

NORMAL DIVISION ALGEBRAS OF DEGREE FOUR OVER AN ALGEBRAIC FIELD*

BY
A. ADRIAN ALBERT

1. **Introduction.** The most important algebras for their applications are normal division algebras of degree n (order n^2) over an algebraic field $R(\theta)$, where R is the field of all rational numbers and θ is a root of an equation with rational coefficients and irreducible in R . All normal division algebras of degree two and three have been shown to be cyclic (Dickson) algebras.† In the following sections the author will prove that all normal division algebras of degree four (order sixteen) over $R(\theta)$ are cyclic (Dickson) algebras.

2. **On crossed products.** We shall assume the following known theory of normal simple algebras of degree n (order n^2) over any non-modular field F .

THEOREM‡ 1. *Let the minimum equation $\phi(\omega) = 0$ of x in A have degree n and be irreducible in F . Then the only quantities of A commutative with x are the quantities of the algebraic field $F(x)$. Moreover, if y in A has the same minimum equation as x , then $y = zxz^{-1}$ where z is in A .*

Let $\phi(\omega) = 0$ have degree n , coefficients in F and a *regular group* for F . Let x be a quantity with $\phi(\omega) = 0$ as its minimum equation so that there exist polynomials $\theta_i(x)$ in $F(x)$ such that

$$(1) \quad \phi(\omega) \equiv [\omega - \theta_n(x)] \cdot [\omega - \theta_{n-1}(x)] \cdots [\omega - \theta_1(x)]$$

where $\theta_1(x) = x$. It is then true that there exist a set of integers $t_{i,j}$ determined by the group of $\phi(\omega) = 0$ such that

$$(2) \quad \theta_i[\theta_j(x)] = \theta_{t_{i,j}}(x) \quad (i, j = 1, \cdots, n).$$

An associative algebra A is called a *crossed product*§ if A has a basis

$$(3) \quad x^{i-1}y_j \quad (i, j = 1, \cdots, n)$$

* Presented to the Society, October 31, 1931; received by the editors September 29, 1931.

† For algebras of degree two by L. E. Dickson, *Algebren und ihre Zahlentheorie*, Zurich, 1927, p. 45; for algebras of degree three by J. H. M. Wedderburn, these Transactions, vol. 22 (1921), p. 132.

‡ This is an immediate consequence of the corresponding theorems on n -rowed square matrices and the fact that it is possible to extend F by a scalar of finite degree so that A' over the extension F' is a total matrix algebra. Cf. the author's *On the construction of cyclic algebras with a given exponent*, to be published in the American Journal of Mathematics.

§ See Hasse, *Theory of cyclic algebras over an algebraic field*, these Transactions, January, 1932, for an exposition of the theory of crossed products and the results given in the remainder of this section.

where $y_1 = 1$, and a multiplication table

$$(4) \quad \phi(x) = 0, \quad y_i x = \theta_i(x) y_i, \quad y_j y_i = g_{i,j}(x) y_{t_{i,j}},$$

with the $g_{i,j}(x)$ in $F(x)$ and *all* not zero. A necessary and sufficient condition that a normal simple algebra be a crossed product is that it contain a quantity x whose minimum equation has degree equal to the degree of the algebra and regular group. Conversely every crossed product is a normal simple algebra. With Noether and Hasse we give the crossed product the notation

$$(5) \quad A = (g, Z)$$

where $Z = F(x)$ and g is the set of quantities

$$(6) \quad g = (g_{i,j}).$$

Let B be another crossed product with the same Z but a new set of $g_{i,j}$ so that $B = (\gamma, Z)$, where

$$(7) \quad \gamma = (\gamma_{i,j}).$$

Then we have the known result

THEOREM 2. *Algebra $A \times B$ has the expression*

$$(8) \quad A \times B = M \times C,$$

where M is a total matrix algebra of degree n over F and C is the crossed product

$$(9) \quad C = (g\gamma, Z), \quad g\gamma = (g_{i,j} \cdot \gamma_{i,j}).$$

For the particular case where all the $g_{i,j}$ are unity we write $g = 1$. We then have the known result

THEOREM 3. *A crossed product $(1, Z)$ is a total matrix algebra.*

3. An abelian group with two generators. We shall consider crossed products in which the group of $\phi(\omega) = 0$ in (1) is an abelian group with two generators so that $n = pq$, and the polynomials $\theta_i(x)$ are given by the pq quantities

$$(10) \quad \theta_1^i [\theta_2^j(x)] = \theta_2^j [\theta_1^i(x)] \quad \left\{ \begin{array}{l} i = 0, 1, \dots, p-1; \\ j = 0, 1, \dots, q-1 \end{array} \right\}$$

such that

$$(11) \quad \theta_1^p(x) = \theta_2^q(x) = x.$$

But then if $Z = F(x)$

$$(12) \quad Z = P \times Q$$

where P is a cyclic field of order p over F and Q is a cyclic field of order q over F . This corresponds to the fact that the group of $\phi(\omega)=0$ in this case is a direct product of two cyclic groups. In fact P is the field of all quantities of Z symmetric in $\phi_2(x)$ and its iteratives, Q is the field of all quantities in Z symmetric in $\phi_1(x)$ and its iteratives. If $a(x)$ is any quantity in Z we define three types of norms for a . First

$$(13) \quad N(a) = \prod_{\substack{i=0,1,\dots,p-1 \\ j=0,1,\dots,q-1}} a\{\theta_1^i[\theta_2^j(x)]\}$$

is a quantity of F . Then

$$(14) \quad N_1(a) = \prod_{i=0,1,\dots,p-1} a[\theta_1^i(x)]$$

is in Q , and

$$(15) \quad N_2(a) = \prod_{j=0,1,\dots,q-1} a[\theta_2^j(x)]$$

is in P . Obviously

$$(16) \quad N(a) = N_1[N_2(a)] = N_2[N_1(a)].$$

The crossed product A has a basis

$$(17) \quad x^{i-1}y_1^{j-1}y_2^{k-1} \quad (i = 1, \dots, n; \quad j = 1, \dots, p; \quad k = 1, \dots, q)$$

and a multiplication table given as before but with now

$$(18) \quad y_1x = \theta_1(x)y_1, \quad y_2x = \theta_2(x)y_2, \quad y_2y_1 = \alpha(x)y_1y_2,$$

$$(19) \quad y_1^p = g_1, \quad y_2^q = g_2,$$

where α, g_1 , and g_2 are in $F(x)$. L. E. Dickson has proved* that A is associative if and only if

$$(20) \quad g_1 \text{ is in } Q, \quad g_2 \text{ is in } P,$$

$$(21) \quad N_1(\alpha)g_1 = g_1[\theta_2(x)],$$

$$(22) \quad N_2(\alpha)g_2[\theta_1(x)] = g_2.$$

Consider the algebra $A^p = M^{p-1} \times B$, where, by Theorem 2, M is a total matrix algebra of degree n and B is a crossed product with a basis (17) and a multiplication table as before with

$$(23) \quad y_1x = \theta_1(x)y_1, \quad y_2x = \theta_2(x)y_2,$$

but now, by Theorem 2,

$$(24) \quad y_1^p = g_1^p, \quad y_2^q = g_2^p, \quad y_2y_1 = \alpha^py_1y_2.$$

* *Algebren*, p. 62, Theorem 17.

We shall consider in detail the structure of algebra B . We replace y_1 in the basis of B by a new quantity

$$(25) \quad j_1 = g_1^{-1}y_1,$$

where then

$$(26) \quad j_1^p = 1, \quad y_2 j_1 = \{g_1[\theta_2(x)]\}^{-1} \alpha^p g_1 j_1 y_2.$$

Let $P = F(u)$. Then obviously

$$(27) \quad j_1 u = \Theta_1(u) j_1, \quad \Theta_1(u) = u[\theta_1(x)].$$

The algebra

$$M_p = (u^i j_1^j) \quad (i, j = 0, 1, \dots, p-1)$$

is a cyclic algebra of degree p over F with a multiplication table $(27)_1, (26)_1$. By Theorem 3 algebra M_p is a total matrix algebra. It follows from the well known Wedderburn Theorem that

$$(28) \quad B = M_p \times C$$

where C contains $Q = F(v)$ and is a cyclic algebra with a basis

$$(29) \quad (v^i j_2^j) \quad (i, j = 0, 1, \dots, q-1),$$

and a multiplication table

$$(30) \quad j_2 v = \Theta_2(v) j_2, \quad j_2^q = \delta, \quad \Theta_2(v) = v[\theta_2(x)],$$

where δ is in F . We shall actually obtain the quantity j_2 and hence its q th power δ .

Using (21) we have

$$(31) \quad \alpha^p g_1 g_1(\theta_2)^{-1} = \alpha^p N_1(\alpha)^{-1}.$$

But evidently

$$(32) \quad \alpha^p N_1(\alpha)^{-1} = a a[\theta_1(x)]^{-1},$$

where

$$(33) \quad a = \alpha^{p-1} \cdot \alpha[\theta_1(x)]^{p-2} \cdots \alpha[\theta_1^{p-2}(x)].$$

Hence if we let $b = a^{-1}$ we have

$$(34) \quad y_2 j_1 = b[\theta_1(x)] b^{-1} j_1 y_2 = b^{-1} j_1 (b y_2).$$

Let

$$(35) \quad j_2 = a^{-1} y_2 = b y_2.$$

Then (34) is really

$$(36) \quad j_2 j_1 = j_1 j_2.$$

Since also $y_2 u = u y_2$, we have $j_2 u = u j_2$ and j_2 is commutative with all of the quantities of M_p and is in C . Also

$$(37) \quad y_2 v = \Theta_2(v) y_2, \quad \Theta_2(v) = v[\theta_2(x)],$$

so that

$$(38) \quad j_2 v = \Theta_2(v) j_2.$$

Now

$$(39) \quad j_2^q = N_2(b) y_2^q = N_2(a)^{-1} g_2^p,$$

by (24). Also, by (22),

$$N_2(\alpha) = g_2 g_2 [\theta_1(x)]^{-1}.$$

Hence

$$(40) \quad \begin{aligned} N_2(a) &= N_2(\alpha)^{p-1} N_2[\alpha(\theta_1)]^{p-2} \cdots N_2[\alpha(\theta_1^{p-1})] \\ &= \frac{g_2^{p-1}}{g_2(\theta_1)^{p-1}} \cdot \frac{g_2(\theta_1)^{p-2}}{g_2(\theta_1^2)^{p-2}} \cdots \frac{g_2[\theta_1^{p-2}]}{g_2[\theta_1^{p-1}]} = \frac{g_2^p}{N_1(g_2)}. \end{aligned}$$

It follows that

$$(41) \quad j_2^q = N_1(g_2).$$

The quantity $g_2 \neq 0$ of P has a non-zero norm so that j_2 has an inverse in C and is the desired quantity of (29). We have proved

THEOREM 4. *Let A be a normal simple algebra of degree $n = pq$ over F such that A is a crossed product defined by a basis (17) and a multiplication table (18), (19); the case where $Z = F(x)$ is defined by an equation with a regular abelian group with two generators of orders p and q respectively. Then Z is the direct product $Z = P \times Q$ of a cyclic field of order p and a cyclic field of order q respectively, the quantity g_2 of (19) is in P and has a norm*

$$(42) \quad \delta = N_1(g_2),$$

and

$$(43) \quad A^p = H \times C,$$

where H is a total matrix algebra and C is a cyclic algebra of degree q over F with a basis (29), and a multiplication table (30) so that C is a crossed product defined by Q and δ .

4. **Algebras of order sixteen.** The author has proved that every normal division algebra of degree four (order sixteen) has a basis

$$(44) \quad u^i v^j y_1^k y_2^r \quad (i, j, k, r = 0, 1),$$

and a multiplication table

$$(45) \quad uv = vu, \quad y_1 u = -u y_1, \quad y_2 u = u y_2, \quad y_1 v = v y_1, \quad y_2 v = -v y_2,$$

$$(46) \quad y_3 = y_1 y_2, \quad y_2^2 = \gamma_1 + \gamma_2 u, \quad y_1^2 = \gamma_3 + \gamma_4 v, \quad y_3^2 = \gamma_5 + \gamma_6 uv,$$

$$(47) \quad u^2 = \rho, \quad v^2 = \sigma, \quad y_2 y_1 = \alpha y_1 y_2,$$

$$(48) \quad y_1^2 = g_1, \quad y_2^2 = g_2, \quad y_3^2 = g_3,$$

$$\alpha = \frac{g_3(-uv)}{g_2 g_1(-v)},$$

with $\rho, \sigma, \gamma_1, \dots, \gamma_6$ in F and such that

$$(49) \quad \gamma_5^2 - \gamma_6^2 \sigma \rho = (\gamma_1^2 - \gamma_2^2 \rho)(\gamma_3^2 - \gamma_4^2 \sigma),$$

the associativity condition.* But then $N_1(g_2) = \gamma_1^2 - \gamma_2^2 \rho$, and we have proved, by Theorem 4,

THEOREM 5. *Let A be any normal division algebra of order sixteen over a non-modular field F so that A can be given the notation of (44)–(49). Then*

$$(50) \quad A^2 = H \times C,$$

where H is a total matrix algebra of degree eight over F and C is a generalized quaternion algebra

$$(51) \quad C = (1, v, y, vy), \quad yv = -vy, \quad v^2 = \sigma, \quad y^2 = \gamma_1^2 - \gamma_2^2 \rho.$$

As is well known† algebra C is a division algebra if and only if $\gamma_1^2 - \gamma_2^2 \rho \neq \lambda_1^2 - \lambda_2^2 \sigma$ for any λ_1 and λ_2 in F . The exponent of A is defined to be the least integer ρ such that A^ρ is a total matrix algebra, and when A is a normal division algebra of order sixteen its exponent is either two or four.‡ Suppose first that there exist λ_1 and λ_2 in F such that $\gamma_1^2 - \gamma_2^2 \rho = \lambda_1^2 - \lambda_2^2 \sigma$ so that Q is not a division algebra. Then if we write $y_0 = (\lambda_1 + \lambda_2 v)^{-1} y$ we have $y_0^2 = (\lambda_1^2 - \lambda_2^2 \sigma)^{-1} (\gamma_1^2 - \gamma_2^2 \rho) = 1$, and C is a crossed product with $g = 1$, and is a total

* See the author's papers in these Transactions, vol. 31 (1929), pp. 253–260, and vol. 32 (1930), pp. 171–195.

† Cf. L. E. Dickson, *Algebren*, p. 47.

‡ Cf. the author's paper *On direct products*, these Transactions, July, 1931, for the properties of the exponent of an algebra which give this result.

matric algebra by Theorem 3. Hence A has exponent two. Conversely if A has exponent two then A^2 is a total matric algebra, so that, by Theorem 5, $H \times C$ and hence C is a total matric algebra. But then there exist λ_1 and λ_2 in F such that $\gamma_1^2 - \gamma_2^2 \rho = \lambda_1^2 - \lambda_2^2 \sigma$.

LEMMA 1. *The exponent of A is two if and only if there exist λ_1 and λ_2 in F such that*

$$(52) \quad \gamma_1^2 - \gamma_2^2 \rho = \lambda_1^2 - \lambda_2^2 \sigma.$$

The author has given* a rational proof holding for any non-modular field F of

LEMMA 2. *If there exist λ_1 and λ_2 in F such that (52) holds, then A is the direct product of two generalized quaternion algebras.*

Hence A has exponent two if and only if A is the direct product of two generalized quaternion algebras. For when A has exponent two, Lemma 1 and Lemma 2 imply that A is the direct product of two generalized quaternion algebras. Conversely, since, as is well known, the square of any generalized quaternion algebra is a total matric algebra, if A has an expression as a direct product of generalized quaternion algebras, A has exponent two.

If A is not expressible as a direct product of two generalized quaternion algebras so that C is a division algebra, then $A^4 = H^2 \times C^2$ is a total matric algebra and A has exponent four. The converse is obvious as we have shown above and we have proved

THEOREM 6. *A normal division algebra A of degree four (order sixteen) over any non-modular field F has exponent two or four according as A is or is not expressible as a direct product of two generalized quaternion algebras over F . A necessary and sufficient condition that A be so expressible is that there exist λ_1 and λ_2 in F such that*

$$\gamma_1^2 - \gamma_2^2 \rho = \lambda_1^2 - \lambda_2^2 \sigma$$

where $\rho, \sigma, \gamma_1, \gamma_2$ are given by the constants in (44)–(49) for A .

We shall consider finally a property of the generalized quaternion algebra C assuming that it is a division algebra, that is, that A has exponent four. We have

$$\gamma_5^2 - \gamma_6^2 \sigma \rho = (\gamma_1^2 - \gamma_2^2 \rho)(\gamma_3^2 - \gamma_4^2 \sigma),$$

so that

$$\gamma_5^2 - \gamma_1^2(\gamma_3^2 - \gamma_4^2 \sigma) = \rho[\gamma_6^2 \sigma - \gamma_2^2(\gamma_3^2 - \gamma_4^2 \sigma)].$$

* These Transactions, vol. 32 (1930), pp. 171–195; p. 180.

Then

$$(\gamma_1^2 - \gamma_2^2 \rho)[\gamma_6^2 \sigma - \gamma_2^2(\gamma_3^2 - \gamma_4^2 \sigma)] = (\gamma_1 \gamma_6)^2 \sigma - (\gamma_2 \gamma_5)^2,$$

and

$$(\gamma_1^2 - \gamma_2^2 \rho)[\sigma(\gamma_6^2 + \gamma_4^2 \gamma_2^2) - (\gamma_2 \gamma_3)^2] = (\gamma_1 \gamma_6)^2 \sigma - (\gamma_2 \gamma_5)^2.$$

Multiplying by $\sigma(\gamma_1^2 - \gamma_2^2 \rho)^{-1}$ and transposing we have

$$(\gamma_2 \gamma_4 \sigma)^2 + (\gamma_6 \sigma)^2 = (\gamma_2 \gamma_3)^2 + [(\gamma_1 \gamma_6 \sigma)^2 - (\gamma_2 \gamma_5)^2 \sigma](\gamma_1^2 - \gamma_2^2 \rho)^{-1}.$$

But then if

$$\xi_1 = \gamma_2 \gamma_3, \quad \xi_2 = \gamma_1 \gamma_6 \sigma (\gamma_1^2 - \gamma_2^2 \rho)^{-1}, \quad \xi_3 = \gamma_2 \gamma_5 (\gamma_1^2 - \gamma_2^2 \rho)^{-1}$$

we obtain

$$(53) \quad (\gamma_2 \gamma_4 \sigma)^2 + (\gamma_6 \sigma)^2 = \xi_1^2 \sigma + (\xi_2^2 - \xi_3^2 \sigma)(\gamma_1^2 - \gamma_2^2 \rho).$$

Suppose first that $\xi_1 = \xi_2 = \xi_3 = 0$. If then A has the generalized quaternion sub-algebra $\gamma_6 = 0$,

$$(1, u, y_3, uy_3), \quad u^2 = \rho, \quad y_3^2 = \gamma_5, \quad y_3 u = -u y_3,$$

over F , and, by the Wedderburn direct product theorem, A is the direct product of two generalized quaternion algebras, a contradiction of our hypothesis that A has exponent four. Hence $\sigma \gamma_6 \neq 0$ and

$$-1 = (\gamma_2 \gamma_4 \gamma_6^{-1})^2.$$

Similarly $\gamma_2 \neq 0$, so that, since $\xi_3 = 0$, $\gamma_1^2 - \gamma_2^2 \rho \neq 0$, we have $\gamma_5 = 0$. But then $y_3^2 = \gamma_6 u v$, $y_3^4 = \gamma_6^2 \sigma \rho$. The field $F(y_3)$ is a cyclic quartic field over F which contains a quantity whose square is -1 , and A is a cyclic algebra.

Let next ξ_1, ξ_2, ξ_3 be not all zero. Then the quantity

$$(54) \quad t = \xi_1 v + (\xi_2 + \xi_3 v) y$$

is not in F and has the property that

$$(55) \quad t^2 = \xi_1^2 \sigma + (\xi_2^2 - \xi_3^2 \sigma)(\gamma_1^2 - \gamma_2^2 \rho) = \Delta_1^2 + \Delta_2^2,$$

where $\Delta_1 = \gamma_2 \gamma_4 \sigma$ and $\Delta_2 = \gamma_6 \sigma$ are in F . We have proved

THEOREM 7. *Let A be a normal division algebra of degree four over F and let A have exponent four. Then either -1 is the square of a quantity of F and A is a cyclic algebra or*

$$A^2 = H \times C,$$

where H is a total matrix algebra and C is a generalized quaternion division algebra over F which contains a quantity t not in F and such that

$$t^2 = \Delta_1^2 + \Delta_2^2$$

for Δ_1 and Δ_2 in F .

5. **Algebras over an algebraic field.** Let R be the field of all rational numbers, and let

$$(56) \quad F = R(\theta)$$

where θ is a root of an equation with rational coefficients and irreducible in R . The quantity θ may be any abstract quantity, a matrix, or a number, but in any case the field F is *simply isomorphic* with a field of algebraic numbers. We shall assume the following known* results:

LEMMA 1. *The direct product of two generalized quaternion algebras over $R(\theta)$ is not a division algebra.*

LEMMA 2. *Let A be a normal simple algebra of degree n over F and let Z be an algebraic field over F . Then $A \times Z$ is a normal simple algebra with the same basis and multiplication table as A over Z .*

LEMMA 3. *Let A be a normal division algebra over F and let $Z = F(\xi)$ be an algebraic field of prime order over F . Then $A' = A \times Z$ is not a division algebra if and only if A contains a sub-field $F(u)$ simply isomorphic with Z .*

LEMMA 4. *Let A be a normal division algebra of degree n over F and let ξ be a scalar root of the minimum equation of degree n of a quantity x in A . Then $A \times F(\xi)$ is a total matrix algebra over $F(\xi)$.*

LEMMA 5. *A normal division algebra of degree four over a field $F = R(\theta)$ is a cyclic (Dickson) algebra if A contains a quantity u not in F such that*

$$u^2 = \Delta_1^2 + \Delta_2^2 \quad (\Delta_1 \text{ and } \Delta_2 \text{ in } F).$$

We shall now apply our lemmas. First the application of Lemma 1 to Theorem 6 gives immediately

THEOREM 8. *The exponent of any normal division algebra of order sixteen over $F = R(\theta)$ is four.*

Next we use Theorem 5 and have $A^2 = H \times C$. By Theorem 7 either A is a cyclic algebra or C contains a quantity t not in F but such that $t^2 = \Delta_1^2 + \Delta_2^2$

* For Lemmas 1 and 5 see the author's *Division algebras over an algebraic field* which has been offered for publication to the Bulletin of the American Mathematical Society. For the remaining lemmas see the author's *On direct products*, loc. cit.

with Δ_1 and Δ_2 in F . In the latter case let ξ be a scalar such that $\xi^2 = \Delta_1^2 + \Delta_2^2$. The field $F(\xi) = R(\theta, \xi)$ is an algebraic field over R . Consider the algebra $A' = A \times F(\xi)$, a normal simple algebra of order sixteen over $F(\xi)$, by Lemma 2. Evidently

$$(A')^2 = H \times C', \quad C' = C \times F(\xi),$$

is a total matrix algebra by Lemma 4. Hence the exponent of A' is not four, and by Theorem 8, algebra A' is not a division algebra. But $F(\xi)$ is a quadratic field over F , two is a prime, and Lemma 3 implies that there exists a quantity u in A and not in F such that $u^2 = \Delta_1^2 + \Delta_2^2$ with Δ_1 and Δ_2 in F . By Lemma 5 algebra A is a cyclic algebra. Hence A is a cyclic algebra in all cases.

THEOREM 9. *Every normal division algebra of order sixteen over an algebraic field $R(\theta)$ is a cyclic (Dickson) algebra.**

* (Note added to proof, February 1, 1932.) Since this paper was written, Theorem 9 has been proved by other methods for *any order* n^2 . A proof by A. A. Albert and H. Hasse has been offered for publication to these Transactions. This does not, of course, affect the priority of the result in Theorem 9. Also the theory in the sections preceding §5 still represents results which have not been extended to the general case (order n^2) for algebras over any non-modular field F .