NON-CYCLIC ALGEBRAS OF DEGREE AND EXPONENT FOUR*

BY

A. ADRIAN ALBERT

1. **Introduction.** I have recently† proved the existence of non-cyclic normal division algebras. The algebras I constructed are algebras A of order sixteen (degree four, so that every quantity of A is contained in some quartic sub-field of A) containing no *cyclic* quartic sub-field and hence not of the cyclic (Dickson) type. But each A is expressible as a direct product of two (cyclic) algebras of degree two (order four). Hence the question of the existence of non-cyclic algebras *not* direct products of cyclic algebras, and therefore of essentially more complex structures than cyclic algebras, has remained unanswered.

The exponent of a normal division algebra A is the least integer e such that A^e is a total matric algebra. A normal division algebra of degree four has exponent two or four according as it is or is not expressible as a direct product of algebras of degree two.‡ I shall prove here that there exist non-cyclic normal division algebras of degree and exponent four, algebras of a more complex structure than any previously constructed normal division algebras.

2. **Algebras of order sixteen.** We shall consider normal simple algebras of order sixteen (degree four) over a field K. Algebra A has a quartic sub-field $K(u, v)$ where

$$u^2 = \rho, \quad v^2 = \sigma \qquad (\rho, \sigma \text{ in } K), \tag{1}$$

such that neither ρ, σ, nor $\sigma\rho$ is the square of any quantity of K. Algebra A contains quantities

$$j_1, j_2, j_3 = j_1 j_2,$$

such that

$$j_1 u = u j_1, \quad j_1 v = -v j_1, \quad j_1^2 = g_1 = \gamma_1 + \gamma_2 u \neq 0 \quad (\gamma_1, \gamma_2 \text{ in } K), \tag{2}$$

$$j_2 v = v j_2, \quad j_2 u = -u j_2, \quad j_2^2 = g_2 = \gamma_3 + \gamma_4 v \neq 0 \quad (\gamma_3, \gamma_4 \text{ in } K), \tag{3}$$

$$j_2 j_1 = \alpha j_3, \quad j_3^2 = g_3 = \gamma_5 + \gamma_6 uv \qquad (\gamma_5, \gamma_6 \text{ in } K), \tag{4}$$

* Presented to the Society, August 31, 1932; received by the editors June 9, 1932.

† In a paper published in the Bulletin of the American Mathematical Society, June, 1932. (Designated by Albert 1.)

‡ See Theorem 6 of my *Normal division algebras of degree four*, etc., these Transactions, vol. 34 (1932), pp. 363–372. (Designated by Albert 2.)

$$\alpha = \frac{\gamma_5 - \gamma_6 uv}{(\gamma_1 + \gamma_2 u)(\gamma_3 - \gamma_4 v)}. \tag{5}$$

A necessary and sufficient condition that A be associative is that

$$\gamma_5^2 - \gamma_6^2 \sigma\rho = (\gamma_1^2 - \gamma_2^2 \rho)(\gamma_3^2 - \gamma_4^2 \sigma). \tag{6}$$

A necessary and sufficient condition* that A be not expressible as a direct product of two algebras of degree two (that is, have exponent four) is that the equation

$$\alpha_1^2 - \alpha_2^2 \sigma - (\gamma_1^2 - \gamma_2^2 \rho)\alpha_3^2 = 0 \tag{7}$$

be impossible for any $\alpha_1, \alpha_2, \alpha_3$ not all zero and in K.

Algebra† A has a sub-algebra $B = (1, v, j_1, vj_1)$ over $K(u)$. This algebra is a generalized quaternion algebra and it is well known that B is a division algebra if and only if

$$g_1 \neq a_1^2 - a_2^2 \sigma \tag{8}$$

for any a_1 and a_2 in $K(u)$. But if $a_1 = \alpha_1 + \alpha_2 u$, $a_2 = \alpha_3 + \alpha_4 u$, the equation $g_1 = a_1^2 - a_2^2 \sigma$ implies that $\gamma_1 + \gamma_2 u = [\alpha_1^2 + \alpha_2^2 \rho - \sigma(\alpha_3^2 + \alpha_4^2 \rho)] + 2(\alpha_1\alpha_2 - \sigma\alpha_3\alpha_4)u$ so that $\gamma_1 = \alpha_1^2 + \alpha_2^2\rho - \sigma(\alpha_3^2 + \alpha_4^2\rho)$. We have now

THEOREM 1. *A sufficient condition that B be a division algebra is that the quadratic form*

$$Q = (\alpha_1^2 + \alpha_2^2 \rho) - \sigma(\alpha_3^2 + \alpha_4^2 \rho) - \gamma_1 \alpha_5^2 \tag{9}$$

in the variables $\alpha_1, \cdots, \alpha_5$ *shall not vanish for any* $\alpha_1, \cdots, \alpha_5$ *not all zero and in K.*

For if the sufficient condition of Theorem 1 were satisfied and yet B were not a division algebra we would have $\gamma_1 = \alpha_1^2 + \alpha_2^2\rho - \sigma(\alpha_3^2 + \alpha_4^2\rho)$ so that $Q = 0$ for $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in K and $\alpha_5 = 1$, a contradiction.

It is also known‡ that, when B is a division algebra, A is also a division algebra if and only if there is no quantity X in B for which

$$g_2 = X'X, \tag{10}$$

where if $X = b + dj_1$ then $X' = b(-u) + d(-u)\alpha j_1$ with a and b of course in $K(u, v)$.

* See Albert 2.

† For the properties of this section see my paper in these Transactions, vol. 32 (1930), pp. 171–195. (Designated hereafter by Albert 3.)

‡ See L. E. Dickson's *Algebren und ihre Zahlentheorie*, p. 64, for both the condition that B be a division algebra and A be a division algebra.

I have proved* that

$$(11)\qquad (bj_2)^2 = f_3 + f_4 v, \qquad (dj_3)^2 = f_5 + f_6 uv,$$

where if

$$(12)\qquad b = \beta_1 + \beta_2 v + (\beta_3 + \beta_4 v)u, \quad d = \delta_1 + \delta_2 uv + (\delta_3 + \delta_4 uv)u$$

and

$$(13)\qquad b_1 = \beta_1^2 + \beta_2^2\sigma - \rho(\beta_3^2 + \beta_4^2\sigma), \qquad b_2 = 2(\beta_1\beta_2 - \rho\beta_3\beta_4),$$

$$(14)\qquad d_1 = \delta_1^2 + \delta_2^2\sigma\rho - \rho(\delta_3^2 + \delta_4^2\sigma\rho), \quad d_2 = 2(\delta_1\delta_2 - \sigma\rho\delta_3\delta_4),$$

then

$$(15)\qquad \begin{aligned} f_3 &= b_1\gamma_3 + b_2\sigma\gamma_4, \quad & f_4 &= b_1\gamma_4 + b_2\gamma_3, \\ f_5 &= d_1\gamma_5 + d_2\sigma\rho\gamma_6, \quad & f_6 &= d_1\gamma_6 + d_2\gamma_5. \end{aligned}$$

I have also shown that if $g_2 = X'X$ then

$$(16)\qquad f_4 = f_6 = 0, \quad f_3 + f_5 = \gamma_3^2 - \gamma_4^2\sigma.$$

But then $\gamma_3 b_2 = -\gamma_4 b_1$, $\gamma_5 d_2 = -\gamma_6 d_1$, so that from (16_2), (15),

$$(17)\qquad \gamma_3\gamma_5(\gamma_3^2 - \gamma_4^2\sigma) = (\gamma_3^2 - \gamma_4^2\sigma)\gamma_5 b_1 + (\gamma_5^2 - \gamma_6^2\sigma\rho)\gamma_3 d_1.$$

If A is associative then (6) is satisfied. Also $g_2 \neq 0$ so that $g_2(-v) \neq 0$, $\gamma_3^2 - \gamma_4^2\sigma \neq 0$. Then (17) is equivalent to

$$(18)\qquad \gamma_3\gamma_5 = \gamma_5 b_1 + \gamma_3 d_1(\gamma_1^2 - \gamma_2^2\rho).$$

As in the proof of Theorem 1 we have immediately

THEOREM 2. *A sufficient condition that A with division sub-algebra B be a division algebra is that the quadratic form*

$$(19)\qquad \begin{aligned} Q \equiv\ & \gamma_5[(\alpha_1^2 + \alpha_2^2\sigma) - \rho(\alpha_3^2 + \alpha_4^2\sigma)] \\ & + \gamma_3(\gamma_1^2 - \gamma_2^2\rho)[(\alpha_5^2 + \alpha_6^2\sigma\rho) - \rho(\alpha_7^2 + \alpha_8^2\sigma\rho)] - \gamma_3\gamma_5\alpha_9^2 \end{aligned}$$

shall not vanish for any $\alpha_1, \cdots, \alpha_9$ not all zero and in K.

3. **Algebras over $K(q)$.** Let $L = K(q)$ be a quadratic field over K where

$$(20)\qquad q^2 = \delta = \delta_1^2 + \delta_2^2 \qquad (\delta_1 \text{ and } \delta_2 \text{ in } K).$$

It is well known that if K contains no quantity k such that $k^2 = -1$ then every cyclic quartic field over K contains a quadratic sub-field L of the above type. Hence a sufficient condition that an algebra of degree four be non-cyclic is that A contain no quadratic sub-field L as above. But also A contains no sub-

* Albert 3, p. 178.

field equivalent to any given quadratic field L if and only if $A \times L$ is a division algebra.* Hence we have

THEOREM 3. *If no k in K has the property $k^2 = -1$, a sufficient condition that a normal simple algebra A of order sixteen over K be a non-cyclic normal division algebra is that $A \times L$ be a division algebra for every quadratic field $L = K(q)$,*

$$q^2 = \delta = \delta_1^2 + \delta_2^2 \qquad (\delta_1 \text{ and } \delta_2 \text{ in } K). \tag{21}$$

We shall apply Theorem 3 as follows. We shall choose a particular field of reference, K. We shall then define A by a choice of $\rho, \sigma, \gamma_1, \cdots, \gamma_6$. Then also $A \times L$ is evidently a normal simple algebra (of the same kind as A over K) over L when we show that neither ρ, σ, nor $\sigma\rho$ is the square of any quantity of L (not merely K). We shall then prove that A(not $A \times L$ which can have exponent two) has exponent four, while $A \times L$ is a division algebra. This latter step will be an application of Theorems 1 and 2 applied to $A \times L$ over L. The algebras A over K will be non-cyclic algebras of exponent four by Theorem 3.

4. **The field K.** Let F be any *real number* field, and let x, y, and z be independent marks (indeterminates). The field $F(x, y, z) \equiv K$ is a function field consisting of all rational functions with (real) coefficients in F of x, y, z. We shall deal with quadratic forms Q and equations $Q = 0$ so that we shall always be able to delete denominators and hence take our quantities in

$$J = F[x, y, z],$$

the domain of integrity consisting of all polynomials in x, y, z with coefficients in F. We shall of course also consider the domains $F[x]$, $F[x, y]$, etc.

Consider a field $K(q)$ as in §3. It is evident that the quantity q defining such a quadratic field may always be chosen so that $\delta, \delta_1, \delta_2$ are in J. Also in a quadratic form $Q = 0$ with coefficients in J and variables over $K(q)$ we may always take the variables to be in the domain of integrity $J[q]$ of all quantities of the form

$$a + bq$$

where a and b are in J.

Every quantity $a = a(x, y, z)$ of J has a highest power z^n with coefficient in $F[x, y]$ not identically zero. We shall call n the z-degree of a, the coefficient of z^n the *z-leading coefficient* of a. Similarly a has an x-degree, y-degree, x-leading coefficient, y-leading coefficient. A restriction of the z-degree of a certain expression and its z-leading coefficient evidently does not affect its x-degree, etc.

* Cf. Albert 1.

If the coefficient of z^n above is $b(y, x)$ and the coefficient of the highest power y^m of y in b is $c(x)$, then m is called the (z, y)-degree of a, $c(x)$ the (z, y)-leading coefficient of a. Finally the degree of $c(x)$ is the (z, y, x)-degree of a, its leading coefficient in F, the (z, y, x)-leading coefficient of a.

We have similarly (x, y, z)-degree and leading coefficient, etc. Using these definitions an elementary result is

LEMMA 1. *The field K contains no quantity k such that $k^2 = -1$.*

For let $k^2 = -1$. Then $rk = s$, where r and s are in J and are both not zero. It follows that $s^2 = -r^2$. The (x, y, z)-leading coefficient of s^2 is evidently a real square and is positive, that of $-s^2$, negative so that the polynomial identity $r^2 = -s^2$ is impossible.

LEMMA 2. *There exist quantities λ, μ in $F[x, y]$ such that $\lambda^2+\mu^2$ is not the square of any quantity of $F(x, y)$.*

We prove the above lemma with the example $\lambda = x$, $\mu = y$. If $x^2+y^2 = b^2$, where b is a rational function of x and y, it is evident that b must be a polynomial in x and y. For the square of a rational function in its lowest terms and with denominator not unity is never a polynomial. Hence we may put $b = b_1x+b_2$ where b_2 is in $F[y]$, b_1 merely in $F[x, y]$. Then $x^2+y^2 = b_1^2x^2 +2b_1b_2x+b_2^2$ identically in x and y. It follows that $b_2^2 = y^2$, $b_2 = \pm y$. Then $x^2 = b_1^2x^2 \pm 2b_1xy$. Hence b_1 divides x and is a power of x. But then $\pm(2b_1)y = x - b_1^2x$ in $F[x]$, b_1 in $F(x)$, which is impossible.

5. **The S-polynomials.** The quadratic forms (9), (19) over L shall be treated as follows. If $Q = \sum \alpha_i^2\lambda_i$ with λ_i in J (not in $J[q]$) vanishes for α_i in L and not all zero, then obviously, by multiplying Q by the square of the least common denominator, not zero and in J, of the $\alpha_i = \alpha_{i1}+\alpha_{i2}q$ (α_{i1}, α_{i2} in K), we shall have $Q = 0$ for α_i in $J[q]$, that is, α_{i1} and α_{i2} in J. But then

$$Q = \sum \lambda_i[(\alpha_{i1}^2 + \alpha_{i2}^2\delta) + (2\alpha_{i1}\alpha_{2i})q] = 0$$

so that

$$\sum \lambda_i S_i = 0,$$

where

$$S_i = (\alpha_{i1})^2 + (\alpha_{i2}\delta_1)^2 + (\alpha_{i2}\delta_2)^2. \tag{22}$$

We shall call a polynomial of the form (22) an S-polynomial. All such polynomials have the properties that all their degrees are even, all their (, ,)-leading coefficients positive. Moreover such a polynomial is zero if and only if $\alpha_i = \alpha_{i1} = \alpha_{i2} = 0$. Hence we have

LEMMA 3. *A sufficient condition that a quadratic form* $\sum \lambda_i \alpha_i^2$ *with* λ_i *in* J *shall not vanish for any* α_i *not all zero and in* $K(q)$ *is that* $\sum \lambda_i S_i$ *shall not vanish for any S-polynomials* S_i *not all zero.*

6. **The multiplication constants of** A. We now choose $\rho, \sigma, \gamma_1, \cdots, \gamma_6$ in J. We shall take

(23) σ *of even z-degree, even* (z, y)*-degree, odd* (z, y, x)*-degree.*

We shall define γ_1 and γ_5 in terms of certain quantities ϵ_1, ϵ_5, where

(24) (*the z-degree of* ϵ_5 *is odd*) $>$ (*z-degree of* $\epsilon_1\gamma_3$);

(25) (*the z-degree of* γ_3 *is odd*) $>$ (*z-degree of* $\gamma_4\sigma$);

(26) (*the z-degree of* γ_2) $>$ (*z-degree of* $\gamma_6\sigma$);

(27) *the* (z, y)*-degree of* γ_3 *even, of* ϵ_5 *odd.*

The above conditions are restrictions merely on the z-leading coefficients of our quantities. By making the corresponding z-degrees sufficiently large we evidently only restrict a single term in each quantity, satisfy the above conditions, and yet permit any desired inequalities between x-degrees, y-degrees of the same quantities. Moreover (, ,)-leading coefficients other than the $(z,$,)-leading coefficients may be taken to have any desired sign, and the evenness or oddness of (,)-degrees, etc., other than those already given above are still at our choice. We therefore may continue with

(28) σ *of even y-degree, odd* (y, x)*-degree*;

(29) (*y-degree of* ϵ_1 *odd*) $>$ (*y-degree of* ϵ_5);

(30) (*y-degree of* γ_2) $>$ (*y-degree of* $\gamma_6\sigma$);

(31) (*y-degree of* γ_3) $>$ (*y-degree of* $\gamma_4\sigma$);

(32) σ *of odd x-degree.*

Let the x-leading coefficient of γ_6 be π_1, that of $\gamma_2\gamma_4$ be π_2 such that

(33) $\pi_1^2 + \pi_2^2 \neq \lambda^2$ *for any* λ *of* $F(y, z)$.

This restriction may be satisfied by Lemma 2 and there merely restricts the x-leading coefficients of γ_6 and $\gamma_2\gamma_4$. Also take

(34) (*x-degree of* γ_6) $=$ (*x-degree of* $\gamma_2\gamma_4$) $>$ (*x-degree of* $\gamma_2\gamma_3$),

that is, the x-degree of γ_4 greater than the x-degree of γ_3, and, if we desire, the x-leading coefficient of γ_2 unity, that of γ_4, y, that of γ_6, z, and (33) is satisfied.

Finally let

$$e = \gamma_2^2(\gamma_3^2 - \gamma_4^2\sigma) - \gamma_6^2\sigma, \tag{35}$$

$$\rho = e[\epsilon_1^2(\gamma_3^2 - \gamma_4^2\sigma) - \epsilon_5^2], \tag{36}$$

$$\gamma_1 = \epsilon_1 e, \quad \gamma_5 = \epsilon_5 e. \tag{37}$$

Then

$$\begin{aligned}\gamma_1^2 - \gamma_2^2\rho &= \epsilon_1^2 e^2 - \gamma_2^2\rho \\ &= e\epsilon_1^2[\gamma_2^2(\gamma_3^2 - \gamma_4^2\sigma) - \gamma_6^2\sigma] - e\gamma_2^2\epsilon_1^2(\gamma_3^2 - \gamma_4^2\sigma) + \gamma_2^2\epsilon_5^2 e,\end{aligned}$$

and

$$\gamma_1^2 - \gamma_2^2\rho = e[(\gamma_2\epsilon_5)^2 - (\gamma_6\epsilon_1)^2\sigma]. \tag{38}$$

Also

$$\begin{aligned}\gamma_5^2 - \gamma_6^2\sigma\rho &= \epsilon_5^2 e^2 - \gamma_6^2\sigma\rho \\ &= e\gamma_2^2\epsilon_5^2(\gamma_3^2 - \gamma_4^2\sigma) - e\gamma_6^2\epsilon_5^2\sigma + e\gamma_6^2\sigma\epsilon_5^2 - e\gamma_6^2\sigma\epsilon_1^2(\gamma_3^2 - \gamma_4^2\sigma) \\ &= (\gamma_3^2 - \gamma_4^2\sigma)e[(\gamma_2\epsilon_5)^2 - (\gamma_6\epsilon_1)^2\sigma].\end{aligned}$$

By (38) we have

THEOREM 4. *If $\rho, \sigma, \gamma_1, \cdots, \gamma_6$ are chosen as in* (35), (36), (37), *the corresponding algebra A satisfies*

$$\gamma_5^2 - \gamma_6^2\sigma\rho = (\gamma_1^2 - \gamma_2^2\rho)(\gamma_3^2 - \gamma_4^2\sigma) \tag{39}$$

and is associative.

7. **Elementary properties.** In (25) we chose the z-degree of γ_3 to be greater than the z-degree of $\gamma_4\sigma$. In (26) we took the z-degree of γ_2 greater than that of $\gamma_6\sigma$. It now follows that the only term of e containing its highest power of z is $(\gamma_2\gamma_3)^2$. Similarly, by (24), (25) the term of $[\epsilon_1^2(\gamma_3^2 - \gamma_4^2\sigma) - \epsilon_5^2]$ containing its highest power of z is $-\epsilon_5^2$. Hence the term of ρ containing its highest power of z is $-(\gamma_2\gamma_3\epsilon_5)^2$.

LEMMA 4. *The z-degree of ρ is positive, even, and the z-leading coefficient of ρ is the negative of a perfect square.*

Consider the y-degree of ρ. By (31) the y-degree of $\gamma_3^2 - \gamma_4^2\sigma$ is positive and its y-leading coefficient is a perfect square (in γ_3^2). By (35) the leading y-term of e is then in $(\gamma_2\gamma_3)^2$, while the leading y-term of $\epsilon_1^2(\gamma_3^2 - \gamma_4^2\sigma) - \epsilon_5^2$ is then in $(\epsilon_1\gamma_3)^2$. Hence the term of ρ containing its highest power of y is $(\epsilon_1\gamma_2\gamma_3^2)^2$.

LEMMA 5. *The y-degree of ρ is positive and even, and its y-leading coefficient is a perfect square.*

Consider the x-degree of e. We have taken the x-degree of γ_6 equal to the x-degree of $\gamma_2\gamma_4$ and the x-degree of γ_4 greater than the x-degree of γ_3. But $e = -[(\gamma_2\gamma_4)^2 + \gamma_6^2]\sigma + (\gamma_2\gamma_3)^2$. Hence the x-leading coefficient of e is the product of the x-leading coefficient of $-\sigma$ by $\pi_1^2 + \pi_2^2$. But the x-degree of σ has been taken odd.

LEMMA 6. *Let σ_0 be the x-leading coefficient of σ. Then the x-leading coefficient of e is $-\sigma_0(\pi_1^2+\pi_2^2)$ and the x-degree of e is a positive odd integer.*

The quantity $\gamma_1^2 - \gamma_2^2\rho$ is determined by (38). We shall require

LEMMA 7. *The z-degrees of $\gamma_1^2 - \gamma_2^2\rho$ are all even.*

For proof we notice that we have already shown that the z-degree of e is even, in fact the leading term of e when arranged according to powers of z is a perfect square. Also we have taken the z-degree of $(\gamma_2\epsilon_5)^2$ greater than that of $(\gamma_6\epsilon_1)^2\sigma$. Hence the z-degree of $\gamma_1^2 - \gamma_2^2\rho$ is even. In fact its z-leading coefficient occurs only in $(\gamma_2^2\epsilon_5\gamma_3)^2$ and is a perfect square, so that all its z-degrees are even.

One of the properties required in our definition of A is that neither ρ, σ, nor $\sigma\rho$ shall be the square of any quantities of K. We shall prove

LEMMA 8. *Neither ρ, σ, nor $\sigma\rho$ is the square of any quantity of $K(q)$.*

For let $\rho = \alpha^2$ where α is in $K(q)$. Then $\mu\alpha = \lambda$ where λ is in $J[q]$ and μ is in J. Then $\rho\mu^2 = \lambda^2$ in J. A quantity λ of $K(q)$ has its square in K if and only if it is either in K or a multiple of q by a quantity of k. If λ in $J[q]$ is in K then λ is in J so that $\rho\mu^2 = \lambda^2$ is impossible because the (z, y, x)-leading coefficient of ρ and hence $\rho\mu^2$ is negative while that of λ^2 is positive. Hence $\lambda = \nu q$ with ν in J. Then $\lambda^2 = \nu^2\delta$ is an S-polynomial and cannot be identical with $\rho\mu^2$ of negative (z, y, x)-leading coefficient.

Similarly $\sigma \neq \alpha^2$ where we now use the property that σ has odd x-degree. Finally by (28) and Lemma 5 $\sigma\rho$ has odd (y, x)-degree and $\sigma\rho \neq \alpha^2$ for any α of $K(q)$.

COROLLARY 1. *The quantities ρ, σ, $\sigma\rho$ are not the squares of any quantities of K.*

It follows from Corollary 1 that $K(u, v)$ is a quartic field over K and that $g_1 = 0$ if and only if $\gamma_1 = \gamma_2 = 0$. By Lemma 7, $g_1 \neq 0$. Also (31) implies that $g_2 \neq 0$, while the associativity condition (38) implies that $g_3 \neq 0$.

8. **The exponent of A.** We shall use (7) to prove that A has exponent four, that is, A is not a direct product of two algebras of degree two. Assume that A has not exponent four so that (7) is satisfied for $\alpha_1, \alpha_2, \alpha_3$ in K and not all zero. As we have already remarked we may take $\alpha_1, \alpha_2, \alpha_3$ in J. If $\alpha_2 = \alpha_3 = 0$,

$$(\alpha_1^2 - \alpha_2^2\sigma = (\gamma_1^2 - \gamma_2^2\rho)\alpha_3^2 \tag{7}$$

implies that $\alpha_1^2 = \alpha_1 = 0$, a contradiction. Hence if $\alpha_3 = 0$ then $\alpha_2 \neq 0$ and $\sigma = (\alpha_1\alpha_2^{-1})^2$, a contradiction of Corollary 1. Thus $\alpha_3 \neq 0$.

By Lemma 7 $\gamma_1^2 - \gamma_2^2\rho \neq 0$ so that $h = (\gamma_2\epsilon_5)^2 - (\gamma_6\epsilon_1)^2\sigma \neq 0$. The equation $\gamma_1^2 - \gamma_2^2\rho = he$ gives

$$(\alpha_1^2 - \alpha_2^2\sigma)h = (\alpha_3 h)^2 e.$$

Let $\beta_3 = \alpha_3 h \neq 0$, $\beta_1 = \alpha_1\gamma_2\epsilon_5 + \alpha_2\gamma_6\epsilon_1\sigma$, $\beta_2 = \alpha_1\gamma_6\epsilon_1 + \alpha_2\gamma_2\epsilon_5$. Then, as may be easily computed,*

$$\beta_1^2 - \beta_2^2\sigma = e\beta_3^2 \qquad (\beta_3 \neq 0,\ \beta_1,\ \beta_2,\ \beta_3 \text{ in } J). \tag{40}$$

But then $\beta_1^2 = \sigma\beta_2^2 + e\beta_3^2$. The x-leading coefficient of $e\beta_3^2$ has the form $-\sigma_0(\pi_1^2 + \pi_2^2)\beta_{30}^2$ by Lemma 6. The x-leading coefficient of $\sigma\beta_2^2$ has the form $\sigma_0\beta_{20}^2$. But $(\pi_1^2 + \pi_2^2)\beta_{30}^2 \neq 0$ is not the square of any quantity of $K(y, z)$. Hence the x-leading coefficient of $\sigma\beta_2^2 + e\beta_3^2$ is not zero. But the x-degree of this expression is odd since σ has odd x-degree, e has odd x-degree, $\beta_3 \neq 0$. It follows that (40) is impossible for $\beta_3 \neq 0$, a contradiction.

9. **The first norm condition.** We wish to prove that algebra B is a division algebra, that is, prove that $g_1 \neq a \cdot a(-v)$ for any a of $K(u, v)$, the so called *first norm condition*. As we have shown this condition will be satisfied if we can show that the equation

$$S_1 + S_2\rho - \sigma(S_3 + S_4\rho) = \gamma_1 S_5 \tag{41}$$

is impossible for S-polynomials $S_1, \cdots, S_5$ not all zero, a consequence of §5 applied to (9).

By Lemma 2 the y-degree of ρ is even and the (y, z, x)-leading coefficient of ρ is positive. Also the y-degree of σ is even. Hence the y-degree of each of S_1, $S_2\rho$, S_3, $S_4\rho$ is even. But the (y, z, x)-leading coefficients of these terms are all positive. Moreover $S_1 + S_2\rho$, $S_3 + S_4\rho$ have even (y, z)-degree, while σ has odd (y, z)-degree. Hence the (y, z)-degree of $S_1 + S_2\rho - \sigma(S_3 + S_4\rho)$ is either even or odd according as the (y, z)-degree of $S_1 + S_2\rho$ is greater or less than the (y, z)-degree of $(S_3 + S_4\rho)\sigma$. In any case the corresponding (y, z, x)-leading coefficient is zero if and only if $S_1 = S_2 = S_3 = S_4 = 0$. We have shown that $T = S_1 + S_2\rho - \sigma(S_3 + S_4\rho)$ has even y-degree and (y, z, x)-leading coefficient zero if and only if $S_i = 0$ $(i = 1, \cdots, 4)$.

By (35), (30), (31) the y-degree of e is even. By (37), (29) the y-degree of γ_1 is odd. Hence the y-degree of $\gamma_1 S_5$ is odd unless $S_5 = 0$. But $\gamma_1 S_5 = T$ has even y-degree. Hence $S_5 = 0$, $T = 0$, T has (y, z, x)-leading coefficient zero so that $S_i = 0$ $(i = 1, \cdots, 5)$.

* That is, let $a = \alpha_1 + \alpha_2 v$, $b = \gamma_2\epsilon_5 + \gamma_6\epsilon_1 v$. Then $ab = (\alpha_1\gamma_2\epsilon_5 + \alpha_2\gamma_6\epsilon_1\sigma) + (\alpha_1\gamma_6\epsilon_1 + \alpha_2\gamma_2\epsilon_5)v = \beta_1 + \beta_2 v$, and $a \cdot a(-v) \cdot b \cdot b(-v) = (\alpha_1^2 - \alpha_2^2\sigma) \cdot h = ab \cdot \overline{ab}(-v) = \beta_1^2 - \beta_2^2\sigma$.

10. The second norm condition. This is the condition $g_2 = X'X$ which, by §5 and (19), is satisfied if we can prove that

$$(42)\quad \gamma_5[S_1 + S_2\sigma - \rho(S_3 + S_4\sigma)] + \gamma_3(\gamma_1^2 - \gamma_2^2\rho)[S_5 + S_6\sigma\rho - \rho S_7 - \sigma S_8] = \gamma_3\gamma_5 S_9$$

is impossible for S-polynomials $S_i(i=1, \cdots, 9)$ not all zero. Notice that we have replaced $\rho\alpha_8^2\rho = (\rho\alpha_8)^2$ of (19) by the S-polynomial S_8 instead of the formally corresponding $\rho^2 S_8$.

By (24) the z-degree of γ_3 is odd. By the proof of Lemma 4 the z-degree of e is even and the z-leading coefficient of e is a perfect square. Applying (27) we have

LEMMA 9. *The z- and (z, y)-degrees of γ_5 are odd.*

We have taken ρ to have all even degrees and *negative* (z, y, x)-leading coefficient by Lemma 4. Also σ has even z-degree, (z, y)-degree, but odd (z, y, x)-degree. Hence the (z, y, x)-leading coefficient of any $S_i - \rho S_j$ is positive or zero according as not both or both of S_i, S_j are zero. Hence the (z, y, x)-leading coefficient of a combination $T = S_i - \rho S_j \pm \sigma(S_r - \rho S_t)$ is zero if and only if the four S_i are zero. Moreover T has even (z, y)-degree and (z, y)-leading coefficient which is identically zero only when all the four S_i are zero. But the (z, y)-degree of γ_3 is even, the (z, y)-degree of $\gamma_1^2 - \gamma_2^2\rho$ is even, while that of γ_5 is odd. Hence the (z, y)-leading coefficient of

$$R = \gamma_5[(S_1 - \rho S_3) + \sigma(S_2 - \rho S_4)] + \gamma_3(\gamma_1^2 - \gamma_2^2\rho)[S_5 - \rho S_7 - \sigma(S_6 - \rho S_8)]$$

is either the (z, y)-leading coefficient of its first bracket or of its second bracket, while R has z-leading coefficient identically zero if and only if $S_i = 0$ $(i = 1, \cdots, 8)$. But the z-degree of R is *odd* unless the S_i are zero since the z-degree of γ_3 is odd by (25), that of γ_5 odd by Lemma 9. By (42) $R = \gamma_3\gamma_5 S_9$ has *even* z-degree. Hence $R = 0$, $S_9 = 0$, and R has z-leading coefficient zero. This proves that $S_i = 0$ $(i = 1, \cdots, 9)$ as desired. We have proved

LEMMA 10. *Let F be a real number field, x, y, z indeterminates, and let A be an algebra of order sixteen over $K = F(x, y, z)$ defined by* (1)–(5), (23)–(37). *Then A is a normal division algebra of degree and exponent four over K, $A \times L$ is a normal division algebra of degree four over L for every quadratic field $L = K(q)$, $q^2 = \delta = \delta_1^2 + \delta_2^2$ (δ_1, δ_2 in K).*

As an immediate corollary of Lemma 10 we then have

THEOREM. *The algebras of Lemma* 10 *are non-cyclic algebras of degree four not expressible as direct products of cyclic algebras of degree two.*

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.