidade da Beira Interior
6201-001 Covilhã, Portugal
e-mail: celino@ubi.pt

Antonio M. Oller-Marcén (Corresponding Author)
Centro Universitario de la Defensa de Zaragoza
50090 Zaragoza, Spain
e-mail: oller@unizar.es