NON-CYCLIC ALGEBRAS WITH PURE MAXIMAL SUBFIELDS*

A. A. ALBERT

One of the most elementary consequences of the assumption that a normal division algebra A is cyclic of degree n over its centrum K is that A contains a quantity j whose minimum equation is $\omega^n = \gamma$ in K. In 1933 I conjectured the truth of the converse proposition. The proof is easily reducible† to the case where n is a power p^e of a prime p. Let q be the characteristic of K. I succeeded in proving the theorem for $q = p$, e arbitrary,‡ as well as for $q \neq p$, $e = 1$.§ There remained the case $q \neq p$, $e \geqq 2$.

My hope for the truth of the theorem was heightened by H. Hasse's remark|| that it would provide an essential simplification of the arithmetic existence properties required for the proof of the theorem that all normal division algebras over an algebraic number field are cyclic. However this hope is at an end. For the conjecture is actually false in the remaining case. This is shown by a demonstration of the validity of the following theorem:

THEOREM. *Let x, y, z be independent indeterminates over a field F of real numbers,¶ $K = F(x, y, z)$. Then there exist non-cyclic normal division algebras of degree and exponent four over K, each with a subfield $K(j)$ of degree four over K such that $j^4 = \gamma$ in K.*

Our example is obtained from a class of non-cyclic algebras given in my paper in the Transactions of this Society, vol. 35 (1933), pp.

* Presented to the Society, February 26, 1938.

† For, every A is a direct product of division algebras A_i of degrees $n_i = p_i^{e_i}$ for distinct primes p_i, and A is cyclic if and only if the A_i are cyclic. Moreover the field defined by $\omega^n = \gamma$ splits A if and only if the fields defined by $\omega^{n_i} = \gamma$ split the A_i. For references to the results used see M. Deuring's *Algebren*.

‡ Transactions of this Society, vol. 39 (1936), pp. 183–188.

§ Ibid., vol. 36 (1934), pp. 885–892.

|| In a letter to the author. The arithmetic existence theorem is that of W. Grünwald, Journal für die reine und angewandte Mathematik, vol. 169 (1933), pp. 103–107. The proof of Hasse applicable for the case $n = p$ is as follows. Assume that γ is in K and is exactly divisible by the first power of P for every prime ideal P of K such that the P-index of A is not unity. Let also γ be negative for all real fields conjugate to K. Then $K(\gamma^{1/n})$ splits A and is equivalent to a maximal subfield of A. When n is a prime p this implies that A is cyclic.

¶ Our existence theorem is for F non-modular. It seems likely that a modification can be made with F of characteristic any $p > 2$.

112–121. We shall require only slight modifications of the choice of parameters of that paper, and shall be so closely concerned with its content that we shall refer to its equations, lemmas, and theorems by the numbers used therein. Any new equations and lemmas will be numbered consecutively with those of this earlier paper, and we shall indicate modified results by an accent.

Put $\epsilon_1=\gamma_1=0$ in (37). This necessitates the deletion of (29) and gives

$$\rho = -\epsilon_5^2 e. \tag{36'}$$

From (2) we have

$$j_1^2 = g_1 = \gamma_2 u, \qquad j_1^4 = \gamma_2^2\rho = \gamma \text{ in } K. \tag{43}$$

Then j_1 is the quantity j of our theorem. We shall assume (23)–(27), (28), (30)–(34), but shall make some further restrictions. These will be necessary in order that the property proved in the original §9 shall again hold.

Observe first that the condition (7) that our algebra A have exponent four has now become

$$\alpha_1^2 - \alpha_2^2\sigma - (\gamma_2\alpha_3\epsilon_5)^2 e = 0 \tag{7'}$$

for $\alpha_1, \alpha_2, \alpha_s$ in K only if $\alpha_1=\alpha_2=\alpha_s=0$. But this is equivalent to (40), and the proof of §8 depends only upon (33), (34). Hence this proof is valid, and A is a normal division algebra of degree and exponent four with a maximal subfield $K(j)$, $(j^4=\gamma \text{ in } K)$.

We prove that A is non-cyclic by showing that $A\times L$ is a division algebra for every quadratic field $L=K(q)$, $(q=\delta_1^2+\delta_2^2)$.* Observe that it is not possible to prove this by showing that $A\times L$ has exponent four over L. For it is known† that every normal division algebra A of degree four over K has exponent two over an existing field L of our type. Our theorem will thus imply the following corollary:

COROLLARY. *There exist normal division algebras A of degree and exponent four over K and quadratic fields L such that L splits A^2 but $A\times L$ is a division algebra.*

Observe now that (9) becomes $Q=\alpha_1^2+\alpha_2^2\rho-\sigma(\alpha_3^2+\alpha_4^2\rho)$. The vanishing of Q for α_i not all zero is equivalent to the non-trivial vanishing of $\alpha_1^2+\alpha_2^2\rho-\alpha_3^2\sigma$, since $\alpha_3^2+\alpha_4^2\rho$ is the norm form of a quadratic field. But this is precisely the condition (7'). Hence the sufficient

* This is as in the earlier paper referred to above.

† A consequence of Theorem 7 of the author's paper in the Transactions of this Society, vol. 34 (1932), pp. 363–372.

condition of (9) and §9 is not satisfied, and we shall have to investigate the question more deeply. Observe finally that the proof in §10 depends only upon the z degrees of our quantities as given in (23)–(27) and is valid provided that we can prove the result of §9, namely, that the algebra $B \times L$ is a division algebra. To do this we first make the additional assumptions

(43) γ_2 of odd y degree, $\epsilon_5\gamma_3$ of odd y degree.

We then prove the following lemma:

LEMMA 11. *There exist polynomials a, b in $F[x, z]$ such that a^2+b^4 is not the square of any quantity of the field $F(x, z)$.*

For as in Lemma 2 the equation $a^2+b^4=c^2$ for c in $F(x, z)$ implies that c is a polynomial in $F[x, z]$. The condition is easily seen to be satisfied by $a=x^2$, $b=z$.

Our choice of γ_2, γ_3, ϵ_5, γ_4, γ_6 in (30), (31), (43) now implies the truth of the following lemma:

LEMMA 12. *The y degree of ρ is a multiple of four, and its y-leading coefficient is $-a^2$ with a an arbitrary polynomial of $F[x, z]$.*

Choose a as in Lemma 11 with a corresponding to b, and put

$$\phi = (by^n)^4 - \rho, \tag{44}$$

where $4n$ is the y degree of ρ. Then ϕ also has y degree $4n$ and y-leading coefficient

$$\phi_y = b^4 + a^2 \neq c^2 \tag{45}$$

for any c of $F[x, z]$. Observe our introduction of the notation α_y for the y-leading coefficient of any quantity α of $F[y, x, z]$.

We next prove the lemma:

LEMMA 13. *Let $\alpha_1, \cdots, \alpha_8$ be variables over K, and let*

$$S = \sigma(\alpha_1^2 - \alpha_2^2\phi) - (\alpha_7^2 + \alpha_8^2), \quad T = \gamma_2[\alpha_3^2 + \alpha_4^2\rho\phi - \sigma(\alpha_5^2 + \alpha_6^2\rho\phi)].$$

Then the form $S-T$ is not a null form over K.

For let $S-T$ be a null form so that $S=T$ for α_i in K, not all zero. There is clearly no loss of generality if we assume the α_i polynomials in x, y, z. The formal y degree of $\alpha_3^2+\alpha_4^2\rho\phi$ is even, and its y-leading coefficient is evidently a sum of three squares. Similarly the y-leading coefficient of $\sigma(\alpha_5^2+\alpha_6^2\rho\phi)$ is σ_y multiplied by a sum of three squares. But by (28) σ_y has odd x degree. Hence the sum of the y-leading coefficients of $\alpha_3^2+\alpha_4^2\rho\phi-\sigma(\alpha_5^2+\alpha_6^2\rho\phi)$ is zero only if $\alpha_3=\alpha_4=\alpha_5=\alpha_6$

$=0$. But (43) then implies that T either has odd y degree or is zero.

The y-leading coefficient of $\alpha_1^2-\alpha_2^2\phi$ is a sum of terms such as $\alpha_{1y}^2-\alpha_{2y}^2(b^4+a^2)$ and cannot be zero by our choice in Lemma 11 unless $\alpha_1=\alpha_2=0$. Hence the y-leading coefficient of $\sigma(\alpha_1^2-\alpha_2^2\rho)$ has odd x degree or is zero, that of $\alpha_2^2+\alpha_3^2$ has even x degree, and S clearly has even y degree. This shows that $S=T$ implies that $T\equiv 0$, $\alpha_3=\alpha_4=\alpha_5=\alpha_6=0$. Our proof also implies that $\alpha_1=\alpha_2=\alpha_7=\alpha_8=0$, a contradiction. This proves our lemma.

We now replace the argument of §9 by the property that $B\times L$ is not a division algebra if and only if

$$\delta_1^2+\delta_2^2=\beta_1^2\sigma+\beta_2^2 g_1-\beta_3^2\sigma q, \tag{46}$$

for β_1, β_2, β_3 in the centrum $K(u)$ of B, $L=K(q)$, $q^2=\delta_1^2+\delta_2^2$, and δ_1, δ_2 in K. This is a well known property of quaternion algebras.* We write $\beta_i=\xi_i+u\eta_i$ and equate coefficients of u, obtaining the equivalent pair of conditions

$$\delta_1^2+\delta_2^2=(\xi_1^2+\eta_1^2\rho)\sigma+2(\xi_2\eta_2-\sigma\xi_3\eta_3)\gamma_2\rho, \tag{47}$$

$$0=2\xi_1\eta_1\sigma+[(\xi_2^2+\eta_2^2\rho)-\sigma(\xi_3^2+\eta_3^2\rho)]\gamma_2, \tag{48}$$

for ξ_i, η_i, δ_1, δ_2, not all zero, in K. Multiply (48) by λ^2 and add to (47). We obtain

$$\begin{aligned}\delta_1^2+\delta_2^2=&[(\xi_1+\lambda^2\eta_1)^2+\eta_1^2(\rho-\lambda^4)]\sigma+\gamma_2[(\lambda\xi_2+\rho\eta_2\lambda^{-1})^2\\&+\eta_2^2\lambda^{-2}(\lambda^4-\rho)\rho-\sigma(\lambda\xi_3+\rho\eta_3\lambda^{-1})^2-\sigma\eta_3^2\lambda^{-2}(\lambda^4-\rho)\rho].\end{aligned} \tag{49}$$

Put $\lambda=by^n$, $\delta_1=\alpha_1$, $\delta_2=\alpha_8$, $\xi_1+\lambda^2\eta_1=\alpha_1$, $\eta_1=\alpha_2$, $\lambda\xi_2+\rho\eta_2\lambda^{-1}=\alpha_3$, $\eta_2\lambda^{-1}=\alpha_4$, $\lambda\xi_3+\rho\lambda_3\lambda^{-1}=\alpha_5$, $\eta_3\lambda^{-1}=\alpha_6$, and obtain the form $S-T$ of (45). By Lemma 13 the form $S-T$ is not a null form. Hence neither is (49); and (47), (48) cannot have a simultaneous solution. This proves our final result.

THE UNIVERSITY OF CHICAGO

* It is a corollary of the theorem stating that if L is a field of degree n over K, and if A is a division algebra of degree n over K, then L splits A if and only if L is equivalent to a subfield of A. For our quaternion algebras these are fields $K(\beta)$ with $\beta=\beta_1 v+\beta_2 j_1+\beta_3 v j_1$, and we must have $\beta^2=\delta_1^2+\delta_2^2$ as in (46).