HOUSTON JOURNAL OF MATHEMATICS, Volume 1, No. 1, 1975.

THREE-DIMENSIONAL DIVISION ALGEBRAS. II

Irving Kaplansky

1. Introduction. In the preceding paper [7] I reviewed Dickson's results on three-dimensional commutative division algebras and then proved them again in an "algebraically closed" style, as opposed to Dickson's "rational" style. Since then I have pushed the algebraically closed method further, so as to cover algebras in which all commutators are scalar. In §2 I give an appropriate structure theorem over an algebraically closed field; then in §4 the transition to division algebras is made by Galois descent.

Now it happens that in the three-dimensional case the twisted fields introduced by Albert in [1] have the property that commutators are scalar. This property is lost in the more general twisted fields of [2]. (The still more general twisted fields of [3] do not add additional division algebras in the three-dimensional case.) The main result of this paper may be stated as follows: a three-dimensional division algebra over a finite field in which all commutators are scalar is a twisted field in the sense of [1].

In the rest of the paper I record the remaining observations that I have been able to make concerning three-dimensional division algebras.

2. Dickson algebras in which commutators are scalar. I repeat two definitions from [7], inserting the adjective "right" to take account of possible non-commutativity. Let an algebra A have basis $u_1,\ldots,u_n$. The *right norm form* of A (relative to the basis) is the determinant of the right multiplication by the general element $\Sigma x_i u_i$ (the x's being indeterminates). A is a *right Dickson algebra* if its right norm form is a product of linearly independent linear factors; this is independent of the choice of basis. The concepts of left and two-sided Dickson algebra are presumably self-explanatory.

In Theorems 1 and 2 below it will turn out that, in the circumstances of those theorems, assumption of the Dickson property on one side implies it on the other. But this is not always true. Let A have basis 1, u, v with $u^2 = u$, $v^2 = 0$, $uv = 1 - u + v$, $vu =$

1 - u. The right norm form of A is $x(x + y)(x - z)$ and the left norm form is

$$(x + y)(x^2 + xy - xz - 2yz),$$

with the second factor irreducible for characteristic $\neq 2$.

Before stating the first theorem I exhibit the target algebras. In a given field F fix an element b satisfying $b \neq 0$, 1, or ½ and $b^2 - b + 1 \neq 0$. Define an algebra E(b) as having a basis 1, u, v with multiplication table $u^2 = u$, $v^2 = v$, $uv = a + b(u + v)$, $vu = p + b(u + v)$, where

(1) $a = b^3/(1 - 2b)$, $p = (b^3 + b^2 - b)/(1 - 2b)$.

Note that the mapping interchanging u and v induces an involution of E(b).

Some properties of E(b) will now be noted, with verification left to the reader. E(b) is non-commutative and simple. Its right norm form is

(2) $(x + y + bz)(x + by)(x + z)$,

and its left norm form is

(3) $(x + by + z)(x + y)(x + bz)$.

Thus E(b) is a two-sided Dickson algebra. All commutators in E(b) are scalar multiples of 1 (it is enough to glance at uv - vu). There are eight idempotents in E(b): 0, 1, u, 1 - u, v, 1 - v, u + v - b, 1 + b - u - v. Other choices of basis are easily inspected and one concludes that E(b) and E(b′) are isomorphic if and only if $b = b'$ or $b' = 1 - b$.

THEOREM 1. *Let K be an algebraically closed field. Let A be a three-dimensional algebra over K with 1, which is non-commutative, right Dickson, and has the property that every commutator is a scalar multiple of 1. Then A is isomorphic to E(b) for some b in K.*

REMARK. For the application to division algebras the full force of Theorem 1 is not needed. By using the results in §5 one could restrict the discussion to just Case III. But Theorem 1, as presented, is perhaps of independent interest.

PROOF. We follow the pattern of the proof of Theorem 2 in [7], using a provisional basis 1, u, v, with $u^2 = \epsilon u$ ($\epsilon = 0$ or 1), $v^2 = d + eu + fv$. Since uv - vu is a scalar multiple of 1 we can write

$$uv = a + bu + cv, \quad vu = p + bu + cv.$$

As in [7], the condition for inability to change v so as to satisfy $v^2 = \eta v$ ($\eta = 0$ or 1) is

(4) $\epsilon - 2c = 2b - f = 0$, $e \neq 0$.

We make a division into cases in essentially the same way as in [7], but there are

some differences of detail. We use seven cases instead of six; for ease of comparison we number the new case as 0. Another difference is the introduction of still another case distinction cutting across the others: the distinction between $b = c$ and $b \neq c$. Our first observation is that if $b \neq c$ holds we are entitled to assume in addition that $b + c \neq 1$. Here is the reason. If we examine the result of changing basis by replacing v by $1 - v$ we find that c is unchanged and b is replaced by $1 - b$. Suppose then that $b + c = 1$. After this change of basis the new b and c are equal. Thus $b + c = 1$ can be reverted to $b = c$. The upshot of this is that whenever we encounter $b + c = 1$ we can pass right on to $b = c = \frac{1}{2}$. This will come up twice, and no other use will be made of this sub-distinction.

We proceed to the first four cases, labelled 0 and I-III. In these cases we have $v^2 = \eta v$ with $\eta = 0$ or 1 (in addition to the permanent normalization $u^2 = \epsilon u$ with $\epsilon = 0$ or 1). The right norm form of A works out to be

(5) $x^3 + (\epsilon + c)x^2y + (\eta + b)x^2z + \epsilon cxy^2 + \eta bxz^2 + (-ac + cp - \epsilon p)y^2z + (ab - bp - \eta a)yz^2 + (\epsilon\eta - a - p)xyz.$

Note that there are no terms in y^3 or z^3 in (5). A factorization of (5) into linear factors can normally be put in the form

(6) $(x + Py + Qz)(x + Ry)(x + Sz).$

Now comes our first case.

CASE 0. Assume that the factorization of (5) into linear factors cannot be put in the form (6). It will then have to be the case that (5) is divisible by x and that there are no terms in y^2z or yz^2:

(7) $-ac + cp - \epsilon p = ab - bp - \eta a = 0.$

Furthermore, if either ϵ or η vanishes then again the factorization will have the desired form (6). Hence $\epsilon = \eta = 1$ may be assumed. Subtract the two expressions in (7) and cancel $a - p$ (which is non-zero by non-commutativity). The result is $b + c = 1$. This implies (as noted above) that we have $b = c = \frac{1}{2}$. Add the equations in (7) to get $a + p = 0$. The expression (5) now reads

$$x(x^2 + 3/2xy + 3/2xz + 1/2y^2 + 1/2z^2 + yz)$$

and does not factor further.

With case 0 finished, from now on the factorization (6) is in effect. On equating coefficients in (5) and (6) we get seven equations.

(8) $P + R = \epsilon + c$,

(9) $PR = \epsilon c$,

(10) $Q + S = \eta + b$,

(11) $QS = \eta b$,

(12) $PRS = -ac + cp - \epsilon p$,

(13) $QRS = ab - bp - \eta a$,

(14) $RS + PS + QR = \epsilon\eta - a - p$.

We are able to treat the next two cases simultaneously and dispose of them quickly. (These are listed as two cases rather than one only to facilitate comparison with [7].) The assumption is that either ϵ or η vanishes; by symmetry it might as well be η.

I-II. $\eta = 0$. Since (11) vanishes, so does (13). This gives $b = 0$, since $a \neq p$ by non-commutativity. Then (10) and (11) yield $Q = S = 0$. But this implies that z does not appear in (6), contradicting the assumed linear independence of the factors.

III. $\epsilon = \eta = 1$. Equations (8) and (9) tell us that P and R equal 1 and c in some order; likewise (10) and (11) identify the pairs Q, S and 1, b. This gives four subcases which reduce to three by symmetry.

(a) $P = Q = 1$, $R = c$, $S = b$. Equations (12)-(14) become

(15) $bc = -ac + cp - p$,

(16) $bc = ab - bp - a$,

(17) $bc + b + c = 1 - a - p$.

On subtracting (15) and (16) and cancelling $a - p$ we get $b + c = 1$. Again we pass to $b = c = \frac{1}{2}$. Now (15) yields $a + p = -\frac{1}{2}$. This contradicts (17).

(b) $R = S = 1$, $P = c$, $Q = b$. Equations (12)-(14) become

(18) $c = -ac + cp - p$,

(19) $b = ab - bp - a$,

(20) $1 + c + b = 1 - a - p$.

On subtracting (20) from the sum of (18) and (19) we are led to $b = c$. Then by subtracting (19) from (18) and again cancelling $a - p$ we get $b = \frac{1}{2}$. So $b = c = \frac{1}{2}$. But now the factors in (6) are linearly dependent.

(c) $P = 1$, $R = c$, $S = 1$, $Q = b$. Equations (12)-(14) become

(21) $c = -ac + cp - p$,

(22) $bc = ab - bp - a$,

(23) $c + 1 + bc = 1 - a - p$.

Again subtraction of (23) from the sum of (21) and (22) leads to $b = c$. We rule out $b = \frac{1}{2}$ just as in (b). On solving (21) and (22) for a and p we get (1). The possibilities $b = 0$ and $b = 1$ are ruled out since they imply $a = p$. We cannot have $b^2 - b + 1 = 0$, since that makes the factors of (6) linearly dependent. We have reached the algebra E(b).

In the rest of the proof of Theorem 1 we have to exclude the possibilities that arise on assuming (4).

IV. Assume (4) and characteristic 2. Then ϵ has to be 0 and we have $f = 0$. We distinguish two subcases.

(a) $c = 0$. We can normalize v so that $v^2 = u$.

The right norm form is

(24) $x^3 + bx^2z + az^3 + (a + p)byz^2 + (a + p)xyz$.

We examine (24) for singularities. The partial derivative with respect to y is

(25) $(a + p)bz^2 + (a + p)xz$.

We have $a + p \neq 0$ by non-commutativity. So the vanishing of (25) entails $z = 0$ or $x = bz$. From $z = 0$ we get $x = 0$ by (24). From $x = bz$ we get $az^3 = 0$ by (24). Now if $a = 0$ then (24) becomes $(x + bz)(x^2 + pyz)$ and this factors no further since $p \neq 0$. So $a \neq 0$, and hence $x = bz$ implies $z = 0$. In sum we find only one singularity (given by $x = z = 0$) instead of the three required if (24) is to factor into linearly independent linear factors.

(b) $c \neq 0$. Right-multiplication by u has c as a simple characteristic root. A corresponding characteristic vector t can serve as a new choice for a third basis vector, replacing v. Then $tu = ct$, and ut has the form $h + ct$ where h is a non-zero scalar. Since v^2 is a linear combination of 1 and u, the same is true of t^2. We can therefore normalize t^2 to be $d + u$. The right norm form is then

$$x^3 + cx^2y + (c + d)xz^2 + hz^3 + hxyz + chy^2z + cdyz^2.$$

Set the three partial derivatives equal to 0:

(26) $x^2 + (c + d)z^2 + hyz = 0$,

(27) $cx^2 + hxz + cdz^2 = 0$,

(28) $hz^2 + hxy + chy^2 = 0$.

If $z = 0$ we get $x = 0$ from (27) and then $y = 0$ from (28). So we can take $z = 1$. Equation (27) has two roots for x. Each leads to a unique y by (26). We lack three singularities.

V. Assume (4), characteristic $\neq 2$ and $\epsilon = 0$. The procedure in [7] can be repeated nearly verbatim. We have $c = 0$ and $f = 2b$. Normalize v so that $d = 0$, $e = 1$ (this can be accomplished by adding an appropriate scalar to v). Take $t = v - b$ as a new choice for a third basis element. Then $ut = a$, $tu = p$, $t^2 = b^2 + u$. The right norm form is

(29) $x^3 - (a + p)xyz - b^2xz^2 + az^3$.

The possibility of factoring (29) can be dismissed at a glance as in [7], because of the unique term involving y.

VI. Assume (4), characteristic $\neq 2$, and $\epsilon = 1$. Then $c = \frac{1}{2}$. Right-multiplication by u has characteristic roots 0, 1, and $\frac{1}{2}$. We take $tu = \frac{1}{2}t$, and $ut = h + \frac{1}{2}t$ follows. Since $b = 0$ and $f = 2b$, we have $f = 0$, and the normalization $t^2 = d + u$ is feasible. The right norm form is

$$x^3 + 3x^2y/2 + \tfrac{1}{2}xy^2 - (d + \tfrac{1}{2})xz^2 - \tfrac{1}{2}dyz^2 + hz^3 - \tfrac{1}{2}hy^2z - hxyz.$$

We assume a factorization

$$(x + Py + Qz)(x + Ry + Tz)(x + Sz).$$

This leads to eight equations (the last from the missing term x^2z).

(30) $P + R = 3/2$,

(31) $PR = \frac{1}{2}$,

(32) $QT + S(T + Q) = -d - \frac{1}{2}$,

(33) $S(PT + QR) = -\frac{1}{2}d$,

(34) $QTS = h$,

(35) $PRS = -\frac{1}{2}h$,

(36) $PT + QR + S(P + R) = -h$,

(37) $Q + T + S = 0$.

From (31) and (35) we get $S = -h$. From (34), $Qt = -1$. From (37), $Q + T = h$. Putting this into (32) yields

(38) $h^2 = d - \frac{1}{2}$

Using (30) we find from (36) that $PT + QR = \frac{1}{2}h$. By putting this into (33) we get $d = h^2$, contradicting (38). With this the proof of Theorem 1 is complete.

3. Dickson algebras containing elements with square 0. This section presents one further theorem on the structure of Dickson algebras. The target algebras are labelled $D(\lambda)$, λ being a scalar different from 0 or -1. $D(\lambda)$ has basis 1, u, v with $u^2 = v^2 = 0$, $uv = -\lambda/(\lambda + 1) + u + v$, $vu = \lambda uv$. $D(\lambda)$ is a Dickson algebra, its right and left norm forms being $x(x + \lambda y)(x + z)$ and $x(x + y)(x + \lambda z)$. It is to be noted that $D(1)$ coincides with the algebra D of [7], and Theorem 2 is thus a generalization of case I of Theorem 4 in [7].

THEOREM 2. *Let A be a three-dimensional simple right Dickson algebra with unit. Assume that A possesses two linearly independent elements with square zero. Then A is isomorphic to $D(\lambda)$ for some λ.*

PROOF. Let u and v be the given elements. Write $uv = a + bu + cv$, $vu = p + qu + rv$. The right norm form of A is

$$(39)\quad x^3 + rx^2y + bx^2z + (cp - ar)y^2z + (aq - bp)yz^2 + (br - cq - a - p)xyz.$$

We claim that

$$(40)\quad cp - ar = aq - bp = 0.$$

Assume that (40) is false. Then a factorization of (39) into linear factors can be put in the form (6). Four of the resulting equations read

$$PR = 0,\ QS = 0,\ PRS = cp - ar,\ QRS = aq - bp,$$

showing that (40) holds after all. So (39) is divisible by x. The other factor is a quadratic form which must factor into $(x + ry)(x + bz)$. We must have b and r non-zero and we also have

$$(41)\quad cq + a + p = 0.$$

We claim that $a \neq 0$. For if $a = 0$, then $p \neq 0$ by simplicity, and $b = 0$ by (40), a contradiction. Write $p = \lambda a$; then (40) gives us $q = \lambda b$ and $r = \lambda c$. We now know that a, b, c, λ are all non-zero. From (41) we get

$$(42)\quad (1 + \lambda)a + \lambda bc = 0,$$

showing in particular that $\lambda \neq -1$. Replace u by u/c and v by v/b. Then using (42) we get that $uv = -\lambda/(\lambda + 1) + u + v$. This completes the proof of Theorem 2.

4. Galois descent.

THEOREM 3. *Let A be a three-dimensional division algebra over a finite field F. Assume that all commutators in A are scalar multiples of the unit element. Then A is a twisted field in the sense of [1].*

PROOF. We can assume that A is non-commutative (the commutative case was in essence known to Dickson seventy years ago and was redone in [7]). Let L be an algebraic closure of F and write $C = L \otimes A$ (tensored over F). Then C is a Dickson algebra over L (cf. the discussion of this theorem of Dickson's in [7]). The hypothesis that A is non-commutative with all commutators scalar is multilinear and hence is maintained in C. Hence Theorem 1 is applicable to show that C is isomorphic to E(b) for some b in L. We shall simply transfer the notation from E(b) to C; thus, C has a basis 1, u, v with the multiplication table of Theorem 1.

Let K denote the unique subfield of L which is cubic over F. Let $w = x + yu + zv$ be any non-scalar in A ($x, y, z \in L$). We have that the determinant $|R_w|$ of R_w, the right-multiplication by w on A, is irreducible over F and hence factors completely in K. Now the characteristic roots of $|R_w|$ are given by the factors of (2). Hence $x + y + bz$, $x + by$, and $x + z$ all lie in K. Similarly, use of the left-multiplication by w leads to the information that $x + by + z$, $x + y$, and $x + bz$, the factors of (3), lie in K. Combining these six elements, we readily deduce that the elements x, y, z, and b must themselves lie in K. Write $B = K \otimes A$. Then u and v lie in B. It follows that the isomorphism between C and E(b) can be lowered to an isomorphism between B and the version of E(b) defined over K.

We now invoke the theory of Galois descent, as set forth for example in Chapter 10 of [6]. Let ϕ be a generating automorphism of K over F. There is a natural induced automorphism ϕ^* of B, and the elements of B left fixed by ϕ^* are precisely the members of A (note that ϕ^* is F-linear but not K-linear). Let us examine what ϕ^* does to the idempotents of B.

Right-multiplication by the idempotents u, v, and $1 + b - u - v$ yields linear transformations having the following characteristic roots: 0, 1, and b. For the complementary idempotents $1 - u$, $1 - v$, and $u,+ v - b$ the characteristic roots are 0, 1, and $1 - b$. We assert that ϕ^* cannot send an idempotent of the first set into one of the second set. For if it does, we have $\phi(b) = 1 - b$, from which we deduce $\phi(\phi(b)) = b$, and this is inconsistent with the fact that ϕ has order 3. Thus ϕ^* must permute u, v, and $1 + b - u - v$. It cannot leave any of them fixed, for a fixed element must lie in A, and the division algebra A contains no non-trivial idempotents. Hence ϕ^* must act on them as a 3-cycle.

The K-linear mapping ψ on B that keeps 1 fixed and permutes u, v, and 1 + b - u - v cyclically is readily checked to be an automorphism of B. Let us adjust ϕ^* by either ψ or ψ^{-1}, as appropriate. The result is an F-linear automorphism θ of B which leaves all idempotents of B fixed. Like ϕ^*, θ is semi-linear relative to ϕ. The fixed subalgebra of B under θ is a three-dimensional F-algebra containing u and v; it is necessarily isomorphic to E(b) over F. We have thus established that b lies in F.

Now that we have on hand a copy of E(b) defined over F, the rest of the Galois descent argument is standard. The automorphism group of E(b) is of order 3 (generated by ψ), as we leave it to the reader to check. Therefore there are three forms of E(b) over F; one is E(b) itself, and another is the division algebra A with which we started. We could easily argue at this point that the remaining form of E(b) is also a division algebra, but this will in any event follow from the argument below.

We can conclude our business by a crude counting argument. Let us count the three-dimensional twisted fields over F (of course, we mean the twisting to be taken in the sense of [1], the parameter γ being an element of F). The results in [4] show that all admissible values of γ yield non-isomorphic algebras. The restrictive conditions on γ are $\gamma \neq 0$, $\gamma^3 \neq 1$, and in addition $\gamma \neq -1$ (since $\gamma = -1$ is the commutative case). This yields the following enumeration, where q is the order of F:

$q \not\equiv 1 \pmod 3$, characteristic $\neq 2$	q - 3
$q \equiv 1 \pmod 3$, characteristic $\neq 2$	q - 5
$q \not\equiv 1 \pmod 3$, characteristic 2	q - 2
$q \equiv 1 \pmod 3$, characteristic 2	q - 4

Next we count the possible number of division algebras that we encountered above. Recall first that E(b) is isomorphic to E(b′) if and only if $b' = 1 - b$. Since $b = \frac{1}{2}$ is excluded, there is no overlapping between b and 1 - b. Therefore the number of eligible b's must be cut precisely in half. On the other hand, for each b we found *at most two* division algebras occurring as a form over F of E(b). This calls for doubling and thus restoring the full number of b's. The conditions on b are: $b \neq 0, 1$, or $\frac{1}{2}$, and $b^2 - b + 1 \neq 0$. This gives as our upper bound exactly the same count as listed above. Everything we stated is now established and the proof of Theorem 3 is complete.

5. Galois ascent. In this section we reverse our point of view. We start with a three-dimensional division algebra A over a field F and seek to describe what A

"splits" into over an algebraic closure of F. Actually, following a trail blazed by Dickson in [5], we broaden the study so as to encompass algebras with no quadratic elements (other than scalars). These results are being recorded in the hope that they will be helpful in future studies of three-dimensional algebras.

A preliminary glance at quadratic elements is needed. Let a general three-dimensional algebra A have basis 1, u, v and write

$$u^2 = \text{scalar} + au + bv,$$

$$uv + vu = \text{scalar} + cu + dv,$$

$$v^2 = \text{scalar} + eu + fv.$$

Then

$$(43)\quad (yu + zv)^2 = \text{scalar} + (ay^2 + cyz + ez^2)u + (by^2 + dyz + fz^2)v.$$

For $yu + zv$ to be quadratic it is necessary and sufficient that the coefficients in (43) be proportional to y and z. This leads to the cubic

$$C = by^3 + (d - a)y^2z + (f - c)yz^2 - ez^3,$$

which occurs in [5] at the bottom of page 371, where it is also labelled C.

The condition for A to be quadratic is that C be identically 0. The condition for A to have no quadratic elements is that C be irreducible. A change of basis in A switches C to an equivalent binary cubic form, equivalence here meaning that multiplication of C by a non-zero scalar is permitted in addition to a non-singular change of variable. It is thus meaningful to call A *separable* if C is separable. I have not studied the inseparable case, and it will not be treated in this paper.

We proceed to study a three-dimensional algebra A over a field F, assuming that it has a unit element, that it has no quadratic elements other than scalars, and that it is separable. A quadratic extension of F keeps C irreducible and can thus be performed without changing the project. Let us make a quadratic extension, if necessary, so as to arrange that the splitting field K of C is three-dimensional over F. Let ϕ generate the Galois group of K over F, and write ϕ^* for the induced automorphism of $B = K \otimes A$. Since C factors over K into three distinct factors, B has exactly three two-dimensional subalgebras containing 1. We claim that ϕ^* permutes them cyclically. If this is not true, each is carried into itself by ϕ^*. Call one of them G; note that G is a six-dimensional algebra over F and that the elements of G fixed by ϕ^* are just F. This is impossible if G is a field. The alternative is that G is generated over K by an element

u satisfying $u^2 = u$ or $u^2 = 0$. If $u^2 = u$, then $\phi^*(u)$ must be $1 - u$, and this is incompatible with the fact that ϕ^* has order 3. Suppose that $u^2 = 0$. We must have $\phi^*(u) = \alpha u$, $\alpha \in K$. Then $\phi^*(\phi^*(u)) = \phi(\alpha)\alpha u$. Application of ϕ^* one more time returns us to u. This implies that α has norm 1. By Hilbert's Theorem 90, $\alpha = \beta/\phi(\beta)$ for some β in K. But then βu is fixed under ϕ^*, a contradiction.

When we enlarge K further to an algebraic closure L of F, the three two-dimensional subalgebras of B split. The upshot is that in $L \otimes A$ there is a uniform pattern for the three two-dimensional subalgebras: all three are generated by an element with square 0 or all three are generated by an idempotent. Let us call the two possible cases types D and E respectively.

For type D there is a structure theorem; we state it in a self-contained elementary way. For an algebra A of characteristic $\neq 2$, we write A^+ for A made commutative, the new multiplication being given by $(xy + yx)/2$.

THEOREM 4. *Let A be a three-dimensional algebra over a field F. Assume that A has a unit element, is not quadratic, and contains three elements with square 0 with the property that any two are linearly independent. Then the characteristic of F is not 2 and A^+ is isomorphic to the algebra D of [7].*

PROOF. Let u, v, and w be the given elements. Necessarily 1, u, and v are linearly independent and form a basis. Write

$$uv + vu = a + bu + cv, \quad w = x + yu + zv.$$

From $w^2 = 0$ we get

$$(44)\quad x^2 + ayz = 0,\ 2xy + byz = 0,\ 2xz + cyz = 0.$$

If b and c are both 0, then A is quadratic. So at least one is non-zero. Now assume $x = 0$. Then either the second or the third equation in (44) implies that y or z is 0, and then we find w to be a scalar multiple of u or v. So x must be non-zero. From the first equation in (44) we deduce that y and z are also non-zero. Characteristic 2 can now be ruled out quickly, for a further use of the second or third equation in (44) yields a contradiction.

We can now assume A to be commutative. With x, y, and z all known to be non-zero, (44) shows that *both* b and c are non-zero. Cancel y and z from the second and third equations in (44) to get $x = -bz/2$ and $x = -cy/2$. Hence $x^2 = bcyz/4$. Comparison with the first equation in (44) shows that $4a + bc = 0$. Let $u' = 2u/c$,

$v' = av/b$. Then the elements 1, u', and v' form a new basis for A. We find $u'v' = -\frac{1}{2} + u' + v'$. This identifies A with D.

For division algebras over a finite field we can carry the type D case to a conclusion.

THEOREM 5. *A three-dimensional division algebra of type D over a finite field is commutative.*

PROOF. Let F be the given field, L an algebraic closure of F, A the given algebra, and $B = L \otimes A$. We know that B is a Dickson algebra and so Theorem 2 is applicable to show that B is isomorphic to some $D(\lambda)$. But it is easily checked that, for $\lambda \neq 1$, $D(\lambda)^+$ is not isomorphic to D. Hence λ must equal 1 and A is commutative.

Theorem 5 does not extend to infinite fields. I shall give just one example. Let $F = Q(t)$ where Q is the field of rational numbers and t is an indeterminate over Q. Let A have basis 1, u, u^2 with $u^2u = 2 - t$, $uu^2 = 2 + t$, $(u^2)^2 = -16u$. The right norm form is

$$(45)\quad x^3 + (2 - t)y^3 - 16(2 + t)z^3 + 12xyz.$$

Our problem is to show that the cubic form (45) represents 0 only trivially, In an alleged representation of 0 we can assume x, y, z to be polynomials in t with no common factor. But when t is set equal to 0, (45) becomes the norm form of a commutative division algebra of Dickson's type. Hence x, y, z must all be divisible by t, a contradiction.

6. Automorphisms and antiautomorphisms. We begin this section with an easy self-contained theorem.

THEOREM 6. *Let A be a three-dimensional algebra with a unit element and no quadratic elements other than scalars. Then A cannot admit an automorphism or antiautomorphism of order two.*

PROOF. Let ϕ be an automorphism or antiautomorphism of A with square equal to the identity. Let S be the subspace of A consisting of the elements fixed under ϕ. S cannot be three-dimensional. If S is two-dimensional, take $s \in S$, s a non-scalar. Then $\phi(s^2) = (\phi(s))^2 = s^2$, so $s^2 \in S$, s^2 is a linear combination of 1 and s, s is quadratic. Thus S must be one-dimensional, spanned by 1. We now make a case distinction.

Characteristic $\neq 2$. We have a non-scalar t with $\phi(t) = -t$. Then $t^2 \in S$, t^2 is scalar, t is quadratic, a contradiction.

Characteristic 2. The null space of $(\phi - I)^2$, where I is the identity, is two-dimensional. It can be spanned by 1 and t, where $\phi(t) = 1 + t$. Then $\phi(t^2) = 1 + t^2$, so that t^2 is a linear combination of 1 and t, again a contradiction.

Rapid further progress can be made by using Galois ascent. Let A be as in Theorem 6 and assume further that A is separable. We leave to the reader the easy deduction from the results in §5 that the group of automorphisms of A is finite. Now assume that A admits an antiautomorphism and is not commutative. Then the group of automorphisms and antiautomorphisms of A is a finite group of even order, contradicting Theorem 6. We deduce the first conclusion in Theorem 7.

THEOREM 7. *Let A be a three-dimensional algebra with unit. Assume that A has no quadratic elements other than scalars and that it is separable (as defined in §5). Then if A is noncommutative it admits no antiautomorphisms. The automorphism group of A has order 1 or 3.*

For characteristics other than 2 and 3 the final statement in Theorem 7 was proved by Dickson [5, p. 177]. I have reproved it in the algebraically closed style, including characteristics 2 and 3. I record in Theorem 8 the essential point of this proof; Theorem 8 also serves to identify the split form of the algebras in question.

We need a further class of target algebras. Define an algebra E(b,a) as having a basis 1, u, v with multiplication table

$$u^2 = u,\ v^2 = v,\ uv = a + bu + bv,\ vu = -a - b - b^2 + bu + bv.$$

One easily sees that E(b,a) is quadratic if and only if $2b = 1$, and that

$$u \to v \to 1 + b - u - v \to u$$

induces an automorphism of E(b,a) of order 3. Note that the previous E(b) is $E(b, (1 - 2b)^{-1}b^3)$, and that for characteristic $\neq 2$, E(b,a) is the general algebra whose + algebra is isomorphic to $E(b)^+$.

THEOREM 8. *Let A be a non-quadratic three-dimensional algebra with unit. Let u be an idempotent of A, ϕ an automorphism of A; write $v = \phi(u)$, $w = \phi(v)$. Assume that neither v nor w is equal to u or 1 - u. Then A is isomorphic to some E(b,a) with $2b \neq 1$. Furthermore, ϕ is of order 3.*

PROOF. The only idempotent linear combinations of 1 and u are 1, 0, u, and 1 - u. Since v is none of these, we have that the elements 1, u, v form a basis of A. Write $w = P + Qu + Rv$. Here $R \neq 0$, since w is not a linear combination of 1 and u. It

follows further from our hypotheses that w is not equal to v or 1 - v; hence $Q \neq 0$.

Write $uv = a + bu + cv$, $vu = p + qu + rv$. The traces of R_u and R_v are $1 + r$ and $1 + b$, respectively. These must be equal and so $r = b$. Similarly from L_u and L_v we get $q = c$. Thus $vu = p + cu + bv$. From the hypothesis that A is not quadratic one deduces readily

(46) $b + c \neq 1$.

The fact that w is idempotent yields the following equations when we equate coefficients of u and v:

(47) $Q^2 + 2PQ + QR(b + c) = Q$,

(48) $R^2 + 2PR + QR(b + c) = R$.

Since Q and R are non-zero we may cancel them in (47) and (48). Then on subtracting and using (46) we get $Q = R$. The simplified form of (47) is now

(49) $2P + Q(b + c + 1) = 1$.

When we expand the equations $\phi(uv) = \phi(u)\phi(v)$ and $\phi(vu) = \phi(v)\phi(u)$ and equate the coefficients of 1 and v we get four equations.

(50) $a + cP = pQ$,

(51) $b + cQ = P + bQ + Q$,

(52) $p + bP = aQ$,

(53) $c + bQ = P + Q + cQ$.

We now make an indirect argument that $b = c$. Suppose on the contrary that $b \neq c$. Then on subtracting (51) from (53) we get $2Q = 1$. On putting this into (51) and (49) and eliminating P we get a contradiction of (46) unless the characteristic is 3. In that case we argue further that (50) and (52) combine to give $P = 0$, which makes (49) and (46) contradictory. Thus $b = c$ from which it follows that $2b \neq 1$.

Equations (49), (50), and (51) now simplify to

(54) $2P + Q(2b + 1) = 1$,

(55) $a + bP = pQ$,

(56) $P + Q = b$.

On eliminating P between (54) and (56), and recalling that $2b \neq 1$, we get $Q = -1$. Insertion of $Q = -1$, $P = b + 1$ into (55) yields $a + p + b^2 + b = 0$. This identifies A with E(b,a). Furthermore $\phi(w)$ works out to be u, and so ϕ has order 3. The proof of Theorem 8 is complete.

7. Concluding remarks. I venture the following conjecture: any three-dimensional division algebra over a finite field F is associative or a twisted field. Here "twisted field" is meant in the extended sense of [2], that is, the twisting parameter c is allowed to range over the cubic extension field K of F which is being twisted.

It is easy to count the number of twisted fields. It is proved in [4] that the parameters c and d yield isomorphic twisted fields if and only if an automorphism of K over F carries c into d. The conditions that need to be imposed on c are: c is not 0 and the norm of c is not 1. The count works out as follows. Let the order of F be q. From the $q^3 - 1$ non-zero elements of K we delete the $q^2 + q + 1$ elements having norm 1. If $q \not\equiv 1 \pmod 3$ we keep the $q - 2$ elements that are in F and divide the number of others by 3, getting

$$(q - 2) + [(q^3 - 1) - (q^2 + q + 1) - (q - 2)]/3 = (q - 2)(q^2 + q + 3)/3.$$

If $q \equiv 1 \pmod 3$ we lose two cube roots of 1 in F and the count is

$$(q - 4) + [(q^3 - 1) - (q^2 + q + 1) - (q - 4)]/3 = (q^3 - q^2 + q - 10)/3.$$

Take q = 3. There are 5 twisted fields. On deleting the commutative one (c = -1), we have 4 left. This agrees with Dickson's count on page 378 of [5].

Take q = 5. We have 33 - 1 = 32 noncommutative twisted fields. But Dickson lists 36 on page 379. The conjecture seems to be defeated. However, there is at least one error in Dickson's list. The algebra in the second column, second line, with the lower choice of signs, has basis 1, i, j satisfying

$$ij = 2 + 2i,\ ji = 2 + i,\ j^2 = 2 - i - j.$$

We find

$$(i + 2j)(-2 + i + j) = 10 - 5j,$$

which vanishes for characteristic 5. So the algebra has divisors of zero. (The error was detected in the middle of an attempt to sort out Dickson's list into the anti-isomorphic pairs which should exist according to Theorem 7 - there was no anti-isomorphic mate for the culprit. At this point the computation was dropped.)

It seems to me that it is going to be difficult to obtain any results on n-dimensional division algebras ($n > 3$) by Dickson's methods or by mine. A new idea is needed. In the meantime here are two remarks.

1. The theory is virtually certain to be sensitive to the number-theoretic

properties of n. In particular, n = 4 may well be harder than n = 5.

2. For $n > 3$, the pertinent results about rational points on varieties normally hold only for large enough finite fields. So one presumes that a hypothesis of this kind will be appropriate for theorems on division algebras. This is reinforced by the known examples of four-dimensional and five-dimensional division algebras over the field of two elements. I am bold enough to make one explicit conjecture: any five-dimensional division algebra over a sufficiently large finite field is a twisted field. A particular case that might be tried first is this: there exist no commutative non-associative five-dimensional division algebras over a sufficiently large finite field of characteristic 2.

The literature on non-associative division algebras is sparse enough that I thought it worth while to try to compile a complete bibliography. To get this bibliography, add the following: the references in [7] and [11], and references [126], [141], [173], and [174] in [10]. I should add that I have not included papers dealing primarily with topology or with projective planes.

REFERENCES

1. A. A. Albert, *On nonassociative division algebras,* Trans. Amer. Math. Soc. 72(1952), 296-309.
2. ———, *Finite noncommutative division algebras,* Proc. Amer. Math. Soc. 9(1958), 928-932.
3. ———, *Generalized twisted fields,* Pac. J. Of Math, 11(1961), 1-8.
4. ———, *Isotopy for generalized twisted fields,* An. Acad. Brazil. Ci., 33(1961), 265-275.
5. L. E. Dickson, *Linear algebras in which division is always uniquely possible,* Trans. Amer. Math. Soc., 7(1906), 370-390.
6. N. Jacobson, *Lie Algebras,* Interscience, 1962.
7. I. Kaplansky, *Three-dimensional division algebras,* J. of Alg.
8. E. Becker, *Kennzeichnung quasi-alternativer quadratischer Divisionsalgebren,* Hamb. Abh. 38(1972), 88-105.
9. ———, *Über eine Klasse flexibler quadratischer Divisionsalgebren,* J. Reine Angew. Math., 256(1972), 25-57.
10. N. Jacobson, *Abraham Adrian Albert 1905-1972,* Bull. Amer. Math. Soc., 80(1974), 1075-1100.
11. D. E. Knuth, *Finite semifields and projective planes,* J. of Alg., 2(1965), 182-217.
12. ———, *A class of projective planes,* Trans. Amer. Math. Soc., 115(1965), 541-549.
13. E. N. Kuzmin, *Certain classes of division algebras,* Algebra i Logika Sem., 5(1966), 57-102(Russian; MR34, no. 4314).
14. ———, *A class of anticommutative algebras,* Algebra i Logika, 6(1967), 31-50 (Russian; MR 37, no. 2829).
15. ———, *Algebras with division over the field of real numbers,* Dokl. Akad. Nauk SSSR, 172(1967), 1014-1017. AMS translation Soviet Math. Dokl., 8(1967), 220-223.
16. J. M. Osborn, *Quadratic division algebras,* Trans. Amer. Math. Soc., 105(1962), 202-221.
17. H. Petersson, *Quai composition algebras,* Hamb. Abh., 35(1971), 215-222.

18. ———, *Eine Bemerkung zu quadratischen Divisionsalgebren,* Arch. Math., 22(1971), 59-61.
19. ———, *Exceptional Jordan division algebras over a field with a discrete valuation,* J. für reine und angew. Math., 274-275(1975), 1-20.
20. D. Rees, *The nuclei of non-associative division algebras,* Proc. Camb. Phil. Soc., 46(1950), 1-18.
21. H. Strade, *Einige Bemerkungen über Divisionsalgebren,* Hamb. Abh., 38(1972), 80-87.

University of Chicago
Chicago, Illinois

Received September 1, 1975