A DETERMINATION OF ALL NORMAL DIVISION ALGEBRAS IN SIXTEEN UNITS*

BY

A. ADRIAN ALBERT

INTRODUCTION

The chief outstanding problem in the theory of linear associative algebras over an infinite field F is the determination of all division algebras. This problem is equivalent to that of the determination of all normal division algebras, or algebras A in which the only elements of A commutative with every element of A are the quantities of its reference field F.

The order of a normal division algebra is the square of an integer. All normal division algebras in 1^2†, 2^2‡, and 3^2§ units have been determined. In this paper all normal division algebras in 4^2 units, the next case, are determined and shown to be the algebras of Cecioni.||

1. RESULTS¶ PRESUPPOSED

THEOREM I. *Every normal division algebra of order n^2 over a non-modular field has rank n.*

THEOREM II. *Every normal division algebra A of order n^2 contains an element q whose minimum equation is of degree n.*

Evidently the minimum equation of any element q of A is irreducible, and conversely, if an element of A is the root of an irreducible equation in F with leading coefficient one, then this equation is its minimum equation. We shall say that an element q of the algebra A is of rank k if the division algebra $F(q)$ is of rank k and thus if the minimum equation of q is of degree k. An equation will be said to be an irreducible equation in F if its coefficients are in F and if it is irreducible with respect to the field F.

---

* Presented to the Society, April 6, 1928; received by the editors in September, 1928.

† The only division algebras in one unit are fields.

‡ See Dickson, *Algebren und ihre Zahlentheorie*, p. 46.

§ Wedderburn, these Transactions, vol. 22 (1921), p. 132.

|| Rendiconti del Circolo Matematico di Palermo, vol. 47 (1923), pp. 209–254.

¶ See Dickson, *Algebras and their Arithmetics*, German and English editions, for these results and their proofs.

THEOREM III. *The order of any sub-algebra of a division algebra is a divisor of the order of the main algebra.*

THEOREM IV. *Every element q of a normal division algebra A of order n^2 which is the root of an irreducible equation of degree n in F has the property that every element of A which is commutative with q is a polynomial in q with coefficients in F.*

THEOREM V. *The only elements of a normal division algebra A which are commutative with every element of A are elements of the reference field F.*

Evidently every rational function with coefficients in F of any element q of A is expressible as a polynomial in q with coefficients in F and is commutative with q. It may also be easily shown that any transform yqy^{-1} of an element q of A satisfies the minimum equation of q.

Hence the algebra A of order 16 over the non-modular field F contains an element satisfiying the reduced irreducible equation

$$\phi(\omega) \equiv \omega^4 + \alpha\omega^2 + \beta\omega + \gamma, \quad \alpha, \beta, \gamma \text{ in } F. \tag{1}$$

LEMMA 1. *If $A = BC$ where B and C are polynomials in an indeterminate ω over a division algebra D, and if $\omega - t$ is a right divisor of A but not of C, where t is in D, so that $C = Q(\omega - t) + R$, where $R \neq 0$ is independent of ω, then $\omega - y$ is a right divisor of B, where $y = RtR^{-1}$.*

THEOREM VI. *If A is a normal division algebra of order sixteen and if* (1) *is the minimum equation of an element q of A, then there exist further elements j, k, l of A which are transforms of q by elements of A such that*

$$\phi(\omega) \equiv (\omega - l)(\omega - k)(\omega - j)(\omega - q), \tag{2}$$

and also $\phi(\omega)$ is the product of the same factors permuted cyclically.

As a corollary of the proof of the above theorem we have the following theorem:

THEOREM VII. *If $\phi(\omega) = LM$, where L and M both contain ω, there exists a transform of q, $y = vqv^{-1}$, such that $\omega - y$ is not a right divisor of M and hence, if $M = Q(\omega - y) + R$, then $\omega - RyR^{-1}$ is a right divisor of L.*

2. REDUCTION TO THE DETERMINATION OF ALGEBRAS ASSOCIATED WITH THE GROUP G_8

Let A be any normal division algebra in sixteen units. If A contains an element i satisfying an irreducible equation in F such that, in the algebraic

sense, three of its distinct roots are rational functions of i and are distinct from i, then the algebra A is said to be of type Γ and is known.*

We shall now prove a theorem of fundamental importance in our determination.

THEOREM VIII. *If A is a normal division algebra in sixteen units containing an element q which satisfies the irreducible equation* (1) *with the property that not all of its ordinary complex roots are rational functions with coefficients in F of one of them, then A contains an element i satisfying the irreducible equation*

$$\psi(\omega) = \omega^4 + \delta\omega^2 + \epsilon = 0, \qquad \delta, \epsilon \text{ in } F. \tag{3}$$

By Theorem VI we may write the equation (2), where j, k, and l are transforms of q by elements of A. If $jq = qj$ then j is a polynomial in q with coefficients in F, by Theorem IV. Let $j = yqy^{-1}$. Then $j = \theta(q) = yqy^{-1}$. Therefore $\theta^2(q) = y\cdot\theta(q)\cdot y^{-1} = y^2qy^{-2}$. But $j \neq i$ since (1) is irreducible. Thus $\theta^2(q) \neq \theta(q) = j$. If $\theta^2(q) \neq q$ then the roots of (1) are q, j, $\theta^2(q)$, $-q-j-\theta^2(q)$, and are all polynomials in q. But this is impossible since then the ordinary complex roots of (1) are all rational functions of one of them with coefficients in F. Hence $q = \theta^2(q) = y^2qy^{-2}$. Therefore $y^2q = qy^2$ and, by Theorem IV, y^2 is a polynomial in q. But if y^2 is of rank four then $(1, y^2, y^4, y^6) = F(y^2)$ is an algebra of order four contained in $F(y)$, of order at most four, and hence is $F(y)$. Hence y is a polynomial in y^2 and consequently in q and is commutative with q. Hence, in this case, $j = yqy^{-1} = q$, a contradiction. Hence y^2 is not of rank 4 but is of rank 1 or 2 and satisfies $\omega^2+\delta\omega+\epsilon=0$, δ, ϵ in F, and thus $y^4+\delta y^2+\epsilon=0$, and y, in A, satisfies an equation of the desired type and is taken as the desired element if its rank is four. If not, then, since its rank is evidently not one, y is the root of an irreducible quadratic. (y could not be of rank 3 since A contains no sub-algebras of order 3, a non-divisor of 16.) Hence $y^2 = -\xi y+\eta$. If $\xi \neq 0$ this equation expresses y as a polynomial in y^2 and hence as a polynomial in q, which is not possible since $yq \neq qy$. Hence $\xi = 0$ and $y^2 = \eta$ in F. Let $z = qy$. Then $z^2 = qyqy = qjy^2 = qj\eta$. If z is of rank 2 then it satisfies $z^2 = \lambda z+\mu$. If $\lambda \neq 0$, this expresses $z = qy$ as a linear function of z^2 and thereby as a polynomial in q since j is a polynomial in q by hypothesis. This same relation gives $y = q^{-1}z$ as a polynomial in q which contradicts the hypothesis. Hence $\lambda = 0$. But $z^2 = \eta qj$. Hence $j = \kappa/q$ is a root of (1), where $\kappa = \mu/\eta \neq 0$ is in F. Substituting this value for the indeterminate in (1) and multiplying by q^4 we obtain $\gamma q^4+\beta\kappa q^3+\kappa^2q^2+\kappa^4=0$. Substituting the value of q^4 from (1) we obtain a linear combination of 1, q, q^2, q^3 equal to zero and thus have the property that the coefficients are all zero. The coeffi-

* See Dickson, *New division algebras*, these Transactions, vol. 28 (1926), pp. 207–234.

cient of q^3 is $\beta\kappa=0$ and since $\kappa\neq 0$, $\beta=0$ and (1) is the desired equation. The only remaining case is thus the case where z is of rank 4. But $RzR^{-1}=-z$ where $R=j-q$ and $yj=qy$, $yq=jy$. Hence $-z$ is a root of the quartic equation satisfied by z and thus the equation satisfied by z has only even powers and is (3).

We shall prove, as the next step in our proof, the following lemma:

LEMMA 2. *If x is of rank 4 and $F(x)$ contains an element r of rank 2, then $F(x)$ and hence A contains an element i satisfying an equation of type* (3).

Let the equation of the element r be $r^2+\gamma_1 r+\gamma_2=0$, γ_1, γ_2 in F. Let $s=r+\gamma_1$. Then $s^2=\epsilon$ in F. The elements 1, s, x, sx are linearly independent for, if not, then $a+bx=0$, for a and b not both zero, where a and b are in $F(s)$. Thus if $b=0$ the equation becomes $a=0$, a contradiction, and if $b\neq 0$, then it has an inverse in the quadratic field $F(s)$, whence $x=c$ where $c=\lambda+\mu s$, an element of $F(s)$. But every element of $F(s)$ evidently satisfies a quadratic with coefficients in F, since the element s^2 is in F. Hence x is of rank 2, contrary to the hypothesis that x is of rank 4. Hence we may take the elements 1, s, x, sx as the basal units of $F(x)$. Therefore x^2, which is in $F(x)$, is expressible as a linear combination of the four units with coefficients in F and we obtain

$$(4)\qquad x^2 = 2ax + b - a^2 \quad \text{or} \quad (x+a)^2 = b, \quad a, b \quad \text{in} \quad F(s).$$

If the element $y=x+a$ is of rank two then b is in F, since then $y^2+\lambda y+\mu=0$ and thus $b+\lambda(x+a)+\mu=0$, or $\lambda x+(\lambda a+b+\mu)=0$. But 1, x, s are linearly independent. Hence $\lambda=0$ and $b=-\mu$ in F. Take the expression $a=\alpha_1+\alpha_2 s$. We have $[(x+\alpha_1)+\alpha_2 s]^2=\beta$ in F. The element $x+\alpha_1$ is of rank 4, since if not, then $\psi(x+\alpha_1)\equiv\theta(x)=0$ and x is the root of a quadratic in F, a contradiction. Let $x+\alpha_1=u$, of rank 4. Then $u^2+2\alpha_2 su+\alpha_2^2\epsilon=\xi$. Let $r=-2\alpha_1 s$, and $\beta-\alpha_2^2\epsilon=\gamma$. Then $u^2=ru+\gamma$ where $r^2=\xi$ of F, and $u^3=ru^2+\gamma u=r(ru+\gamma)=\gamma u=\xi u+\gamma u+\gamma r$, so that we have $u^4=(\xi+\gamma)u^2+\gamma(u^2-\gamma)=(2\gamma+\xi)u^2-\gamma^2$, an equation of the desired form. (The Greek letters of (1) are not these above.)

There remains only the case where y is of rank 4. We then have $b=\beta_1+\beta_2 s$, and obtain $y^4=\beta_1^2+2\beta_1\beta_2 s+\beta_2^2=\beta_1^2+\beta_2^2\epsilon+2(y^2+\beta_1)$, an equation with coefficients in F, and which is in the desired form. Thus the lemma is proved.

We shall now consider the remaining case, that where $jq\neq qj$. Equating the coefficients in (1) and (2) we have

$$(5)\qquad q + j + k + l = 0, \quad lk + (lj + lq) + (kj + kq) + jq = \alpha,$$

$$(6)\qquad lkjq = \gamma, \quad lkj + lkq + ljq + kjq = -\beta,$$

from which, if we let $s=jq$, $t=q+j$, we obtain

$$\gamma s^{-1} + s = t + \alpha, \qquad \gamma s^{-1} = ts + \beta. \tag{7}$$

Hence t^2 is expressible as a polynomial in the element s of A with coefficients in F by the fact that s^{-1} is so expressible.

Case A. If t is of rank 4, then, if t^2 is of rank 2, by the lemma A contains an element of the desired kind. It is thus sufficient to treat the case t^2 of rank 4, since if t^2 is of rank one, the only other possible case, then t is the root of the quadratic $t^2=a$, a in F, a contradiction. Then 1, t^2, t^4, t^6 are linearly independent and may be taken as the basal units of $F(t)$ whence t is expressible as a polynomial in t^2 and hence in the element s. Hence $st=ts$. Hence, since t is of rank 4, s is in $F(t)$. Hence, from $(7)_2$ and $(6)_1$ where $r=s^{-1}$, $r+s=t^2+\alpha$, $rs=\gamma$, and since all of the elements are commutative, we have, by elementary algebra, that r and s are roots of the equation $w^2-(t^2+\alpha)w+\gamma=0$ or thus $s^2=(t^2+\alpha)s-\gamma$. Also we obtain from $(7)_1$ by multiplying it on the right by t

$$rt + st = (t^2 + \alpha)t. \tag{8}$$

Adding (8) and the equation $st-rt=-\beta$ which is obtained from $(7)_2$ by the property that $st=ts$, we obtain

$$2st = t^3 + \alpha t + \beta \equiv z. \tag{9}$$

Thus $z-\beta=t(t^2+\alpha)$. Squaring equation (9) and applying the relation $s^2=s(t^2+\alpha)-\gamma$, we have $z^2-2\beta z=4t^2\gamma$, and replacing $z-\beta$ by its value $t^3+\alpha t$ in the equation

$$(z - \beta)^2 = 4t^2\gamma + \beta^2, \tag{10}$$

we have $t^2(t^2+\alpha)^2=4t^2\gamma+\beta^2$, a cubic in t^2, contrary to the hypothesis that t^2 is of rank four. Hence we need only consider the case t of rank two.

Case B. Here $t^2+\lambda t+\mu=0$. If $\lambda\neq 0$ then this equation expresses t as a function of t^2 and hence of s. Hence t is commutative with s and $(7)_2$ becomes $r-s=-\beta t^{-1}$. Subtracting this from $(7)_1$ we obtain the relation $2s$ equals a polynomial in t, or $s=\xi+\eta t$, since t is of rank 2. Hence $jq=\xi+\eta(j+q)$, $j(q-\eta)=\xi+\eta q$. But $q-\eta\neq 0$. Hence it has an inverse and j is expressible as a rational function of q, a contradiction, and $\lambda=0$, $t^2=f$, in F. But $t^2=(j+q)^2=q^2+qj+jq+j^2$. We have $j^2-q^2=f-qj-jq-2q^2=f-(qj+q^2+jq+q^2)=f-(qt+tq)$. But $t(qt+tq)=tqt+ft=tqt+tf=(qt+tq)t$. Hence t is commutative with j^2-q^2. If this element is of rank 4, then, by Lemma 2, $F(z)$, where $z=j^2-q^2$, contains t of rank 2 and hence an element of the desired type. If this is not so, then, if $z+t$ is of rank 4, the theorem is satisfied, since t is commutative with $z+t$ and hence is in $F(z+t)$ and is of rank 2.

The conclusion then follows by Lemma 2. Hence the only remaining case is that where z and $z+t$ are both of rank 2, where $zt=tz$. Let $z^2=\lambda z+\mu$, λ, μ in F. Let $(z+t)^2+\xi(z+t)+\eta=0$, ξ, η in F. Then we have that $z^2+2tz+t^2+\xi(z+t)+\eta=0$, whence $z(\lambda+\xi+2t)=-(\mu-f+\eta+\xi t)$. But $\lambda+\xi+2t\neq 0$ since t is not in F. Hence the above equation expresses z as a rational function of t and since t is of rank 2 we have $z=\rho+\sigma t$, ρ, σ in F. Hence we have, by the definition of z and t, that $j^2-i^2=\rho+\sigma(i+j)$ or $j^2-\sigma j=i^2+\sigma i+\rho$. Hence $y=j^2-\sigma j$ is commutative with i and is a polynomial in i. If y is of rank 2, then, by Lemma 2, the theorem is satisfied. If not, then y, in $F(j)$, is of rank 4 and hence the elements 1, y, y^2, y^3 may be taken as a basis of $F(j)$ and hence j is expressible as a polynomial in y with coefficients in F and thereby as a polynomial in i with coefficients in F, a contradiction, since we assumed at the beginning of this section that $ij-ji\neq 0$. This proves the theorem.

If the normal division algebra A contains an element satisfying an equation of type (3) such that all of its roots are rational functions of one of them, then A is of type Γ. If A does not, then it contains an element satisfying an equation of type (3) such that not all of its roots are rational functions of one of them, by the theorem just proved. The algebras of type Γ are of two known kinds. They are either algebras of type D associated with an element satisfying a cyclic quartic, or are algebras of type E satisfying a non-cyclic abelian quartic or quartic with group G_4. Also every normal division algebra in sixteen units containing an element satisfying a cyclic quartic is an algebra of type D, and every normal division algebra containing an element satisfying a quartic with group G_4 is an algebra of type E. The necessary and sufficient condition that a quartic have group G_4 is that it be irreducible and that all of its roots be rational functions of one of them such that, if i and $\theta(i)$ are roots then $\theta^2(i)=i$, so that the equation is non-cyclic. We shall prove

THEOREM IX. *Every normal division algebra in sixteen units over a field F contains an element p satisfying a quartic with coefficients in F and group G_4. Hence every normal division algebra in sixteen units is an algebra of type E.*

Let A be a normal division algebra in sixteen units over F. Then, by the argument just made, A is of type Γ or A contains an element i satisfying the quartic equation

$$\phi(\omega)\equiv\omega^4+\alpha\omega^2+\beta=0,\quad \alpha,\beta \text{ in } F, \tag{11}$$

irreducible in F, and such that not all of its roots are rational functions of one of them. Since i is a root of (11) so is $-i$. Applying Lemma 1 with $C=-i$ and $t=-i$ to $A=\phi(\omega)$ we have $R=-2i$ and $RtR^{-1}=-i$. Hence

$\phi(\omega)=Q(\omega)(\omega+i)(\omega-i)$. By Theorem VII there exists an element v of A such that $\omega-x$ is not a right divisor of $C=\omega^2-i^2$, where $x=viv^{-1}$. Hence, where the remainder on division of C by $\omega-x$ may be easily verified to be $R=x^2-i^2$, $\omega-RxR^{-1}$ is a right divisor of Q. Since Q is a polynomial in ω^2, $\omega+RxR^{-1}$ is a right divisor of Q and hence, by Lemma 1, $Q=(\omega+k)(\omega-k)$ where $k=ziz^{-1}$ and $z=Rv=(x^2-i^2)v$. We hence have the decomposition of (11) in the form (2) where here $l=-k$ and $j=-i$. Comparing coefficients in this decomposition with (11) we obtain the relations

$$k^2+i^2=-\alpha, \qquad k^2i^2=\beta. \tag{12}$$

Since $k=ziz^{-1}$, $zi=kz$, $zi^2=k^2z$, $z^2i^2=zzi^2=zk^2z=z(-\alpha-i^2)z=(-\alpha+\alpha+i^2)z^2=i^2z^2$. Obviously k^2 is a polynomial in i^2 and hence is commutative with i. Similarly i^2 is commutative with k. Also if $g(i)$ is any polynomial in i then $zg=g(k)z$. Let $z^2=s$, where s is in F. Then $z^2i=iz^2$. Let $y=ik-ki$, so that $iy=i^2k-iki=ki^2-iki=-yi$. Hence $iyi^{-1}=-y$. Also $z(ik-ki)=kzk-zki=kzziz^{-1}-zziz^{-1}i=ksiz^{-1}-siz^{-1}i=kiz-izi=(ki-ik)z=-yz$, so that $zyz^{-1}=-y$. The element $p=i^2+y$ is in the algebra consisting of all polynomials in y and i^2, with coefficients in F. This algebra is a field since $yi^2=-iyi=i^2y$. Hence, since A is of rank four, it is a field of order four or of order two. Its order is not two since y is not in the quadratic sub-field $F(i^2)$ for otherwise y would be a polynomial in i^2 and hence commutative with i, a contradiction of $yi=-iy$; while $y\neq 0$ since if $y=0$ then $ik=ki$ and k is a polynomial in i and the roots of (11) are all polynomials in i, contrary to hypothesis. Hence the field $F(i^2, y)$ is of order 4. The element p is not of rank 1 since it is obviously not in F. It is not of rank 2, for then $y^2=bp+c$, where b and c are in F, whence $i^4+2i^2y+y^2=bi^2+by+c$. But since $y^2i=yyi=-yiy=iy^2$ then y^2 is a polynomial in i. But $yg(i)=g(-i)y$, for any polynomial $g(i)$, and $yy^2=y^2y$. Hence y^2 is a polynomial in i^2. Hence, since y is not in $F(i^2)$, $2i^2=b$, and a contradiction is secured since i is the root of an irreducible quartic. Hence p is of rank 4. But $F(p)$ is then of order 4 and is contained in $F(i^2, y)$ of order 4. Hence $F(p)=F(i^2, y)$ and every polynomial in i^2 and y is a polynomial in p. Let $p_2=ipi^{-1}=i(i^2+y)i^{-1}=i^2-y$, $p_3=zpz^{-1}=zyz^{-1}+zi^2z^{-1}=-y+k^2$, $p_4=zp_2z^{-1}=ip_3i^{-1}=y+k^2$. These elements are transforms of the element p and hence are roots of the irreducible quartic satisfied by p. They are in the field $F(i^2, y)$ and hence are polynomials in p. Since z^2 and i^2 are both commutative with both i^2 and y they are commutative with p and hence $p_2^2(p)=p_3^2(p)=p_4^2(p)=p$. The elements p, p_2, p_3, p_4 are all distinct since $k^2\neq i^2$ and $y\neq -y$ while y is not a polynomial in i^2. Hence the quartic satisfied by p has the four distinct roots p, p_3, p_2, p_4 all of which are

polynomials in p, such that the iterative of the polynomial gives p and hence such that the group of the equation is G_4.

We shall next consider $z^2=s$ not in F. Let $z^2iz^{-2}=m$. If $m=i$ then z^2 is a polynomial $a(i)$. Since $zz^2=z^2z$, $a(i)=a(k)$. Let $a(i)=a_1+a_2i$, where a_1 and a_2 are in $F(i^2)$. Then $a_1+a_2i=a_1'+a_2'k$ where $a_1'=a_1(k^2)$ and $a_2'=a_2(k^2)$; both a_1' and a_2' are hence in $F(i^2)$. But k is not a polynomial in i. Hence $a_2'=0$. Hence $a_2=0$. Hence $a_1=a_1'$ which is true only if a_1 is in F, since $i^2\neq k^2$ and hence the coefficient of i^2 in a_1 must vanish. Hence s is in F, a contradiction. Hence $m\neq i$. Hence $j=m-i\neq 0$. If s is of rank four then the field $F(s)=F(z)$ since s and hence $F(s)$ is contained in $F(z)$, a field of order less than or equal to four. In this case z is a polynomial in s and hence is commutative with i^2 since s is. But z is not commutative with i^2. Hence s is not of rank four. But, by hypothesis, s is not in F and hence is not of rank 1. Hence the rank of s is 2 and s is a root of $w^2+2bw+c$ where b and c are in F. Let $t=s+b$. Hence $t^2=e$ in F. Since $t+b=s+2b=-cs^{-1}$, we have $jt+tj=(m-i)(s+b)+(s+b)(m-i)=ms-si+sm+2b(m-i)=ms-ms+(s+2b)m-i(s+2b)=-cs^{-1}(sis^{-1})+c(is^{-1})=-cis^{-1}+cis^{-1}=0$. Therefore $jt=-tj$. Hence $jtj^{-1}=-t$. Since $z^2i^2=i^2z^2$ and $ii^2=i^2i$, $mi^2=i^2m$, and $ji^2=i^2j$. Also $j^2t=tj^2$. Hence if $p=t+i^2$, then $jpj^{-1}=-t+i^2$, $zpz^{-1}=t+k^2$, $(jz)p(jz)^{-1}=t+k^2$. The field $F(t, i^2)$ is of order four since t is not a polynomial in i^2. The element p is of rank 4, since if it is of rank 2 then the resulting equation gives $2i^2$ equals a quantity in F, a contradiction. Hence the results here are the same as in the first case and we have an element p satisfying an equation with group G_4.

It remains to consider the cases where the algebra A is of type Γ. If A is of type E then, by the definition of algebras of type E, A contains the proper element and is of the desired type. If A is of type D, then by the definition of these cyclic algebras, A contains an element y which is a root of the quartic $w^4=d$, where d is in F. The group of this equation is either G_4 or G_8. If it is the group G_4 then y is the desired element. If not then the group of the equation is G_8 and not all of its roots are rational functions of one of them, since if its roots are x_1, $x_2=-x_1$, x_3, x_4, then if x_3 is a polynomial in x_1, by applying the substitution (34) of the group G_8, x_4 is the same rational function of x_1 and is equal to x_3, contrary to the hypothesis that the equation satisfied by y is irreducible. Hence we may apply the proof for algebras containing an element i satisfying (11) and obtain the desired result.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.