ON THE SUBALGEBRAS OF FINITE DIVISION ALGEBRAS

JOSEPH L. ZEMMER, Jr.

1. Introduction. In 1893 it was shown by Moore that the only commutative, associative division algebras with a finite number of elements are the well-known Galois fields [**10**, p. 220]. Twelve years later it was shown by Wedderburn that every associative division algebra with a finite number of elements is commutative [**11**], and hence a Galois field. It is conceivable that these results, particularly the theorem of Moore, motivated some of the work done by Dickson and published in two papers in 1906 [**4**;**5**]. The work referred to is an attempt to determine all commutative, non-associative[1] division algebras with a finite number of elements. The most complete result of Dickson states that there are only two commutative division algebras with unit element of order 3 over a Galois field $GF(q^k)$. One of these is the associative algebra $GF(q^{3k})$ and the other an algebra in which the multiplication is not associative. Since this non-associative algebra is discussed briefly in §4 the details will be omitted here. The methods used by Dickson in this connection are not capable of immediate generalization, and the problem of determining all commutative division algebras of order n over a finite field is still unsolved. Although Dickson apparently abandoned the problem shortly after the publication of the papers referred to above, his work in this connection should not be taken too lightly. It has been conjectured that this work may have led Dickson to his important discovery of cyclic algebras.

Before discussing the results contained in the present paper, it is desirable to make several definitions and some obvious remarks concerning finite division rings and finite division algebras.

A set G of elements is called a *quasigroup* with respect to a binary operation $(\cdot)$, if and only if:

(i) $x \cdot y$ is uniquely determined for each ordered pair $x, y \in G$,

(ii) the equations $a \cdot x = b$, $y \cdot a = b$ have unique solutions for each ordered pair $a, b \in G$.

A quasigroup with unit element is called a *loop*.

A set A of elements is called a *division ring* with respect to two binary operations, $(+)$ and $(\cdot)$, defined on A, if and only if:

Received April 18, 1951. This paper contains the substance of a thesis prepared under the direction of Professor R. H. Bruck and submitted for a Ph. D. degree at the University of Wisconsin.

[1] Here, non-associative algebra means one which is not necessarily associative. In the remainder of the paper, however, non-associative algebra will mean an algebra in which the multiplication is actually not associative.

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

(i) the elements of A are an abelian group under $(+)$,

(ii) the non-zero elements of A are a quasigroup under $(\cdot)$,

(iii) the two distributive laws $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$ hold for all $x, y, z \in A$.

A division ring A is called a *division algebra* of order n over a field F, if and only if:

(i) the additive group of A is a linear vector space of order n over F,

(ii) $\alpha (a \cdot b) = a \cdot (\alpha b) = (\alpha a) \cdot b$ for all $\alpha \in F$ and $a, b \in A$.

Note that if a division algebra A contains a unit element e, then the set of all multiples, αe, $\alpha \in F$, is a subalgebra of A isomorphic to F. There is no loss of generality in denoting αe by α.

Let A be a division ring, and a any non-zero element of A. Then the mappings $x \rightarrow xa$ and $x \rightarrow ax$ are clearly non-singular mappings of A upon A. These mappings are denoted by $R(a)$ and $L(a)$ respectively. Let a, b be any two non-zero elements of A, and consider the system A_0, consisting of the same elements as A, with multiplication defined by $x \bullet y = xR(a)^{-1} \cdot yL(b)^{-1}$. Denote by e the product $b \cdot a$, then clearly $e \bullet y = y \bullet e = y$ for all $y \in A_0$. Thus e is a unit element of A_0; furthermore, it is easily seen that A_0 is a division ring, and that it is commutative if A is commutative and $a = b$. It is seen then that the study of division rings is reduced to a study of division rings with unit element.

Now, if A is a finite division ring with unit e_1, then clearly A contains a subring M isomorphic to a finite prime field $GF(p)$ for some rational prime p. By finite induction it may be shown that A has a basis $e_1, \ldots, e_n$ with respect to M. Thus a study of finite division rings is reduced to a study of division algebras with unit element over a Galois field.

In §2 finite commutative division algebras with unit element are studied. It is shown that every such algebra of even order contains a subalgebra of order 2, and that no such algebra of odd order contains a subalgebra of order 2. A well-known, and rather elementary, result in the theory of associative division algebras states that the order of every subalgebra of a division algebra is a divisor of the order of the algebra. Whether or not this result is valid for non-associative division algebras is not known. One application of the results obtained in §2 gives a little information in this connection in the case where the division algebra is a finite commutative algebra with unit element.

An attempt is made in §3 to determine, by the use of Theorem 1, all finite, commutative division algebras with unit element of order 4 over a Galois field. A theorem due to Dickson is sharpened somewhat, but not enough to solve the problem completely. In fact, Theorem 1 does not seem to give enough information to solve the weaker problem of determining all finite, commutative division algebras of order 4 whose automorphism group relative to the base field contains the cyclic group of order 4. It is possible, however, to find out something about the subalgebras of finite division algebras of order n whose automorphism group relative to the base field contains the cyclic group of order n. This is done in

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

§6, after it has been shown in §5 that there exist finite algebras of this kind which are not associative.

2. Finite commutative division algebras.

Before proceeding to the main theorem of this section, it is necessary to make some remarks concerning normality of subloops of a given loop L. The subloop G of L is said to be *normal* in L if and only if the following condition is satisfied [**2**, p. 256]: for arbitrary x, $y \in L$, if in the equation $(xy)g_1 = (xg_2)(yg_3)$, any two of the elements g_1, g_2, g_3, are arbitrary elements of G, then the third is a uniquely determined element of G.

Let A be a division algebra over a field F. Denote by L the set of non-zero elements of A, and by G the set of non-zero elements of F. It is clear that G is a normal subloop of L and that the set of all distinct cosets xG, $x \in L$, is a loop, called the quotient loop of L modulo G, and denoted by L/G.

The following lemma is due to Griffin [**8**, p. 728].

Lemma 1. *If Q is a finite, commutative quasigroup with an even number of elements, then the equation $y^2 = a$ has an even number of distinct solutions for each $a \in Q$.*

The proof, which will be omitted, follows from a consideration of the main diagonal of the multiplication table of Q.

Lemma 2. *If A is a commutative division algebra of order $2n$ over a field $F = GF(q^k)$, $q > 2$, and if L and G denote the non-zero elements of A and F respectively, then in the quotient loop L/G the equation $X^2 = C$ has either two distinct solutions or no solution.*

Proof. First note that the loop L/G contains

$$t = 1 + q^k + q^{2k} + \ldots + q^{(2n-1)k}$$

elements. Clearly t is even, and hence by Lemma 1, the equation $X^2 = C$ has an even number of distinct solutions in L/G. Suppose that for some $C = cG \in L/G$ the equation $X^2 = C$ has more than two distinct solutions. Then there exist at least three distinct elements xG, yG, $zG \in L/G$ such that $(xG)^2 = (yG)^2 = (zG)^2$. These imply $x^2G = y^2G = z^2G$, and hence $x^2 = \alpha y^2 = \beta z^2$, where α, β are non-squares in F. Thus $y^2 = \alpha^{-1}\beta z^2$, or since $\alpha^{-1}\beta = \gamma^2$ in F, $y^2 = \gamma^2 z^2$, which implies that $y = \pm \gamma z$, or $yG = zG$, a contradiction.

Corollary. *Exactly half of the equations $X^2 = C$, $C \in L/G$ have solutions in L/G.*

Theorem 1. *If A is a commutative division algebra with unit element of order $2n$ over a field $F = GF(q^k)$, $q > 2$, then A contains a unique subalgebra M of order 2 over F. The subalgebra M is isomorphic to the field $GF(q^{2k})$, and may be characterized as the set of all elements of A which satisfy quadratic equations with coefficients in F.*

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

Proof. Denote by 1 the unit element of A. Then, with the notation of Lemma 2, since the equation $X^2 = 1G$ has a solution $X = 1G$ in L/G, it follows that the equation has exactly two distinct solutions. Let $X = eG$ be the second solution. It is clear that 1, e are linearly independent over F, and that $e^2 = \phi$, where ϕ is a non-square in F. Thus the subspace spanned by 1 and e is a subalgebra M of A. Denote by ρ a zero of the polynomial $\lambda^2 - \phi$, irreducible in $F[\lambda]$; it is easily seen that M is isomorphic to the field $F(\rho) = GF(q^{2k})$ under the correspondence $\alpha + \beta e \leftrightarrow \alpha + \beta\rho$. A contains no other subalgebra of order 2 over F. This follows from the fact that $1G$ and eG are the only solutions of $X^2 = 1G$ in L/G. Clearly, every element of M satisfies a quadratic equation with coefficients in F. Let S denote the set of all such elements, so that $M \subseteq S$. If $x \in S$, and x is a scaler, then $x \in M$, since $F \subset M$. Let $x \in S$, and assume that x is not a scalar. Then $x^2 = \alpha x + \beta$, for some α, $\beta \in F$, and

$$(x - \tfrac{1}{2}\alpha)^2 = \beta + (\tfrac{1}{2}\alpha)^2.$$

Thus $(x - \frac{1}{2}\alpha)G$ satisfies $X^2 = 1G$ in L/G, and it follows that $(x - \frac{1}{2}\alpha)\, G = eG$ since $x \notin G$. Hence $x - \frac{1}{2}\alpha = \gamma\, e$ for some $\gamma \in G$, and $x = \frac{1}{2}\alpha + \gamma e \in M$. Clearly then $S \subseteq M$, which together with $M \subseteq S$ implies that $S = M$. This completes the proof of the theorem.

In a finite commutative loop of odd order the equation $x^2 = a$ has a unique solution for each a (as in Lemma 1, consider the main diagonal of the multiplication table). It follows that if A is a commutative division algebra with unit element of odd order over a field $GF(q^k)$, $q > 2$, then $x^2 = \alpha \in F$ implies that $x \in F$. Thus, if G, C are the sets of non-zero elements of A and F respectively, then the loop G/C is of odd order. Hence the equation $X^2 = C$ has the unique solution $X = C$. Let $x^2 = \alpha \in C$ for some $x \in G$, then $(xG)^2 = C$, which implies that $xG = C$, or $x \in C \subset F$. Now, $x^2 \in F$ implies $x \in F$ is equivalent to saying that A contains no subalgebra of order two over F. This, together withTheorem 1, implies that no finite commutative division algebra with unit of odd order over a field $GF(q^k)$, $q > 2$, can contain a subalgebra of even order.

3. Finite commutative division algebras of order 4. Theorem 1 may be used to sharpen somehwat a theorem of Dickson [**4**, p. 381]. This will be accomplished by proving Lemma 4, from which the desired result readily follows. The proof of Lemma 3 follows immediately from the observation that in any commutative division ring $b^2 = a^2$ implies $b = \pm\, a$.

LEMMA 3. *Let A be a commutative division ring and M any proper subring of A. If b is an element of A such that $b^2 \in M$, then b^2 is a non-square in M if and only if*[2] *$b \in A - M$.*

LEMMA 4. *If A is a commutative division algebra with unit of order* 4 *over a finite field $F = GF(q^k)$, $q > 2$, and if M is the unique subalgebra of order* 2 *over F described in Theorem* 1, *then every element of M is the square of some element of A.*

[2] $A - M$ means the usual set-theoretic complement of M in A.

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

Proof. Let 1, e be a basis for M. Then, if $x \in A - M$, 1, e, x, ex, are a basis for A. Thus, every $x \in A - M$ satisfies a quadratic equation with coefficients in M, for if $x \in A - M$, then there exist in F four elements α_i $(i = 0, 1, 2, 3)$ such that $x^2 = \alpha_0 + \alpha_1 e + \alpha_2 x + \alpha_3 ex = \psi + \mu x$, where ψ, $\mu \in M$. Define y by $y = x - (\frac{1}{2}\mu)$, then $y \in A - M$ and $y^2 = \psi + (\frac{1}{2}\mu)^2 \in M$. Let $\nu = \psi + (\frac{1}{2}\mu)^2$, so that $y^2 = \nu$. By Lemma 3, ν is a non-square in M. Since yG satisfies the equation $X^2 = \nu\, G$ in L/G, it follows from Lemma 2 that there exists a second solution $X = zG \neq yG$. Clearly, $z^2 = \gamma y^2 = \gamma\nu$, where γ is a non-square in F. By Theorem 1, M is isomorphic to $GF(q^{2k})$, and since $GF(q^{2k})$ is the root field of the polynomial $\lambda^2 - \gamma$, it follows that γ is the square of some element of M. Thus, $z^2 = \gamma\nu$ is a non-square in M, and hence $z \in A - M$ by Lemma 3.

Suppose that $\beta_0 + \beta_1 e + \beta_2 y + \beta_3 z = 0$, where the $\beta_i \in F$. Then

$$(\beta_0 + \beta_1 e)^2 + 2\beta_2(\beta_0 + \beta_1 e)y + \beta_2{}^2 y^2 = \beta_3{}^2 z^2,$$

and since y^2, $z^2 \in M$, this equation implies that $\beta_2(\beta_0 + \beta_1 e)y \in M$. Thus, $\beta_2(\beta_0 + \beta_1 e) = 0$, for otherwise $y \in M$, a contradiction. If $\beta_2 = 0$, so that $\beta_0 + \beta_1 e + \beta_3 z = 0$, then, since $z \in A - M$, it follows that each of the remaining β_i is zero. However, if $\beta_0 + \beta_1 e = 0$, so that $\beta_2 y + \beta_3 z = 0$, then $\beta_2 = \beta_3 = 0$, for otherwise $yG = zG$ in L/G, a contradiction. It is seen then that 1, e, y, z, are linearly independent over F.

Assume that the elements of G have been ordered in some way and let η_i denote the ith element in this ordering. Then for each $i = 1, \ldots, q^k - 1$, define y_i by $y_i = y + \eta_i z$. Clearly each $y_i \in A - M$, and hence there exist $\mu_i \in M$ such that $(y_i - \mu_i)^2 = \nu_i \in M$ for $i = 1, \ldots, q^k - 1$. Let $y'_i = y_i - \mu_i$, and note that each $y'_i \in A - M$. It is easily verified that the $q^k + 1$ cosets $y'_i G$, yG, and zG are distinct. It follows that the $q^{2k} - 1$ elements of A contained in these cosets are distinct elements of $A - M$. Denote these elements by b_j, $(j = 1, \ldots, q^{2k} - 1)$. By Lemma 3, each $b_j{}^2$ is a non-square in M. Furthermore, it is easily seen that if b is an element of the set $\{b_j\}$, then $-b$ is also an element of the set. Hence, the set $\{b_j{}^2\}$ contains no more than $\frac{1}{2}(q^{2k} - 1)$ elements. Since the b_j are distinct, it follows from the remark immediately preceeding Lemma 3 that the set $\{b_j{}^2\}$ contains exactly $\frac{1}{2}(q^{2k} - 1)$ elements. Finally, since there are $\frac{1}{2}(q^{2k} - 1)$ elements of M which are non-squares in M, it is seen that the set $\{b_j{}^2\}$ is precisely the set of all non-square elements of M. This completes the proof of the lemma.

THEOREM 2. *If A is an algebra satisfying the hypotheses of Lemma* 4, *then A has a basis* 1, f, f^2, f^3, *with multiplication given by*

$$(1)\qquad (f^2)^2 = \alpha_0 + \alpha_1 f^2, \qquad (f^3)^2 = \beta_0 + \beta_1 f + \beta_2 f^2 + \beta_3 f^3,$$
$$ff^3 = \gamma_0 + \gamma_1 f + \gamma_2 f^2 + \gamma_3 f^3, \qquad f^2 f^3 = \delta_0 + \delta_1 f + \delta_2 f^2 + \delta_3 f^3.$$

Proof. First, note that $f^2 f = f f^2$ by commutativity, and hence that f^3 is unambiguous. As in Lemma 4 let M be the subalgebra of A of order 2 over F. Then M has a basis 1, e, with $e^2 = \phi$, where ϕ is a non-square in F. Let the

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

elements of M be ordered in some way and denote by $\eta_0 + \eta_1 e$ the first non-square in M with respect to this ordering. By Lemma 4 there exists an element $f \in A - M$ such that $f^2 = \eta_0 + \eta_1 e$. Furthermore, it is clear that $1, f, f^2, f^3$ are linearly independent over F. Define α_0 and α_1 by $\alpha_0 = \phi\eta_1^2 - \eta_0^2$, $\alpha_1 = 2\eta_0$, then clearly

$$(f^2)^2 = (\eta_0 + \eta_1 e)^2 = \eta_0^2 + \phi\,\eta_1^2 + 2\,\eta_0\,\eta_1 e = \eta_0^2 + \phi\,\eta_1^2 + 2\,\eta_0 f^2 - 2\,\eta_0^2$$
$$= \alpha_0 + \alpha_1 f^2.$$

Note that the constants α_0 and α_1 depend only upon the choice of $\phi \in F$ and the ordering of the elements of M. Nothing can be said about the twelve constants $\beta_i, \gamma_i, \delta_i$ $(i = 0, 1, 2, 3)$.

The theorem of Dickson, mentioned earlier, states that an algebra A satisfying the hypotheses of Lemma 4 has a basis $1, f, f^2, f^3$ with multiplication given by $(f^2)^2 = \zeta_0 + \zeta_1 f + \zeta_2 f^2 + \zeta_3 f^3$, and $(f^3)^2, ff^3, f^2f^3$ the same as in (1), where the polynomial $\lambda^4 - \zeta_3\lambda^3 - \zeta_2\lambda^2 - \zeta_1\lambda - \zeta_0$ is irreducible in $F[\lambda]$.

4. Finite commutative division algebras of order 3. Let A be a commutative division algebra of order 3 over a field $F = GF(q^k)$, $q > 2$. It has been shown by Dickson [**3**; **4**; **6**; **7**] that if A is not associative, then A has a basis $1, e, e^2$ with multiplication given by

$$(2) \qquad ee^2 = \gamma + \delta e, \qquad e^2e^2 = -\delta^2 - 8\gamma e - 2\delta e^2,$$

where $\lambda^3 - \delta\lambda - \gamma$ is irreducible in $F[\lambda]$, and conversely if $\lambda^3 - \delta\lambda - \gamma$ is irreducible in $F[\lambda]$, then the algebra over F with basis $1, e, e^2$ and multiplication given by (2) is a division algebra. Dickson has shown further that there is at most one commutative, non-associative division algebra with unit element of order 3 over a Galois field $GF(q^k)$, $q > 2$, and that this unique non-associative division algebra has as its automorphism group relative to the base field, the cyclic group of order 3.

The question of the existence of finite, non-associative, commutative division algebras of order a prime $p > 3$ appears to be rather difficult to answer. In fact, to the best of the author's knowledge, there exist no examples of such algebras. The most obvious approach to the problem is a study of p-ary, p-ic forms, p a prime, over a Galois field, which vanish only when each of the p variables vanishes. The connection between these two problems is seen by noting that (i) an algebra A, of order p over a field F, is a division algebra if and only if $|R(x)| = 0$ implies that $x = 0$, where $R(x)$ is the linear transformation defined by $aR(x) = ax$ for all $a \in A$; and (ii) $|R(x)|$ is a p-ary, p-ic form[3] in the p components of x. The problem of determining all "definite" p-ary, p-ic forms over a Galois field has been solved by Dickson [**7**] for the case $p = 3$, and this is one reason for a fairly complete knowledge of finite, commutative division algebras of order 3.

[3] For a further discussion of this see Bruck [**1**] and Dickson [**4**].

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

In the next section an important method due to Dickson [**5**, p. 515] will be employed to obtain non-associative, commutative division algebras of order $2n$ over a Galois field, whose automorphism group relative to the base field is the cyclic group of order $2n$. This result of Dickson may be summarized as follows: if

$$f(\lambda) = \lambda^n - \alpha_1\lambda^{n-1} + \alpha_2\lambda^{n-2} - \ldots \pm \alpha_n \in F[\lambda]$$

(where α_n is a non-square in the field F) is an irreducible, normal, cyclic polynomial, if ρ is a zero of $f(\lambda)$ and S a generating automorphism of the automorphism group of $F(\rho)$ relative to F, then the set A of all ordered pairs (x, y), $x, y \in F(\rho)$ is a division algebra of order $2n$ over F under the operations

$$\alpha(x, y) = (x, y)\alpha = (\alpha x, \alpha y), \qquad \alpha \in F,$$

$$(x, y) + (a, b) = (x + a, y + b), \quad (x, y)\,(a, b) = (xa + ySbS\rho, ya + xb).$$

5. The existence of finite non-associative division algebras. As noted earlier, the non-zero elements of a division algebra with unit element form a loop under multiplication. It is interesting, and somewhat useful, as the next theorem will indicate, to be able to determine whether or not the set of non-zero elements of a given division algebra with unit contains a subloop of index 2. No non-associative, commutative, finite, division algebras with this property are known to the author. However, the set of all squares in a Galois field is a subgroup of index 2 in the group of non-zero elements, and it is easy to see that if the loop of non-zero elements of a finite, commutative division algebra contains a subloop of index 2, then this subloop is necessarily the set of all squares. It should be mentioned at this point that there exist non-associative division algebras, not finite, with this property. Thus, in the linearly ordered algebras constructed by Zelinsky [**12**] the set of all positive elements is the desired subloop of index 2.

The following theorem is closely related to the result of Dickson referred to at the end of the last section and will be applied to the Galois fields.

THEOREM 3. *Let A be a division algebra (not necessarily associative) with unit element of order n over a field K. Denote by G the set of all non-zero elements of A. If the loop G contains a subloop H of index 2 in G, then the set A^* of all ordered pairs $(x, y), x, y \in A$, is a division algebra with unit element of order $2n$ over K under the operations*

$$\alpha(x, y) = (x, y)\alpha = (\alpha x, \alpha y), \qquad \alpha \in K, \tag{3}$$

$$(x, y) + (z, w) = (x + z, y + w), \; (x, y)\,(z, w) = (xz + [yUwV]e, yz + xw),$$

where e is any fixed element of $G - H$, and U, V are non-singular linear transformations of A such that $HU = HV = H$.

Proof. First note that if $(x, y)\,(z, w) = (0, 0)$, $(x, y) \neq (0, 0)$, $(z, w) \neq (0, 0)$ then x, y, z, w are all different from zero. Suppose that there exist elements $x, y, z, w \in G$ such that $(x, y)\,(z, w) = (0, 0)$. Then by (3) it is seen that

$$\text{(i)} \quad xz + (yUwV)e = 0, \qquad \text{(ii)} \quad yz + xw = 0. \tag{4}$$

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

Eliminating x from equations (4) it is found that

$$yz = yUR(wV)R(e)R(z)^{-1}R(w). \tag{5}$$

Now, denote by 1 and -1 the elements of C_2, the cyclic group of order 2, and define the mapping F of G upon C_2 by $F(x) = 1$, if $x \in H$, and $F(x) = -1$, if $x \notin H$. Clearly F is a homomorphism of G upon C_2, and it is easily verified that $F[aR(b)^{-1}] = F(a)F(b)$, and $F(aU) = F(aV) = F(a)$, for all a, $b \in G$. From equation (5) it follows that $F(yz) = F(y)F(w)F(e)F(z)F(w)$, which implies that $F(e) = 1$, contrary to the hypothesis $e \notin$ H. Thus, (x, y) $(z, w) = (0, 0)$ implies either $x = y = 0$, or $z = w = 0$. The absence of divisors of zero in the set of non-zero elements of A^* insures, in this case, that they form a loop with respect to the multiplication defined in (3). It is readily verified that the remaining postulates for a division algebra are satisfied by A^*. This completes the proof of the theorem.

It is easily seen that if the algebra A of Theorem 3 is a Galois field, if $U = V = I$, and if e is a non-square in A, then the algebra A^* of Theorem 3 is simply $A(e)$, the quadratic extension of A. It should be noted, however, that if $U = V \neq I$, then the algebra A^* is not associative. Thus, let $A = GF(q^{nk})$, so that A is an associative division algebra of order n over $F = GF(q^k)$. Choose U and $V = U$ from the set of automorphisms of A relative to F. Then, if $e \notin H$, that is, if e is a non-square in A, the algebra A^* is a commutative, non-associative division algebra with unit element of order $2n$ over F. The following theorem shows that under certain conditions the automorphism group A^* contains the cyclic group of order $2n$.

THEOREM 4. *Let F be the Galois field $GF(q^k)$, $q > 2$, and A the field $GF(q^{nk})$, where n is any positive integer. Let S be a generating automorphism of the automorphism group of A relative to F. If A^* is the non-associative algebra of order $2n$ over F defined as in Theorem 3 with $U = V = S$, and e any non-square in A, then the automorphism S of A may be extended to an automorphism T of A^* relative to F. Furthermore, if n is odd, T has period $2n$.*

Proof. Since e is a non-square in A, it follows that e^{-1} and eS are non-squares in A, and hence that $e^{-1} \cdot eS$ is a square. Denote by c either of the two square roots of $e^{-1} \cdot eS$. For any $x \in A$, let $N(x)$ be the usual norm of x over F, that is $N(x) = x \cdot xS \cdot xS^2 \ldots xS^{n-1}$, then clearly $N(c) = \pm 1$. Note that if n is odd, c may be chosen so that $N(c) = -1$. Let $f = cS^{n-1}$, and define the linear transformation T of A^* by $(a, b)T = (aS, f \cdot bS)$. It is readily verified that T is an endomorphism of A^* and that $T^{2n} = I$. These two facts imply that T is an automorphism of A^*. When n is odd, f may be chosen so that $N(f) = -1$. If j is the period of T, and b a non-zero element of A, it is readily verified that $(a, b)T^n \neq (a, b)$. It follows that $j \neq n$. However, $(a, b)T^j = (aS^j, *) = (a, b)$, for all a, $b \in A$, whence $aS^j = a$, for all $a \in A$. Hence $j = hn$, for some positive integer h. Finally, $T^{2n} = I$ implies that $2n = rj$, for some positive integer r. From these relations involving the integers j, h, n, and r it may be inferred that $j = 2n$. This completes the proof of the theorem.

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

Before proceeding to the next theorem it is necessary to make the following definition. Let A be a division algebra with unit element of order n over a field F. If A has a basis $1, e, e^2, \ldots, e^{n-1}$, with multiplication given by[4]

$$(6) \qquad e^n = \phi, \qquad e^i \cdot e^j = \phi(i, j)e^{i+j}, \qquad i, j = 1, \ldots, n-1,$$

where it is understood that $i + j$ is reduced modulo n, and ϕ, $\phi(i, j) \in F$, then A is said to have a *cyclic basis* relative to F.

THEOREM 5. *Let n be any positive integer and $F = GF(q^k)$, $q > 2$, a Galois field with $q^k = 2ns + 1$, for some positive integer s. Then there exists a commutative, non-associative division algebra A^* of order $2n$ over F with the following properties:*

(i) *A^* has a cyclic basis relative to F,*

(ii) *the automorphism group of A^* relative to F is the cyclic group of order $2n$,*

(iii) *A^* contains a unique associative subalgebra of order n over F isomorphic to the field $GF(q^{nk})$.*

Proof. Note that $q^k = 2ns + 1$ is equivalent to the statement: F contains $2n$ distinct $(2n)$th roots of unity. In this case there exists a polynomial $\lambda^n - \phi$, irreducible in $F[\lambda]$, and such that if n is even, $-\phi$ is a non-square in F, and if n is odd, ϕ is a non-square in F. Let $A = GF(q^{nk})$ and denote by S a generating automorphism of the automorphism group of A relative to F. Now, there exists an element $e \in A$, which satisfies $\lambda^n - \phi = 0$, and is a non-square in A. With this choice of e, and with $U = V = S$, the algebra A^* of Theorem 3 is clearly a commutative division algebra with unit element of order $2n$ over F. First it will be shown that A^* possesses a cyclic basis. Denote by $\zeta \in F$ a primitive $(2n)$th root of unity. Then ζ^2 is a primitive nth root of unity and without loss of generality it may be assumed that $eS = \zeta^2 e$. If $g = (0, e^{n-1})$, it is easily verified, by finite induction on i, that the relations

$$(7) \qquad \text{(i)} \quad g^{2i-1} = \alpha_{2i-1}(0, e^{n-i}), \qquad \text{(ii)} \quad g^{2i} = \alpha_{2i}(e^{n-i}, 0),$$

where $\alpha_j \neq 0$, $\alpha_j \in F$ $(j = 1, \ldots, 2n)$ hold for $i = 1, \ldots, n$. Since $1, e, e^2, \ldots, e^{n-1}$ is a basis for A over F, it follows that $1, g, g^2, \ldots, g^{2n-1}$ is a basis for A^* over F. Again, by induction it may be shown that there exist non-zero elements $\phi(r, s) \in F$ $(r, s = 1, \ldots, 2n-1)$ such that $g^r \cdot g^s = \phi(r, s)g^{r+s}$, where $r + s$ is reduced modulo $2n$ if necessary. Note also that, by relation (7, ii), $g^{2n} = \alpha_{2n}\phi \in F$. Thus, A^* has a cyclic basis relative to F.

Now, it is evident that the mapping T of A^* upon A^* defined by $g^i T = \zeta^{-1} g^i$ is an automorphism of period $2n$. Thus, the automorphism group of A^* relative to F contains the cyclic group of order $2n$. Let K be any automorphism of A^* relative to F and note that for the case $n = 2$, the uniqueness (see Theorem 1) of the subalgebra of order 2 implies that K induces an automorphism of this subalgebra. It will be assumed then that $n > 2$, and it will be shown that the

[4] The following convention is adopted for positive integral powers in a non-associative algebra: if x is any element of the algebra and t any positive integer, then x^t denotes the right power of x, defined by $x^t = x[R(x)]^{t-1}$.

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

subalgebra A is a unique associative subalgebra of A^*, of order n over F. Indeed, if it is assumed that K does not induce an automorphism of A, then K maps A into an isomorphic subalgebra B of A^*. Since $1, e, e^2, \ldots, e^{n-1}$ is a basis for A over F, it follows that $(eK)^i$ $(i = 0, 1, \ldots, n-1)$ is a basis for B. Then, $eK = (a, b) \notin A$, so that $b \neq 0$. Let $f = eK = (a, b)$, then, since B is an associative subalgebra of A^*, it follows that $(f^2)^2 = f^3f$. This last equation, written in terms of a, b, is

$$[*, 4ab(a^2 + (bS)^2e)] = [*, 4a^3b + 2ab(bS)^2e + 2(aS)b(bS)^2e].$$

Equating the second "components" of $(f^2)^2$ and f^3f, it is found that $a = aS$. Thus $a \in F$, and denoting a by α, the relation $(f^2)^2 = f^3f$, in terms of a, b simplifies to

$$[\alpha^4 + 6\alpha^2(bS)^2e + (bS)^4e^2, *] = [\alpha^4 + 6\alpha^2(bS)^2e + (bS)^2(bS^2)^2eeS, *].$$

Equating the first "components" and noting that $eS = \zeta^2e$, it is seen that $(bS)^2 = \zeta^2(bS^2)^2$. This last equation may be written $(b^2S)S = \zeta^{-2}(b^2S)$, from which it follows that $b^2S = \psi e^{n-1}$, $\psi \in F$. Now,

$$f^2 - 2\alpha f + \alpha^2 - \psi\,\phi = (f - \alpha)^2 - \psi\,\phi = (0, b)^2 - \psi\,\phi = 0.$$

Thus, $1, f, f^2$ are linearly dependent over F, which implies $n = 2$, contrary to the assumption $n > 2$. This shows that the subalgebra A is the only associative subalgebra of order n over F, contained in A^*. In particular then, the arbitrary automorphism K of A^* induces an automorphism of A, so that $(e, 0)K = \zeta^{2j}(e, 0)$ for some positive integer j. Since $[(0, 1)]^2 = (e, 0)$, it follows that $(0, 1)K = \pm \zeta^j(0, 1)$; hence

$$gK = (0, e^{n-1})K = [(0, 1)]\,[(e^{n-1}, 0)K] = \pm \zeta^{j(2n-1)}g.$$

Thus, gK is the product of g and a $(2n)$th root of unity, that is, K coincides with a power, T^r, of the automorphism T defined above. It is seen then that the automorphism group of A^* relative to F is the cyclic group of order $2n$. This completes the proof of the theorem.

6. Finite division algebras of order n whose automorphism group contains the cyclic group of order n. Let A be a division algebra of order n over an arbitrary field F. If A has a cyclic basis relative to F and if m is a divisor of n, then it is evident that A contains a subalgebra of order m. The following theorem gives a sufficient condition, not quite as immediate as the above, for a finite division algebra of order n to contain a subalgebra of order m, where m is any divisor of n.

THEOREM 6. *Let A be a division algebra of order n over a field $F = GF(q^k)$, where $n = hq^t$, $(h, q) = 1$. Let T be an automorphism of A relative to F with period n. If the minimum function of T is of degree n, then, for every divisor m of n, A contains a subalgebra A_m, of order m over F, whose automorphism group relative to F contains the cyclic group of order m.*

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

Proof. Let Ω be the root field of the polynomial $\lambda^h - 1 \in F[\lambda]$. Then there exists an element $\zeta \in \Omega$ such that

$$\lambda^h - 1 = \prod_{i=0}^{h-1} (\lambda - \zeta^i)$$

in $\Omega[\lambda]$. Since T satisfies $\lambda^n - 1 = 0$, and since its minimum function is of degree n, it follows that $\lambda^n - 1 = 0$ is the minimum equation of T. Now in $\Omega[\lambda]$,

$$\lambda^n - 1 = (\lambda^h - 1)^{q^t} = \prod_{i=0}^{h-1} (\lambda - \zeta^i)^{q^t}.$$

Thus, there exists a basis for the algebra A_Ω such that a representation for T is given by [**9**, p. 128, Theorem 65]

$$T = E_0 \oplus E_1 \oplus \ldots \oplus E_{h-1}, \quad E = \zeta^i I + E \qquad (i = 0, 1, \ldots, h-1),$$

where I is the $q^t \times q^t$ identity matrix and E is the $q^t \times q^t$ matrix with 1 everywhere in the diagonal just below the main diagonal and zeros elsewhere. If m is a divisor of n, let q^r be the highest power of q which divides m, so that $m = sq^r$ $(s, q) = 1$, and s divides h. Since $(s, q) = 1$, it is seen that the field Ω contains s distinct sth roots of unity, each of which is also an hth root of unity. Thus in the matrix T^s given by $T^s = E_0{}^s \oplus E_1{}^s \oplus \ \ldots \ \oplus E_{h-1}{}^s$, exactly s of the components $E_i{}^s$ will have 1 everywhere in the main diagonal and the remaining $h - s$ components will have diagonal elements different from 1. Let $E_j{}^s$ be one of the components with 1 along the main diagonal, that is, let ζ^j be one of the sth roots of unity. Then,

$$E_j{}^s = (\zeta^j I + E)^s = I + s\zeta^{j(s-1)}E + \binom{s}{2}\zeta^{j(s-2)}E^2 + \ldots + E^s = I + EF,$$

where

$$F = s\zeta^{j(s-1)}I + \binom{s}{2}\zeta^{j(s-2)}E + \ldots + E^{s-1}.$$

By the definition of E, and since $(s, q) = 1$, F is non-singular. Furthermore,

$$E_j{}^m - I = (E_j{}^s - I)^{q^r} = E^{q^r} \cdot F^{q^r},$$

and hence the nullity of $E_j{}^m - I$ is equal to the nullity of E^{q^r}. Noting that the first v rows of E^v consist entirely of zeros, and that the remaining $q^t - v$ rows are linearly independent, it follows that the nullity of the matrix $E_j{}^m - I$ is exactly q^r. If ζ^p is one of the $h - s$ hth roots of unity which is not an sth root of unity, then clearly $E_p{}^m - I$ has nullity zero. Thus, in the expression of $T^m - I$ as a direct sum, given by[5]

$$T^m - I = (E_0{}^m - I) \oplus (E_1{}^m - I) \oplus \ldots + (E_{h-1}{}^m - I),$$

exactly s of the components have nullity q^r, and the remaining components have nullity zero. Thus, the nullity of $T^m - I$ is $sq^r = m$. Since the nullity of a

[5] In $T^m - I$ it is understood that I denotes the $n \times n$ identity matrix.

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

matrix with elements in a field F is invariant under an extension of F, it follows that in the original algebra A over the given field F there exist exactly m linearly independent elements in the null space of $T^m - I$. Thus, the subalgebra A_m, consisting of all elements of A which are mapped into themselves by T^m, is of order m over F. It is obvious that the automorphism T of A induces an automorphism T' of A_m of period m. Hence the group of automorphisms of the algebra A_m relative to F contains the cyclic group of order m. This completes the proof.

Suppose that F is a Galois field, $F = GF(q^k)$, and $n = hq^t$, $(h, q) = 1$. If h divides $q^k - 1$, then F contains h distinct hth roots of unity. If A is an algebra of order n over F whose automorphism group relative to F contains the cyclic group of order n, then it is seen that every hth root of unity is a characteristic root of any automorphism T of A which generates the cyclic group of automorphisms of order n. Thus, if

$$M = T^{q^t},$$

so that the transformation M has period h, then it is clear that every characteristic root of M is an hth root of unity. Furthermore, the set of distinct characteristic roots of M is a subgroup of the set of hth roots of unity, for if η_1, η_2, are any two characteristic roots, then there exist $a_1, a_2, \in A$, $a_1 \neq 0$, $a_2 \neq 0$, such that $a_1 M = \eta_1 a_1$, $a_2 M = \eta_2 a_2$, whence

$$(a_1 a_2)\ (M - \eta_1\, \eta_2 I) = 0, \qquad a_1 a_2 \neq 0,$$

so that $\eta_1\, \eta_2$ is a characteristic root. If the set of distinct characteristic roots does not contain all of the hth roots of unity, then it is the set of sth roots of unity for some $s < h$, with s dividing h. Since a basis for A may be chosen in such a way that M is represented by a diagonal matrix, whose diagonal elements are sth roots of unity, it follows that $M^s = I$, contrary to the hypothesis that M is of period h. Thus, every hth root of unity is a characteristic root of M. Finally, since the mapping

$$\alpha \rightarrow \alpha^{q^t}$$

of F upon F, is a premutation of the hth roots of unity, it is seen that every characteristic root of M is a characteristic root of T. If $t > 0$, it is not known whether or not the minimum function of T is of degree n. However, if $t = 0$, so that $n = h \mid (q^k - 1)$, then the previous remarks indicate that the minimum function of T is of degree n, and Theorem 6 is applicable. In fact, in this case, it is possible to choose a basis $1, e_1, \ldots, e_{n-1}$ for A over F in such a way that $e_i T = \zeta^i e_i$, where ζ is a primitive nth root of unity. It is readily verified that the multiplication for A is given by (6). Thus the following theorem has been proved.

THEOREM 7. *If A is a division algebra of order n over a field $F = GF(q^k)$, where $q^k = hn + 1$ for some positive integer h, and if the automorphism group of A*

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press

relative to F contains the cyclic group of order n, then A has a cyclic basis relative to F.

Added in proof. The question discussed in the second paragraph of §4 has been answered by A. A. Albert. See abstract 421, Bull. Amer. Math. Soc., vol. 57 (1951), p. 457.

References

1. R. H. Bruck, *Some results in the theory of linear non-associative algebras*, Trans. Amer. Math. Soc., vol. 56 (1944), 141–198.
2. ———, *Contributions to the theory of loops*, Trans. Amer. Math. Soc., vol. 60 (1946), 245–354.
3. L. E. Dickson, *On finite algebras*, Nachr. Ges. Wiss. Göttingen (1905), 358–393.
4. ———, *Linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc., vol. 7 (1906), 370–390.
5. ———, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc., vol. 7 (1906), 514–522.
6. ———, *On linear algebras*, Amer. Math. Monthly, vol. 13 (1906), 201–205.
7. ———, *On triple algebras and ternary cubic forms*, Bull. Amer. Math. Soc., vol. 14 (1907–08) 160–169.
8. Harriet Griffin, *The abelian quasigroup*, Amer. J. Math., vol. 62 (1940), 725–734.
9. C. C. MacDuffee, *Vectors and matrices* (Carus Mathematical Monographs, No. 7, 1943).
10. E. H. Moore, *A double infinite system of simple groups*, International Mathematical Congress, 1893.
11. J. H. M. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc., vol. 6 (1905), 349–352.
12. Daniel Zelinsky, *Nonassociative valuations*, Bull. Amer. Math. Soc., vol. 54 (1948), 175–183.

University of Missouri

https://doi.org/10.4153/CJM-1952-044-6 Published online by Cambridge University Press