A CONSTRUCTION OF NON-CYCLIC NORMAL DIVISION ALGEBRAS*

BY A. A. ALBERT

1. *Introduction.* We know now that every normal division algebra over an algebraic number field is a cyclic (Dickson) algebra. This result was proved by highly refined arithmetic means† and the proof cannot be extended to obtain a like result for algebras over a general field. The very important question of whether or not any non-cyclic algebras exist has thus remained unanswered up to the present.

I shall give a construction of non-cyclic algebras of order sixteen over a function field‡ in this paper. These algebras will be proved to be normal division algebras; they furnish the first example in the literature of linear associative algebras of division algebras definitely known to be not of the Dickson type.

2. *A Type of Division Algebra.* Let K be a non-modular field and $K(z)$, $z^2=\Delta$ in F, be a quadratic field over K, so that Δ is not the square of any quantity of K. I have proved§ the following proposition.

LEMMA 1. *Let A be a division algebra over K. Then $A\times K(z)$ is a division algebra if and only if A contains no sub-field $K(z_0)$, $z_0^2=\Delta$, equivalent to $K(z)$.*

We shall restrict further attention to fields

$$K = F(u, v),$$

where F is any real number field and u and v are independent indeterminates. Then K is the field of all rational functions with

* Presented to the Society, April 9, 1932.

† A proof by H. Hasse (to whom are due the arithmetic considerations) and by myself will appear very soon in the Transactions of this Society.

‡ Algebras of the type constructed here were first considered by R. Brauer who proved (falsely) that they were all division algebras. See Section 4 of this paper for a discussion which points out the error in Brauer's work and which gives simple examples of Brauer algebras not division algebras. (See also, however, a footnote on p. 455, added in proof.)

§ This theorem is a consequence of a result of L. E. Dickson, *Algebren und ihre Zahlentheorie*, pp. 63–64. For my application to prove the above Lemma see this Bulletin, April, 1931, pp. 301–312; p. 309.

(real) coefficients in F of two independent marks u and v. We shall also consider the corresponding domain of integrity

$$J = F[u, v],$$

of all polynomials in u and v with coefficients in F. We shall similarly consider quadratic fields $K(z)$ and the corresponding domains of integrity

$$J[z],$$

of all quantities of the form $\alpha+\beta z$ with α and β in J.

Let δ and ϵ be in K so that we may write

$$\delta = \frac{\lambda}{\nu}, \quad \epsilon = \frac{\mu}{\nu}, \tag{1}$$

where λ, μ, and ν are in J. If $u=\delta^2+\epsilon^2$, then

$$\nu^2 u = \lambda^2 + \mu^2 \tag{2}$$

identically in u and v. The degree in u of the right member of (2) is even while that of the left member is obviously odd. Hence (2) and the equation $u=\delta^2+\epsilon^2$ for δ and ϵ in K are both impossible. Similar considerations of degrees give the following result.

LEMMA 2. *The quantities u, v, uv are each not expressible in the form $\delta^2+\epsilon^2$ for any δ and ϵ of K.*

In particular $u\neq\delta^2$, $v\neq\delta^2$ for any δ of K so that if

$$i^2 = u, \quad x^2 = v, \tag{3}$$

then $K(i)$ and $K(x)$ are quadratic fields over K. The only elements $\delta+\epsilon i$ in $K(i)$ and not in K whose squares are in K are obviously elements of the form ϵi. Hence, if x is in $K(i)$, then

$$x = \epsilon i, x^2 = v = \epsilon^2 u,$$

so that $uv=(\epsilon u)^2$, a contradiction of Lemma 2. Hence the field $K(i, x)$ is a quartic field with 1, i, x, ix as basis. In fact the group of $K(i, x)$ is the Vierergruppe G_4, $K(i, x) = K(i)\times K(x)$. Moreover, as I have shown,* every quadratic sub-field of $K(i,x)$ is equivalent to one of the fields $K(i)$, $K(x)$, $K(ix)$. From Lemma 2, we have the following lemma.

* See Lemma 10 of my paper in the Transactions of this Society, vol. 32 (1930), pp. 171–195; p. 189 for a rational proof of this very elementary result.

LEMMA 3. *The field $K(i, x)$ defined by* (3) *has no quadratic subfield $K(z)$, $z^2=\delta^2+\epsilon^2=\Delta$ in K, δ and ϵ in K.*

Let $L=K(z)$, z as in Lemma 3, be a quadratic field over K. By Lemma 1 the algebra $K(i, x)\times L$ is a division algebra over L and in fact is the quartic field $L(i, x)=L(i)\times L(x)$, where $L(i)=L\times K(i)$ and $L(x)=L\times K(x)$ are quadratic fields over L. In particular we notice that the quadratic equations $\xi^2=u$, $\xi^2=v$ defining $L(i)$ and $L(x)$ are cyclic (irreducible) equations in L.

If we consider two generalized quaternion algebras

$$(4)\ B = (1, i, j, ij), \quad ji = -ij, \quad i^2 = u, \quad j^2 = a \neq 0 \text{ in } K,$$

$$(5)\ C = (1, x, y, xy), \quad yx = -xy, \quad x^2 = v, \quad y^2 = b \neq 0 \text{ in } K,$$

over K, the algebras $B\times L$ and $C\times L$ over L still remain generalized quaternion algebras over their reference field L; that is, the equations $\xi^2=u$, $\xi^2=v$ are still cyclic quadratic equations when we extend the reference field from K to L. If A is the normal simple algebra $A=B\times C$, then $A_0=A\times L$ over L is the direct product $A_0=B_0\times C_0$, where $B_0=B\times L$, $C_0=C\times L$ over L. Hence $A\times L$ is a direct product of two generalized quaternion algebras over L and, as I have proved,* the following statement holds.

LEMMA 4. *A necessary and sufficient condition that A_0 over L be a division algebra is that the quadratic form*

$$(6)\qquad u\lambda_1^2 + a\lambda_2^2 - ua\lambda_3^2 - (v\lambda_4^2 + b\lambda_5^2 - vb\lambda_6^2) \equiv Q$$

in the variables $\lambda_1, \lambda_2, \cdots, \lambda_6$ in L shall not vanish for any $\lambda_1, \cdots, \lambda_6$ not all zero in L.

We shall now select a and b of (4), (5). Take

$$(7)\quad a = \sum_{i=0}^{n} a_i v^i,\quad b = \sum_{i=0}^{m} b_i v^i,\quad a_i = \sum_{j=0}^{r_i} \alpha_{ij} u^j,\quad b_i = \sum_{j=0}^{s_i} \beta_{ij} u^j,$$

where α_{ij} and β_{ij} are in F so that a and b are in J. This is no restriction on the generality of algebras B and C. We shall further select

$$(8)\qquad \begin{cases} n \text{ even}, m \text{ odd}, r = r_n \text{ odd}, s = s_m \text{ odd}, \\ \alpha_0 = \alpha_{nr_n} > 0, \beta_0 = \beta_{ms_m} > 0, \end{cases}$$

* This Bulletin, loc. cit., p. 311, Theorem 3.

a set of restrictions which enables us to apply Lemma 4 to prove the following theorem.

THEOREM 1. *Let* $A=B\times C$ *be defined by* (7), (8), (4), (5), *and let* $L=K(z)$, $z^2=\delta^2+\epsilon^2=\Delta$, δ *and* ϵ *in* K, *be a quadratic field over* K. *Then* $A_0=A\times L$ *is a division algebra.*

Without loss of generality we may take δ and ϵ in J since if $\nu\delta=\lambda$, $\nu\epsilon=\mu$ with λ, μ, ν in J, then $z_0=\nu z$ has the property $z_0^2=\lambda^2+\mu^2$ as desired while $L=K(z)=K(z_0)$. Suppose then that A_0 is not a division algebra so that, if Q is defined by (6), there exist $\lambda_1, \lambda_2, \cdots, \lambda_6$ not all zero in L such that $Q=0$. Without loss of generality we may take the λ_i to be in $J[z]$ (by multiplying the equation $Q=0$ by the square of the least common denominator, in J, of the λ_i). Hence we may write

$$\lambda_i = \alpha_i + \beta_i z \qquad (i = 1, \cdots, 6), \tag{9}$$

where the α_i and β_i are in J. Then $\lambda_i^2=(\alpha_i^2+\beta_i^2\Delta)+2\alpha_i\beta_i z$, so that if

$$P_i = \alpha_i^2 + \beta_i^2\Delta, \quad Q_i = 2\alpha_i\beta_i, \tag{10}$$

the equation $Q=0$ becomes

$$\begin{cases} uP_1 + aP_2 - uaP_3 - vP_4 - bP_5 + vbP_6 \\ \qquad + (uQ_1 + aQ_2 - uaQ_3 - vQ_4 - bQ_5 + vbQ_6)z = 0. \end{cases} \tag{11}$$

But 1 and z are linearly independent with respect to K so that (11) implies that

$$\phi(u, v) \equiv uP_1 + aP_2 - uaP_3 - vP_4 - bP_5 + vbP_6 \equiv 0 \tag{12}$$

in u and v, where the P_i are defined by (10) with α_i and β_i not all identically zero in u and v.

We have assumed that $z^2=\delta^2+\epsilon^2=\Delta$ so that $P_i=\alpha_i^2+(\beta_i\delta)^2+(\beta_i\epsilon)^2$ must have even degree in v. In fact

$$P_i \equiv p_i v^{2\rho_i} + S_i(u, v), \qquad S_i \equiv S_i(u, v) \text{ in } J, \tag{13}$$

where the degree of S_i in v is less than $2\rho_i$; and

$$p_i \equiv \tau_i u^{2\sigma_i} + q_i(u),\ q_i \equiv q_i(u) \text{ in } F[u],\ \tau_i \geqq 0, \tag{14}$$

where q_i has degree less than $2\sigma_i$ in u. Moreover

$$\tau_i \geqq 0,\ \tau_i = 0 \text{ if and only if } P_i \equiv \lambda_i = 0. \tag{15}$$

The polynomial (12) is a sum of six terms. We use (13), (14) to arrange each of these six terms according to descending powers of v whose coefficients are polynomials in u arranged according to descending powers of u. Since $\phi(u, v) \equiv 0$ in u and v, the total coefficient of the highest power of v appearing in the six terms is a sum of possibly six polynomials in u which is identically zero. Since this term is to appear explicitly because the λ_i and hence the P_i are not all zero, at least one of these six (or fewer) polynomials must be not identically zero. But their sum is zero so that at least *two* of them must be not identically zero in u.

Suppose that this highest power of v were an odd power. It must appear only in

$$(16) \qquad - vP_4 - bP_5$$

since the remaining terms of (12) all have even degree in v. Then this power must appear in *both* vP_4 and bP_5 and its total coefficient is evidently

$$(17) \qquad - (p_4 + p_5 b_m) \equiv 0 \text{ in } u.$$

But p_4 has even degree in u and $p_5 b_m$ has odd degree in u by (14) and (8), so that (17) is impossible. Hence the highest power of v cannot be an odd power.

It follows that the highest power of v in (12) appears only in

$$(18) \qquad uP_1 + aP_2 + vbP_6 - uaP_3.$$

The leading coefficients in the terms of (18) are respectively

$$(19) \qquad up_1,\ a_n p_2,\ b_m p_6,\ - ua_n p_3\,,$$

so that the total coefficient of the highest power of v is a sum of the expressions in (19). These expressions have leading terms

$$(20) \qquad \tau_1 u^{2\sigma_1+1},\ \alpha_0\tau_2 u^{2\sigma_2+r},\ \beta_0\tau_6 u^{2\sigma_6+s},\ -\alpha_0\tau_3 u^{2\sigma_3+r+1}$$

when arranged according to descending powers of u. If the highest power of u appearing in the total coefficient we are discussing were an even power, it would appear only in the single term $-\alpha_0\tau_3 u^{2\sigma_3+r+1}$ and could not have *total* coefficient zero. Hence this power is odd and its total numerical coefficient is a sum of the real numbers $\tau_1 \geqq 0$, $\alpha_0\tau_2 \geqq 0$, $\beta_0\tau_6 \geqq 0$. But these real numbers are all positive or zero, they must not all be zero, and yet *this sum must be zero*, which is impossible. Hence the assumption that the λ_i are not all zero has led to a contradiction and we have proved Theorem 1.

Since $A \times L$ is thus a division algebra so must algebra A be a division algebra. Hence we have also the following result.

THEOREM 2. *The algebra A of Theorem* 1 *is a division algebra. By its form it is a normal division algebra of order sixteen over K.*

3. *The Existence of Non-Cyclic Algebras.* We shall prove that the algebras A of Section 2 are non-cyclic, that is, they contain no cyclic quartic sub-field. We shall first require the following rather trivial lemma.

LEMMA 5. *The field K contains no quantity whose square is* -1.

For if $a^2 = -1$, a in K, then $b = ca$, where b and c are in J, so that $b^2 + c^2 = 0$. But, as we saw in (10), (13), (14) this is impossible unless $b = c = 0$, whereas c is the denominator of a and hence $c \neq 0$.

When a field K contains no a such that $a^2 = -1$ it has the following property.*

LEMMA 6. *Every cyclic quartic field C over K has a quadratic sub-field $K(z)$, $z^2 = \delta^2 + \epsilon^2$, δ, ϵ in K.*

We shall prove that the algebras A of Section 2 contain no quadratic sub-field $K(z)$ as above and hence no cyclic quartic field C containing $K(z)$. For if $K(z)$ is any such field, Theorem 1 says that $A \times K(z)$ is a division algebra. But Lemma 1 states that then A contains no quadratic sub-field equivalent to $K(z)$ and hence no C. We have proved the first known theorem on the existence of non-cyclic algebras.

THEOREM 3. *The normal division algebras A of Section* 2 *are non-cyclic algebras.*

4. *The Algebras of Brauer.* We have considered algebras of order sixteen over a function field $F(u, v)$. Moreover these algebras were direct products of algebras of order four. R. Brauer was the first author to consider such algebras. He stated that any algebra $A = B \times C$, where B and C are given by (4), (5) is a division algebra if the fields $K(i)$, $K(x)$ are merely distinct

* A canonical form of the cyclic quartic is well known to be $x^4 + 2\nu\rho x^2 + \nu^2\epsilon^2\rho = 0$, $\rho = \delta^2 + \epsilon^2$. Every cyclic quartic field will then contain a quadratic sub-field $K(z)$, $z^2 = \rho = \delta^2 + \epsilon^2$. See R. Garver, *Quartic equations with certain groups*, Annals of Mathematics, vol. 29 (1928), pp. 47–51.

quadratic fields. But this is not true since we may take $a=-u$, $b=-v$, so that as in our proof of Lemma 3, $K(i, x)$ is a quartic field, while

$$(i+j)^2=i^2+j^2+ij+ji=u-u=0.$$

which is impossible in a division algebra. Brauer's proof of this false theorem is of course incorrect.* He gave a matrix representation of the algebra A as an algebra of four-rowed square matrices with elements in $K(a^{1/2}, b^{1/2})$ and wrote

$$(21)\quad \xi_1 = X_1 + X_2a^{1/2} + X_3b^{1/2} + X_4a^{1/2},\ b^{1/2}\ (X_1, \cdots, X_4\ in K).$$

He had three other quantities η_1, ζ_1, ω_1 of similar type and defined ξ_2, ξ_3, ξ_4 to be the result of replacing respectively $a^{1/2}$ by $-a^{1/2}$, $b^{1/2}$ by $-b^{1/2}$, and both $a^{1/2}$ by $-a^{1/2}$, $b^{1/2}$ by $-b^{1/2}$ in ξ_1; similarly for η_ν, ζ_ν, and ω_ν. Brauer's matrices were thus given when sixteen independent variables ranged over all quantities of K. He then attempted to prove§ that the determinant of the general matrix (a quartic form in the sixteen variables) could not vanish (identically in u and v) for any values of the variables in K. He put $v=0$ and obtained

$$(\xi_1\xi_2 - u\eta_1\eta_2)(\xi_3\xi_4 - u\eta_3\eta_4) = 0.$$

He then concluded that since either $\xi_1\xi_2$ or $\xi_3\xi_4$ has u as a factor then some one ξ_ν has u as a factor, whence all the ξ_ν have u as factor. This is false as, for example, $\xi_1=u+(-u)^{1/2}$ gives $\xi_2=u-(-u)^{1/2}$ and $\xi_1\xi_2=u^2+u$ has u as factor while neither factor of the product has u as factor. In fact under Brauer's initial assumptions we know nothing of the nature of a and b when we put $v=0$. Brauer was also able to conclude from the above false argument that it followed that ξ_ν vanished at $v=0$ and hence had v as factor. But this is also false as a and b might both vanish at $v=0$ and the coefficients of ξ_1 in (21) might still not have v as factor. It is in fact true that Brauer's arguments only hold true when a and b are rational,‡ an assumption that he seems to have had in mind.§

---

* See, however, footnote on p. 455, added in proof.

† See Brauer's paper in the Mathematische Zeitschrift, vol. 31 (1929), pp. 733–747 for his consideration of these algebras. He gave his proof on pp. 746–747. Brauer used a and b respectively where we have used b and a so that his ξ_2 is obtained from ξ_1 by replacing $b^{1/2}$ by $-b^{1/2}$ instead of $a^{1/2}$ by $-a^{1/2}$.

‡ Brauer took $F=R$, the field of all rational numbers.

In my Lemma 4, I have in fact reduced the condition that A be a division algebra from a condition that a quartic form in sixteen variables be not a null form to an equivalent condition on a quadratic form in only six variables. It is the application of this far simpler condition that has enabled me to prove the existence of non-cyclic algebras.

I have shown in the above that among the algebras considered by Brauer there exist non-cyclic division algebras and also algebras not division algebras. There remains the question as to whether any of the algebras of Brauer are cyclic division algebras. I have recently proved* that the algebra $A = B \times C$ over $R(u, v)$, where we replace u by $-2u^3$, take a to be a rational number which is a sum of two squares and not a square, and take $b = -1$, is a cyclic normal division algebra. This is one of the algebras of Brauer when we pass to a new basis of B by taking i to be replaced by $u^{-1}i$ whose square is $-2u$, and then replace u by the equivalent indeterminate $-2u$.

I have therefore proved the existence of cyclic and non-cyclic division algebras among the algebras considered by Brauer as well as the existence of algebras not division algebras. I have also given, in Lemma 4, a necessary and sufficient condition that a Brauer algebra be a division algebra.

THE UNIVERSITY OF CHICAGO

§ A recent communication from Brauer verifies this conjecture. Brauer used "*Zahl in K*" to mean rational number as opposed to non-constant function of u and v. With this interpretation, his work is correct, but it does not extend to the general case considered here. The difficulty was thus one of the interpretation of language, rather than a mathematical error. [Note added May 10, 1932.]

* This Bulletin, October, 1931, pp. 727–730.

ERRATUM

On page 186 of the March issue of this Bulletin (vol. 38, No. 3), in line 3 from the foot of the page, condition (2) should read

$$\sum n\,|\Delta^2 a_n| \text{ instead of } \sum a_n\,|\Delta^2 a_n|.$$

C. N. MOORE