*Geometriae Dedicata* **63:** 69–94, 1996.



# $n$-Dimensional Algebras over a Field with a Cyclic Extension of Degree $n$

GIAMPAOLO MENICHETTI*
*Dipartimento di Mathematica, Università di Bologna, Piazza di Porta S. Donato 5, 40127 Bologna, Italy. e-mail: menichet@dm.unibo.it*

(Received: 5 April 1995; revised version: 27 July 1995)

**Abstract.** We give a geometric method of classifying algebras $\mathbf{A}_{n,K}$, $n$-dimensional over a field $K$, with a cyclic extension of degree $n$. Algebras $\mathbf{A}_{n,K}$ without zero divisors satisfying some conditions are classified. In particular, we determine all $n$-dimensional division algebras over a finite field $F_q$ when $n$ is prime and $q$ is large enough.

**Mathematics Subject Classification (1991):** 17A01, 17A35.

**Key words:** determinantal hypersurfaces, division rings, twisted fields.

In [9], [10] Kaplansky formulates the following conjectures concerning division algebras $\mathbf{D}_{n,q}$ $n$-dimensional over a finite field $F_q$:

(K1) *Any algebra* $\mathbf{D}_{3,q}$ *is a field or a twisted field.*
(K2) *If* $q$ *is large enough, then an algebra* $\mathbf{D}_{5,q}$ *is a field or a twisted field.*

(K1) is proved in [12], [13]. In Section 3 of this paper we prove the following proposition:

(P) *If* $n$ *is prime and if* $q$ *is large enough, then an algebra* $\mathbf{D}_{n,q}$ *is a field or a twisted field.*

Result (P) is obtained at the end of a general treatment, in Section 2 and 3, of algebras $\mathbf{A}_{n,K}$ $n$-dimensional over a field $K$ with a cyclic extension of degree $n$.

Section 1 is devoted to proving some properties of autocirculant matrices (cf. [14]) that are used in the following sections.

In Section 2 we show that an algebra $\mathbf{A}_{n,k}$ defines a rational map $\overline{\mu} : \overline{\Lambda} \to \overline{\mathrm{P}}$ between determinantal hypersurfaces $\overline{\Lambda}, \overline{\mathrm{P}}$ of degree $n$ of $\mathcal{P}_{n-1}(\overline{K})$. Hence we prove that the classification of algebras $\mathbf{A}_{n,K}$ up to isotopisms is equivalent to the classification of maps $\overline{\mu} : \overline{\Lambda} \to \overline{\mathrm{P}}$ where $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ are determined up to linear automorphisms of $\mathcal{P}_{n-1}(K)$. In the case $K = F_q$ we also prove that if $\mathbf{A}_{n,K}$

* This research was supported in part by a grant from the M U R S T (40 % funds).

is without zero divisors and if $q$ is large enough, then $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ are unions of hypersurfaces of the same degree $d < n$.

In Section 3 we study a class of division algebras $\mathbf{D}_{n,K}$ that is the natural extension of the class of twisted fields introduced in Albert [2], to the case that $K$ is infinite. Hence we prove that an $n$-dimensional division algebra $\mathbf{A}_{n,K}$, such that $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ are unions of hyperplanes, is a field or an algebra $\mathbf{D}_{n,K}$.

## Section 1

We denote by $K$ a field that has a cyclic extension field $F, [F : K] = n \geq 2$, and by $\alpha$ a fixed generator of the Galois group, $\mathrm{Gal}(F/K)$, of $F$ over $K$. In particular when $K = F_q$ we suppose that $\alpha$ coincides with the Frobenius automorphism $x \mapsto x^q$.

For simplicity we indicate by $\alpha^h, 0 \leq h \leq n-1$, both an element of $\mathrm{Gal}(F/K)$ and the automorphism induced in the natural way by $\alpha^h$ in $F[z_0, z_1, \ldots, z_{n-1}]$, in the ring $R(n, F)$ of $n \times n$ matrices over $F$, etc.

From the Fundamental Theorem of Galois Theory (cf. [8, p. 232]) we deduce the following

PROPOSITION 1. *If $F'$ is a field, $K \subseteq F' \subseteq F$, then there exists a divisor $d$ of $n$ so that*

$$[F' : K] = d, \quad \mathrm{Gal}(F'/K) \quad \textit{is isomorphic to} \quad \langle\alpha\rangle/\langle\alpha^d\rangle \tag{1}$$

*and*

$$[F : F'] = n/d, \quad \mathrm{Gal}(F/F') = \langle\alpha^d\rangle. \tag{2}$$

*Conversely, if $d|n$, then there exists a field $F', K \subseteq F' \subseteq F$, so that (1) and (2) are satisfied.*

Let $k \in F', K \subseteq F' \subseteq F, [F' : K] = d$. We shall say that the elements $k^{\alpha^\nu}, \nu = 0, 1, \ldots, d-1$, are *conjugate in $F'$ over $K$*. Analogously we define polynomials and matrices conjugate in $F'$ over $K$.

Put $l = n/d$,

$$J_l := \begin{pmatrix} 0 & I_{l-1} \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}(l, K), \tag{3}$$

where $I_{l-1}$ is the $(l-1) \times (l-1)$ identity matrix, and

$$D_l(k) := \mathrm{diag}(k, k^{\alpha^d}, \ldots, k^{\alpha^{(l-1)d}}), \quad k \in F. \tag{4}$$

DEFINITION 2. An *autocirculant matrix* in $F$ over $F'$ is a matrix

$$A_l = A_l(k_0, k_1, \ldots, k_{l-1}) = \sum_{h=0}^{l-1} D_l(k_h) J_l^h, \quad k_h \in F. \tag{5}$$

$\mathrm{Auc}(F/F')$ denotes the set of these matrices.

If $F' = F$, then for simplicity we shall leave out the index $l = n$ in (3), (4) and (5).

Obviously $\mathrm{Auc}(F/F')$ is a subring of $R(n, F)$ and contains the ring of $l \times l$ circulant matrices over $F'$.

LEMMA 3. *The $n$-tuple $(u_0, u_1, \ldots, u_{n-1}) \in F^n$ is a base of $F$ over $K$ if and only if*

$$U = \begin{pmatrix} u_0 & u_1 & \cdots & u_{n-1} \\ u_0^{\alpha} & u_1^{\alpha} & \cdots & u_{n-1}^{\alpha} \\ \vdots & & & \\ u_0^{\alpha^{n-1}} & u_1^{\alpha^{n-1}} & \cdots & u_{n-1}^{\alpha^{n-1}} \end{pmatrix} \tag{6}$$

*is not singular* (cf. also [8, p. 281]).

*Proof.* If $\det(U) \neq 0$, then the linear system

$$\sum_{i=0}^{n-1} u_i^{\alpha^j} x_i = 0, \quad j = 0, 1, \ldots, n-1, \tag{*}$$

has only the trivial solution.

Conversely, suppose that $(u_0, u_1, \ldots, u_{n-1})$ is a basis of $F$ over $K$ and, by way of contradiction, that $\det(U) = 0$.

The system (*) has some non-trivial solutions $(x_0, x_1, \ldots, x_{n-1}) \in F^n$: e.g. let $x_0 \neq 0$. $F$ possesses a normal basis over $K$ (cf. [8, p. 283]), so there exists some elements $a \in F$ so that

$$\mathrm{tr}(ax_0) = \sum_{i=0}^{n-1} (ax_0)^{\alpha^i} \neq 0$$

Acting on the (*) subsequently by the automorphisms $\alpha^k, k = 0, 1, \ldots, n-1$, we obtain

$$\sum_{i=0}^{n-1} u_i^{\alpha^j} x_i^{\alpha^k} = 0, \quad k, j = 0, 1, \ldots, n-1.$$

From this we deduce

$$\sum_{i=0}^{n-1} u_i \mathrm{tr}(ax_i) = 0,$$

in contradiction with the hypothesis.

PROPOSITION 4. *The following three conditions on a matrix $M \in R(n, F)$ are equivalent:*

(a) $M \in \mathrm{Auc}(F/K)$;
(b) $M^\alpha = JMJ^{-1}$;
(c) $U^{-1}MU \in R(n, K)$.

*Proof.* (a) $\Rightarrow$ (b): This follows from (5) and from $JD(k)J^{-1} = D(k^\alpha)$, $\forall k \in F$.

(b) $\Rightarrow$ (a): For every $M \in R(n, F)$ the diagonal matrices $C_i = \mathrm{diag}(c_{i0}, c_{i1}, \ldots, c_{in-1}), i = 0, 1, \ldots, n-1$, such that $M = \sum_{i=0}^{n-1} C_i J^i$, are uniquely determined. Hence from (b) we deduce $C_i^\alpha = JC_iJ^{-1}$ and so $C_i D(c_{i0}), i = 0, 1, \ldots, n-1$.

(b) $\Rightarrow$ (c): We observe that

$$U^\alpha = JU. \tag{*}$$

From this and from (b) it follows that $(U^{-1}MU)^\alpha = U^{-1}MU$.

(c) $\Rightarrow$ (b): From (*) and from (c) we deduce $(U^\alpha)^{-1}M^\alpha U^\alpha = (U^\alpha)^{-1}JMJ^{-1}U^\alpha$

The equivalence of (a) with (b) implies $\det(A) \in K, \forall A \in \mathrm{Auc}(F/K)$. Hence, in general,

$$\det(A_l) \in F', \quad \forall A_l \in \mathrm{Auc}(F/F'). \tag{7}$$

PROPOSITION 5. *Let*

$$A = \sum_{w=0}^{s-1} D(k_{i_w}) J^{i_w} \in \mathrm{Auc}(F/K),$$

*with* $0 \leq i_0 < i_1 < \cdots < i_{s-1} \leq n-1, k_{i_w} \neq 0, w = 0, 1, \ldots, s-1$. *If* $d = \mathrm{G.C.D.}(n, i_0, i_1, \ldots, i_{s-1})$, *then*

$$\det(A) = \prod_{\nu=0}^{d-1} (\det(A_l))^{\alpha^\nu}, \quad A_l = \sum_{w=0}^{s-1} D_l(k_{i_w}) J_l^{r_w} \in \mathrm{Auc}(F/F'),$$

*where* $K \subseteq F' \subseteq F, [F' : K] = d, l = n/d$ *and* $r_w = i_w/d$. *Furthermore* $(\det(A_l))^{\alpha^\nu}$, $\nu = 0, 1, \ldots, d-1$, *are conjugate elements in* $F'$ *over* $K$.

The proof of this proposition needs some remarks on the symmetric group, $S_n$, of $\underline{n_0} = \{0, 1, \ldots, n-1\}$.

Let

$$\tau = (0\,1\,\ldots\,n-1) \in S_n \tag{8}$$

be the cycle that maps 0 to 1, 1 to $2, \ldots, n-1$ to 0, and let $i \in \underline{n_0}$. If $d$ divides the G.C.D.$(n, i)$ and if $i = rd$, then

$$\tau^i = (\tau_0\tau_1\ \ldots\ \tau_{d-1})^r,\ \tau_\nu = (\nu\ \nu+d\ \ldots\ \nu+d(l-1)) \in S_n,$$
$$\nu = 0, 1, \ldots, d-1.$$

If

$$\chi = \chi_0\chi_1\ \cdots\ \chi_{d-1},\ \chi_\nu = (\nu l\ \nu l+1\ \ldots\ \nu l+(l-1)) \in S_n,$$
$$\nu = 0, 1, \ldots, d-1, \tag{9}$$

and if

$$\gamma = \begin{pmatrix} 0 & 1 & \ldots & l-1 & \ldots & (d-1)l & \ldots & dl-1 \\ 0 & d & \ldots & (l-1)d & \ldots & d-1 & \ldots & dl-1 \end{pmatrix}, \tag{10}$$

then $\tau_0\tau_1 \ldots \tau_{d-1} = \gamma^{-1}\chi\gamma$. Hence

$$\tau^i = \gamma^{-1}\chi^r\gamma, \quad i = rd. \tag{11}$$

Let $P : S_n \to \mathrm{GL}(n, F)$ be the linear representation in which

$$P(\sigma) = (c_{ij}), \quad c_{ij} = \begin{cases} 1, j = \sigma(i), \\ 0, j \neq \sigma(i). \end{cases} \tag{12}$$

If $\tau$ and $\chi$ denote the permutations (8) and (9) respectively, then

$$P(\tau) = J \tag{13}$$

and

$$P(\chi^r) = \mathrm{diag}(J_l^r, J_l^r, \ldots, J_l^r) \quad \text{(cf.(3))}. \tag{14}$$

Moreover, for every $\mathrm{diag}(k_0, k_1, \ldots, k_{n-1}) \in \mathrm{GL}(n, F)$ and for every $\sigma \in S_n$,

$$P(\sigma)\mathrm{diag}(k_0, k_1, \ldots, k_{n-1})P(\sigma^{-1}) = \mathrm{diag}(k_{\sigma(0)}, k_{\sigma(1)}, \ldots, k_{\sigma(n-1)}). \tag{15}$$

PROOF OF PROPOSITION 5. If $\gamma$ denotes the permutation (10), then (cf. (11) and (13))

$$\det\left(\sum_{w=0}^{s-1} D(k_{i_w})J^{i_w}\right) = \det\left(\sum_{w=0}^{s-1} P(\gamma)D(k_{i_w})P^{-1}(\gamma)P(\chi^{r_w})\right).$$

From (10) and (15) we deduce

$$P(\gamma)D(k_{i_w})P^{-1}(\gamma) = \operatorname{diag}(D_l(k_{i_w}), D_l^{\alpha}(k_{i_w}), \ldots, D_l^{\alpha^{d-1}}(k_{i_w})).$$

The first statement follows from this, from (14) and from Proposition 1. The second is an obvious consequence of (7).

We denote by $\mathbf{F}$ the field $F$ with the natural structure of $n$-dimensional $K$-algebra and by $V$ its $K$-vector space.

PROPOSITION 6. *The endomorphisms of $V$ are all and only the maps $\varepsilon : V \to V$,*

$$\varepsilon(x) = \sum_{i=0}^{n-1} k_i x^{\alpha^i}, \quad k_i \in F. \tag{16}$$

*$U^{-1}A(k_0, k_1, \ldots, k_{n-1})U$ is the matrix of $\varepsilon$ relative to the base $(u_0, u_1, \ldots, u_{n-1})$* (cf. also [15] and [17]).

*Proof.* Obviously $\varepsilon \in \operatorname{End}(V)$. If $B = (b_{ij}) \in R(n, K)$ is the matrix of $\mu \in \operatorname{End}(V)$ relative to the base $(u_0, u_1, \ldots, u_{n-1})$, then

$$\mu : x = \sum_{j=0}^{n-1} x_j u_j \mapsto x' = \sum_{i=0}^{n-1} x'_i u_i, \quad x_j, x'_i \in K, \tag{*}$$

$$x'_i = \sum_{j=0}^{n-1} b_{ij} x_j, \quad j = 0, 1, \ldots, n-1. \tag{*}'$$

Acting in succession by the automorphisms $\alpha^k, k = 0, 1, \ldots, n-1$, on the expressions of $x$ and $x'$ that are in (*), we obtain

$$x_j = \sum_{k=0}^{n-1} \nu_{jk} x^{\alpha^k}, \quad x'_i = \sum_{k=0}^{n-1} \nu_{ik} x'^{\alpha^k},$$

where $(\nu_{ij}) = U^{-1}$.

Substituting in (*)′ we have

$${}^t(x' \quad x'^{\alpha} \quad \ldots \quad x'^{\alpha^{n-1}}) = UBU^{-1}{}^t(x \quad x^{\alpha} \quad \ldots \quad x^{\alpha^{n-1}}). \tag{*}''$$

From Proposition 4 we deduce

$$UBU^{-1} = A(k_0, k_1, \ldots, k_{n-1}) \in \operatorname{Auc}(F/K).$$

Hence (*)″ is equivalent to (16).

DEFINITION 7. We say that $A(k_0, k_1, \ldots, k_{n-1})$ is the autocirculant matrix of the automorphism (16).

COROLLARY 8. *The automorphisms of $V$ are all and only the maps (16) whose autocirculant matrices are non-singular* (cf. also [5] and [14]).

## Section 2

Up to isomorphisms an $n$-dimensional $K$-algebra is a structure $\mathbf{A} = (V, f)$ whose multiplication $f : V^2 \to V$ is a bilinear map, i.e. (cf. Proposition 6)

$$f(x, y) = \sum_{i,j=0}^{n-1} a_{ij} x^{\alpha^i} y^{\alpha^j}, \quad a_{ij} \in \mathbf{F}.$$

We shall say that $\mathbf{A}$ is a *division algebra* if it possesses the unity element and has no zero divisors.

The autocirculant matrices of left and right multiplication $\lambda_x : y \mapsto f(x, y)$ and $\rho_y : x \mapsto f(x, y)$ are

$$A(l_0(x), l_1(x), \ldots, l_{n-1}(x)), \quad l_j(x) = \sum_{i=0}^{n-1} a_{ij} x^{\alpha^i},$$

and

$$A(r_0(y), r_1(y), \ldots, r_{n-1}(y)), \quad r_i(y) = \sum_{j=0}^{n-1} a_{ij} y^{\alpha^j},$$

respectively.

We shall say that $\mathbf{A}' = (V, f')$ is $(\beta_1, \beta_2, \beta_3)$-*isotopic* to $\mathbf{A} = (V, f)$ (or simply that $\mathbf{A}'$ is *isotopic* to $\mathbf{A}$ and we shall write $\mathbf{A}' \approx \mathbf{A}$) if there exists an *isotopism* $(\beta_1, \beta_2, \beta_3) \in (\mathrm{Aut}(V))^3$ so that

$$f'(x, y) = (f(x^{\beta_1}, y^{\beta_2}))^{\beta_3}, \quad \forall x, y \in V.$$

In particular, if $\beta_1 = \beta_2 = \beta_3^{-1}$, then $\mathbf{A}'$ is isomorphic to $\mathbf{A}$ ($\mathbf{A}' \cong \mathbf{A}$).

The group $(\mathrm{Aut}(V))^3$ determines a partition into isotopism classes of the set of algebras. The same occurs in the set of algebras without zero divisors, and in this case every isotopism class contains some division algebras. In fact we prove the following

PROPOSITION 9. *Let $\mathbf{A} = (V, f)$ be an algebra without zero divisors. Up to isomorphism the division algebras isotopic to $\mathbf{A}$ are those $\mathbf{A}' = (V, f')$ in which*

$$f'(x, y) = f(x^{\rho_a^{-1}}, y^{\lambda_b^{-1}}), \forall x, y \in V,$$

*with $a, b \in \mathbf{A} - 0$. The element $f(b, a)$ is the unit of $\mathbf{A}'$.*

*Proof.* Up to isomorphism $\mathbf{A}'$ is isotopic to $\mathbf{A}$ if and only if $f(x,y) = f'(x^{\beta_1}, y^{\beta_2}), \beta_1, \beta_2 \in \mathrm{Aut}(V)$.

Let $e \in V - 0, b = e^{\beta_1^{-1}}, a = e^{\beta_2^{-1}}$. $e$ is the unit of $\mathbf{A}'$ if and only if

$$y^{\beta_2} = f'(e, y^{\beta_2}) = f(b,y), \quad \forall y \in V,$$

and

$$x^{\beta_1} = f'(x^{\beta_1}, e) = f(x,a), \quad \forall x \in V.$$

Hence

$$f(x,y) = f'(x^{\rho_a}, y^{\lambda_b}), \quad \forall x, y \in V.$$

Moreover, we observe that

$$f'(f(b,a),y) = f(b, y^{\lambda_b^{-1}}) = y, \quad f'(x, f(b,a)) = f(x^{\rho_a^{-1}}, a) = x.$$

The isotopism relation comes from the theory of projective planes. In fact we can prove that every division algebra $\mathbf{D}$ – or more exactly its ring (semifield) – is the coordinate ring for a non-Desarguesian plane $\pi(\mathbf{D})$ of type V.1 in the Lenz–Barlotti classification. Moreover, if $\mathbf{D}' \approx \mathbf{D}$, then $\pi(\mathbf{D}')$ is isomorphic to $\pi(\mathbf{D})$ (cf. [4]).

In this note we mainly study algebras without zero divisors and, in particular, division algebras. So afterwards we shall refer to the classification of algebras in isotopism classes.

The left zero divisors (respectively right zero divisors) of the algebra $\mathbf{A} = (V, f)$ are the non-null solutions in $F$ of the equation

$$L(x) = \det(A(l_0(x), l_1(x), \ldots, l_{n-1}(x)) = 0 \tag{17}$$

(respectively of the equation

$$R(y) = \det(A(r_0(y), r_1(y), \ldots, r_{n-1}(y)) = 0). \tag{18}$$

The implicit functions

$$f^{\alpha^k}(x,y) = 0, \quad k = 0, 1, \ldots, n-1, \tag{19}$$

yields a correspondence from the set of solutions of (17) to the set of solutions of (18).

We shall suppose always that (17) and (18) are not identities.

In order to study the above-mentioned equations – particularly when **A** has no zero divisors – it is expedient to include $F$ in $\overline{K}$ or rather **A** in $\mathbf{A} \otimes \overline{K}$. We shall do this using a geometric language.

Let $\mathcal{P}(V) = \mathcal{P}_{n-1}(K)$ the $(n-1)$-dimensional projective space over $K$. We denote by $\Sigma$ the projective coordinate system corresponding to the base $(u_0, u_1, \ldots, u_{n-1})$ of $V$. So if

$$x = \sum_{i=0}^{n-1} x_i u_i \tag{20}$$

is a point, then $(x_0, x_1, \ldots, x_{n-1})$ is the $n$-tuple of its coordinate in $\Sigma$.

In $\mathcal{P}_{n-1}(\overline{K}) \supseteq \mathcal{P}_{n-1}(K)$ we fix the coordinate system $\Sigma_0$ defined from $\Sigma$ by the following coordinate transformation:

$$z_j = \sum_{i=0}^{n-1} x_i u_i^{\alpha^j}, \quad j = 0, 1, \ldots, n-1. \tag{21}$$

By the comparison of these equations with those obtained from (20) acting subsequently by the automorphisms $\alpha^j, j = 0, 1, \ldots, n-1$ (cf. also Proposition 4), we deduce the following

*Remark 10.* In the coordinate system $\Sigma_0$ the points lying in $\mathcal{P}_{n-1}(K)$ have coordinates $(kx, kx^{\alpha}, \ldots, kx^{\alpha^{n-1}}), x \in F^* = F - 0, k \neq 0$. The linear automorphisms of $\mathcal{P}_{n-1}(K)$ have equations $z_i' = \Sigma_{j=0}^{n-1} a_{ij} z_j, i = 0, 1, \ldots, n-1, (a_{ij}) \in \mathrm{Auc}(F/K), \det(a_{ij}) \neq 0$.

The homogeneous equation

$$L\left(\sum_{i=0}^{n-1} x_i u_i\right) = 0 \tag{22}$$

of degree $n$ has coefficients in $K$ (cf. (7)). Hence in $\Sigma$ it is the equation of a hypersurface $\Lambda$ that we shall call the *hypersurface of left zero divisors of* **A**. Analogously we define

$$\mathrm{P}: R\left(\sum_{j=0}^{n-1} y_j u_j\right) = 0 \tag{23}$$

as the *hypersurface of right zero divisors of* **A**.

The functions

$$f^{\alpha^k}\left(\sum_{i=0}^{n-1} x_i u_i, \sum_{j=0}^{n-1} y_j u_j\right) = 0, \quad k = 0, 1, \ldots, n-1, \tag{24}$$

give a rational map $\mu : \Lambda \to \mathrm{P}$.

We deduce the equation of $\Lambda$ and P in $\Sigma_0$ substituting (21) respectively in (22) and (23). Hence (cf. Remark 10):

*Remark 11.* (17) and (18) are the equations in $\Sigma_0$ of the zero-divisor hypersurfaces $\Lambda$, P of $\mathbf{A}$. The functions (19) give a rational map $\mu : \Lambda \to \mathrm{P}$.

Let $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ be the set of $\overline{K}$-rational points of $\Lambda$ and P respectively (i.e. the zero-divisor hypersurfaces of the algebra $\mathbf{A} \otimes \overline{K}$).

*Remark 12.* If $\overline{L}(z_0, z_1, \ldots, z_{n-1})$ and $\overline{R}(z'_0, z'_1, \ldots, z'_{n-1})$ are the polynomials deduced from (17) and (18) respectively by the substitutions

$$x^{\alpha^k} = z_k, \quad y^{\alpha^k} = z'_k, \quad k = 0, 1, \ldots, n-1, \tag{25}$$

then in $\Sigma_0$

$$\overline{\Lambda} : \overline{L}(z_0, z_1, \ldots, z_{n-1}) = 0, \quad \overline{\mathrm{P}} : \overline{L}(z'_0, z'_1, \ldots, z'_{n-1}) = 0.$$

The functions

$$\overline{f}_k(z_0, z_1, \ldots, z_{n-1}, z'_0, z'_1, \ldots, z'_{n-1}) = 0, \quad k = 0, 1, \ldots, n-1, \tag{26}$$

analogously deduced from (19), give a rational map $\overline{\mu} : \overline{\Lambda} \to \overline{\mathrm{P}}$.

We remark also that in the coordinate system $\Sigma_0$ the equations of $\Lambda, \overline{\Lambda}$, $\mathrm{P}, \overline{\mathrm{P}}$ are independent of the choice of a base in $V$.

Let

$$\Lambda' : L'(x) = \det(A(l'_0(x), l'_1(x), \ldots, l'_{n-1}(x)) = 0 \tag{27}$$

and

$$\mathrm{P}' : R'(y) = \det(A(r'_0(y), r'_1(y), \ldots, r'_{n-1}(y)) = 0 \tag{28}$$

be the zero-divisor hypersurfaces of the algebra $\mathbf{A}' = (V, f')$. Moreover, let

$$f'^{\alpha^k}(x, y) = 0, \quad k = 0, 1, \ldots, n-1, \tag{29}$$

be the functions that define a rational map $\mu' : \Lambda' \to \mathrm{P}'$.

PROPOSITION 13. $\mathbf{A}' = (V, f'))$ *is* $(1, 1, \beta_3)$*-isotopic to* $\mathbf{A} = (V, f)$ *if and only if* $\overline{\Lambda}' = \overline{\Lambda}, \overline{\mathrm{P}}' = \overline{\mathrm{P}}$ *and functions* (26) *and*

$$\overline{f}'_k(z_0, z_1, \ldots, z_{n-1}, z'_0, z'_1, \ldots, z'_{n-1}) = 0, \quad k = 0, 1, \ldots, n-1, \tag{30}$$

*give the same map* $\overline{\mu} : \overline{\Lambda} \to \overline{\mathrm{P}}$.

*Proof.* If $\mathbf{A}'$ is $(1, 1, \beta_3)$-isotopic to $\mathbf{A}$, then (cf. Corollary 8)

$$f'(x, y) = \sum_{i=0}^{n-1} k_i f^{\alpha^i}(x, y), \quad \det(A(k_0, k_1, \ldots, k_{n-1})) \neq 0. \tag{*}$$

Hence

$$\begin{aligned} &A(l'_0(x), l'_1(x), \ldots, l'_{n-1}(x)) \\ &\quad = A(k_0, k_1, \ldots, k_{n-1}) A(l_0(x), l_1(x), \ldots, l_{n-1}(x)), \\ &A(r'_0(x), r'_1(x), \ldots, r'_{n-1}(x)) \\ &\quad = A(k_0, k_1, \ldots, k_{n-1}) A(r_0(x), r_1(x), \ldots, r_{n-1}(x)). \end{aligned}$$

Moreover, systems (26) and (30) are equivalent.

On the other hand, if $\overline{\Lambda}' = \overline{\Lambda}, \overline{\mathrm{P}}' = \overline{\mathrm{P}}, \bar{\mu}' = \bar{\mu}$, then there exists a matrix $M \in \mathrm{GL}(n, F)$ such that

$${}^t(\overline{f}'_0\ \overline{f}'_1 \ldots \overline{f}'_{n-1}) = M\, {}^t(\overline{f}_0\ \overline{f}_1 \ldots \overline{f}_{n-1}).$$

In particular, assuming $z_h = x^{\alpha^h}, z'_h = y^{\alpha^h}$, we have

$${}^t(f'\ f'^{\alpha} \ldots f'^{\alpha^{n-1}}) = M\, {}^t(f\ f^{\alpha} \ldots f^{\alpha^{n-1}}).$$

From

$$\begin{aligned} {}^t(f\ f^{\alpha} \ldots f^{\alpha^{n-1}})^{\alpha} &= J\, {}^t(f\ f^{\alpha} \ldots f^{\alpha^{n-1}}),\ {}^t(f'\ f'^{\alpha} \ldots f'^{\alpha^{n-1}})^{\alpha} \\ &= J\, {}^t(f'\ f'^{\alpha} \ldots f'^{\alpha^{n-1}}) \end{aligned}$$

we deduce that $M = J^{-1} M^{\alpha} J$ and hence (cf. Proposition 4) $M = A(k_0, k_1, \ldots, k_{n-1})$.

We can formulate the last proposition referring to the hypersurfaces $\Lambda, \mathrm{P}, \Lambda', \mathrm{P}'$ instead of $\overline{\Lambda}, \overline{\mathrm{P}}, \overline{\Lambda}', \overline{\mathrm{P}}'$, but it would have no real content if the algebras have no zero divisors.

PROPOSITION 14.1. *If $\mathbf{A}' = (V, f')$ is $(\beta_1, 1, 1)$-isotopic to $\mathbf{A} = (V, f)$, then $\Lambda'$ is projectively equivalent to $\Lambda$ and $\mathrm{P}' = \mathrm{P}$.*

*If $\Lambda'$ is a hypersurface projectively equivalent to $\Lambda$, then there exists an algebra $\mathbf{A}'$ isotopic to $\mathbf{A}$, whose left and the right zero-divisor hypersurfaces are $\Lambda'$ and $\mathrm{P}$ respectively.*

*Proof.* If $\mathbf{A}'$ is $(\beta_1, 1, 1)$-isotopic to $\mathbf{A}$, then (cf. Corollary 8)

$$f'(x,y) = f\left(\sum_{i=0}^{n-1} k_i x^{\alpha^i}, y\right), \quad \det(A(k_0, k_1, \ldots, k_{n-1})) \neq 0. \tag{*}$$

Hence the hypersurface

$$\Lambda' : L\left(\sum_{i=0}^{n-1} k_i x^{\alpha^i}\right) = 0 \tag{*}'$$

is projectively equivalent to $\Lambda : L(x) = 0$ (cf. Remark 12). Moreover, $R'(y) = R(y)A(k_0, k_1, \ldots, k_{n-1})$.

If $\Lambda'$ is projectively equivalent to $\Lambda$, then there exists a non-singular matrix $A(k_0, k_1, \ldots, k_{n-1})$ such that $(*)'$ is the equation of $\Lambda'$. Then we observe that the algebra $\mathbf{A}' = (V, f')$, with $f'$ given by $(*)$, satisfies the required conditions.

Likewise we prove the following

PROPOSITION 14.2. *If* $\mathbf{A} = (V, f')$ *is* $(1, \beta_2, 1)$*-isotropic to* $\mathbf{A} = (V, f)$, *then* $\Lambda' = \Lambda$ *and* $\mathrm{P}'$ *is projectively equivalent to* P.

*If* $\mathrm{P}'$ *is a hypersurface projectively equivalent to* P, *then there exists an algebra* $\mathbf{A}'$ *isotopic to* $\mathbf{A}$, *whose left and right zero-divisor hypersurfaces are* $\Lambda$ *and* $\mathrm{P}'$ *respectively.*

From Propositions 13, 14.1 and 14.2 we see that the classification of algebras into isotopism classes requires the determination of the possible couples $(\Lambda, \mathrm{P})$ two-by-two projectively non-equivalent, and for every couple $(\Lambda, \mathrm{P})$ the admissible rational maps $\overline{\mu} : \overline{\Lambda} \to \overline{\mathrm{P}}$.

In any case, $\Lambda$ and P are determinantal hypersurfaces that can be either absolutely irreducible or reducible in a suitable extension of $K$.

EXAMPLE. $\mathbf{A} = (V, f), f(x,y) = xy + (x^{\alpha^2} - x)y^{\alpha}, \dim_K \mathbf{A} = 3.$

$$\begin{aligned} L(x) \;=\; R(x) &= \det(D(x) + D(x^{\alpha^2} - x)J) = xx^{\alpha}x^{\alpha^2} \\ &\quad + (x - x^{\alpha})(x^{\alpha^2} - x)(x^{\alpha} - x^{\alpha^2}), \end{aligned}$$

$$\overline{\Lambda}, \overline{\mathrm{P}} : z_0 z_1 z_3 + (z_0 - z_1)(z_2 - z_0)(z_1 - z_2) = 0.$$

These cubic curves are invariant under the action of the group generated by the linear automorphism $(z_0, z_1, z_2) \to (z_1, z_2, z_0)$. Hence their possible singular points have coordinates $(1, k, k^2), k^2 + 3k - 3 = 0, k^2 + k + 1 = 0$.

We deduce that $\overline{\Lambda} = \bar{P}$

(a) is the union of the conic $z_0z_1 + z_1z_2 + z_2z_0 = 0$ and the line $z_0 + z_1 + z_2 = 0$ when $\mathrm{Char}(K) = 2$;
(b) has a double point in (1,2,4) if $\mathrm{Char}(K) = 7$;
(c) is elliptic in the other cases.

From Proposition 5 we deduce the following

*Remark 15.* Let be $\mathbf{A} = (V, f)$

$$f(x,y) = \sum_{h=0}^{T-1} \sum_{k=0}^{S-1} c_{hk} x^{\alpha^{t_h}} y^{\alpha^{s_k}}, \quad c_{hk} \in F,$$

$0 \le t_0 < t_1 < \cdots < t_{T-1} \le n-1, 0 \le s_0 < s_1 < \cdots < s_{S-1} \le n-1$. Suppose that for every $h \in \{0,1,\ldots,T-1\}$ and for every $k \in \{0,1,\ldots,S-1\}$ some constants are non-zero.

If $d = \mathrm{G.C.D.}(n, s_0, s_1, \ldots, s_{S-1}), d' = \mathrm{G.C.D.}(n, t_0, t_1, \ldots, t_{T-1})$, then

(a) $\Lambda$ is the union of the $d'$ hypersurfaces

$$\Lambda_\nu : \det \left( \sum_{k=0}^{S-1} D_l \left( \sum_{h=0}^{T-1} c_{hk} x^{\alpha^{t_h}} \right) J_l^{r_k} \right)^{\alpha^\nu} = 0, \quad l = n/d,$$

$$r_k = s_k/d, \quad \nu = 0,1,\ldots,d-1,$$

that are conjugate in an extension of degree $d$ of $K$;

(b) P is the union of $d'$ hypersurfaces

$$\mathrm{P}_{\nu'} : \det \left( \sum_{h=0}^{T-1} D_{l'} \left( \sum_{k=0}^{S-1} c_{hk} y^{\alpha^{s_k}} \right) J_{l'}^{r'_h} \right)^{\alpha^{\nu'}} = 0, \quad l' = n/d',$$

$$r'_k = t_h/d', \quad \nu' = 0,1,\ldots,d'-1,$$

that are conjugate in an extension of degree $d'$ of $K$.

The hypersurfaces $\Lambda_\nu$ or $\mathrm{P}_{\nu'}$ may be reducible. Moreover, we can choose $t_h, s_k$ and $c_{hk}$ in such a way that $\Lambda_\nu$ and $\mathrm{P}_{\nu'}$ have no $K$-rational points. Some examples are in the next section.

If $K = F_q$ and if $\mathbf{A}$ has no zero divisors, then the possible components of $\Lambda$ and P satisfy the conditions imposed by Propositions 16 and 17.

Let $\Phi : g(z_0, z_1, \ldots, z_{n-1}) = 0$ be a hypersurface of degree $n > 2$ lying in $\mathcal{P}_{n-1}(F_q)$.

PROPOSITION 16. *If $\Phi$ is reducible and has no $F_q$-rational points, then it has $m = n/d$ components, each of degree $d < n$ and conjugate in $F_{q^m}$ over $F_q$.*

*Proof.* Let $F_{q^{m'}}[z_0, z_1, \ldots, z_{n-1}]$, $m' \geq 1$, the ring in which

$$g = \prod_{r=1}^{l} g_r \qquad (*)$$

where the $g_r$ are absolutely irreducible homogeneous polynomials. We divide the proof into two parts.

(a) *A polynomial* $g = \Pi_{j=1}^{l'} g_{r_j}$, *product of* $l' < l$ *polynomials among the* $g_r$ *does not lie in* $F_q[z_0, z_1, \ldots, z_{n-1}]$.

Suppose $g' \in F_q[z_0, z_1, \ldots, z_{n-1}]$. If $g'$ depended on $n' < n$ variables (for instance $z_0, z_1, \ldots, z_{n'}$), then $(0, 0, \ldots, 1)$ would be a non-trivial zero of $g$. If $g'$ depended on all variables, then, since $\deg(g') \leq n, g'$ would have at least a non-trivial zero in $F_q^n$ according to the Chevalley–Warning theorem (cf. [16, p. 13]).

(b) *If* $g_1 \in F_{q^m}[z_0, z_1, \ldots, z_{n-1}], 2 \leq m \leq m'$, *then* $l = m$ *and the factors* $g_r$ *of* $(*)$ *are conjugate in* $F_{q^m}$ *over* $F_q$.

We observe that every polynomial $g_1^{q^j}, j = 0, 1, \ldots, m-1$, is a factor of $g$ because $\Pi_{r=1}^{l} g_r = \Pi_{r=1}^{l} g_r^{q^j}, j = 0, 1, \ldots, m-1$, and $F_{q^{m'}}[z_0, z_1, \ldots, z_{n-1}]$ is factorial.

From (a) and from $\Pi_{j=0}^{m-1} g_1^{q^j} \in F_q[z_0, z_1, \ldots, z_{n-1}]$ we deduce that $g_1^{q^j}, j = 0, 1, \ldots, m-1$, are the only factors of $(*)$.

PROPOSITION 17. *If* $q$ *is large enough, i.e. greater than an integer* $B(n)$ *depending only on* $n$, *then a hypersurface* $\Phi \in \mathcal{P}_{n-1}(F_q)$, $\deg(\Phi) > 2$, *without* $F_q$*-rational points, is reducible in a suitable extension of* $F_q$.

*Proof.* Putting $N = 0, r = n-2$ and $d = n$ in the Lang–Weil inequality proved in [11], we deduce

$$q^{n-2} \leq (n-1)(n-2)q^{n-2-1/2} + A'(n)q^{n-3},$$

where $A'(n)$ is a constant depending only on $n$. Hence

$$q \leq (n-1)(n-2)\sqrt{q} + A'(n)$$

or $q \leq B(n)$.

PROPOSITION 18. $B(3) = 1$.

*Proof.* The Hasse–Weil inequality

$$|N - (q+1)| \leq 2g\sqrt{q} \quad \text{(cf. [7] and [18])}$$

assures that an irreducible cubic has $N > 0$ rational points over $F_q$ for every $q$.

From Proposition 17 we deduce the following

COROLLARY 19. *Let* **A** *be an algebra without zero divisors $n$-dimensional over $F_q$. There exists an integer $\nu(n) \leq B(n)$ depending only on $n$, so that the following condition holds: If $q > \nu(n)$ then the zero-divisor hypersurfaces of* **A** *are reducible.*

An estimate of the constant $A(n, d, r)$ in the Lang–Weil inequality would give an upper bound for $\nu(n)$. We know neither general results nor examples that suggest a significant lower bound for $\nu(n), n \geq 4$.

## Section 3

Let $\mathbf{A}(F, s, t, c)$ be the algebra whose multiplication is given by the bilinear map

$$f(x, y) = xy - cx^{\alpha t}y^{\alpha s}, \quad c \in F - 0, \quad 0 \leq s, t \leq n - 1. \tag{31}$$

LEMMA 20. *The zero-divisor hypersurfaces of* $\mathbf{A}(F, s, t, c)$ *are*

$$\Lambda : L(x) = \begin{cases} \prod_{i=0}^{n-1} (x - cx^{\alpha^t})^{\alpha^i} = 0, & s = 0, \\ \prod_{\nu=0}^{d-1} \left[ \prod_{h=0}^{l-1} x^{\alpha^{hd}} - \prod_{h=0}^{l-1} c^{\alpha^{hd}} \prod_{h=0}^{l-1} x^{\alpha^{hd+t}} \right]^{\alpha^\nu} = 0, & s \neq 0, \end{cases} \tag{32}$$

$d = \text{G.C.D.}(n, s), \quad n = ld;$

$$\text{P} : R(y) = \begin{cases} \prod_{i=0}^{n-1} (y - cy^{\alpha^s})^{\alpha^i} = 0, & t = 0, \\ \prod_{\nu'=0}^{d'-1} \left[ \prod_{h=0}^{l'-1} x^{\alpha^{hd'}} - \prod_{h=0}^{l'-1} c^{\alpha^{hd'}} \prod_{h=0}^{l'-1} x^{\alpha^{hd'+s}} \right]^{\alpha^{\nu'}} = 0, & t \neq 0, \end{cases} \tag{33}$$

$d' = \text{G.C.D.}(n, t), \quad n = l'd'.$

*Proof.* If $s = 0$, then $A(l_0(x), l_1(x), \ldots, l_{n-1}(x)) = D(x - cx^{\alpha t})$ (cf. (4)).

If $s \neq 0$, then putting $s = rd$ and using Remark 15, we have

$$L(x) = \prod_{\nu=0}^{d-1} \det[D_l(x) + D_l(-cx^{\alpha^t}) J_l^r]^{\alpha^\nu},$$

$$\det[D_l(x) + D_l(-cx^{\alpha^t}) J_l^r] = \prod_{h=0}^{l-1} x^{\alpha^{hd}} + (-1)^{r(l-r)+l} \prod_{h=0}^{l-1} c^{\alpha^{hd}} \prod_{h=0}^{l-1} x^{\alpha^{hd+t}}.$$

Moreover, $\text{G.C.D.}(r, l) = 1$ implies that $r(l - r) + l$ is odd.

The second statement is proved similarly.

Using Remark 12, from (32) and from (33) we deduce the equations of the hypersurfaces $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ of $\mathbf{A}(F, s, t, c)$:

$$\overline{\Lambda} : \overline{L}(z_0, z_1, \ldots, z_{n-1}) = \begin{cases} \prod_{i=0}^{n-1} (z_i - c^{\alpha^i} z_{i+t}) = 0, & s = 0, \\ \prod_{\nu=0}^{d-1} \left[ \prod_{h=0}^{l-1} z_{hd+\nu} - \prod_{h=0}^{l-1} c^{\alpha^{hd+\nu}} \prod_{h=0}^{l-1} z_{hd+\nu+t} \right] = 0, & s \neq 0, \end{cases} \tag{34}$$

$d = \text{G.C.D.}(n, s), \quad n = ld;$

$$\overline{\mathrm{P}} : \overline{R}(z_0, z_1, \ldots, z_{n-1}) = \begin{cases} \prod_{i=0}^{n-1} (z'_i - c^{\alpha^i} z'_{i+s}) = 0, & t = 0, \\ \prod_{\nu=0}^{d-1} \left[ \prod_{h=0}^{l'-1} z'_{hd'+\nu} - \prod_{h=0}^{l'-1} c^{\alpha^{hd'+\nu}} \prod_{h=0}^{l'-1} z'_{hd'+\nu+s} \right] = 0, & t \neq 0, \end{cases} \tag{35}$$

$d' = \text{G.C.D.}(n, t), \quad n = l'd'.$

*The indices of the variables $z$ and $z'$ in* (34) *and* (35) *must be evaluated* mod $n$.

LEMMA 21. *Let* $0 \leq i, j \leq n-1, d = \text{G.C.D.}(n, i)$ *and* $n = ld$.

(a) *The elements* $ha + k, h = 0, 1, \ldots, l-1, k = 0, 1, \ldots, d-1$, *with* $a = d$ *or* $a = i$, *form a complete system* mod $n$

(b) $xd = j + hd (\text{mod } n), 0 \leq h \leq l-1$ *has exactly one solution* $x \in \{0, 1, \ldots, l-1\}$ *if and only if* $d$ *divides* $j$.

*Proof.* Cf. [6, ch.V].

PROPOSITION 22. *If*

$$N(c) = cc^{\alpha} \ldots c^{\alpha^{n-1}} \neq 1, \tag{36}$$

*then* $\mathbf{A}(F, s, t, c)$ *has no zero divisors.*

*Proof.* The conclusion is trivial if $t = s = 0$. Suppose $s \neq 0$.

$\mathbf{A}(F, s, t, c)$ has zero divisors if and only if there exists $x_0 \in F - 0$ so that $L(x_0) = 0$. In this case (cf. Lemma 20)

$$\prod_{h=0}^{l-1} x_0^{\alpha^{hd+\nu}} = \prod_{h=0}^{l-1} c^{\alpha^{hd+\nu}} \prod_{h=0}^{l-1} x_0^{\alpha^{hd+\nu+t}}, \quad \nu = 0, 1, \ldots, d-1.$$

Hence multiplying over all $\nu$, we deduce (cf. Lemma 21(b))

$$\prod_{i=0}^{n-1} x_0^{\alpha^i} = \prod_{i=0}^{n-1} c^{\alpha^i} \prod_{i=0}^{n-1} x_0^{\alpha^i}, \quad x_0 \neq 0,$$

in contradiction with the hypothesis.

If $t \neq 0$, an analogous argument with $R(y) = 0$ instead of $L(x) = 0$ concludes the proof.

PROPOSITION 23. *If* $|K| > 2$, *then there exists some element* $c \in F - 0$ *satisfying condition* (36).

*Proof.* When the cardinality of $K$ is infinite it is sufficient to observe that the equation $x^n - 1 = 0$ has at most $n$ roots in $K$.

If $|K| = q > 2$, then the equation $x^{1+q+\cdots+q^{n-1}} = 1$ has at most $1 + q + \cdots + q^{n-1} < q^n - 1$ roots in $F_{q^n} - 0$.

When one of the integers $s$ or $t$ is prime to $n$, condition (36) is also necessary in order for $\mathbf{A}(F, s, t, c)$ to have no zero divisors. In fact, if, for example, G.C.D.$(n, s) = 1$, then $l = n$ and

$$\Lambda : L(x) = \prod_{h=0}^{n-1} x^{\alpha^h} \left(1 - \prod_{h=0}^{n-1} x^{\alpha^h}\right) = 0.$$

If $\mathbf{A}(F, s, t, c) = (V, f)$ has no zero divisors, then $\mathbf{D}_a(F, s, t, c) = (V, f')$, $f'(x, y) = f(x^{\rho_a^{-1}}, y^{\lambda_a^{-1}})$ is a division algebra isotopic to $\mathbf{A}(F, s, t, c)$ for every $a \in V - 0$ (cf. Proposition 9). Moreover, different values of $a$ give algebras isotopic to one another. Hence is not restrictive to suppose $a = 1$.

For simplicity we pose $\mathbf{D}_1(F, s, t, c) = \mathbf{D}(F, s, t, c)$ and we call these division algebras *twised fields*.

We can determine $f(x^{\rho_1^{-1}}, y^{\lambda_1^{-1}})$ explicitly, observing that if $0 \leq i \leq n - 1$ and $N(c) \neq 1$, then the inverse of $\varepsilon : V \to V, x \mapsto x - cx^{\alpha^i}$ is the automorphism

$$\varepsilon^{-1} : x \mapsto c'(x + cx^{\alpha^i} + cc^{\alpha^i} x^{\alpha^{2i}} + \cdots + cc^{\alpha^i} \ldots c^{\alpha^{(l-2)i}} x^{\alpha^{(l-1)i}}),$$

with $d = \text{G.C.D.}(n, i), ld = n$ and $c' = (1 - cc^{\alpha^i} \ldots c^{\alpha^{(l-1)i}})^{-1}$ (cf. also Lemma 21(a)).

The algebras $\mathbf{A}(F_{q^n}, s, t, c)$ without zero divisors and the twisted fields $\mathbf{D}(F_{q^n}, s, t, c)$ have been introduced and studied by Albert in [1], [2] and [3]. In those papers, Results 24 and 25 are proved.

RESULT 24. *If*

$$c \neq k^{q-1}, \quad k \in F_{q^n} - 0, \tag{37}$$

*then* $\mathbf{A}(F_{q^n}, s, t, c)$ *has no zero divisors.*

We remark that condition (37) is equivalent to (36) with $c \neq 0$. In fact there are $(q^n - 1)(q-1)^{-1}$ elements $x = k^{q-1}$, $k \in F_{q^n} - 0$. Moreover, every one of them is a root of the equation $x^{1+q+\cdots+q^{n-1}} = 1$.

RESULT 25. *Let* $\mathbf{D}'$ *be a division algebra isotopic to a twisted field* $\mathbf{D}(F_{q^n}, s, t, c)$. *Then* $\mathbf{D}'$ *is isomorphic to a twisted field* $\mathbf{D}(F_{q^n}, s, t, c')$.

*Remark 26.* Result 25 is valid for twisted fields over any field $K$ because the proof given in [3] does not require that $K$ be a finite field.

LEMMA 27. *If* $c' \neq 0$ *then the polynomial*

$$g(z_{i_0}, z_{i_1}, \ldots, z_{i_{2l-1}}) = \prod_{h=0}^{l-1} z_{i_h} + c' \prod_{h=0}^{l-1} z_{i_{l+h}} \in F[z_0, z_1, \ldots, z_{n-1}],$$

$$2 \leq 2l \leq n,$$

*is absolutely irreducible.*

*Proof.* Put $g_0 = \prod_{k=0}^{l-1} z_{i_k}$, $g_1 = c' \prod_{h=0}^{l-1} z_{i_{l+h}}$, then $g = g_0 z_{i_0} + g_1 \in F'[z_{i_0}]$, $F' = F[z_{i_1}, z_{i_2}, \ldots, z_{i_{2l-1}}]$. $F'$ is factorial and $g_0, g_1$ are relatively prime.

PROPOSITION 28. *If* $d$ *does not divide* $t$, *the hypersurface* (34) *is the union of* $d$ *hypersurfaces of degree* $l$, *absolutely irreducible and conjugate in an extension* $F'$ *over* $K$, $[F' : K] = d$. *If* $d | t$ *then* (34) *is the union of the hyperplanes*

$$z_i = 0, i = 0, 1, \ldots, n-1, \tag{38}$$

*conjugate in* $F$ *over* $K$, *or coincides with the entire space according to whether*

$$N_d(c) = \prod_{h=0}^{l-1} c^{\alpha^{hd}} \neq 1 \tag{39}$$

*or* $N_d(c) = 1$. *The analagous result holds for the hypersurface* (35).

*Proof.* When $s = 0$, the hypersurface $\overline{\Lambda}$ is the union of the linear components $\overline{\Lambda}_i : z_i - c^{\alpha^i} z_{i+t} = 0, i = 0, 1, \ldots, n-1$, whose equation becomes $(1 - c^{\alpha^i}) z_i = 0$ if $d$ divide $t$.

If $s \neq 0$, then $\overline{\Lambda}$ is the union of the components

$$\overline{\Lambda}_\nu : \prod_{h=0}^{l-1} z_{hd+\nu} - \prod_{h=0}^{l-1} c^{\alpha^{hd+\nu}} \prod_{h=0}^{l-1} z_{hd+\nu+t} = 0, \quad \nu = 0, 1, \ldots, d-1,$$

that are absolutely irreducible if and only if $d$ does not divide $t$ (cf. Lemmas 21(b) and 27).

When $d$ divides $t$ we have (cf. Lemma 21)

$$\overline{\Lambda} : \prod_{\nu=0}^{d-1} (1 - N_d(c))^{\alpha^\nu} \prod_{i=0}^{n-1} z_i = 0.$$

COROLLARY 29. *Both the hypersurfaces* $\overline{\Lambda}$ *and* $\overline{\mathrm{P}}$ *of the algebra* $\mathbf{A}(F, s, t, c)$ *are the union of the hyperplanes* (38) *if and only if*

$$d' = d \tag{40}$$

*and* (39) *is satisfied.*

We remark that (39) is a necessary and sufficient condition for $\mathbf{A}(F, s, t, c), d' = d$ to have no zero divisors.

We verify easily that the hypersurfaces $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ of the algebra (field) $\mathbf{F}$ are also the union of the hyperplanes (38).

Finally we remark that if $n$ is a prime, both hypersurfaces $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ of an algebra $\mathbf{A}(F, s, t, c)$ without zero divisors, are the unions of linearly independent hyperplanes conjugate in $F$ over $K$. In fact, in this case $t = 0$ or $s = 0$, unless $d' = d = 1$.

PROPOSITION 30. *If the hypersurfaces* $\overline{\Lambda}$ *and* $\overline{\mathrm{P}}$ *of an algebra* $\mathbf{A}(V, f)$ *are the unions of the hyperplanes* (38), *then* $\mathbf{A} \approx \mathbf{F}$ *or* $\mathbf{A} \approx \mathbf{A}(F, s, t, c)$, *where* $s, t, c$ *satisfy* (39) *and* (40).

*Proof.* If $n = 2$ the conclusion follows from a simple calculation. Hence, suppose $n \geq 3$.

We divide the proof into three parts.

*First part*

*In this part we prove that there is a matrix* $M \in \mathrm{Auc}(F/K)$ *such that*

$$M\,{}^t(\overline{f}_0\ \overline{f}_1 \dots \overline{f}_{n-1}) = {}^t(\overline{p}_0\ \overline{p}_1 \dots \overline{p}_{n-1}), \tag{41}$$

*where*

$$\overline{p}_r(z_0, \dots, z_{n-1}, z'_0, \dots, z'_{n-1})$$

$$= \left( \sum_{j=1}^{n-1} a_j^{\alpha^r} z'_{j+r} \right) z_{i+r} + z'_r \left( \sum_{k=0}^{n-1} b_k^{\alpha^r} z_{k+r} \right), r = 0, 1, \dots, n-1, \tag{42}$$

$i \in \{0, 1, \dots, n-1\}$ *and at least one coefficient* $a_j$ *is different from zero.*

By hypothesis, functions (26) give a rational map of the hypersurface

$$\sum_{r=0}^{n-1} z'_r = 0 \tag{43}$$

into

$$\sum_{r=0}^{n-1} z_r = 0. \tag{44}$$

Hence if we fix a non-trivial $n$-tuple $(z'_0, z'_1, \ldots, z'_{n-1})$ in which $z'_0 = 0$, then from (26) we obtain a linear system of equations in the unknowns $z_0, z_1, \ldots, z_{n-1}$ with a non-trivial solution in which at least one component $z_i$ is equal to zero. Therefore, there exists a matrix $M' \in \mathrm{GL}(n, F)$ so that

$$M' {}^t(\overline{f}'_0\ \overline{f}'_1 \ldots \overline{f}'_{n-1}) = {}^t(g'_0\ g'_1 \ldots g'_{n-1}), \tag{45}$$

where

$$\overline{f}'_r = f_r(z_0, \ldots, z_{n-1}, 0, z'_1, \ldots, z'_{n-1})$$

and

$$g'_r = g'_r(z_0, \ldots, z_{n-1}, z'_1, \ldots, z'_{n-1}), \quad r = 0, 1, \ldots, n-1,$$

are linear functions in $z_0, z_1, \ldots, z_{n-1}$ and in $z'_1, z'_2, \ldots, z'_{n-1}$. Moreover, there is at least one index $k \in \{0, 1, \ldots, n-1\}$ such that

$$g'_k = z_i \left( \sum_{j=0}^{n-1} a_j z'_j \right)$$

where some coefficient $a_j \in F$ is different from zero.

If we set

$$M' {}^t(\overline{f}_0\ \overline{f}_1 \ldots \overline{f}_{n-1}) = {}^t(g_0\ g_1 \ldots g_{n-1}), \tag{46}$$

then obviously

$$g'_r = g_r(z_0, z_1, \ldots, z_{n-1}, 0, z'_1, \ldots, z'_{n-1}), \quad r = 0, 1, \ldots, n-1.$$

In particular

$$g_k = z_i \left( \sum_{j=1}^{n-1} a_j z'_j \right) + z'_0 \left( \sum_{k=0}^{n-1} b_k z_k \right). \tag{47}$$

If $\chi$ is the automorphism of $F[z_0, z_1, \ldots, z_{n-1}, z'_0, z'_1, \ldots, z'_{n-1}]$ defined by

$$\chi(q(z_0, z_1, \ldots, z_{n-1}, z'_0, z'_1, \ldots, z'_{n-1})) = q^{\alpha}(z_1, z_2, \ldots, z_{n-1}, z_0, z'_1, z'_2, \ldots, z'_{n-1}, z'_0),$$

then $\chi^n = 1$ and (cf. (26))

$$\chi(\overline{f}_i) = \overline{f}_{i+1}, \quad i = 0, 1, \ldots, n-1, \ (\overline{f}_n = \overline{f}_0). \tag{48}$$

Acting on the polynomials $\overline{f}'_r$ and $g'_r$ by the automorphism $\chi$, from (45) we get analogous relations fixing $(z'_0, z'_1, \ldots, z'_{n-1}) \neq 0$ and $z'_1 = 0$:

$$\begin{aligned} &M'^{\alpha} J\, {}^t(\overline{f}''_0\ \overline{f}''_1 \ldots \overline{f}''_{n-1}) = {}^t(\chi(g'_0)\ \chi(g'_1) \ldots \chi(g'_{n-1})), \\ &\overline{f}''_r = f_r(z_0, z_1, \ldots, z_{n-1}, z'_0, 0, \ldots, z'_{n-1}) \end{aligned} \tag{49}$$

(cf. also (48) and (3)).

Now if $(z'_0, z'_1, \ldots, z'_{n-1}) \neq 0$ and $z'_0 = z'_1 = 0$, then (45) and (49) coincide. Conseqently, there is a permutation matrix (12) such that $P(\sigma)M'^{\alpha}J = M'$.

From this, from (46) and from

$$M'^{\alpha} J\, {}^t(\overline{f}_0\ \overline{f}_1 \ldots \overline{f}_{n-1}) = {}^t(\chi(g_0)\ \chi(g_1) \ldots \chi(g_{n-1}))$$

we deduce

$$S = \{g_0, g_1, \ldots, g_{n-1}\} = \{\chi(g_0), \chi(g_1), \ldots, \chi(g_{n-1})\}.$$

By a simple calculation we prove that $g_k = \chi^s(g_k)$ if and only if

$$g_k = a_s z_i z'_s + a_s^{\alpha^s} z_{i+s} z'_0, \quad s = n/2. \tag{50}$$

In this case the condition

$$\sum_{i=0}^{n-1} c_i \overline{f}_i = g_k, \quad c_i \in F \quad \text{(cf. (46))},$$

implies

$$\sum_{j=0}^{s-1} c_j \overline{f}_j = a_s z_i z'_s \quad \text{or} \quad \sum_{j=0}^{s-1} c_j \overline{f}_j = a_s^{\alpha^s} z_{i+s} z'_0.$$

Hence we deduce (41) and (42) with

$$M = A(c_0, c_1, \ldots, c_{s-1}, 0, 0, \ldots, 0) \text{ or } M = A(0, 0, \ldots, 0, c_0^{\alpha^s}, c_1^{\alpha^s}, \ldots, c_{s-1}^{\alpha^s})$$

and

$$\overline{p}_r = a_s^{\alpha^r} z_{i+r} z'_{s+r}, \quad r = 0, 1, \ldots, n-1,$$

$i \in \{0, 1, \ldots, n-1\}, s = n/2, a_s \neq 0.$

If condition (50) is not satisfied, then $S = \{\chi^r(g_k) | r = 0, 1, \ldots, n-1\}$. Therefore, there is a permutation matrix (12) such that

$$P(\sigma')\, {}^t(g_0\ g_1 \ldots g_{n-1}) = {}^t(g_k\ \chi(g_k) \ldots \chi^{n-1}(g_k)).$$

From this and from (46) we deduce equations (41) and (42) with $M = P(\sigma')M'$ and $\overline{p}_r = \chi^r(g_k)$, where $g_k$ is given by (47).

Acting on the polynomials $\overline{f}_r$ and $\overline{p}_r$ by the automorphism $\chi$, from (41) we deduce

$$M^{\alpha} J\, {}^t(\overline{f}_0\ \overline{f}_1 \ldots \overline{f}_{n-1}) = J\, {}^t(\overline{p}_0\ \overline{p}_1 \ldots \overline{p}_{n-1})$$

and hence (cf. Proposition 4)

$$M = A(k_0, k_1, \ldots, k_{n-1}) \in \mathrm{Auc}(F/K). \tag{51}$$

*Second part*

*In this part we prove that*

$$\overline{p}_0 = a_h z_i z'_h + b_u z_u z'_0, \quad a_h \neq 0, \quad i \neq u, \quad h \neq 0. \tag{52}$$

*Moreover, if* $b_u \neq 0$, *then*

$$d = \mathrm{G.C.D.}(n, h) = d' = \mathrm{G.C.D.}(n, u - i) \tag{53}$$

*and*

$$\prod_{k=0}^{l-1} a_h^{\alpha^{kd}} + \prod_{k=0}^{l-1} b_u^{\alpha^{kd}} \neq 0 \ (ld = n). \tag{54}$$

Let $W = W(z_0, z_1, \ldots, z_{n-1})$ and $W' = W'(z'_0, z'_1, \ldots, z'_{n-1})$ be the coefficient matrices of the variables $z'_r$ and $z_r$ respectively, of the system

$$\overline{p}_r(z_0, z_1, \ldots, z_{n-1}, z'_0, z'_1, \ldots, z'_{n-1}) = 0, \quad r = 0, 1, \ldots, n-1. \tag{55}$$

From the hypothesis and from (41) it follows that

$$\det(W(z_0, z_1, \ldots, z_{n-1})) = w \prod_{r=0}^{n-1} z_r, \quad w \in F - 0, \tag{56}$$

and

$$\det(W'(z'_0, z'_1, \ldots, z'_{n-1})) = w' \prod_{r=0}^{n-1} z'_r, \quad w' \in F - 0. \tag{57}$$

If we fix $(0, z'_1, \ldots, z'_{n-1}) \neq 0$, then the corresponding linear system of equations (55) has some solution $(z_0, z_1, \ldots, z_{n-1}) \neq 0$. Hence $\operatorname{rank} W'(0, z'_1, \ldots, z'_{n-1}) \leq n - 1$.

Impose on the $n$-tuple $(0, z'_1, \ldots, z'_{n-1})$ the further condition $\Sigma_{j=1}^{n-1} a_j z'_j = 0$. The (cf. (42)) the equation $\bar{p}_0(z_0, z_1, \ldots, z_{n-1}, 0, z'_1, \ldots, z'_{n-1}) = 0$ turns into an identity and the rank of $W'$ decreases and becomes $\leq n - 2$. By a well-known derivation rule of the determinant, all the first-order partial derivatives of the function $\det(W')$ evaluated at the point $(0, z'_1, \ldots, z'_{n-1})$ are equal to zero. Hence $(0, z'_1, \ldots, z'_{n-1})$ is a singular point of the hypersurface $\det(W') = 0$ lying on the component $z'_0 = 0$. Since such points are the common points of $z'_0 = 0$ with the other linear components of $\det(W') = 0$, we have

$$\sum_{j=0}^{n-1} a_j z'_j = a_h z'_h, \quad h \neq 0, \quad a_h \neq 0.$$

In order to prove that

$$\sum_{k=0}^{n-1} b_k z_k = b_u z_u, \quad u \neq i,$$

we distinguish two cases: $b_k = 0, k = 0, 1, \ldots, i-1, i+1, \ldots, n-1$, and $b_u \neq 0$ for at least one index $u \neq i$.

In the first case $\bar{p}_0 = z_i(a_h z'_h + b_i z'_0), W' = D(a_h z'_h + b_i z'_0) J^i$ (cf. Section 1). Hence

$$\det(W') = \prod_{r=0}^{n-1} (a_h^{\alpha^r} z'_{h+r} + b_i^{\alpha^r} z'_r), \quad h \neq 0, \quad a_h \neq 0,$$

coincides with (57) if and only if $b_i = 0$.

Suppose $b_u \neq 0, u \neq i$.

If we fix $(z_0, z_1, \ldots, z_{n-1}) \neq 0, z_i = 0$ so that $\Sigma_{k=0}^{n-1} b_k z_k \neq 0$, then the corresponding linear system (55) has some non-trivial solution $(0, z'_1, \ldots, z'_{n-1})$. Arguing as above with $\operatorname{rank}(W)$ instead of $\operatorname{rank}(W')$, we get

$$B_{00} = \sum_{k=0}^{n-1} b_k z_k = b_i z_i + b_u z_u.$$

Hence (cf. also Proposition 5)

$$\det(W) = \prod_{\nu=0}^{d-1} W_\nu, \quad W_\nu = \prod_{k=0}^{l-1} B_{k\nu} + a^{\alpha^\nu} \prod_{k=0}^{l-1} z_{i+kd+\nu}, \tag{58}$$

where $d = \text{G.C.D.}(n,h), n = ld, B_{k\nu} = b_i^{\alpha^{kd+\nu}} z_{i+kd+\nu} + b_u^{\alpha^{kd+\nu}} z_{u+kd+\nu}$ and $a = \Pi_{k=0}^{l-1} a_h^{\alpha^{kd}}$.

For every $m \in \{0,1,\ldots,n-1\}$ there are $k_0 \in \{0,1,\ldots,l-1\}$ and $\nu_0 \in \{0,1,\ldots,d-1\}$ such that $z_m = z_{i+k_0 d+\nu_0}$ (cf. Lemma 21(a)).

If $d|(u-i)$, then (cf. Lemma 21) only the factor $W_{\nu_0}$ of (58) depends on the varible $z_m$. So (56) and (58) imply $z_m | \Pi_{k=0}^{l-1} B_{k\nu_0}$ and this condition is satisfied if and only if $b_i = 0$. Consequently, also condition (54) is satisfied.

Let $d' = \text{G.C.D}(n, u-i)$. Using Proposition 5 and Lemma 21, from (57) we deduce $d'|h$.

We complete the proof of the second part showing that (56) and (58) are incompatible if $d$ does not divide $u-i$.

In fact in this case there are two factors $W_\nu$ depending on a fixed variable $z_m : W_{\nu_0}$ and $W_{\nu_1}, m = u+k_1 d+\nu_1, k_1 \in \{0,1,\ldots,l-1\}, \nu_1 \in \{0,1,\ldots,d-1\}$. Hence $z_m$ must divide one of them. But this is impossible because $b_u \neq 0$ and the polynomial

$$b_i^{\alpha^{k_1 d+\nu_1}} \prod_{\substack{k=0 \\ k\neq k_1}}^{l-1} B_{k\nu_1} + a^{\alpha^{\nu_1}} \prod_{\substack{k=0 \\ k\neq k_1}}^{l-1} z_{i+kd+\nu_1}$$

is not identically zero.

*Third part*

Let $\mathbf{A}' = (V,p)$ be the algebra defined by

$$p(x,y) = a_h x^{\alpha^i} y^{\alpha^h} + b_u x^{\alpha^u} y,$$

where $a_h \neq 0, i \neq u, h \neq 0$. Moreover, if $b_u \neq 0$, conditions (53) and (54) are satisfied. Let $\beta_3 : V \to V, x \mapsto \Sigma_{r=0}^{n-1} k_r x^{\alpha^r}$ be the automorphism defined by the autocirculant matrix (51).

From the results of the first and second parts it follows that $\mathbf{A} = (V,f)$ is $(1,1,\beta_3)$-isotopic to an algebra $\mathbf{A}' = (V,p)$. Hence, to conclude, it is enough to verify that $\mathbf{A}'$ is $(\gamma_1,\gamma_2,\gamma_3)$-isotopic either to $\mathbf{F}$ or to an algebra $\mathbf{A}(F,s,t,c)$ with $s,t,c$ satisfying (39) and (40).

We easily prove that this condition is satisfied assuming $\gamma_1 : x \mapsto x^{\alpha^{n-i}}, \gamma_2 : y \mapsto y^{\alpha^{n-h}}, \gamma_3 : z \mapsto a_h^{-1} z$, $t = n+u-i$, $s = n-h$, $b_u a_h^{-1} = -c$.

COROLLARY 31. *It the hypersurfaces $\overline{\Lambda}'$ and $\overline{\mathrm{P}}'$ of an algebra $\mathbf{A}' = (V,f')$ without zero divisors are the unions of hyperplanes of $P_{n-1}(F)$, then either $\mathbf{A}' \approx \mathbf{F}$ or $\mathbf{A}' \approx \mathbf{A}(F,s,t,c)$ with $s,t,c$ satisfying conditions* (39) *and* (40).

*Proof.* The hypersurfaces $\Lambda'$ and $\mathrm{P}'$ have no $K$-rational points. Hence each one of them is the union of $n$ linearly independent hyperplanes conjugate in $F$ over $K$. In other words, $\Lambda'$ and $\mathrm{P}'$ are projectively equivalent to $\Phi : \Sigma_{r=0}^{n-1} x^{\alpha^r} = 0$.

From Propositions 14.1 and 14.2 we deduce that $\mathbf{A}'$ is isotopic to an algebra $\mathbf{A}$ whose zero-divisor hypersurfaces coincide with $\Phi$.

COROLLARY 32. *Let* $\mathbf{D}$ *be a* $n$*-dimensional division* $K$*-algebra and let* $\overline{\Lambda}, \overline{\mathrm{P}}$ *be its zero-divisor hypersurfaces. If* $\overline{\Lambda}$ *and* $\overline{\mathrm{P}}$ *are the unions of hyperplanes of* $P_{n-1}(F)$*, then either* $\mathbf{D} = \mathbf{F}$ *or* $\mathbf{D} = \mathbf{D}(F, s, t, c)$.

*Proof.* Corollary 31 implies that either $\mathbf{D} \approx \mathbf{A}(F, s, t, c)$ or $\mathbf{D} \approx \mathbf{F}$. In the first case, $\mathbf{D} \approx \mathbf{D}(F, s, t, c)$ (cf. Proposition 9) and so $\mathbf{D} \cong \mathbf{D}(F, s, t, c')$ (cf. Result 25 and Remark 26). In the other case, $\mathbf{D} \cong \mathbf{D}' = (V, f'), f'(x, y) = kxy, k \in \mathbf{F} - 0$ (cf. Proposition 9). Moreover, $\chi : \mathbf{F} \to \mathbf{D}', x \mapsto k^{-1}x$, is an algebra isomorphism.

COROLLARY 33. *If* $n$ *is prime and if* $q$ *is large enough, then an* $n$*-dimensional division* $F_q$*-algebra is either a field or a twisted field.*

*Proof.* If $q > \nu(n)$, then (cf. Corollary 19) the zero-divisor hypersurfaces $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ of an $n$-dimensional $F_q$-algebra without zero divisors, are reducible. As $n$ is prime, Proposition 16 implies that $\overline{\Lambda}$ and $\overline{\mathrm{P}}$ are the unions of hyperplanes of $P_{n-1}(F_{qn})$. The conclusion follows from this and from previous corollaries.

When $n = 3$ the statement of Corollary 33 is verified for every $q$ (cf. Proposition 18). Hence we find again the main result proved in [13].

For $n = 5$, Corollary 33 proves the conjecture of Kaplansky formulated in [10].

Some of the above results are also true when a less restrictive condition is imposed on the Galois group $\mathrm{Gal}(F/K)$ provided that we can express the multiplication of the algebras $\mathbf{A}$ in terms of the multiplication of $\mathbf{F}$ and of the automorphisms lying in $\mathrm{Gal}(F/K)$. This subject will probably be treated in a future note.

## References


1. Albert, A. A.: On nonassociative division algebras, *Trans. Amer. Math. Soc.* **72** (1952), 296–309.
2. Albert, A. A.: Generalized twisted fields, *Pacific J. Math.* **11** (1961), 1–8.
3. Albert, A. A.: Isotopy for generalized twisted fields, *An. Acad. Brasil. Cienc.* **33** (1961), 265–275.
4. Dembowski, P.: *Finite Geometries*, Springer, Berlin, Heidelberg, New York, 1968.
5. Dickson, L. E.: *Linear Groups which an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.
6. Hardy, G. H. and Wright, E. M.: *An introduction to the Theory of Numbers*, Clarendon, Oxford, 1979.
7. Hasse, H: Zur Theorie der abstrakten elliptischen Funktionenkörper, *J. reine angew. Math.* **175** (1936), 55–62, 69–88, 193–208.
8. Jacobson, N.: *Basic Algebra I*, Freeman, San Francisco, 1974.
9. Kaplansky, I: Three-dimensional division algebras, *J. Algebra* **40** (1976), 384–391.
10. Kaplansky, I.: Three-dimensional division algebras II, *Houston J. Math.* **1** (1975), 63–79.
11. Lang, S. and Weil, A.: Number of points of varieties in finite fields, *Amer. J. Math.* **76** (1954), 819–827.

12. Menichetti, G.: Algebre tridimensionali su un campo di Galois, *Ann. Mat. Pura Appl.* **97** (1973), 283–301.
13. Menichetti, G.: On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field, *J. Algebra* **47** (1977), 400–410.
14. Menichetti, G.: Roots of affine polynomials, in: Combinatorics '84, *Ann. Discrete Math.* **30** (1986), 303–310.
15. Pele, R. L.: Some remarks on the vector subspaces of cyclic Galois extensions, *Acta Math. Acad. Sci. Hungar.* **20** (1969), 237–240.
16. Serre, J. P.: *Cours d'aritmétiques*, Presses Univ. de France, Paris, 1970.
17. Vaughan, T. P.: Polynomials and linear transformations over finite fields, *J. reine angew. Math.* **267** (1974), 179–206.
18. Weil, A.: *Sur les courbes algébriques et les variétés qui s'en deduisent*, Hermann, Paris, 1948.