CARPATHIAN J. MATH.
Volume **37** (2021), No. 1,
Pages 91 - 100

Online version at https://www.carpathian.cunbm.utcluj.ro/
Print Edition: ISSN 1584 - 2851; Online Edition: ISSN 1843 - 4401
DOI: https://doi.org/10.37193/CJM.2021.01.09

Quadratic maps in two variables on arbitrary fields

R. DURÁN DÍAZ[1], L. HERNÁNDEZ ENCINAS[2] and J. MUÑOZ MASQUÉ[2]

ABSTRACT. Let $\mathbb{F}$ be a field of characteristic different from 2 and 3, and let V be a vector space of dimension 2 over $\mathbb{F}$. The generic classification of homogeneous quadratic maps $f\colon V \to V$ under the action of the linear group of V, is given and efficient computational criteria to recognize equivalence are provided.

1. INTRODUCTION

Let $\mathbb{F}$ be a field of characteristic $p \neq 2, 3$ and let V be a 2-dimensional $\mathbb{F}$-vector space. In this paper we classify homogeneous quadratic maps $f\colon V \to V$ that satisfy certain generic condition to be introduced later. Since there is a natural bijection between homogeneous quadratic maps on V and symmetric bilinear composition laws $F\colon V \times V \to V$, the classification is carried out over the latter considering the action of the general linear group $GL(V)$.

The topic has not elicited much attention and the literature is scarce. As far as we know, only our previous work [2] has clearly focused this topic. However, homogeneous quadratic maps play a major role in the dynamics of discrete systems (see, for example, [1]) and may give rise to new or revamped one-way functions potentially interesting for cryptographic applications.

Our purpose in this work is to apply to arbitrary fields the classification obtained in [2], where such goal was achieved only for the case of an an algebraically closed field. However, it will become apparent along the coming sections that the methods employed to classify in the latter case are no longer applicable. Actually, the main role for the present case is played by the Clifford algebra associated to the quadratic form defining the symmetric bilinear law. In particular, this new tool has allowed us to deal with both the hyperbolic and the elliptic cases of the quadratic form under a unified framework. We want to stress that the new methods are totally different from those used in [2] so that the present contribution cannot be qualified as a plain generalization or extension of the former one.

The main results of the paper can summarized as follows: We give both the general form of any symmetric bilinear law such that its associated quadratic form takes the value -1, and the explicit expression for the maps in the group of isometries. It turns out that such maps are parametrized by an element of the Clifford algebra whose Clifford norm is 1. Next we compute the isotropy group, which is discrete. Last, in order to perform the classification, we resort to the invariants computed in [2] transposed to the case we are dealing with now. While it is true that this technique do not provide a perfect classification, we do supply efficient computational criteria, allowing one to recognize such equivalence.

Received: 17.01.2019. In revised form: 07.07.2020. Accepted: 14.07.2020
2010 *Mathematics Subject Classification.* 15A72, 11E88, 12E20, 12E30, 13A50, 15A66.
Key words and phrases. *Clifford algebra, homogeneous quadratic map, invariant function, linear representation, linear group, symmetric bilinear composition law.*
Corresponding author: R. Durán Díaz; raul.duran@uah.es

We stick here, as we did in [2], to the case of a 2-dimensional vector space V. The reason will become clear, since the deployed techniques are deeply connected to the 2-dimensional case. Apparently, each dimension claims specific techniques and tools in order to achieve the classification. In a sense, the procedure shows a kind of "artistic" flavor that renders it not immediately or easily exportable to higher dimensions.

The paper is organized as follows: after a first section explaining some preliminaries and notation, we focus on the topic of Clifford algebras, making it apparent the role played by them in the present work; next we classify generic symmetric bilinear laws, followed by the computation of the isotropy group; finally we undertake the task of computing the criteria to recognize the equivalence of symmetric bilinear laws.

2. Preliminaries and notation

If $\{v_1, v_2\}$ is a basis for V, then $f(x) = f_1(x)v_1 + f_2(x)v_2$ where

$$\begin{aligned} f_1(x_1, x_2) &= a_1(x_1)^2 + 2b_1x_1x_2 + c_1(x_2)^2, \qquad a_i, b_i, c_i \in \mathbb{F}, 1 \leq i \leq 2, \\ f_2(x_1, x_2) &= a_2(x_1)^2 + 2b_2x_1x_2 + c_2(x_2)^2, \qquad x = x_1v_1 + x_2v_2. \end{aligned}$$

As $p \neq 2$, there is a natural bijection between homogeneous quadratic maps on V and symmetric bilinear composition laws $F\colon V \times V \to V$, $F(x, y) = x \star y$ (in short: SBLs), which is given by the polarization formula, e.g., see [4, XV, §§2–3]. Remember that two bilinear laws $\star\colon (x, y) \in V^2 \mapsto x \star y \in V$ and $\circ\colon (x, y) \in (V')^2 \mapsto x \circ y \in V'$ are isomorphic—or $GL(V)$-equivalent—if and only if there is a vector-space isomorphism $u\colon V \xrightarrow{\simeq} V'$ such that, $\forall (x, y) \in V^2$, $u(x) \circ u(y) = u(x \star y)$.

If V, V' are two $\mathbb{F}$-vector spaces, the space of bilinear maps is denoted by $L^2(V, V')$, with the natural identification $L^2(V, V) \cong L(V \otimes V, V) \cong \otimes^2 V^* \otimes V$. Hence, the classification problem that we tackle transforms into a classification problem in the subspace of symmetric tensors of type $(1, 2)$ on the plane, $S^2V^* \otimes V \subset \otimes^2 V^* \otimes V$. The natural action of the linear group $GL(V)$ on $S^2V^* \otimes V$ is given by

$$\begin{aligned} &\forall x, y \in V, F \in S^2V^* \otimes V, \ \forall u \in GL(V), \\ &(u \cdot F)(x, y) = u\left(F\left(u^{-1}(x), u^{-1}(y)\right)\right). \end{aligned} \tag{2.1}$$

Let $\{v_1^*, v_2^*\}$ be the dual basis of $\{v_1, v_2\}$; i.e., $v_i^*(v_j) = \delta_{ij}$. Every $F \in S^2V^* \otimes V$ is written as

$$\begin{aligned} F = {} & v_1^* \otimes v_1^* \otimes (a_1v_1 + a_2v_2) + (v_1^* \otimes v_2^* + v_2^* \otimes v_1^*) \otimes (b_1v_1 + b_2v_2) \\ & + v_2^* \otimes v_2^* \otimes (c_1v_1 + c_2v_2), \end{aligned} \tag{2.2}$$

or matricially,

$$\begin{aligned} &F(x, y) = \left((x_1, x_2)\begin{pmatrix} a_1 & b_1 \\ b_1 & c_1 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, (x_1, x_2)\begin{pmatrix} a_2 & b_2 \\ b_2 & c_2 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right), \\ &x = x_1v_1 + x_2v_2, y = y_1v_1 + y_2v_2. \end{aligned}$$

Let $\mathrm{tr}\colon S^2V^* \otimes V \to V^*$ be the trace mapping. From (2.2) we obtain

$$\mathrm{tr}\, F = (a_1 + b_2)v_1^* + (b_1 + c_2)v_2^*. \tag{2.3}$$

The homomorphism $F \in S^2V^* \otimes V \mapsto \mathrm{tr}\, F \in V^*$ is proved to be $GL(V)$-equivariant. For a given $x \in V$, let $F_x\colon V \to V$ be the $\mathbb{F}$-linear endomorphism

$$\forall y \in V, \quad F_x(y) = F(x, y). \tag{2.4}$$

For each bilinear symmetric map $F\colon V \times V \to V$, let $q_F\colon V \to \mathbb{F}$ be the quadratic form defined by $q_F(x) = \det(F_x)$, where F_x is the endomorphism defined in (2.4). As a computation shows,

$$q_F(x) = (x_1, x_2) \begin{pmatrix} a_1b_2 - a_2b_1 & \frac{1}{2}(a_1c_2 - a_2c_1) \\ \frac{1}{2}(a_1c_2 - a_2c_1) & b_1c_2 - b_2c_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \tag{2.5}$$
$$= (a_1b_2 - a_2b_1)\,(x_1)^2 + (a_1c_2 - a_2c_1)\,x_1x_2 + (b_1c_2 - b_2c_1)\,(x_2)^2,$$

F being given as in (2.2) and $x = x_1v_1 + x_2v_2$.

3. The Clifford algebra of q_F

First of all, let $\star$ be a non-degenerate traceless SBL on V, with associated symmetric bilinear map $F\colon V \times V \to V$, and let $q = q_F$ be the quadratic form introduced in the section 2.

Given $x \in V$, the Cayley-Hamilton theorem yields $(F_x)^2 = -q(x) \cdot \mathrm{id}\, V$, where F_x is the endomorphism defined in (2.4). Hence, by the universal property of the Clifford algebra (e.g., see [4, XIX, section 4]), the linear map

$$i\colon V \to \mathrm{End}(V), \quad i(x) = F_x, \quad \forall x \in V,$$

extends to a homomorphism $\bar{\imath}\colon C(-q) \to \mathrm{End}(V)$ from the Clifford algebra of $-q$ to $\mathrm{End}(V)$. Since $-q$ is non-degenerate with dimension 2, the algebra $C(-q)$ is central simple (e.g., see [3, Proposition 11.6–(1)]); hence $\bar{\imath}$ is injective, and since $\dim \mathrm{End}(V) = 4 = \dim C(-q)$, we actually conclude that $\bar{\imath}$ is an isomorphism of $\mathbb{F}$-algebras.

Moreover, $C_0(-q)$ is a quadratic $\mathbb{F}$-algebra and according to [3, Proposition 12.1], the form $-q$ represents 1, i.e., q represents -1.

Consequently, a non-degenerate quadratic form $Q\colon V \to \mathbb{F}$ is of the form $Q = q_F$ for some F if and only if Q takes the value -1. If $\mathbb{F}$ is a finite field, then every quadratic form of rank ≥ 2 on $\mathbb{F}$ takes any value of $\mathbb{F}^*$ (see [5, 1.7. Proposition 4]), but this does not necessarily happen in an arbitrary field.

Let $x \mapsto \bar{x}$ be the conjugation in the Clifford algebra $C(-q)$; it is the unique anti-automorphism of $C(-q)$ that restricts to $x \mapsto -x$ on V. As q is a 2-dimensional form, it is known that the map $x \mapsto N(x) = x \cdot \bar{x}$ is multiplicative, maps into the ground field $\mathbb{F}$ and extends q: This is the Clifford norm. Next, we choose $v_1 \in V$ such that $q(v_1) = -1$, leading to $N(v_1) = -1$. We consider the linear isomorphism $u\colon V \xrightarrow{\simeq} C_0(-q)$, $u(x) = v_1 \cdot x$, $\forall x \in V$, which is actually an isometry from (V, q) to $(C_0(-q), N)$. A new SBL $\circ$ is defined on $C_0(-q)$ as follows: $x \circ y = u\left(u^{-1}(x) \star u^{-1}(y)\right)$, $\forall (x, y) \in C_0(-q)^2$. Hence, $(C_0(-q), \circ)$ is isomorphic to (V, F), and its associated quadratic form is N. As $-q$ represents 1, there exists an *orthogonal* basis $\{v_1, v_2\}$ with respect to the symmetric bilinear form attached to q, such that,

$$q(v_1) = -1, \quad q(v_2) = -\beta, \qquad \text{for some } \beta \in \mathbb{F}^*. \tag{3.6}$$

Accordingly, $C(-q) = \langle 1, v_1, v_2, v_1 \cdot v_2 \rangle$ over $\mathbb{F}$, where the dot denotes the Clifford product, and $(v_1 \cdot v_2) \cdot (v_1 \cdot v_2) = -\beta$.

If $x = x_0 + x_1v_1 + x_2v_2 + x_{12}(v_1 \cdot v_2)$, $\bar{x} = x_0 - x_1v_1 - x_2v_2 - x_{12}(v_1 \cdot v_2)$, then, $x \cdot \bar{x} = (x_0)^2 - (x_1)^2 - \beta(x_2)^2 + \beta(x_{12})^2$.

4. Classification of SBLs

Proposition 4.1. *Every SBL on $C_0(-q)$ can be written in the following form:*

$$F_{abc}(x, y) = a \cdot x \cdot y + b \cdot (\bar{x} \cdot y + x \cdot \bar{y}) + c \cdot \overline{x \cdot y}, \qquad \forall x, y \in C_0(-q), \tag{4.7}$$

for some $(a, b, c) \in C_0(-q)^3$.

Proof. We have $C_0(-q) = \{x = x_0 + x_{12}(v_1 \cdot v_2) : x_0, x_{12} \in \mathbb{F}\}$. Hence the elements of degree zero of the Clifford algebra admit the basis $\{1, v_1 \cdot v_2\}$.

The mappings (4.7) are obviously $\mathbb{F}$-bilinear and symmetric, since the Clifford product is $\mathbb{F}$-bilinear and the conjugation $x \mapsto \bar{x}$ is an $\mathbb{F}$-linear anti-automorphism. Letting $a = a_0 + a_{12}(v_1 \cdot v_2)$, $b = b_0 + b_{12}(v_1 \cdot v_2)$, $c = c_0 + c_{12}(v_1 \cdot v_2)$, it follows that the mappings F_{abc} depend on the 6 parameters a_0, a_{12}, b_0, b_{12}, c_0, c_{12}. As $\dim(S^2V^* \otimes V) = 6$, we can conclude. □

The equations of the isomorphism $u\colon V \xrightarrow{\simeq} C_0(-q)$, $u(x) = v_1 \cdot x$, where $x = x_1v_1 + x_2v_2 \in V$ (introduced in the section 3) and those of its inverse are the following:

$$u(x) = x_1 + x_2(v_1 \cdot v_2), \quad u^{-1}\left(x_0 + x_{12}(v_1 \cdot v_2)\right) = x_0v_1 + x_{12}v_2.$$

In what follows, we shall identify the mappings F_{abc} and $F = u^{-1} \circ F_{abc} \circ (u, u)$. As a computation shows, we have the following formulas:

$$\begin{aligned}
\begin{pmatrix} a_1 & b_1 \\ b_1 & c_1 \end{pmatrix} &= \begin{pmatrix} a_0 + 2b_0 + c_0 & -\beta\left(a_{12} - c_{12}\right) \\ -\beta\left(a_{12} - c_{12}\right) & -\beta\left(a_0 - 2b_0 + c_0\right) \end{pmatrix}, \\
\begin{pmatrix} a_2 & b_2 \\ b_2 & c_2 \end{pmatrix} &= \begin{pmatrix} a_{12} + 2b_{12} + c_{12} & a_0 - c_0 \\ a_0 - c_0 & -\beta\left(a_{12} - 2b_{12} + c_{12}\right) \end{pmatrix}.
\end{aligned} \tag{4.8}$$

Theorem 4.1. *The SBLs on* $C_0(-q)$ *with attached quadratic form* N *are the maps of the form* $F_{a,c}(x, y) = a \cdot x \cdot y + c \cdot \overline{x \cdot y}$, *for some* $(a, c) \in C_0(-q) \times C_0(-q)$ *with* $N(c) - N(a) = 1$.

If $G = \{\lambda \in C_0(-q) : N(\lambda) = 1\}$, *then two mappings* F_{ac} *and* $F_{a'c'}$ *are isomorphic if and only if there exists* $\lambda \in G$ *such that* $(a', c') = (\lambda^{-1}a, \lambda^3 c)$ *or* $(a', c') = (\lambda^{-1}\bar{a}, \lambda^3\bar{c})$.

Proof. According to (4.8) we have

$$\begin{aligned}
&a_1 = a_0 + 2b_0 + c_0, && b_1 = -\beta\left(a_{12} - c_{12}\right), && c_1 = -\beta\left(a_0 - 2b_0 + c_0\right), \\
&a_2 = a_{12} + 2b_{12} + c_{12}, && b_2 = a_0 - c_0, && c_2 = -\beta\left(a_{12} - 2b_{12} + c_{12}\right).
\end{aligned}$$

By replacing these formulas into (2.5), it follows:

$$\begin{aligned}
eq_1 \equiv\ & a_1b_2 - a_2b_1 \\
=\ & (a_0)^2 + \beta(a_{12})^2 + 2a_0b_0 + 2\beta a_{12}b_{12} - 2b_0c_0 - 2\beta b_{12}c_{12} \\
& -(c_0)^2 - \beta(c_{12})^2, \\
eq_2 \equiv\ & \tfrac{1}{2}(a_1c_2 - a_2c_1) \\
=\ & 2\beta a_0b_{12} - 2\beta a_{12}b_0 + 2\beta b_{12}c_0 - 2\beta b_0c_{12}, \\
eq_3 \equiv\ & b_1c_2 - b_2c_1 \\
=\ & \beta(a_0)^2 + \beta^2(a_{12})^2 - 2\beta a_0b_0 - 2\beta^2 a_{12}b_{12} + 2\beta^2 b_{12}c_{12} + 2\beta b_0c_0 \\
& -\beta(c_0)^2 - \beta^2(c_{12})^2.
\end{aligned}$$

Hence

$$eq_1 = -1, \quad eq_2 = 0, \quad eq_3 = -\beta. \tag{4.9}$$

Dividing $eq_2 = 0$ by 2β and $eq_3 = -\beta$ by β we obtain

$$\begin{aligned}
(a_0)^2 + \beta(a_{12})^2 + 2a_0b_0 + 2\beta a_{12}b_{12} - 2b_0c_0 - 2\beta b_{12}c_{12} - (c_0)^2 - \beta(c_{12})^2 &= -1, \\
a_0b_{12} - a_{12}b_0 + b_{12}c_0 - b_0c_{12} &= 0, \\
(a_0)^2 + \beta(a_{12})^2 - 2a_0b_0 - 2\beta a_{12}b_{12} + 2\beta b_{12}c_{12} + 2b_0c_0 - (c_0)^2 - \beta(c_{12})^2 &= -1.
\end{aligned}$$

By adding and subtracting the first and third equations above and dividing the result by 2,

$$a_0^2 + \beta a_{12}^2 - c_0^2 - \beta c_{12}^2 + 1 = 0,$$
$$a_0 b_0 - b_0 c_0 + \beta a_{12} b_{12} - \beta b_{12} c_{12} = 0.$$

Accordingly, the system (4.9) is equivalent to

$$\begin{aligned} e_1 \equiv &\quad (a_0)^2 + \beta (a_{12})^2 - (c_0)^2 - \beta (c_{12})^2 + 1 = 0, \\ e_2 \equiv &\quad a_0 b_{12} - a_{12} b_0 + b_{12} c_0 - b_0 c_{12} = 0, \\ e_3 \equiv &\quad a_0 b_0 - b_0 c_0 + \beta a_{12} b_{12} - \beta b_{12} c_{12} = 0, \end{aligned}$$

which we use in what follows, because it is easier than the first one. The equation e_1 can equivalently be written as

$$N(c) - N(a) = 1. \tag{4.10}$$

Furthermore, the equations $e_2 = e_3 = 0$ are linear in b_0 and b_{12} and they can be written in matrix notation as

$$\begin{pmatrix} -a_{12} - c_{12} & a_0 + c_0 \\ a_0 - c_0 & \beta(a_{12} - c_{12}) \end{pmatrix} \begin{pmatrix} b_0 \\ b_{12} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{4.11}$$

The determinant of the matrix of the system (4.11) is equal to

$$e_4 \equiv (c_0)^2 + \beta (c_{12})^2 - (a_0)^2 - \beta (a_{12})^2 = N(c) - N(a) = 1,$$

by virtue of (4.10); hence e_4 cannot vanish. Therefore, $b_0 = b_{12} = 0$.

Finally, let us determine the conditions under which $F_{a,c}$ and $F_{a',c'}$ are isomorphic. As is known, any isomorphism between them must be an isometry of $(C_0(-q), N)$, and these isometries are the group $\mathcal{G}$ of the maps that have one of the following forms:

$$\left.\begin{array}{ll} \text{(i)} & x \mapsto \lambda x, \\ \text{(ii)} & x \mapsto \lambda \bar{x}, \end{array}\right\} \quad \forall x \in C_0(-q), \forall\, \lambda \in G. \tag{4.12}$$

Letting $x' = \lambda x$, $y' = \lambda y$, $z' = \lambda z$ into the equation

$$z' = F_{a'c'}(x', y') = a' x' y' + c' \bar{x}' \bar{y}', \tag{4.13}$$

we obtain $\lambda z = a'(\lambda x)(\lambda y) + c'(\bar{\lambda}\bar{x})(\bar{\lambda}\bar{y})$; hence $z = \lambda a' xy + \bar{\lambda}^3 c' \bar{x}\bar{y}$, as $\lambda^{-1} = \bar{\lambda}$ (because $N(\lambda) = \lambda\bar{\lambda} = 1$) and comparing it with the original equation, i.e., $z = F_{ac}(x, y) = axy + c\bar{x}\bar{y}$, we deduce $a' = \lambda^{-1} a$, $c' = \lambda^3 c$. Similarly, letting $x' = \lambda\bar{x}$, $y' = \lambda\bar{y}$, $z' = \lambda\bar{z}$ into (4.13), we obtain $\lambda\bar{z} = a'(\lambda\bar{x})(\lambda\bar{y}) + c'(\bar{\lambda}x)(\bar{\lambda}y)$; hence $\bar{z} = \lambda a' \bar{x}\bar{y} + \bar{\lambda}^3 c' xy$ and conjugating, $z = \bar{\lambda}\bar{a}' xy + \lambda^3 \bar{c}' \bar{x}\bar{y}$. Therefore it follows: $a = \bar{\lambda}\bar{a}'$, $c = \lambda^3 \bar{c}'$, or equivalently, $a' = \lambda^{-1}\bar{a}$, $c' = \lambda^3 \bar{c}$, thus concluding the proof. □

5. Isotropy

Next, we discuss the index of q. The quadratic form q is said to be *hyperbolic* if q admits an isotropic vector $v_1 \neq 0$. If q does not admit any non-zero isotropic vector, then q is said to be *elliptic*; in this case, as we have seen above, there exists a basis $\{v_1, v_2\}$ for V such that, $q(x) = -(x_1)^2 - \beta(x_2)^2$, where $-\beta \notin \mathbb{F}^{*2}$.

If the discriminant of q is different from $1 \bmod \mathbb{F}^{*2}$, then q is elliptic, and if the discriminant of q is equal to $1 \bmod \mathbb{F}^{*2}$, then q is hyperbolic.

With the same notations as in the section 3, we have $(v_1 \cdot v_2)^2 + \beta = 0$. The $\mathbb{F}$-algebra $C_0(-q)$ being quadratic, we deduce $C_0(-q) \cong \mathbb{F}[t]/(t^2 + \beta)$ (e.g., see [3, Example 98.2]). Hence, in the hyperbolic case, $C_0(-q) \cong \mathbb{F} \times \mathbb{F}$, and in the elliptic case $C_0(-q)$ is a quadratic field extension of the ground field $\mathbb{F}$.

Lemma 5.1. *If q is hyperbolic, then the set of zero divisors in $C_0(-q)$ coincides with the set of elements of norm zero.*

Proof. If $N(x) = x \cdot \bar{x} = 0$, then x is a zero divisor obviously. Conversely, if $x, y \in C_0(-q)$ are such that $x \neq 0$, $y \neq 0$, and $x \cdot y = 0$, then we obtain the following homogeneous linear system:

$$\begin{pmatrix} x_0 & -\beta x_{12} \\ x_{12} & x_0 \end{pmatrix} \begin{pmatrix} y_0 \\ y_{12} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{5.14}$$

Since

$$\det \begin{pmatrix} x_0 & -\beta x_{12} \\ x_{12} & x_0 \end{pmatrix} = N(x), \quad y \neq 0,$$

we can conclude the statement. □

Below we compute the isotropy subgroup $\mathcal{G}(F_{ac}) \subset \mathcal{G}$ of the mapping F_{ac} in Theorem 4.1.

We denote by $\phi_\lambda(x) = \lambda x$, $\psi_\lambda(x) = \lambda \bar{x}$, $\lambda \in G$, $x \in C_0(-q)$, the transformations (i) and (ii) respectively in the formula (4.12). As a computation shows, we obtain

$$\phi_\lambda \circ \phi_\mu = \phi_{\lambda\mu}, \quad \phi_\lambda \circ \psi_\mu = \psi_{\lambda\mu}, \quad \psi_\lambda \circ \psi_\mu = \phi_{\lambda\bar{\mu}}, \quad \forall \lambda, \mu \in G.$$

In particular $\psi_\lambda \circ \psi_\lambda = \phi_{\lambda\bar{\lambda}} = \mathrm{id}$, $\forall \lambda \in G$; i.e., every transformation in (ii) is involutive.

Proposition 5.2. *With the previous notations, we have*

If $N(a) \neq 0$ and $ca^3 \notin \mathbb{F}$, then $\mathcal{G}(F_{ac}) = \{\mathrm{id}\}$.

If $N(a) \neq 0$ and $ca^3 \in \mathbb{F}$, then $\mathcal{G}(F_{ac}) = \left\{\mathrm{id}, \psi_{\frac{\bar{a}}{a}}\right\}$.

If $N(a) = 0$, then $\mathcal{G}(F_{ac}) = \left\{\phi_\lambda, \psi_\mu : \lambda^3 = 1, \mu^3 = c^2\right\}$.

Proof. If one of the transformations (i) or (ii) in the formula (4.12) belongs to $\mathcal{G}(F_{ac})$, then either (i) $\lambda a = a$, $c = \lambda^3 c$, or (ii) $\lambda a = \bar{a}$, $c = \lambda^3 \bar{c}$. We distinguish several cases.

Assume the item (i) holds.

(1) If q is elliptic, then $a \neq 0$ implies $\lambda = 1$, as $C_0(-q)$ is a field, and $a = 0$ implies $\lambda^3 = 1$, because in this case c is invertible, as follows from (4.10).

(2) If q is hyperbolic, i.e., $\beta = -\gamma^2$, $\gamma \in \mathbb{F}^*$, then by applying Lemma 5.1 to the equation $(\lambda - 1)a = 0$ it follows that either $\lambda = 1$ or $N(a) = 0$. In the second case c is invertible in $C_0(-q)$ by virtue of (4.10); hence $\lambda^3 = 1$. If $N(a) \neq 0$, then the equation $(\lambda - 1)a = 0$ implies $\lambda = 1$.

If q is elliptic, then $N(a) = 0$ if and only if $a = 0$. Therefore, we can group the two previous items saying that the transformations of type (i) in (4.10) that belong to $\mathcal{G}(F_{ac})$ are as follows: If $N(a) \neq 0$, then such transformations reduce to the identity map, and if $N(a) = 0$, then they correspond to the values $\lambda \in G$ such that $\lambda^3 = 1$.

Assume the item (ii) holds.

From $\lambda a = \bar{a}$ it follows $\lambda a^2 = N(a)$.

If $N(a) = 0$, then $a = 0$, as λ is invertible and $C_0(-q)$ has no nilpotent element. In this case $N(c) = 1$ and from $c = \lambda^3 \bar{c}$ it follows $\lambda^3 = c^2$.

- If q is elliptic, the equation $\lambda^3 = c^2$ may admit none (if c^2 is not a cube in $C_0(-q)$), one (if c^2 is a cube in $C_0(-q)$ and -3 is not a square in $C_0(-q)$) or three solutions in $C_0(-q)$ (if c^2 is a cube in $C_0(-q)$ and -3 is a square in $C_0(-q)$).
- If q is hyperbolic, then by considering the isomorphism

$$\begin{aligned} &\phi\colon \mathbb{F}[t]/(t^2 - \gamma^2) \to \mathbb{F} \times \mathbb{F}, \\ &\phi(u + v\tau) = (u - v\gamma, u + v\gamma), \\ &u, v \in \mathbb{F},\ \tau = t \bmod (t^2 - \gamma^2), \end{aligned} \tag{5.15}$$

and by writing $\phi(w) = (w_1, w_2)$, it follows that the equation $\lambda^3 = c^2$ is equivalent to the pair of equations $(\lambda_1)^3 = (c_1)^2$, $(\lambda_2)^3 = (c_2)^2$ in $\mathbb{F}$. As $N(c) = N(\lambda) = 1$, we have $\lambda_1\lambda_2 = c_1c_2 = 1$, and the equation $(\lambda_2)^3 = (c_2)^2$ is equivalent to $(\lambda_1)^3 = (c_1)^2$. Hence even in the hyperbolic case the number of solutions to $\lambda^3 = c^2$ may be 0, 1 or 3.

If $N(a) \neq 0$, then $\lambda = \frac{\bar{a}}{a}$ and replacing this value into the second equation in (ii) we obtain $a^3c = \overline{a^3c}$, or equivalently $a^3c \in \mathbb{F}$.

In summary, the transformations of type (ii) in (4.10) that belong to $\mathcal{G}(F_{ac})$ are as follows:

- If $N(a) = 0$, then such transformations correspond to the values $\lambda \in G$ such that $\lambda^3 = c^2$, whether q is elliptic or hyperbolic.
- If $N(a) \neq 0$, then such transformations do not exist, except when $ca^3 \in \mathbb{F}$, in which case the only transformation of type (ii) in $\mathcal{G}(F_{ac})$ corresponds to $\lambda = \frac{\bar{a}}{a}$.

Accordingly, we have

$$\text{(i)} \begin{cases} N(a) \neq 0, & \{\mathrm{id}\} \\ N(a) = 0, & \{\lambda \in G : \lambda^3 = 1\} \end{cases} \qquad \text{(ii)} \begin{cases} N(a) \neq 0 \begin{cases} \emptyset, & \text{if } ca^3 \notin \mathbb{F} \\ \lambda = \dfrac{\bar{a}}{a}, & \text{if } ca^3 \in \mathbb{F} \end{cases} \\ N(a) = 0, & \{\lambda \in G : \lambda^3 = c^2\} \end{cases}$$

Putting together transformations of type (i) and type (ii), the statement follows. □

6. The role of the invariants

Let $\sigma\colon V^* \to S^2V^* \otimes V$ be the map defined by,

$$\sigma(v^*)(x,y) = \tfrac{1}{3}\left(v^*(x)y + v^*(y)x\right), \quad x, y \in V,\ v^* \in V^*. \tag{6.16}$$

By using formula (2.1), the homomorphism σ is proved to be a $GL(V)$-equivariant section of tr. If $v^* = \lambda_1 v_1^* + \lambda_2 v_2^*$, then from (6.16) it follows:

$$\begin{aligned} \sigma(v^*)(v_1, v_1) &= \tfrac{2}{3}\lambda_1 v_1, \\ \sigma(v^*)(v_2, v_2) &= \tfrac{2}{3}\lambda_2 v_2, \\ \sigma(v^*)(v_1, v_2) &= \tfrac{1}{3}(\lambda_1 v_2 + \lambda_2 v_1). \end{aligned} \tag{6.17}$$

Therefore, there is a decomposition of $GL(V)$-modules $S^2V^* \otimes V = W \oplus \sigma(V^*)$, where $W = \{F \in S^2V^* \otimes V : \mathrm{tr}F = 0\}$.

For every $F \in S^2V^* \otimes V$ we set $\bar{F} = F - \sigma(\mathrm{tr}F)$. Then, F is said to be *regular* if the quadratic form $Q_{\bar{F}}$ is non-degenerate.

A simple computation proves that F is regular if and only if the following condition holds:

$$\begin{aligned} \det Q_{\bar{F}} = {} & \tfrac{4}{27}a_1b_1b_2c_2 - \tfrac{1}{3}a_1a_2b_1c_1 + \tfrac{2}{3}a_2b_1b_2c_1 + \tfrac{1}{6}a_1a_2c_1c_2 \\ & - \tfrac{1}{3}a_2b_2c_1c_2 - \tfrac{1}{27}(a_1)^3c_1 + \tfrac{1}{27}(a_1)^2(b_1)^2 + \tfrac{1}{108}(a_1)^2(c_2)^2 \\ & + \tfrac{8}{27}(b_2)^3c_1 + \tfrac{4}{27}(b_1)^2(b_2)^2 + \tfrac{1}{27}(b_2)^2(c_2)^2 + \tfrac{8}{27}a_2(b_1)^3 \\ & - \tfrac{1}{27}a_2(c_2)^3 - \tfrac{4}{27}b_1(b_2)^2c_2 - \tfrac{1}{27}(a_1)^2b_1c_2 - \tfrac{4}{9}a(b_2)^2c_1 \\ & + \tfrac{2}{9}(a_1)^2b_2c_1 + \tfrac{2}{9}a_2b_1(c_2)^2 - \tfrac{4}{9}a_2(b_1)^2c_2 - \tfrac{1}{27}a_1b_2(c_2)^2 \\ & - \tfrac{4}{27}a_1(b_1)^2b_2 - \tfrac{1}{4}(a_2)^2(c_1)^2 \\ & \neq 0. \end{aligned} \tag{6.18}$$

From the very definition it follows that the set of regular bilinear symmetric maps is an open subset $R \subset S^2V^* \otimes V$ in the Zariski topology; precisely, the set where the quartic form (6.18) does not vanish.

If the ground field $\mathbb{F}$ is algebraically closed, then in [2, Theorem 4–2] it is proved that two regular elements $F, G \in R \subset S^2V^* \otimes V$ are $GL(V)$-equivalent, if and only if $\mathcal{I}_i(F) = \mathcal{I}_i(G)$, $i = 1, 2$, where $\mathcal{I}_1, \mathcal{I}_2 \colon R \to \mathbb{F}$ are the $GL(V)$-invariant functions defined in [2, Theorem 4–1] and computed in [2, pp. 11–12]), namely,

$$\begin{aligned}\mathcal{I}_1(F) = \ & \tfrac{1}{12 \det Q_{\bar{F}}} \big[(a_1+b_2)^2\big((2b_1-c_2)^2+3(2b_2-a_1)c_1\big) \\ & +(a_1+b_2)(b_1+c_2)((2b_2-a_1)(2b_1-c_2)-9a_2c_1) \\ & +(b_1+c_2)^2((2b_2-a_1)^2+3(2b_1-c_2)a_2)\big],\end{aligned}$$

$$\begin{aligned}\mathcal{I}_2(F) = \ & \tfrac{1}{4 \det Q_{\bar{F}}} \big[-c_1(a_1+b_2)^3+(a_1+b_2)^2(b_1+c_2)(2b_1-c_2) \\ & +(a_1+b_2)(b_1+c_2)^2(2b_2-a_1)-a_2(b_1+c_2)^3\big],\end{aligned}$$

where $\det Q_{\bar{F}}$ is as in (6.18). Next, we discuss the role of these invariants in the classification problem.

The isomorphism $u \colon V \to C_0(-q)$, $u(x) = v_1 \cdot x$, $\forall x \in V$, defined in the section 3, induces an isomorphism

$$S^2(u^{*-1}) \otimes u \colon S^2(V^*) \otimes V \to S^2(C_0(-q)^*) \otimes C_0(-q)$$

which allows one to transport the invariants $\mathcal{I}_1$ and $\mathcal{I}_2$ into a Zariski open subset R' in $S^2(C_0(-q)^*) \otimes C_0(-q)$. Moreover, by applying Theorem 4.1, we can confine ourselves to compute these new invariants $\mathcal{J}_1$ and $\mathcal{J}_2$ only on the maps F_{ac} fulfilling the equation (4.10). This is accomplished by using the formulas (4.8) for $b_0 = b_{12} = 0$, thus obtaining the following expressions:

$$\begin{aligned}&[1] \quad \mathcal{J}_1(F_{ac}) = \ 27\tfrac{K(a,c)+2N(a)^2+3N(a)}{4K(a,c)+8N(a)^2+36N(a)+27}, \\ &[2] \quad \mathcal{J}_2(F_{ac}) = \ 27\tfrac{K(a,c)+2N(a)^2}{4K(a,c)+8N(a)^2+36N(a)+27}, \\ &\qquad K(a,c) = \ a^3c+\bar{a}^3\bar{c},\end{aligned} \tag{6.19}$$

Proposition 6.3. *Let F_{ac}, $F_{a'c'}$ be two symmetric bilinear maps in Zariski open subset R' defined above.*

If the pairs (a, c) and (a', c') are related by one of the two formulas in the second part of Theorem 4.1, *then $\mathcal{J}_i(F_{ac}) = \mathcal{J}_i(F_{a'c'})$, $i = 1, 2$. Therefore, the functions $\mathcal{J}_1$ and $\mathcal{J}_2$ are invariant under the action of the group of transformations $\mathcal{G}$ given in* (4.12).

Moreover, the equations $\mathcal{J}_i(F_{ac}) = \mathcal{J}_i(F_{a'c'})$, $i = 1, 2$, hold if and only if the following two conditions are fulfilled:

$$\text{(i)} \quad N(a') = N(a), \qquad \text{(ii)} \quad K(a', c') = K(a, c). \tag{6.20}$$

In addition, we have the following mutually excluding cases:

1. *If $a = 0$ and* (i) *and* (ii) *in* (6.20) *hold, then $a' = 0$, and the symmetric bilinear maps F_{ac} and $F_{a'c'}$ are $\mathcal{G}$-equivalent if and only if $\frac{c'}{c}$ or $\frac{c'}{\bar{c}}$ is a cube in $C_0(-q)$.*
2. *If $c = 0$, and* (i) *and* (ii) *in* (6.20) *hold, then $c' = 0$, and the symmetric bilinear maps F_{ac} and $F_{a'c'}$ are equivalent under the subgroup $\mathcal{G}^0 \subset \mathcal{G}$ of the transformations of type* (i) *in* (4.12).
3. *If $a \neq 0$ and $c \neq 0$, then the formulas* (i) *and* (ii) *in* (6.20) *hold if and only if the symmetric bilinear maps F_{ac} and $F_{a'c'}$ are $\mathcal{G}$-equivalent.*

Proof. If $a' = \lambda^{-1}a, c' = \lambda^3 c$ or $a' = \lambda^{-1}\bar{a}, c' = \lambda^3\bar{c}$, then taking account of the fact that $\lambda^{-1} = \bar{\lambda}$ as $\lambda \in G$, a straightforward computation shows that $\mathcal{J}_i(F_{ac}) = \mathcal{J}_i(F_{a'c'})$, $i = 1, 2$.

Moreover, solving the equations [1] and [2] in (6.19) with respect to $K(a,c)$ and $N(a)$ it follows

$$\begin{aligned} K(a,c) = &\quad -27\tfrac{6\mathcal{J}_1(F_{ac})^2-2\mathcal{J}_2(F_{ac})^2-27\mathcal{J}_2(F_{ac})}{[12\mathcal{J}_1(F_{ac})-8\mathcal{J}_2(F_{ac})-27]^2}, \\ N(a) = &\quad 9\tfrac{\mathcal{J}_2(F_{ac})-\mathcal{J}_1(F_{ac})}{12\mathcal{J}_1(F_{ac})-8\mathcal{J}_2(F_{ac})-27}. \end{aligned}$$

Hence the equations $\mathcal{J}_i(F_{ac}) = \mathcal{J}_i(F_{a'c'})$, $i = 1,2$, imply $K(a,c) = K(a',c')$ and $N(a) = N(a')$.

(1) From (6.20)-(i) it follows $N(a') = 0$, and by virtue of (4.10), we conclude that $N(c) = N(c') = 1$.

If q is elliptic, this implies $a' = 0$, and c and c' are invertible in $C_0(-q)$. If F_{ac} and $F_{a'c'}$ are $\mathcal{G}$-equivalent, then $\frac{c'}{c}$ or $\frac{c'}{\bar{c}}$ belong to the group G defined in Theorem 4.1; the converse is obvious.

If q is hyperbolic, we can apply the isomorphism (5.15); by using the notations introduced therein, the formulas (i) and (ii) in (6.20) transform respectively into: (i') $a'_1a'_2 = 0$, (ii') $(a'_1)^3c'_1 + (a'_2)^3c'_2 = 0$, and $N(c') = 1$ means (iii') $c'_1c'_2 = 1$. If $a'_1 = a'_2 = 0$, (i.e., $a' = 0$), then (ii') holds identically and we can conclude as in the previous case. If, for example, we had $a'_1 \neq 0$, $a'_2 = 0$, then (ii') implies $(a'_1)^3c'_1 = 0$, and since $c'_1 \in \mathbb{F}^*$ it follows $a'_1 = 0$, thus leading us to a contradiction.

(2) From (4.10) and (6.20)-(i) it follows $N(a) = N(a') = -1$, $N(c) = N(c') = 0$.

If q is elliptic, this implies $c = c' = 0$, and a, a' are invertible in $C_0(-q)$ and $\lambda = \frac{a}{a'}$ belongs to G.

If q is hyperbolic, then by using the isomorphism (5.15), the equation (ii) in (6.20) transforms into (ii') $(a'_1)^3c'_1+(a'_2)^3c'_2 = 0$, and furthermore we have $a_1a_2 = a'_1a'_2 = -1$, $c'_1c'_2 = 0$. If $c'_1 = 0$, then (ii') becomes $(a'_2)^3c'_2 = 0$, and since a'_2 is invertible we deduce that $c'_2 = 0$; similarly, $c'_2 = 0$ implies $c'_1 = 0$. Hence $c' = 0$, in which case we have $\lambda = \frac{a}{a'} \in G$.

(3) If q is elliptic, then $C_0(-q)$ is a field and by virtue of the assumption it follows that the elements a, c, $\bar{a}$, $\bar{c}$, a', c', $\bar{a}'$, and $\bar{c}'$ are invertible. Letting $a' = \frac{a\bar{a}}{\bar{a}'}$, $c' = \frac{c\bar{c}}{\bar{c}'}$ into (6.20)-(ii) we obtain $0 = (\bar{a}^3\bar{c} - \bar{a}'^3\bar{c}')(a^3c - \bar{a}'^3\bar{c}')$. Hence either $a^3c = (a')^3c'$ or $a^3c = (\bar{a}')^3\bar{c}'$. In the first case, letting $\lambda = aa'^{-1}$, it follows: $a' = \lambda^{-1}a$, $c' = \lambda^3c$, and in the second case, letting $\lambda = \bar{a}a'^{-1}$, it follows: $a' = \lambda^{-1}\bar{a}$, $c' = \lambda^3\bar{c}$. As $N(a) = N(a')$, we deduce that $N(\lambda) = 1$, or equivalently $\lambda \in G$.

Therefore, by applying Theorem 4.1 we conclude that the maps F_{ac} and $F_{a'c'}$ are isomorphic.

If q is hyperbolic, then we use the isomorphism (5.15), and the equations (6.20)-(i)-(ii) transform respectively into the following:

$$\text{(i')}\quad a_1a_2 = a'_1a'_2, \qquad \text{(ii')}\quad (a'_1)^3c'_1 + (a'_2)^3c'_2 = (a_1)^3c_1 + (a_2)^3c_2,$$

and from (4.10) we also deduce (iii') $c_1c_2 = c'_1c'_2$. The equations (6.20)-(i)-(ii) being invariant under conjugation, by virtue of the hypothesis we can assume $a_1 \neq 0$, and we distinguish two cases according to whether $c_1 \neq 0$ or $c_1 = 0$ and $c_2 \neq 0$.

(1) If $c_1 \neq 0$, then by replacing $a_2 = \frac{a'_1a'_2}{a_1}$ and $c_2 = \frac{c'_1c'_2}{c_1}$ into (ii') we obtain

$$0 = \left[(a_1)^3c_1 - (a'_1)^3c'_1\right]\left[(a_1)^3c_1 - (a'_2)^3c'_2\right].$$

- If $(a_1)^3c_1 = (a'_1)^3c'_1$, then $a'_1 \neq 0$ and $c'_1 \neq 0$, and letting $\lambda = (\lambda_1, \lambda_2)$, with $\lambda_1 = \frac{a_1}{a'_1}$, $\lambda_2 = \frac{1}{\lambda_1}$, we have $a' = \lambda^{-1}a$, $c' = \lambda^3c$, $\lambda \in G$.
- If $(a_1)^3c_1 = (a'_2)^3c'_2$, then $a'_2 \neq 0$ and $c'_2 \neq 0$. Letting $\lambda_1 = \frac{a'_2}{a_1}$, $\lambda_2 = \frac{1}{\lambda_1}$, we have $a' = \lambda^{-1}\bar{a}$, $c' = \lambda^3\bar{c}$, $\lambda \in G$.

(2) If $c_1 = 0$, $c_2 \neq 0$, then $N(c) = 0$ and $a_1 a_2 = a'_1 a'_2 = -1$ because of (4.10), and letting $a_2 = \frac{-1}{a_1}$, $a'_2 = \frac{-1}{a'_1}$ in (ii') we have

$$0 = (a_1)^3 c'_2 - (a_1)^3 (a'_1)^6 c'_1 - (a'_1)^3 c_2. \tag{6.21}$$

As $N(c') = 0$, either $c'_1 = 0$ or $c'_2 = 0$. In the first case, the equation (6.21) transforms into (ii'-a) $(a_1)^3 c'_2 = (a'_1)^3 c_2$, whereas in the second it transforms into (ii'-b) $c_2 = -(a_1)^3 (a'_1)^3 c'_1$.

- If (ii'-a) holds, then $a' = \lambda^{-1} a$, $c' = \lambda^3 c$, with $\lambda = (\lambda_1, \lambda_2)$, $\lambda_1 = \frac{a_1}{a'_1}$, $\lambda_2 = \frac{1}{\lambda_1}$.
- If (ii'-b) holds, then $a' = \lambda^{-1} \bar{a}$, $c' = \lambda^3 \bar{c}$, with $\lambda = (\lambda_1, \lambda_2)$, $\lambda_1 = \frac{a_2}{a'_1}$, $\lambda_2 = \frac{1}{\lambda_1}$.

This proves that F_{ac} and $F_{a'c'}$ are $\mathcal{G}$-equivalent in both cases. □

Acknowledgments. This research has been partially supported by Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and European Regional Development Fund of the European Union (ERDF, EU) under project COPCIS, reference TIN2017-84844-C2-1-R, and by Comunidad de Madrid (Spain) under project reference P2018/TCS-4566-CM (CYNAMON) also co-funded by ERDF."

References

[1] Durán Díaz, R., Hernández Encinas, L. and Muñoz Masqué, J., *Fractal sets attached to homogeneous quadratic maps in two variables*, Physica D: Nonlinear Phenomena, **245** (2013), 8–18 (DOI: 10.1016/j.physd.2012.11.002)

[2] Durán Díaz, R., Muñoz Masqué, J. and Peinado Domínguez, A., *Classifying quadratic maps from plane to plane*, Linear Algebra Appl., **364** (2003), 1–12 (DOI: 10.1016/S0024-3795(02)00564-5)

[3] Elman, R., Karpenko, N. and Merkurjev, A., *The algebraic and geometric theory of quadratic forms*, Providence, RI, USA: American Mathematical Society Colloquium Publications, **56**, 2008

[4] Lang, S., *Algebra*, 3rd edition, Reading, MA, USA: Addison-Wesley Publishing Company, Inc., 1993

[5] Serre, J.-P., *Cours d'arithmétique*, Collection SUP: "Le Mathématicien", 2, Paris: Presses Universitaires de France, 1970

[1]Escuela Politécnica Superior
Universidad de Alcalá
E-28871 Alcalá de Henares, Spain
Email address: raul.duran@uah.es

[2]Instituto de Tecnologías Físicas y de la Información
Consejo Superior de Investigaciones Científicas
C/ Serrano 144, E-28006 Madrid, Spain
Email address: {luis, jaime}@iec.csic.es