The Number of Nonisomorphic Two-dimensional Algebras over a Finite Field

Holger P. Petersson
Fachbereich Mathematik
FernUniversität in Hagen
D-58084 Hagen
Germany
email: Holger.Petersson@FernUni-Hagen.de

and

Matthias Scherer
Rietstraße 144
CH-8200 Schaffhausen
Switzerland

0. Introduction

Our principal objective in the present paper, which grew out of the second author's Diplomarbeit [6] at the Fachbereich Mathematik der FernUniversität in Hagen, is to establish the following result.

Main Theorem. *Let p be a prime and n a positive integer. Then the number of isomorphism classes of two-dimensional nonassociative algebras, possibly without a unit, over the field $\mathbb{F}_q$ with $q = p^n$ elements is*

$$\begin{aligned} &q^4 + q^3 + 4q^2 + 3q + 6 && (\textit{for } p = 2),\\ &q^4 + q^3 + 4q^2 + 4q + 6 && (\textit{for } p = 3),\\ &q^4 + q^3 + 4q^2 + 4q + 7 && (\textit{for } p \neq 2, 3). \end{aligned}$$

Among these classes, precisely

$$\begin{aligned} &\frac{1}{2}q^4 - q^3 + q^2 && (\textit{for } p = 2,\ n \equiv 0 \mod 2),\\ &\frac{1}{2}q^4 - q^3 + q^2 + 1 && (\textit{for } p = 2,\ n \not\equiv 0 \mod 2),\\ &\frac{1}{2}q^4 - q^3 + q^2 - q + \frac{1}{2} && (\textit{for } p \neq 2,\ q \not\equiv -1 \mod 3),\\ &\frac{1}{2}q^4 - q^3 + q^2 - q + \frac{3}{2} && (\textit{for } p \neq 2,\ q \equiv -1 \mod 3) \end{aligned}$$

are represented by division algebras.

The proof combines the first author's general classification theory [3] for two-dimensional nonassociative algebras over arbitrary base fields with elementary counting arguments over $\mathbb{F}_q$. Most of these counting arguments are addressed to the following situation: Given a finite set X (e.g., the projective linear group of degree 2 over $\mathbb{F}_q$) and a right action of $\Gamma = \mathbb{Z}/2\mathbb{Z}$ on X, the problem is to determine the cardinality of the orbit space X/Γ. To solve this problem in the special cases at hand, refined versions for some of the classification theorems established in [3] are required which seem to be of independent interest and are derived here in a purely algebraic setting. The aforementioned counting arguments can then be carried out without difficulty and immediately lead to a proof of the main theorem.

1. Two-dimensional algebras over arbitrary fields: A Survey.

1.0 All results presented in this section are either standard or taken from [3]. For proofs, the reader is referred to [3] or the sources quoted therein. We fix an arbitrary base field k. The totality of invertible elements in a structure S will invariably be written as $S^\times$, whenever this makes sense.

1.1 Unital algebras of dimension two. Let K be a two-dimensional k-algebra containing a unit. Then precisely one of the following holds.

a) K is étale, so K/k is either a separable quadratic field extension or $K \cong k \times k$ splits.

b) $K = k[\varepsilon]$, $\varepsilon^2 = 0$, is the algebra of dual numbers.

c) char $k = 2$ and K/k is an inseparable field extension.

In any event, K is *quadratic*, so there is a unique pair (t, n) consisting of a linear form $t : K \to k$, the *trace*, and a quadratic form $n : K \to k$, the *norm*, satisfying $x^2 - t(x)x + n(x)1 = 0$ for all $x \in K$. We also have the *conjugation*

$$\tau : K \longrightarrow K,\ x \longmapsto \overline{x} = \tau(x) = t(x)1 - x,$$

which is a k-automorphism of period two.

1.2 Regular algebras and the unital heart. Let A be a two-dimensional k-algebra. Given linear maps $f, g : A \to A$, the product $(x, y) \mapsto f(x)g(y)$ defines a new k-algebra which we denote by $A^{(f,g)}$. The left, right multiplication of A will be written as L_A, R_A, respectively, or simply as L, R if there is no danger of confusion. A is said to be *left* (resp. *right*) *regular* if there exists an element $u \in A$ making $L_A(u)$ (resp. $R_A(u)$) bijective. Algebras that are both left and right regular are called *regular.* A is regular if and only if there exist a unital k-algebra K of dimension 2 and linear maps $f, g : K \to K$ satisfying $A \cong K^{(f,g)}$. In this case, K is unique up to ismorphism, called the *unital heart* of A.

1.3 Étale algebras. Fixing a quadratic étale k-algebra K, with trace t, norm n and conjugation τ, we wish to describe the classification of two-dimensional regular k-algebras with unital heart isomorphic to K. To this end, we put

$$S(K) = \{x \in K \mid n(x) = 1\} = \{\overline{v}v^{-1} \mid v \in K^\times\}, \tag{1.3.1}$$

choose once and for all a full set M of representatives containing 1 of $K^\times$ modulo $S(K)$ and fix an idempotent $c \neq 0, 1$ in K if $K \cong k \times k$ happens to be split. We also write V for the vector space over k underlying K. Every k-linear map $f : V \to V$ has a unique representation as

$$f = L(x) + L(y)\tau \qquad (x, y \in V), \tag{1.3.2}$$

and

(1.3.3) $$\det f = n(x) - n(y).$$

1.4 Tight enumeration of regular algebras with étale heart. *Notations being as in* 1.3, *and writing* $\mathbf{1}$ *for the identity transformation of* V, *let* A *be a regular two-dimensional* k*-algebra with unital heart isomorphic to* K. *Then* A *is isomorphic to precisely one of the following.*

a) $K^{(\mathbf{1}+L(y)\tau,g)}$, $y \in M - \{1\}$, $g \in \mathrm{GL}(V)$.

b) $K^{(\mathbf{1},\tau)}$.

c) $K^{(\tau,L(y)\tau)}$, $y \in S(K)$.

d) $K^{(\rho,\mathbf{1}+L(y)\tau)}$, $\rho \in \{\mathbf{1},\tau\}$, $y \in K$, $n(y) \neq 1$.

e) $K^{(\rho,L(c)+L(y)\tau)}$, K *split*, $\rho \in \{\mathbf{1},\tau\}$, $y \in K^\times$, $cy = c$.

f) $K^{(\mathbf{1}+L(c)\tau,g)}$, K *split*, $g \in \mathrm{GL}(V)$.

g) $K^{(L(c)+\tau,g)}$, K *split*, $g \in \mathrm{GL}(V)$.

1.5 Classification of regular algebras with étale heart. *Notations being as in* 1.3, *we have:*

a) *For* $y, z \in M - \{1\}$, $g, h \in \mathrm{GL}(V)$,
$$K^{(\mathbf{1}+L(y)\tau,g)} \cong K^{(\mathbf{1}+L(z)\tau,h)}$$
if and only if $y = z$ *and there exists an element* $a \in k^\times$ *such that* $h = ag$ *or* $h = a\tau g\tau L(y^{-1})$.

c) *For* $y, z \in S(K)$,
$$K^{(\tau,L(y)\tau)} \cong K^{(\tau,L(z)\tau)}$$
if and only if $y \equiv z \mod S(K)^3$ *or* $y \equiv \overline{z} \mod S(K)^3$.

d) *For* $\rho, \sigma \in \{\mathbf{1},\tau\}$, $y, z \in K$ *satisfying* $n(y) \neq 1 \neq n(z)$,
$$K^{(\rho,\mathbf{1}+L(y)\tau)} \cong K^{(\sigma,\mathbf{1}+L(z)\tau)}$$
if and only if $\rho = \sigma$ *and either* $y = z$ *or* $y = \overline{z}$.

e) *Let* K *be split. For* $\rho, \sigma \in \{\mathbf{1},\tau\}$ *and* $y, z \in K^\times$ *satisfying* $cy = c = cz$,
$$K^{(\rho,L(c)+L(y)\tau)} \cong K^{(\sigma,L(c)+L(z)\tau)}$$
if and only if $\rho = \sigma$ *and* $y = z$.

f) *Let* K *be split. For* $g, h \in \mathrm{GL}(V)$,
$$K^{(\mathbf{1}+L(c)\tau,g)} \cong K^{(\mathbf{1}+L(c)\tau,h)}$$
if and only if there exists an element $a \in k^\times$ *such that* $h = ag$.

g) *Let* K *be split. For* $g, h \in \mathrm{GL}(V)$,
$$K^{(L(c)+\tau,g)} \cong K^{(L(c)+\tau,h)}$$
if and only if there exists an element $a \in k^\times$ *such that* $h = ag$.

1.6 Dual numbers. Let $K = k[\varepsilon]$, $\varepsilon^2 = 0$, be the algebra of dual numbers. As before, we write n for the norm, τ for the conjugation of K and V for the underlying vector space over k. The k-linear map $\partial : V \to V$ determined by $\partial(1) = 0, \partial(\varepsilon) = 1$ is a τ-*derivation*, so

$$\partial(xy) = \partial(x)y + \overline{x}\partial(y) \qquad (x, y \in V). \tag{1.6.1}$$

Given $s \in k^\times$, there is a unique k-automorphism σ_s of K sending ε to $s\varepsilon$. We also have

$$\sigma_s \partial \sigma_s^{-1} = s^{-1}\partial. \tag{1.6.2}$$

Observe

$$\sigma_1 = \mathbf{1},\ \sigma_{-1} = \tau. \tag{1.6.3}$$

Every k-linear map $f : V \to V$ has a unique representation as

$$f = L(x) + L(y)\partial \qquad (x, y \in V), \tag{1.6.4}$$

and

$$\det f = n(x) + \Delta(x \wedge y) \tag{1.6.5}$$

where Δ stands for the k-linear isomorphism $\bigwedge^2 V \xrightarrow{\sim} k$ sending $1 \wedge \varepsilon$ to 1.

1.7 Classification of regular algebras with dual heart. *Notations being as in* 1.6, *let A be a regular two-dimensional k-algebra with unital heart isomorphic to K. Then A is isomorphic to precisely one of the following.*

a) K

b) $K^{(\mathbf{1}, L(b\varepsilon)+\partial)}$ *where* $b \in k^\times$ *is unique* mod $k^{\times 2}$.

c) $K^{(\mathbf{1}, L(1+b\varepsilon)+\partial)}$ *where* $b \in k - \{1\}$ *is unique.*

d) $K^{(\mathbf{1}, a\mathbf{1}+L(\varepsilon)\partial)}$ *where* $a \in k - \{0, -1\}$ *is unique.*

e) $K^{(L(b\varepsilon)+\partial, g)}$, $b \in k^\times$, $g \in \mathrm{GL}(V)$. *Furthermore, given* $b, b' \in k^\times$, $g, g' \in \mathrm{GL}(V)$, *we have*

$$K^{(L(b\varepsilon)+\partial, g)} \cong K^{(L(b'\varepsilon)+\partial, g')}$$

if and only if there are elements $s, a \in k^\times$ *satisfying* $b' = bs^2$, $g' = a\sigma_s g \sigma_s^{-1}$.

f) $K^{(a\mathbf{1}+L(\varepsilon)\partial, L(b\varepsilon)+\partial)}$ *where* $a \in k - \{0, 1, -1\}$ *is unique and* $b \in k^\times$ *is unique* mod $k^{\times 2}$.

g) $K^{(a\mathbf{1}+L(\varepsilon)\partial, L(1+b\varepsilon)+\partial)}$ *where* $a \in k - \{0, 1, -1\}$ *and* $b \in k - \{1\}$ *are unique.*

h) $K^{(\mathbf{1}+L(\varepsilon)\partial, L(b\varepsilon)+\partial)}$ *where* char $k \neq 2$ *and* $b \in k^\times$ *is unique* mod $k^{\times 2}$.

i) $K^{(\mathbf{1}+L(\varepsilon)\partial, L(b\varepsilon)+L(1+\varepsilon)\partial)}$ *where* char $k \neq 2$ *and* $b \in k^\times$ *is unique.*

j) $K^{(a\mathbf{1}+L(\varepsilon)\partial, \alpha\mathbf{1}+L(\varepsilon)\partial)}$ *where* $a, \alpha \in k - \{0, -1\}$ *are unique.*

k) $K^{(a\mathbf{1}+L(\varepsilon)\partial, L(\alpha 1+\varepsilon)+L(\varepsilon)\partial)}$ *where* $a \in k - \{0, -1\}$ *is unique and* $\alpha = -\frac{a}{1+a}$.

l) $K^{(a\mathbf{1}+L(\varepsilon)\partial, \mathbf{1})}$ *where* $a \in k - \{0, -1\}$ *is unique.*

1.8 Bisingular algebras. Two-dimensional k-algebras which are neither left nor right regular are called *bisingular.* Up to isomorphism, they are precisely of the form $A(u, \beta)$ where u is a fixed nonzero element in a two-dimensional k-vector space V and $\beta : V \times V \to k$ is a bilinear form, $A(u, \beta)$ living on V by the multiplication $(x, y) \mapsto \beta(x, y)u$. More specifically, writing e_1 for the first unit vector in two-dimensional column space k^2 and identifying bilinear forms of k^2 with elements of $\mathrm{Mat}_2(k)$ (the algebra of 2-by-2 matrices over k) in the usual way, we have:

1.9 Classification of bisingular algebras. *Notations being as in* 1.8, *a k-algebra A is bisingular of dimension two if and only if it is isomorphic to $A(e_1, S)$ where $S \in \mathrm{Mat}_2(k)$ satisfies one of the following mutually exclusive conditions.*

a) $S = 0$.

b) $S = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

c) $S = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

d) $S = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.

e) $S = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$ *where $a \in k$ is unique.*

f) $S = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$ *where $b \in k$ is unique* $\bmod k^{\times 2}$.

g) $S = \begin{pmatrix} 1 & 0 \\ 1 & b \end{pmatrix}$ *where $b \in k$ is unique.*

1.10 Strictly left singular algebras. Two-dimensional k-algebras which are right regular but not regular are called *strictly left singular.* Dito for *strictly right singular.* Fixing a linear form $u^* \neq 0$ on a fixed two-dimensional k-vector space V, the strictly left singular k-algebras of dimension two up to isomorphism are precisely of the form $A(u^*, f)$ for some $f \in \mathrm{GL}(V)$, where $A(u^*, f)$ lives on V by the multiplication $(x, y) \mapsto u^*(y)f(x)$. We always have

$$A(u^*, f) \cong A(u^*, af) \qquad (a \in k^\times). \tag{1.10.1}$$

More specifically, writing $f^* \in \mathrm{GL}(V^*)$ for the dual of f, the following classification theorem holds.

1.11 Classification of strictly left singular algebras. *Notations being as in* 1.10, *let* $f, g \in \mathrm{GL}(V)$. *Then the following statements are equivalent.*

(i) $A(u^*, f) \cong A(u^*, g)$.

(ii) *There exists an element $a \in k^\times$ satisfying the following conditions: f and ag have the same characteristic polynomial as well as the same minimum polynomial and, for all $b \in k$, $g^*(u^*) = bu^*$ if and only if $f^*(u^*) = abu^*$.*

1.12 Vista. Specifying k to a finite field, it follows that 1.4, 1.5, 1.7, 1.9, 1.11 cover all two-dimensional k-algebras since inseparable quadratic field extensions do not exist. As we shall see below, counting isomorphism classes in the various subcases of these results turns out to be quite straightforward, except for the cases 1.4 a), c), d), 1.7 e) and 1.11. An adequate treatment of these exceptions requires a series of purely algebraic preparations that will have to be presented before we can turn to the proof of the main theorem.

2. Two-dimensional algebras over arbitrary fields: Refinements.

2.0 We continue to work over an arbitrary base field k.

2.1 $\mathbb{Z}/2\mathbb{Z}$-actions. Throughout this paper, we write $\Gamma = \mathbb{Z}/2\mathbb{Z}$ for the group with two elements. Giving a right action of Γ on a set X amounts to giving a map $* : X \to X$, $x \mapsto x^*$, which is involutorial: $x^{**} = x$ for all $x \in X$. Then $X^\Gamma = \{x \in X \mid x^* = x\}$ is the set of fixed points under the action of Γ. If X is finite, then $|X/\Gamma| = |X^\Gamma| + \frac{1}{2}|X - X^\Gamma|$, hence

$$|X/\Gamma| = \frac{1}{2}(|X| + |X^\Gamma|). \tag{2.1.1}$$

2.2 Examples of $\mathbb{Z}/2\mathbb{Z}$-actions. Let K be a unital two-dimensional k-algebra as in 1.1 and write V for the underlying vector space over k. The element of $\mathrm{PGL}(V)$ determined by $f \in \mathrm{GL}(V)$ will be denoted by $[f]$. Given an invertible element $y \in K$, we put

$$[f]^* = [\tau f \tau L(y^{-1})]. \tag{2.2.1}$$

2.3 Lemma. *Notations being as in* 2.1, 2.2, *we have:*

a) *The map* $^* : \mathrm{PGL}(V) \to \mathrm{PGL}(V)$ *is involutorial, hence defines a right action of* Γ *on* $\mathrm{PGL}(V)$.

b) *For* $f \in \mathrm{GL}(V)$, *the following statements are equivalent.*

   (i) $[f] \in \mathrm{PGL}(V)^\Gamma$.

   (ii) $f = a\tau f \tau L(y^{-1})$ *for some* $a \in k^\times$.

   In this case, $n(y) = a^2$.

c) *If* $n(y) \in k^\times$ *is not a square, then* $\mathrm{PGL}(V)^\Gamma = \emptyset$.

Proof. a) We compute

$$\begin{aligned}[f]^{**} &= [\tau\tau f\tau L(y^{-1})\tau L(y^{-1})] = [fL(\overline{y}^{-1}y^{-1})] \\ &= [n(y)^{-1}f] = [f].\end{aligned}$$

b) The first part is obvious and the second one follows by taking determinants in (ii).
c) is an immediate consequence of b). □

If $n(y) \in k^\times$ is a square, we wish to describe the elements of $\mathrm{PGL}(V)^\Gamma$ in an explicit manner. To do so, the cases that K is étale or the algebra of dual numbers will be discussed separately.

2.4 Proposition. *Notations being as in 2.2, let K be étale and suppose $n(y) = b^2$ for some $b \in k^\times$. Then there are element $w_0, w_1 \in K^\times$ satisfying*

$$y = (-1)^i b\tau(w_i)w_i^{-1}$$

for $i = 0, 1$. Moreover, for all such b, w_0, w_1 and all $f \in \mathrm{GL}(V)$, the following statements are equivalent.

(i) $[f] \in \mathrm{PGL}(V)^\Gamma$.

(ii) *There exists $i = 0, 1$ such that either*

(2.4.1) $$[f] = [L\big(\tau(w_i)\big)\tau]$$

or

(2.4.2) $$[f] = [L(w_i) + L\big(c\tau(w_i)\big)\tau]$$

for some $c \in k$, $c \neq \pm 1$.

Proof. The existence of w_0, w_1 follows from (1.3.1). Using (1.3.2), (1.3.3), we find elements $u, v \in K$ satisfying

(2.4.3) $$f = L(u) + L\big(\tau(v)\big)\tau,\ n(u) \neq n(v)$$

and 2.3 b), combined with the computation

$$\begin{aligned}a\tau f\tau L(y^{-1}) &= a\Big(L\big(\tau(u)\big) + L(v)\tau\Big)L(y^{-1}) \\ &= L\big(a\tau(u)y^{-1}\big) + L\big(av\tau(y^{-1})\big)\tau,\end{aligned}$$

shows that (i) is equivalent to

(2.4.4) $$u = a\tau(u)y^{-1},\ v = a\tau(v)y^{-1}$$

for some $a \in k^\times$. This yields the implication (ii) ⇒ (i), so it remains to prove (i) ⇒ (ii). By (2.4.3), at least one of the elements u, v is invertible, so (2.4.4) gives $a = (-1)^i b$ for some $i = 0, 1$. We also claim that all nonzero elements $x \in \{u, v\}$ are invertible and, in fact, scalar multiplies of w_i. Indeed, assuming $n(x) = 0$ implies $x^2 = an(x)y^{-1}$ (by (2.4.4)) $= 0$, hence $x = 0$, a contradiction, and the relation $y = (-1)^i b\tau(x)x^{-1}$ shows $x \in kw_i$. Hence (2.4.1), (2.4.2) for $c = 0$, or (2.4.2) for $c \neq 0$ holds according as $u = 0, v = 0$, or $u \neq 0 \neq v$, respectively. □

Remark. The elements of $\mathrm{PGL}(V)$ described in 2.4 (ii) are independent of the choices of w_0, w_1. Furthermore i in (ii) is unique unless char $k = 2$.

We now turn to the algebra of dual numbers and, with an eye on 1.7 e), confine ourselves to the case $y = 1$.

2.5 Proposition. *Notations being as in* 1.6, 2.1, *let* $K = k[\varepsilon], \varepsilon^2 = 0$, *be the algebra of dual numbers and suppose* $y = 1$.

a) *For* char $k = 2$, Γ *acts trivially on* $\mathrm{PGL}(V)$.

b) *For* char $k \neq 2$ *and* $f \in \mathrm{GL}(V)$, *the following statements are equivalent.*

(i) $[f] \in \mathrm{PGL}(V)^\Gamma$.

(ii) *Either there exists* $a \in k$, $a \neq -1$, *satisfying*

$$[f] = [\mathbf{1}_V + L(a\varepsilon)\partial] \tag{2.5.1}$$

or there exists $a \in k^\times$ *satisfying*

$$[f] = [L(a\varepsilon) + \partial] \tag{2.5.2}$$

Proof. a) We have $\tau = \mathbf{1}_V$ (since char $k = 2$) and the assertion follows from 2.3 b).

b) Again by 2.3 b), (i) holds if and only if $\delta f = \tau f \tau$ for some sign $\delta = \pm 1$. Using (1.6.4), we write

$$f = L(u) + L(v)\partial \qquad (u, v \in K)$$

and compute

$$\begin{aligned}\tau f \tau &= L\big(\tau(u)\big) + L\big(\tau(v)\big)\tau\partial\tau \\ &= L\big(\tau(u)\big) - L\big(\tau(v)\big)\partial \qquad \text{(by (1.6.2) for } t = -1),\end{aligned}$$

so (i) is equivalent to $\tau(u) = \delta u,\ \tau(v) = -\delta v$. Since $n(u) + \Delta(u \wedge v) \neq 0$ by (1.6.5), this amounts to (2.5.1) for $\delta = 1$, and to (2.5.2) for $\delta = -1$. □

2.6 Cube roots of unity. We systematically write $\boldsymbol{\mu}_3$ for the group scheme of cube roots of unity [2]. In this subsection, we assume char $k \neq 3$. Given a quadratic étale k-algebra K as in 1.3, we wish to clarify the relation between $\boldsymbol{\mu}_3$ and $S(K)$. If $K = k \times k$ is split, the assignment $a \mapsto (a, a^{-1})$ yields the identifications

$$S(k \times k) = k^\times, \tag{2.6.1}$$

$$\boldsymbol{\mu}_3(k \times k) \cap S(k \times k) = \boldsymbol{\mu}_3(k). \tag{2.6.2}$$

For separable quadratic field extensions, we record the following observation.

2.7 Proposition. *Notations and assumptions being as in* 1.3, 2.6, *let K/k be a separable quadratic field extension containing the cube roots of unity. Then the following statements are equivalent.*

(i) $\boldsymbol{\mu}_3(K) \cap S(K) \neq \{1\}$.

(ii) $\boldsymbol{\mu}_3(K) \subset S(K)$.

(iii) $\boldsymbol{\mu}_3(k) = \{1\}$.

Proof. The equivalence (i) ⇔ (ii) being obvious, let us assume (ii) and $\zeta \in \boldsymbol{\mu}_3(k) \subset \boldsymbol{\mu}_3(K) \subset S(K)$. Then $\zeta^2 = n(\zeta) = 1$, hence $\zeta = 1$, proving (iii). Conversely, suppose (iii) holds and let $z \in \boldsymbol{\mu}_3(K)$. Then $n(z) \in \boldsymbol{\mu}_3(k) = \{1\}$, giving (ii). □

2.8 Specifications. We wish to make the classification 1.11 of two-dimensional strictly left singular algebras more explicit. Notations being as in 1.10, we are allowed to identify V with two-dimensional column space k^2 and V^* with two-dimensional row space k_2 over k. We may also put $u^* = (1, 0) \in k_2$.

2.9 Theorem. *Notations being as in* 1.10, 2.8, *a k-Algebra A is strictly left singular of dimension two if and only if it is isomorphic to $A(u^*, S)$ where $S \in \mathrm{GL}_2(k)$ satisfies one of the following mutually exclusive conditions.*

a) $S = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ *where $d \in k^\times$ is unique.*

b) $S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

c) $S = \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix}$ *where $c \in k^\times$ is unique* $\mod k^{\times 2}$.

d) $S = \begin{pmatrix} 1 & 1 \\ c & 0 \end{pmatrix}$ *where $c \in k^\times$ is unique.*

Proof. Given $S, T \in \mathrm{GL}_2(k)$, it makes sense by (1.10.1) to call $[S], [T] \in \mathrm{PGL}_2(k)$ *equivalent*, written as $[S] \sim [T]$, if $A(u^*, S)$ and $A(u^*, T)$ are isomorphic. By 1.11, this amounts to some $a \in k^\times$ giving S and aT the same characteristic as well as the same minimum polynomial such that

$$T^*(u^*) = bu^* \Longleftrightarrow S^*(u^*) = abu^* \qquad \text{(for all } b \in k). \tag{2.9.1}$$

We begin by showing that any

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$$

determines a matrix $S \in \mathrm{GL}_2(k)$ as in a) – d) satisfying $[S] \sim [T]$. If T is a scalar multiple of $\mathbf{1}_2$, the 2-by-2 unit matrix, we may choose S as in a), with $d = 1$. Henceforth we may therefore assume $[T] \neq [\mathbf{1}_2]$. Noting that u^* is an eigenvector for T^* iff $b = 0$, we proceed by considering the following cases.

Case 1. $b = 0$.

Then we may assume $a = 1$.

Case 1.2. $d = 1$.

Then $c \neq 0$. Furthermore, S as in b) and T not only satisfy (2.9.1) but also have the same characteristic polynomial, forcing $[S] \sim [T]$ as desired.

Case 1.3. $d \neq 1$.

Then $[S] \sim [T]$ for some S as in a), with $d \neq 1$.

Case 2. $b \neq 0$.

Then we may assume $b = 1$. Comparing traces and determinants yields

$$[T] = \begin{bmatrix} a & 1 \\ c & d \end{bmatrix} \sim \begin{bmatrix} a+d & 1 \\ c-ad & 0 \end{bmatrix},$$

so we are allowed to assume $d = 0$. For $a = 0$, $S = T$ is as in c). For $a \neq 0$,

$$[T] = \begin{bmatrix} 1 & \frac{1}{a} \\ \frac{c}{a} & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 \\ \frac{c}{a^2} & 0 \end{bmatrix},$$

so we have found $[S] \sim [T]$ for some S as in d).

Next we prove that the cases a) – d) are disjoint. First note that u^* is an eigenvector for S^* in cases a), b) but is not in cases c), d). Hence these pairs of cases do not overlap. Furthermore, since all matrices in a) are semi-simple but the one in b) is not, cases a), b) are disjoint. Finally, since the trace form vanishes on all matrices in c) but on no matrix in d), cases c), d) are disjoint as well. It remains to prove that, in each one of the individual cases a) – d), the parameters are unique as indicated. In a), given $d, e \in k^\times$ and putting $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e \end{smallmatrix}\right)$, we must show that $[S] \sim [T]$ implies $d = e$. Since the unit matrix is distinguished from all other matrices in a) by the property of its minimum polynomial having degree 1, we may assume $d \neq 1 \neq e$. By definition, some $a \in k^\times$ satisfying (2.9.1) gives S and aT the same characteristic polynomial. From $S^*(u^*) = T^*(u^*) = u^*$ we conclude $a = 1$, hence $d = e$, as claimed. In c), given $c, c' \in k^\times$ and putting $S = \left(\begin{smallmatrix} 0 & 1 \\ c & 0 \end{smallmatrix}\right)$, $S' = \left(\begin{smallmatrix} 0 & 1 \\ c' & 0 \end{smallmatrix}\right)$, we must show that $[S] \sim [S']$ implies $c \equiv c' \mod k^{\times 2}$ and conversely. But this follows immediately from the fact that $[S] \sim [S']$ iff some $a \in k^\times$ gives S' and aS the same characteristic polynomial. By a similar argument, the parameter c in d) is easily seen to be unique as well. This completes the proof of the theorem. □

3. Proof of the main theorem

3.0 In this section, we fix a prime number p and a positive integer n to put $k = \mathbb{F}_q$, the field with $q = p^n$ elements.

3.1 In order to prove the main theorem, we will have to compute the number of nonisomorphic $\mathbb{F}_q$-algebras belonging to the various subcases of 1.4, 1.7, 1.9 and 1.11. Since we know the number of square classes in $\mathbb{F}_q^\times$, which is 1 or 2 according as p is even or odd, and the order of the group $\mathrm{PGL}_2(\mathbb{F}_q)$, which is given by the formula

(3.1.1) $$|\mathrm{PGL}_2(\mathbb{F}_q)| = (q-1)q(q+1) = q^3 - q,$$

these computations are quite straightforward most of the time and lead to the following results.

3.2 Proposition. *The number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras which are regular with unital heart isomorphic to $\mathbb{F}_q \times \mathbb{F}_q$ and belong to one of the subcases* 1.4 b), e), f), g) *above is*

$$2q^3 - 1.$$

Proof. Applying 1.5 and 3.1 we see that the contributions of the individual cases listed above to the sum total combine to

$$1 + 2(q - 1) + (q^3 - q) + (q^3 - q) = 2q^3 - 1\,,$$

as claimed. □

3.3 Proposition. *The number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras which are regular with unital heart isomorphic to the algebra of dual numbers but do not belong to subcase* 1.7 e) *above is*

$$2q^2 - 2q - 1 \qquad (\textit{for } p = 2),$$
$$2q^2 - q - 2 \qquad (\textit{for } p \neq 2).$$

Proof. This follows immediately from 1.7. □

3.4 Proposition. *The number of nonisomorphic $\mathbb{F}_q$-algebras which are bisingular of dimension two is*

$$2q + 6 \qquad (\textit{for } p = 2),$$
$$2q + 7 \qquad (\textit{for } p \neq 2).$$

Proof. This follows immediately from 1.9. □

3.5 Proposition. *The number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras which are strictly left (resp. right) singular of dimension two is*

$$2q \qquad (\textit{for } p = 2),$$
$$2q + 1 \qquad (\textit{for } p \neq 2).$$

Proof. For strictly left singular algebras, this follows immediately from 1.11 and 2.9. Passing to the opposite algebras yields the rest. □

3.6 We are left with computing the number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras belonging to one of the subcases 1.4 a), c), d), 1.7 e) and begin with 1.4 a), which happens to be the most difficult. Keeping the notations of 1.3, let K be a quadratic étale $\mathbb{F}_q$-algebra, so $K = \mathbb{F}_q \times \mathbb{F}_q$ or $K = \mathbb{F}_{q^2}$. We may assume that K lives on two-dimensional column space $\mathbb{F}_q^2$. Looking at the norm epimorphism $n : K^\times \to \mathbb{F}_q^\times$ with kernel $S(K)$, we see that $n : M \to \mathbb{F}_q^\times$ is bijective, forcing

(3.6.1) $$|M| = q - 1.$$

We put

$$M_1 := \{y \in M - \{1\} \mid n(y) \in \mathbb{F}_q^{\times 2}\} \tag{3.6.2}$$

and conclude

$$M_1 = M - \{1\} \qquad \text{(for } p = 2\text{)}, \tag{3.6.3}$$

$$|M_1| = \frac{q-3}{2} \qquad \text{(for } p \neq 2\text{)}. \tag{3.6.4}$$

Given $y \in M$, 2.3 a) induces a right action of $\Gamma = \mathbb{Z}/2\mathbb{Z}$ on $X = \mathrm{PGL}_2(k)$ depending on y, allowing us to write $X^y = X^\Gamma,\ X_y = X/\Gamma$. Now denote by N the number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras belonging to subcase 1.4 a). Then 1.5 a) implies

$$\begin{aligned} N &= \sum_{y \in M - \{1\}} |X_y| = \frac{1}{2} \sum_{y \in M-\{1\}} (|X| + |X^y|) && \text{(by (2.1.1))} \\ &= \frac{1}{2}(q-2)(q^3-q) + \frac{1}{2} \sum_{y \in M - \{1\}} |X^y| && \text{(by (3.1.1), (3.6.1))} \end{aligned}$$

But $X^y = \emptyset$ for $y \in M - \{1\},\ y \notin M_1$ by 2.3 c). Hence

$$N = \frac{1}{2}(q^4 - 2q^3 - q^2 + 2q) + \frac{1}{2} \sum_{y \in M_1} |X^y| \tag{3.6.5}$$

Given $y \in M_1$, 2.4 implies

$$|X^y| = q \qquad \text{(for } p = 2\text{)}, \tag{3.6.6}$$

$$|X^y| = 2q - 2 \qquad \text{(for } p \neq 2\text{)}. \tag{3.6.7}$$

Combining the relations (3.6.5) – (3.6.7), we obtain:

3.7 Proposition. *The number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras which are regular with unital heart isomorphic to $\mathbb{F}_{q^2}$ (resp. $\mathbb{F}_q \times \mathbb{F}_q$) and belong to subcase* 1.4 a) *above is*

$$\frac{q^4}{2} - q^3 \qquad (\textit{for } p = 2), \tag{3.7.1}$$

$$\frac{1}{2}(q^4 + 3) - q^3 - q \qquad (\textit{for } p \neq 2). \tag{3.7.2}$$

□

3.8 We now turn to subcase 1.4 c) and write N for the number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras arising in that subcase. K being again one of the two quadratic étale $\mathbb{F}_q$-algebras $\mathbb{F}_q \times \mathbb{F}_q$ or $\mathbb{F}_{q^2}$, the short exact sequence

$$1 \to \boldsymbol{\mu}_3(K) \cap S(K) \to S(K) \to S(K)^3 \to 1$$

induced by taking cubes implies that the group $X = S(K)/S(K)^3$ satisfies

$$|X| = |\boldsymbol{\mu}_3(K) \cap S(K)| \tag{3.8.1}$$

The involution τ, which acts on X by inversion, induces a right action of Γ on X via 2.1, and 1.5 c), (2.1.1) imply

$$N = |X/\Gamma| = \frac{1}{2}(|X| + |X^\Gamma|). \tag{3.8.2}$$

Since $N = 1$ for $p = 3$, we may assume $p \neq 3$. Since the group $\mathbb{F}_{p^r}^\times$, for any positive integer r, is cyclic of order $p^r - 1$, the field $\mathbb{F}_{p^r}$ contains the cube roots of unity if and only if $p^r \equiv 1 \mod 3$. Hence, assuming $K = \mathbb{F}_q \times \mathbb{F}_q$, (2.6.2), (3.8.1), (3.8.2) yield $|X| = 3, |X^\Gamma| = 1$, $N = 2$ (resp. $N = |X| = 1$) for $q \equiv 1 \mod 3$ (resp. $q \equiv -1 \mod 3$). By the same token, assuming $K = \mathbb{F}_{q^2}$ and applying 2.7, we conclude $|X| = 3, |X^\Gamma| = 1, N = 2$ (resp. $N = |X| = 1$) for $q \equiv -1 \mod 3$ (resp. $q \equiv 1 \mod 3$). Summing up, we have

3.9 Proposition. *The number of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras which are regular with unital heart isomorphic to $\mathbb{F}_{q^2}$ (resp. $\mathbb{F}_q \times \mathbb{F}_q$) and belong to subcase* 1.4 c) *above is*

$$\begin{array}{lr} 1 & (\textit{for } p = 3), \\ 1 \ (\textit{resp. } 2) & (\textit{for } q \equiv 1 \mod 3), \\ 2 \ (\textit{resp. } 1) & (\textit{for } q \equiv -1 \mod 3). \end{array}$$

□

3.10 For $K = \mathbb{F}_{q^2}$ or $K = \mathbb{F}_q \times \mathbb{F}_q$ as before, the set $X = K - S(K)$ is τ-invariant and hence enherits a right Γ-action via 2.1. Thanks to 1.5 d), the number of two-dimensional $\mathbb{F}_q$-algebras belonging to subcase 1.4 d) is given by

$$\begin{aligned} N &= 2|X/\Gamma| = |X| + |X^\Gamma| \\ &= |K| - |S(K)| + |X^\Gamma|, \end{aligned}$$

so we have

$$N = q^2 - |S(K)| + |X^\Gamma| \tag{3.10.1}$$

Note first $|X^\Gamma| = |\mathbb{F}_q - S(K)| = \mathbb{F}_q - \{\pm 1\}$, which implies

$$|X^\Gamma| = q - 1 \qquad (\text{for } p = 2), \tag{3.10.2}$$

$$|X^\Gamma| = q - 2 \qquad (\text{for } p \neq 2). \tag{3.10.3}$$

On the other hand, the short exact sequence

$$1 \to \mathbb{F}_q^\times \to K^\times \to S(K) \to 1$$

determined by the map $v \mapsto \tau(v)v^{-1}$ gives

$$|S(\mathbb{F}_{q^2})| = q + 1, \tag{3.10.4}$$

$$|S(\mathbb{F}_q \times \mathbb{F}_q)| = q - 1. \tag{3.10.5}$$

Combining (3.10.1) - (3.10.5) we conclude:

3.11 Proposition. *The number of nonisomorphic two-dimensional* $\mathbb{F}_q$*-algebras which are regular with unital heart isomorphic to* $\mathbb{F}_{q^2}$ *(resp.* $\mathbb{F}_q \times \mathbb{F}_q$*) and belong to subcase* 1.4 d) *above is*

$$\begin{aligned} &q^2 - 2 \ (\textit{resp. } q^2) && (\textit{for } p = 2),\\ &q^2 - 3 \ (\textit{resp. } q^2 - 1) && (\textit{for } p \neq 2). \end{aligned}$$

□

3.12 Finally, we are left with counting the number N of nonisomorphic two-dimensional $\mathbb{F}_q$-algebras belonging to subcase 1.7 e). Considering the right action of Γ on $X = \mathrm{PGL}_2(\mathbb{F}_q)$ determined by $y = 1$ via 2.2, we apply 1.7 e), (1.6.3) and obtain

$$N = [\mathbb{F}_q^\times : \mathbb{F}_q^{\times 2}]|X/\Gamma|, \tag{3.12.1}$$

where $|X/\Gamma|$ may be computed by appealing to (2.1.1) und 2.5. Indeed, the latter yields

$$|X^\Gamma| = |X| \qquad (\text{for } p = 2), \tag{3.12.2}$$

$$|X^\Gamma| = 2(q-1) \qquad (\text{for } p \neq 2). \tag{3.12.3}$$

Combining (3.12.1) – (3.12.3), we conclude:

3.13 Proposition. *The number of nonisomorphic two-dimensional* $\mathbb{F}_q$*-algebras which belong to subcase* 1.7 e) *above is*

$$\begin{aligned} &q^3 - q && (\textit{for } p = 2),\\ &q^3 + q - 2 && (\textit{for } p \neq 2). \end{aligned}$$

□

The first part of the main theorem now follows by simply adding up the numbers obtained in 3.2 – 3.5, 3.7, 3.9, 3.11, 3.13 *and* 1, the latter accounting for the fact that the preceding propositions do not cover the case 1.4 b) with $K = \mathbb{F}_{q^2}$. Details are left to the reader.

3.14 Division algebras. It remains to derive the formulae for the number of nonisomorphic two-dimensional division algebras over $\mathbb{F}_q$ enunciated in the main theorem. Such algebras are clearly regular, and their unital heart, being a division algebra itself, must be $\mathbb{F}_{q^2}$. Hence the number we are looking for can be read off immediately from 3.7, 3.9, 3.11 and 1.4 b) for $K = \mathbb{F}_{q^2}$. Again details are left to the reader.

4. Concluding remarks.

It is a natural question to ask whether the formulae of the main theorem extend to higher dimensions. While explicit generalizations seem to be hardly within reach at the moment, a crude lower bound may be obtained quite easily as follows. Given a positive integer r, the totality of

r-dimensional $\mathbb{F}_q$-algebras may be parameterized by $\mathbb{F}_q^{r^3}$. The group $G = \mathrm{GL}_r(\mathbb{F}_q)$ acts on this space by isomorphisms in the obvious way, so the number of nonisomorphic r-dimensional $\mathbb{F}_q$-algebras is

$$\begin{aligned} |G \setminus \mathbb{F}_q^{r^3}| &\geq \frac{\mathbb{F}_q^{r^3}}{|G|} \\ &= \frac{q^{r^3}}{(q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})} = \frac{q^{r^3}}{q^{r^2} - \dots} \end{aligned} \tag{4.0.1}$$

and hence has order of magnitudes at least $q^{r^2(r-1)}$ as $r \to \infty$. Since, by the main theorem, this estimate is sharp for $r = 2$, the crude lower bound just obtained in the general case may not be so crude after all. Another indication pointing in the same direction derives from the fact that the obstructions to (4.0.1) becoming an equality are the stabilizers of the elements in $\mathbb{F}_q^{r^3}$ under the action of G, i.e., the automorphism groups of r-dimensional $\mathbb{F}_q$-algebras, so the sharpness of the corresponding lower bound largely depends on the question of whether these groups are generically trivial. The answer to this question, though affirmative for $r = 2$ (cf. Kaminski [1]), doesn't seem to be known in general. However, further corroborative evidence has been supplied by Röhrl [4], [5]. More precisely, let A be the generic r-dimensional algebra built over an arbitrary base field, so, by definition, the structure constants of A relative to a preassigned basis are independent indeterminates and A lives over the corresponding rational function field, say F. Then, combining [4, Theorem 1] with the theorem in [5], we conclude that the idempotents in A are finite in number and span A as a vector space over F. In particular, the automorphism group of A must be finite as well. Though still far away from generic triviality, this is a step into the right direction.

Acknowledgement

The authors are greatly indebted to H. Röhrl, S. Walcher and, in particular, to M. Schulte for useful comments and generous advice.

References

[1] Kaminski, H. “Die Automorphismengruppe zweidimensionaler Algebren.” Diplomarbeit. Fachbereich Mathematik. FernUniversität in Hagen, 2000.

[2] Knus, M.-A., A.S. Merkurjev, M. Rost, and J.-P. Tignol. “The book of involutions.” Amer. Math. Soc. Coll. Publ. **44**: Providence, RI, USA, 1998.

[3] Petersson, H.P. *The classification of two-dimensional nonassociative algebras.* Result Math. **37** (2000), 120-154.

[4] Röhrl, H. *A theorem on non-associative algebras and its applications to differential equations.* Manuscripta Math. **21** (1977), 181-187.

[5] Röhrl, H. *Finite dimensional algebras without nilpotent elements over algebraically closed fields.* Arch. Math. **32** (1979), 10-12.

[6] Scherer, M. “Die Anzahl der Isomorphieklassen zweidimensionaler nichtassoziativer Algebren über einem endlichen Körper.” Diplomarbeit. Fachbereich Mathematik. FernUniversität in Hagen, 2003.