

ON THE THEORY OF ASSOCIATIVE DIVISION ALGEBRAS*

BY

OLIVE C. HAZLETT

1. Relation to the literature. There is a famous theorem to the effect that the only linear associative algebras over the field of all real numbers in which division is uniquely possible are the field of real numbers, the field of ordinary complex numbers, and real quaternions. The first published proof of this was that given in 1878 by Frobenius in his fundamental memoir† on bilinear forms. Since this proof, there have been numerous others,‡ the most recent being one by Professor Dickson.§

In the last mentioned proof, the theorem is a special case of a more general theorem of the same nature for a certain class of algebras, which Dickson calls Type A . He defines an algebra of this type as a linear associative algebra A , the coördinates of whose numbers range over any given algebraic|| field F , and for which the following properties hold:

(a) There exists in A a number i satisfying an equation $\phi(x) = 0$ of degree n with coefficients in F and irreducible in F .

(b) Any number of A which is commutative with i is in $F(i)$.

(c) There exists in A a number j , not in $F(i)$, such that $ji = \theta j + \sigma$, where θ and σ are in $F(i)$.

All three of these conditions are satisfied by real quaternions, and the first two by any linear associative division algebra D over F , where we take i so that the degree of the irreducible equation in F satisfied by i is the maximum.

Dickson showed¶ that every algebra of Type A over F has a subalgebra

* Presented to the Society, September 4, 1916.

† *Journal für Mathematik*, vol. 84 (1878), p. 59.

‡ C. S. Peirce, *American Journal of Mathematics*, vol. 4 (1881), p. 225; Weyr, *Monatshefte für Mathematik und Physik*, vol. 1 (1890), pp. 163-236; Cartan, *Annales de Toulouse*, ser. 1, vol. 12 (1898), p. 82; F. X. Grisseman, *Monatshefte für Mathematik und Physik*, vol. 11 (1900), pp. 132-147 (the last an elementary proof along the lines of the proof by Frobenius).

§ *These Transactions*, vol. 15 (1914), p. 39; *Linear Algebras*, Cambridge Tracts in Mathematics and Mathematical Physics, 1914, pp. 10-12. Hereafter, references to Dickson in this paper will be to the article in *these Transactions*.

|| He does not explicitly make the restriction that F shall be algebraic, but he makes tacit use of this property in his paper—or, to be more exact, that the field F be "vollkommen."

¶ *These Transactions*, l. c., p. 37.

S over F which can be exhibited as an algebra L over a field K (an Oberkörper of F) with units $i^s j^k$ ($k, s = 0, \dots, r-1$). Multiplication is defined by the relations

$$(1) \quad ji = \theta(i)j, \quad j^r = g,$$

where i is an element of S satisfying in the field K a uniserial abelian equation of degree r , with the roots $i, \theta(i), \dots, \theta^{r-1}(i)$, where $\theta^r(i) = i$ and where j is a number of S not in K , and g is a number in K . Dickson showed* for $r = 2, 3$ that g could be so chosen that, in the algebra L , division (except by zero) is always possible and unique. Wedderburn,† a few months later, showed that, for general r , g can always be so chosen that division is possible and unique—or, as we say, that the algebra is a division algebra.‡

The present paper considers linear associative division algebras over a general algebraic field F , which may be described as sets of numbers satisfying all the conditions for a field, except that multiplication is not necessarily commutative. It turns out that a necessary and sufficient condition that such an algebra satisfy (c) is that θ be a root of a certain algebraic equation which we shall call the Θ -equation. Then, from some fundamental properties of the equation, we show, among other theorems, that, if a linear associative division algebra of a certain general type over an algebraic field F be of rank n , it is of order mn where $m \leq n$. Of this theorem, Frobenius's theorem about real quaternions is a corollary. It also follows that, if a linear associative division algebra over an algebraic field F , of rank n , contain a number i which satisfies a uniserial abelian equation of degree n , then any number in the algebra is a polynomial in a number j , with coefficients in $F(i)$, such that (1) holds.

THE Θ -EQUATION

2. The Θ -equation; definition. Take any linear associative division algebra D over an algebraic field F , and consider the necessary and sufficient condition that, for a fixed number i , it satisfy condition (c) of § 1.

Let i be a number of the algebra satisfying an equation $\phi(x) = 0$ of degree n , irreducible in F . Then the order of D is a multiple of n , say mn .§ If $m = 1$, D is the field $F(i)$. If $m > 1$, then there is a number j_1 in D and not in $F(i)$ and the $2n$ numbers $i^k, i^k j_1$ are linearly independent with respect to F . In fact the mn units of D can be taken as

$$(2) \quad i^k, i^k j_1, \dots, i^k j_{m-1}$$

* These Transactions, l. c., p. 32.

† These Transactions, vol. 15 (1914), pp. 162–166.

‡ Wedderburn calls such an algebra primitive.

§ Dickson, l. c., p. 34.

where j_1 is not in $F(i)$, j_2 is linearly independent of the elements i^k , $i^k j_1$, j_3 is linearly independent of the elements i^k , $i^k j_1$, $i^k j_2$, etc. Then

$$(3) \quad j_k i = \sum_{s=0}^{m-1} \lambda_{k1, s}(i) j_s \quad (j_0 = 1).$$

Now there is a number j satisfying (c) if and only if there is a number J not in $F(i)$ such that

$$(4) \quad Ji = \theta J.$$

Has this a solution J in D ? If J is a number of D , then it is of the form

$$J = \sum_{k=0}^{m-1} \chi_k(i) j_k,$$

where the χ 's are polynomials in i , and hence (4) has a solution $\neq 0$ in D if and only if

$$(5) \quad \sum_{k,s}^{0, m-1} \chi_k(i) \lambda_{k1, s}(i) j_s = \theta \sum_s^{0, m-1} \chi_s(i) j_s$$

has a solution $(\chi_k) \neq (0)$ in $F(i)$. But the $m j$'s are linearly independent with respect to $F(i)$; and thus, in view of the associative law, (5) is equivalent to the set of ordinary linear homogeneous equations

$$(6) \quad \sum_{k=0}^{m-1} \chi_k \lambda_{k1, s}(i) = \theta \chi_s \quad (s = 0, \dots, m-1).$$

Now this has a solution $(\chi_k) \neq (0)$ in $F(i)$ or some extended field of $F(i)$ if and only if θ is a root of the ordinary algebraic equation

$$(7) \quad |\lambda_{k1, s} - d_{ks} \theta| = 0.$$

This equation we shall, for convenience, call the Θ -equation for i . Thus we have

THEOREM 1. *In a linear associative division algebra over a field F , there is a number $J \neq 0$ such that $Ji = \theta(i)J$, where θ is a polynomial in i with coefficients in F , if and only if θ is a root of the Θ -equation for i .*

3. Relation of the Θ -equation to the characteristic equation and rank equation. Furthermore, if θ is a root of the Θ -equation for i considered as an ordinary algebraic equation in $F(i)$, then θ is also a root of the reduced equation $\phi(x) = 0$ for i .

For let $F(i')$ be the least Oberkörper of $F(i)$ such that $F(i')$ is algebraically closed. This field is algebraic, and any two determinations of it are simply isomorphic. Take such a determination of $F(i')$ that $j_0 = 1$, j_1, \dots, j_{m-1} are linearly independent with respect to it, and let n' be the order of $F(i')$. Now enlarge the algebra D to an associative complex D' over F

whose units are

$$i'^k, i'^k j_1, \dots, i'^k j_{m-1} \quad (k = 1, \dots, n'),$$

linearly independent with respect to F .

Suppose that θ is any root of the Θ -equation for i in the above determination of $F(i')$. Then (6) has a set of solutions $(\chi_k) \neq (0)$ in $F(i')$. If we let

$$J = \sum_{k=0}^{m-1} \chi_k j_k,$$

then $Ji = \theta J$; and more generally $Ji^l = [\theta]^l J$. Thus $0 = J\phi(i) = \phi(\theta)J$; and accordingly, since $\phi(\theta)$ is in a field and $J \neq 0$, we must have $\phi(\theta) = 0$. Hence, in such an $F(i')$, the Θ -equation for i breaks up into a product of linear factors,

$$\prod_{l=0}^{m-1} (\Theta - \theta_l) = 0,$$

each of which is a factor of the reduced equation for i . Thus the statement at the beginning of this section follows at once.

But every root of the reduced equation for i is not necessarily a root of the Θ -equation for i . For to say that θ is a root of the reduced equation for i is equivalent to saying that it is a root of the left-hand characteristic equation

$$(8) \quad \delta'(x; \omega) \equiv \left| \sum_f \gamma_{\theta f h} x_f - d_{\theta h} \omega \right| = 0$$

written for i .^{*} This, in turn, is equivalent to the statement that $\omega = \theta$ is such a number in some Oberkörper F' of $F(i)$ that, corresponding to it, there is in F' a solution $(y_\theta) \neq (0)$ of the set of ordinary linear homogeneous equations

$$(9) \quad \sum_f (\gamma_{f1h} - d_{fh} \theta) y_f = 0 \quad (h = 1, \dots, mn),$$

where we have taken $e_1 = i$, for convenience. Now multiplying equation h of (9) by e_h on the right, and summing as to h , we see that there is a number $Y = \sum y_\theta e_\theta$ satisfying $Yi = \theta Y$.

But, since the units e_θ are linearly dependent with respect to the enlarged field F' , this number Y may be zero. If it is, θ is not necessarily a root of the Θ -equation for i . Nevertheless, since § 2 holds for present θ and enlarged field F' , every root θ of the reduced equation for i , which is such that a number Y corresponding is not zero, is also a root of the Θ -equation for i . Accordingly we have

THEOREM 2. *If i be any number in an associative division algebra D over a field F , every root of the Θ -equation for i is a root of the reduced equation for i ,*

^{*} Cartan, l. c., p. 16; Scheffers, *Mathematische Annalen*, vol. 39 (1891), pp. 302-304; Frobenius, l. c., p. 59; Weyr, l. c.

and hence also of the characteristic equation for i ; and a root θ , in the Oberkörper F' of $F(i)$, of the reduced equation for i is also a root of the Θ -equation for i if and only if there corresponds to θ a number $J \neq 0$, linearly dependent on the units of D with respect to F' , such that $Ji = \theta J$.

4. Some properties of the Θ -equation. If θ_1 and θ_2 be two roots in $F(i)$ of the Θ -equation for i , and if corresponding numbers in the algebra are J_1 and J_2 , then, in view of the associative law,

$$(J_2 J_1) i = J_2 (J_1 i) = J_2 (\theta_1 J_1) = \theta_1 (\theta_2) J_2 J_1$$

and

$$(J_1 J_2) i = \theta_2 (\theta_1) J_1 J_2.$$

Thus, by Theorem 1, we have

THEOREM 3. *If i be any number in an associative division algebra over a field F , and if θ_1 and θ_2 be two numbers of $F(i)$ which are roots of the Θ -equation for i , then $\theta_1(\theta_2)$ and $\theta_2(\theta_1)$ are roots of this Θ -equation.*

In particular, the symbolic powers of any root θ of the Θ -equation for i are all roots of this equation; and there is some least positive integer r ($1 < r \leq n$) such that $\theta^r = i$.

Let D be an associative division algebra of rank n over an algebraic field F , and let i be any number of D satisfying an irreducible equation of degree n . Then D has the property (b). Finally, let J_1 and J_2 be two numbers of D , different from zero, such that

$$J_1 i = \theta J_1, \quad J_2 i = \theta J_2,$$

and let r be the least integer such that $\theta^r = i$. Then

$$(J_2 J_1^{r-1}) i = J_2 (J_1^{r-1} i) = (J_2 \theta^{r-1}) J_1^{r-1} = i (J_2 J_1^{r-1}),$$

and hence

$$J_2 J_1^{r-1} = \tau(i),$$

where τ is a polynomial in F . Then, multiplying by J_1 on the right, we have

$$J_2 = \psi(i) J_1,$$

since J_1^r is a number in $F(i)$.

Thus we have proved

THEOREM 4. *In a linear associative division algebra D of rank n over a field F , if i be a number satisfying an equation of degree n irreducible in F , then a number J such that $Ji = \theta(i)J$, where θ is a polynomial in i , is essentially unique, in the sense that every number satisfying this condition is the product of a particular such number by a number in $F(i)$. Moreover, every number of the form $\psi(i)J$, where ψ is a number in $F(i)$ and J is a particular solution of $Ji = \theta(i)J$, satisfies this equation.*

This theorem still holds if i be any number of the algebra such that any number of the algebra which is commutative with it is necessarily in $F(i)$.

COROLLARY. *Under the conditions stated in this theorem, the rank of (6) for $\Theta = \theta$ is $m - 1$.*

At this point, there naturally arises the question as to the multiplicity of a root of the Θ -equation for a number i of the sort described in Theorem 4. From Dickson's work for Type A , it follows that the number i is a simple root of its Θ -equation where i satisfies an irreducible equation in F whose degree is n , the rank of the algebra. More generally, we have

THEOREM 5. *In a linear associative division algebra D over an algebraic field F , whose rank is n , if i be a number satisfying an equation of degree n irreducible in F , then every rational root of the Θ -equation for i is a simple root.*

We shall prove this indirectly. Now if θ be a root in $F(i)$ of multiplicity ≥ 2 , then there is a number $J_1 \neq 0$ in the algebra, such that

$$J_1 i = \theta J_1$$

and also a number J_2 linearly independent of 1 and J_1 with respect to $F(i)$ such that

$$J_2 i = \theta J_2 + \sigma(i) J_1,$$

where σ is a polynomial in i with coefficients in F . Then, by the associative law,

$$J_2 i^s = [\theta]^s J_2 + s [\theta]^{s-1} \sigma J_1,$$

where $[\theta]^k$ is the k th power of θ .

Let $\phi(x) \equiv \sum_{s=0}^n c_s x^s = 0$ ($c_n = 1$) be the irreducible equation in F of degree n satisfied by i . Then, by the above, we have

$$0 = J_2 \phi(i) = \phi(\theta) J_2 + \left(\sum_{s=1}^n c_s s [\theta]^{s-1} \right) \sigma J_1.$$

But J_2 is linearly independent of 1 and J_1 with respect to $F(i)$, and thus

$$\sigma \sum_{s=1}^n s c_s [\theta]^{s-1} = 0.$$

Hence, by Theorem 4, our theorem follows at once.

COROLLARY. *This theorem holds for any number i which is such that any number of the algebra which is commutative with it is necessarily in $F(i)$.*

APPLICATION TO ASSOCIATIVE DIVISION ALGEBRAS

5. General associative division algebras. By arranging the units in a square array, we readily prove the

LEMMA. *For an associative division algebra over any field F , the order of a subalgebra is a factor of the order of the algebra.*

COROLLARY 1. *The order of a linear associative division algebra is a multiple of the rank.*

COROLLARY 2. *An associative division algebra whose order is a prime is necessarily a field.*

If α be an algebraic number satisfying in the algebraic field K an irreducible equation $\phi(x) = 0$ of degree n , then α defines over K an algebraic field $K(\alpha)$. Furthermore, let $\alpha', \dots, \alpha^{(n-1)}$ be the remaining $n - 1$ roots of $\phi(x) = 0$. Then, if $K(\alpha)$ is identical with its conjugate fields $K(\alpha'), \dots, K(\alpha^{(n-1)})$, then $K(\alpha)$ is called a *Galois Field*.*

Then, combining Corollary 1 of the Lemma with Theorems 2 and 5, we have

THEOREM 6. *If D be an associative division algebra over an algebraic field F , which contains a number i satisfying in F an irreducible equation of degree n , such that any number of D commutative with i is in $F(i)$, and such that $F(i)$ is a Galois Field, then D is of order mn where $m \leq n$.*

Since, for a division algebra, the rank equation is a power of the reduced equation, such a number n is a factor of the rank.

From this theorem, we have at once the well-known theorem about quaternions. For if F be the field R of all real numbers, then the rank n must be 1 or 2. If $n = 1$, we have the field R . If $n = 2$, the defining equation for a number i , in D but not in R , may be taken to be $i^2 + 1 = 0$. Then $F(i)$ is simply isomorphic with the field C of ordinary complex numbers, and hence is algebraically closed. Thus every root of the Θ -equation for i is in $F(i)$. But if $n = 2$, $m = 1$ or 2 . If $m = 1$, D is (abstractly) the same as the field C . If $m = 2$, the Θ -equation is of degree 2, every one of its roots is a root of $i^2 + 1 = 0$, and no root is double. The Θ -equation for i accordingly must be $i^2 + 1 = 0$, which has the roots i and $-i$. This means that, in the algebra, there is a number $j \neq 0$ such that $ji = -ij$; and moreover the only numbers satisfying this relation are of the form $\psi(i)j$, where ψ is a polynomial with coefficients in R . Furthermore there are two and only two such numbers linearly independent with respect to R , and these may be taken to be j and $k = ij$. Thus we have the

COROLLARY. *Over the field R of all real numbers, the only linear associative division algebras are the field of reals, the field of ordinary complex numbers, and quaternions.*

6. Algebras over F containing a number i such that $F(i)$ is a Galois field. From Theorem 2 we have at once

THEOREM 7. *If D is an associative division algebra over an algebraic field F which contains a number i satisfying an irreducible uniserial abelian equation (of degree > 1), then the algebra is of Type A .*

* Hilbert, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4, p. 247; Bachmann, Zahlentheorie, vol. 5, p. 30.

Let $i_2 \neq 0$ be a number corresponding to the root θ_2 . Then $i_2 j$ corresponds to $\theta(\theta_2)$; and, in general, since

$$(i_2 j^k) i = i_2 (j^k i) = (i_2 \theta^k) j^k = \theta^k(\theta_2) i_2 j^k,$$

$i_2 j^k$ corresponds to $\theta^k(\theta_2)$. Now the $2rn$ numbers in the array (11') and in

$$(11'') \quad \begin{array}{ccc} i i_2, \dots, i^n i_2 & : \Theta = \theta_2 \\ i i_2 j, \dots, i^n i_2 j & : \Theta = \theta(\theta_2) \\ \cdot & \cdot & \cdot \\ i i_2 j^{r-1}, \dots, i^n i_2 j^{r-1} & : \Theta = \theta^{r-1}(\theta_2) \end{array}$$

are linearly independent with respect to F . For if they were not linearly independent, then there would exist two polynomials, $\psi_2(i)$ and $\chi_2(j)$, neither of which is zero, such that

$$\psi_2(i) i_2 \chi_2(j) = \psi_1(i) i \chi_1(j).$$

But since ψ_2 and χ_2 both have inverses, this is equivalent to saying that

$$i_2 = \psi_1'(i) i \chi_1'(j),$$

which is impossible, since i_2 corresponds to θ_2 , a root of the Θ -equation for i distinct from $\theta_1 = i, \theta(i), \dots, \theta^{r-1}(i)$.

In a similar manner, we show that any number of D is expressible in the form

$$(12) \quad \sum_{k=1}^s X_k(i) i_k Y_k(j);$$

and thus we deduce

THEOREM 9. *If D be an associative division algebra of rank n , over an algebraic field F , which contains a number i satisfying an equation of degree n which is irreducible in F , but completely reducible in $F(i)$, then the algebra can be generated by $s+1$ numbers of the algebra $j, i_1 = i, i_2, \dots, i_s$ where s is a factor of m , where mn is the order of D .*

By (1), we have

COROLLARY 1. *Some power of each of the numbers j, i_2, \dots, i_s is an element of $F(i)$.*

If, in particular, m is a prime, then we have

COROLLARY 2. *An associative division algebra D , which is of rank n and order pn (p , a prime) can be generated by two numbers of the algebra if it contains a number i satisfying an equation of degree n which is irreducible in F , but completely reducible in $F(i)$.*

7. Division algebras of Type A. If, in particular, an algebra of Type A is a division algebra, and if n is the rank of the algebra, then there are certain restrictions on r and n as evidenced by the following theorems.

THEOREM 10. *For an associative division algebra of rank n which satisfies conditions (a), (b), and (c), the integer r of equation (1) is a factor of n .*

For j satisfies an equation in F of degree n , and it satisfies an irreducible equation in F of degree n_1 . Now n_1 must be a factor of n . For let $R(x) = 0$ be the equation in F of lowest degree satisfied by every number x in the algebra—this is called the rank equation. Let $\rho(x) = 0$ be the equation in F of lowest degree satisfied by j . Then it is a well-known fact* that, for any linear associative algebra, every root of $R(x) = 0$ when considered as an ordinary algebraic equation in F is a root of $\rho(x) = 0$ when considered as an ordinary algebraic equation in F ; and conversely every root of $\rho(x) = 0$ is a root of $R(x) = 0$. Then, since we are considering a division algebra, $R(x)$ must be a power of $\rho(x)$, and thus n_1 is a factor of n .

Let $\rho(j)$ be

$$(13) \quad j^{n_1} + f_{n_1-1}j^{n_1-1} + \cdots + f_0 = 0$$

where the f 's are in F . Now $n_1 \geq r$ and therefore $n_1 = qr + r_0$ where $q \geq 1$, and $0 \leq r_0 < r$. Hence, since $j^r = g(i)$, (13) implies

$$(g^q(i) + \cdots)j^{r_0} + \sum_{k=r_0}^{k \leq r} F_k(i)j^k = 0,$$

where the coefficients of the powers of j are polynomials in $g(i)$ with coefficients in F . Since the degree of this equation in $F(i)$ satisfied by j is less than r , the left member must be identically zero in $F(i)$ and, in particular,

$$g^q(i) + \cdots = 0.$$

Thus j satisfies an equation in F of degree $qr \geq r$. Hence $r_0 = 0$, and our theorem is proved.

THEOREM 11. *Given an associative division algebra D which is of order mn and rank n . Let i be a number in D which satisfies an irreducible equation in F of degree n , and let there be in D a number j not in $F(i)$ such that*

$$ji = \theta(i)j + \sigma(i),$$

where θ and σ are polynomials with coefficients in F . Then m necessarily has a factor in common with n .

THEOREM 12. *There is no associative division algebra of Type A and of order $p_1 p_2$ where p_1 and p_2 are distinct primes.*

THEOREM 13. *For an associative division algebra of Type A and order p^2 , where p is a prime, the rank equation for the general number of the algebra is a uniserial abelian equation.*

BRYN MAWR COLLEGE,
BRYN MAWR, PA.

* Scheffers, l. c.; Frobenius, l. c., p. 59; Weyr, l. c.