ON PRIMARY NORMAL DIVISION ALGEBRAS OF DEGREE EIGHT*

BY A. A. ALBERT

1. *Introduction.* A normal division algebra A of degree n over F will be called *primary* if A is not expressible as a direct product of two normal division algebras B and C, where neither B nor C has degree unity. It is well known that necessarily $n=p^e$, p a prime, if A is primary. Moreover, if $n=p^e$, then a *sufficient* condition that A be primary is that A shall have exponent† n.

I have recently proved‡ that if A has degree four then A is primary if and only if A has exponent four. In the present paper I shall prove that there exist primary (cyclic) normal division algebras of degree eight but exponent four so that the above sufficient condition is actually not necessary.§

2. *Cyclic Fields of Degree Eight.*|| Let F be any non-modular field, and let C be a cyclic field of degree eight over F. Then I have proved that $C=F(x)$ contains a sub-field $F(y)$ which is cyclic of degree four over F and is defined by

$$y^2 = \nu(u - \tau),\ u^2 = \tau = 1 + \epsilon^2, \tag{1}$$

where $\nu\neq 0$, $\epsilon\neq 0$ are in F and $\tau=1+\epsilon^2$ is not the square of any quantity of F. I have also proved that

$$-\nu\tau = \xi_1^2 + \xi_2^2\tau,\ -\epsilon = (\eta_1^2 - \eta_2^2\tau)(\xi_1^2 + \xi_2^2\tau), \tag{2}$$

for ξ_1, ξ_2, η_1, η_2 in F. Conversely I have shown that if (1) and (2) are satisfied, then there exists a uniquely defined cyclic field $C=F(x)$ of degree eight over F and with $F(y)$ as cyclic quartic sub-field.

---

* Presented to the Society, February 25, 1933.

† The exponent ρ of A of degree n is the least integer such that the direct power A^ρ is a total matric algebra, and is a divisor of n.

‡ Transactions of this Society, vol. 34 (1932), pp. 363–372.

§ It seems likely, however, that A of degree p^2, p a prime, is primary if and only if A has exponent p^2.

|| For proofs of the results of this section see my paper on cyclic fields of degree eight which has been offered for publication to the editors of the Transactions of this Society.

In particular let F contain no quantity i such that $i^2 = -1$, and let also $-\tau$ be not the square of any quantity of F. Then I have proved that the solution of $(2)_2$ is equivalent to the solution of

$$-\epsilon = \lambda^2 - \mu^2\tau, \tag{3}$$

for $\lambda = \lambda_1 + \lambda_2 i$, $\mu = \mu_1 + \mu_2 i$, $i^2 = -1$, and λ_1, λ_2, μ_1, μ_2 in F, such that

$$\lambda_1\lambda_2 = \mu_1\mu_2\tau, \qquad \lambda_1\eta_2 = \mu_1\eta_1, \qquad \lambda_2\eta_1 = \mu_2\eta_2\tau, \tag{4}$$

while ξ_1 and ξ_2 are determined by

$$\xi_1 = \frac{\mu_1\eta_1 - \lambda_1\eta_2\tau}{\eta_1^2 - \eta_2^2\tau}, \quad \xi_2 = \frac{\mu_2\eta_1 - \lambda_2\eta_2}{\eta_1^2 - \eta_2^2\tau}, \quad \eta_1^2 - \eta_2^2\tau \neq 0. \tag{5}$$

We may evidently take $\lambda = \lambda_2 i$, $\mu = 0$, $\epsilon = -\lambda^2 = \lambda_2^2$ and (3) is satisfied. We also have $\lambda_1\eta_2 = \mu_1\eta_1 = \lambda_1\lambda_2 = \mu_1\mu_2\tau = 0$, while $\lambda_2\eta_1 = \mu_2\eta_2\tau = 0$ implies that $\eta_1 = 0$, and $\eta_2 \neq 0$ is arbitrary. Hence, from (5), $\xi_1 = 0$, while $\xi_2 = -\lambda_2(\eta_2\tau)^{-1}$. We have therefore proved that in this case

$$-\nu = \xi_2^2 = [\epsilon(\eta_2\tau)^{-1}]^2,$$

so that, for properly chosen η_2, we have $\nu = -1$.

THEOREM 1. *Every t in F such that*

$$\epsilon = t^2, \ \tau = 1 + \epsilon^2, \tag{6}$$

and $\pm\tau$ is not the square of any quantity of F, defines a cyclic field $F(x)$ of degree eight over F with a cyclic quartic sub-field

$$y^2 = \tau - u, \ u^2 = \tau, \tag{7}$$

so that $\nu = -1$.

3. *On a Rational Quadratic Form.* Let

$$ax^2 + by^2 + cz^2 + dw^2 \tag{8}$$

be an indefinite form with integer a, b, c, d. Then we may define (i, j) to be the (positive) greatest common divisor of any two integers i and j and may write

$$\begin{cases} a = (a, b)\cdot(a, c)\cdot(a, d)\cdot a_0, & b = (b, a)\cdot(b, c)\cdot(b, d)\cdot b_0, \\ c = (c, a)\cdot(c, b)\cdot(c, d)\cdot c_0, & d = (d, a)\cdot(d, b)\cdot(d, c)\cdot d_0. \end{cases} \tag{9}$$

If no three of a, b, c, d have a common factor greater than unity, it is well known* that (8) is a zero form only if

$$-(a, b)(a, d)(b, c)(c, d)a_0c_0 \tag{10}$$

is a quadratic residue of every odd prime p dividing either (a, c) or (b, d) for which $a_0b_0c_0d_0$ is a quadratic residue of p.

We shall take the t of Theorem 1 to be even so that ϵ is even and τ is odd. Consider the form

$$\tau x^2 - (4\tau^3 - 1)y^2 - 2\tau(2\tau\epsilon + 1)[z^2 - (4\tau^3 - 1)w^2], \tag{11}$$

which is a zero form if and only if

$$x^2 - \tau(4\tau^3 - 1)y^2 - 2(2\tau\epsilon + 1)[z^2 - (4\tau^3 - 1)w^2] \tag{12}$$

is a zero form. In (12) we write

$$\begin{gathered} a = 1,\ b = -\tau(4\tau^3 - 1),\ c = -2(2\tau\epsilon + 1), \\ d = 2(2\tau\epsilon + 1)(4\tau^3 - 1); \end{gathered} \tag{13}$$

but $4\tau^3-1=4\tau^2(1+\epsilon^2)-1=(2\tau\epsilon+1)(2\tau\epsilon-1)+4\tau^2$ is evidently prime to $2(2\tau\epsilon+1)\tau$. Hence no three of a, b, c, d have a factor in common. In fact

$$\begin{cases} a = a_0 = (a, b) = (a, c) = (a, d) = (b, c) = 1, \\ (b, d) = (4\tau^3 - 1), \\ (c, d) = 2(2\tau\epsilon + 1),\ b_0 = -\tau,\ c_0 = -1,\ d_0 = 1, \end{cases} \tag{14}$$

so that, from (10),

$$-(a, b)(a, d)(b, c)(c, d)a_0c_0 = (c, d) = 2(2\tau\epsilon + 1) \tag{15}$$

is a quadratic residue of every odd prime p dividing $(b, d)=h$ $=4\tau^3-1$ such that $a_0b_0c_0d_0=\tau$ is a quadratic residue of p. But if $4\tau^3-1\equiv 0 \pmod p$, then for the Legendre symbol $(\tau \mid p)$,

$$(\tau \mid p) = (4\tau^3 \mid p) = (1 \mid p) = 1. \tag{16}$$

Hence every prime p dividing h has the above property. It follows that if we write $2g=2(2\tau\epsilon+1)$, then $2g$ must be a quadratic residue of h. Hence the Jacobi symbol $(2g \mid h)=1$. But $(h \mid g)=1$, since $h=(2\tau\epsilon-1)g+4\tau^2\equiv 4\tau^2 \pmod g$. Then,†

* See L. E. Dickson, *Studies in the Theory of Numbers*, p. 71.

† We use, of course, the laws $(g \mid h)\cdot(h \mid g)=(-1)^{(g-1)/2\cdot(h-1)/2}$, $(2 \mid h)=(-1)^{(h^2-1)/8}$, for computing $(2g \mid h)$.

$$(17) \qquad (2g \mid h) = (2 \mid h)(g \mid h) = (-1)^{\alpha},$$

where

$$(18) \quad \begin{cases} \alpha = \dfrac{h^2-1}{8} + \dfrac{h-1}{2}\cdot\dfrac{g-1}{2} = \dfrac{h-1}{8}[h+1+2g-2] \\ \quad = \dfrac{4\tau^3-2}{2}\cdot\dfrac{4\tau^3+4\tau\epsilon}{4} = (2\tau^3-1)\tau(\tau^2+\epsilon). \end{cases}$$

But $2\tau^3-1$, τ, τ^2 are odd while $\epsilon = t^2$ is even. Hence α is odd, so that $(2g \mid h) = -1$, a contradiction.

For every even integer t the integer $1+t^4=\tau$ is positive and hence $-\tau \neq x^2$ for rational x. Also $t=2\xi$, $\tau = 1+16\xi^4$ is not identically the square of any polynomial in ξ. It follows that the equation $x^2=\tau$ is irreducible in $R(\xi)$ and, by the Hilbert Irreducibility Theorem, there exist infinitely many integer values of ξ for which $\tau \neq x^2$ for any rational x.

THEOREM 2. *There exist infinitely many cyclic fields of degree eight over R for which the quadratic form* (11) *is not a zero form.*

4. *On Function Fields.* In this section we shall obtain some quite simple theorems to be used later. Let F be any nonmodular field and $y, z, \cdots, w$ be independent indeterminates. Then $F(y, \cdots, w)$ is defined to be the *field* of all rational functions with coefficients in F of $y, \cdots, w$. Also $F[y, \cdots, w]$ is defined to be the *domain of integrity* of all polynomials with coefficients in F of $y, \cdots, w$. Suppose that f is in $F[y]$ and $f = f_1 \cdot f_2$, where the f_i are in $F[y, z]$. The degree of f in z is the sum of the degrees of f_1 and f_2 in z and is zero. Hence we have the following lemma.

LEMMA 1. *If f is in $J = F[y]$, and is a product of two quantities of $F[y, z]$, then these quantities are in J.*

Let next f be in J and let f_1 and f_2 be in $K[y]$, where $K = F(z)$. Then we may write

$$f_1 = \frac{g_1}{h_1}, \quad f_2 = \frac{g_2}{h_2},$$

where g_i is a polynomial in y with coefficients in $F[z]$, h_i is in $F[z]$ and has no factor in $F[z]$ which divides all the coefficients of g_i. But if $f = f_1 \cdot f_2$, then

$$f = \frac{g_1 g_2}{h_1 h_2}$$

is a *polynomial* in y with coefficients in F so that h_1 divides g_2 and h_2 divides g_1. Hence $g_1 = h_2 k_1$, $g_2 = h_1 k_2$, so that

$$f = f_1 f_2 = (k_1 h^{-1})(k_2 h), \qquad h = h_1/h_2.$$

By Lemma 1, k_1 and k_2 have coefficients in F.

LEMMA 2. *Let f be a polynomial in y with coefficients in F. Then, if y and z are indeterminates, f is reducible in $F(z)$ if and only if f is reducible in F.*

By induction the above result may be immediately extended to the case of an arbitrary number of variables y_i and indeterminates z_i. Also, an application of Lemma 2 to the Galois resolvent of any equation without multiple roots yields the following theorems.

THEOREM 3. *Let $f(x) = 0$ have coefficients in F and group G for F. Then, if z is an indeterminate, the group of $f(x) = 0$ for $F(z)$ is also G.*

THEOREM 4. *Let $W = F(x)$ be an algebraic field over F with G as its group of automorphisms. Then $W' = F(x, z)$ is an algebraic field over $F(z)$, with the same degree and group G as W, for any indeterminate z.*

5. *On a Quadratic Form over $R(z)$.* We let R be the field of all rational numbers, z be a parameter, $K = R(z)$, $J = R[z]$. Let $R(x)$ be a cyclic field of degree eight over R chosen so that (11) is not a zero form. By Theorem 4 the field $K(x)$ is cyclic of degree eight over K. Consider the form

$$(19)\quad P(\lambda_1, \cdots, \lambda_6) \equiv \lambda_1^2 \tau + (\lambda_2^2 - \lambda_3^2 \tau)\beta - \lambda_4^2 \gamma - (\lambda_5^2 - \lambda_6^2 \gamma)\delta,$$

in the variables $\lambda_1, \cdots, \lambda_6$ in K, where, since $\nu = -1$,

$$(20)\quad \begin{aligned} \gamma &= \beta_2^2 \tau - \beta_1^2, \ \beta = 2\beta_1 \gamma, \\ \delta &= 2\nu\tau(\beta_2 \epsilon - \beta_1)\beta_1 = -2\tau\beta_1(\beta_2 \epsilon - \beta_1). \end{aligned}$$

Write $\beta_1 = -z$, $\beta_2 = 2\tau z$ and, since β, δ, γ have the factor z^2, the form $P(\lambda_1, \cdots, \lambda_6)$ becomes

$$(21)\quad \begin{cases} Q(\mu_1, \cdots, \mu_6) \equiv \mu_1^2\tau - (4\tau^3 - 1)\mu_2^2 \\ \qquad\qquad - 2\tau(2\tau\epsilon + 1)[\mu_3^2 - (4\tau^3 - 1)\mu_4^2] \\ \qquad\qquad - 2_z(4\tau^3 - 1)(\mu_5^2\tau - \mu_6^2), \end{cases}$$

where $\mu_1=\lambda_1$, $\mu_2=\lambda_4 z$, $\mu_3=\lambda_5 z$, $\mu_4=\lambda_6 z^2$, $\mu_5=\lambda_2 z$, $\mu_6=\lambda_3 z$. Evidently (19) is a zero form if and only if (21) is a zero form. Also (21) vanishes for values not all zero of the μ_i in K if and only if it vanishes for μ_i not all zero in J.

Let us write (21) in the form $Q\equiv 0$ in z, that is,

$$(22)\quad \mu_1^2\tau - (4\tau^3 - 1)\mu_2^2 - 2\tau(2\tau\epsilon + 1)[\mu_3^2 - (4\tau^3 - 1)\mu_4^2] \equiv 2z(4\tau^3 - 1)(\mu_5^2\tau - \mu_6^2),$$

and designate the left member by S. Every term $\alpha_i\mu_i^2$ of S has rational α_i and *even* degree in z. Hence S has *odd* degree if and only if it has leading coefficient

$$x_1^2\tau - (4\tau^3 - 1)x_2^2 - 2\tau(2\tau\epsilon + 1)[x_3^2 - (4\tau^3 - 1)x_4^2]$$

formally equal to zero for $x_1, \cdots, x_4$ not all zero in R. This is contrary to our choice of $R(x)$. Hence S has even degree, $S\equiv 0$ only if $\mu_1 = \cdots = \mu_4 \equiv 0$. But $S\equiv T\equiv 2z(4\tau^3-1)(\mu_5^2\tau-\mu_6^2)$, so that T has even degree. Hence $\mu_5^2\tau-\mu_6^2$ has odd degree and thus has *formal* leading coefficient zero. But this coefficient is $x_5^2\tau-x_6^2$, which must be zero for x_5 and x_6 in R and not both zero unless $T\equiv 0$. But this is impossible by our choice of τ. Hence $T\equiv 0$, $S\equiv 0$, a contradiction. For we have proved now that S and T are both zero only when all the μ_i are zero.

THEOREM 5. *There exist cyclic fields of degree eight over K for which* (19) *does not vanish for* $\lambda_1, \cdots, \lambda_6$ *in K and not all zero.*

6. *A Type of Normal Division Algebra.* Let F be any nonmodular field. It is well known that every normal simple algebra of degree two over F is an algebra

$$(23)\qquad Q(\alpha, \beta) = (1, i, j, ij),$$

where $\alpha\neq 0$, $\beta\neq 0$ are in F. Let $Z = F(d)$ be a cyclic field of degree four over F,

$$(24)\qquad d^2 = \nu(u - \tau),\ u^2 = \tau = 1 + \epsilon^2,$$

where $\nu\neq 0$ is in F, ϵ in F. Define

$$D = (Z, S, \gamma) \tag{25}$$

to be the cyclic algebra

$$(d^i e^j),\ e^j a = a^{S^j} e^j, \qquad (i, j = 0, 1, 2, 3), \tag{26}$$

where if $a = a(d)$ is in Z, then

$$a^{S^i} \equiv a[\theta^i(d)],\ \theta(d) = d\left(\frac{u+1}{\epsilon}\right),$$
$$\theta^2(x) = -x,\ \theta^3(x) = -\theta(x),\ \theta^4(x) = x. \tag{27}$$

I have proved that if D has exponent $\rho < 4$, then

$$\gamma = \beta_2^2 \tau - \beta_1^2,$$

for β_1 and β_2 in F, and conversely. I have also shown* that when $\rho < 4$

$$D = Q(\alpha, \beta) \times Q(\gamma, \delta) \tag{28}$$

is a direct product of two generalized quaternion algebras, where

$$\alpha = \tau,\ \beta = 2\beta_1\gamma,\ \gamma = \beta_2^2\tau - \beta_1^2,\ \delta = 2\nu\tau\beta_1(\beta_2\epsilon - \beta_1). \tag{29}$$

I have also proved that if (28) is satisfied, then D is a division algebra if and only if (19) is not a zero form. Hence, if $F = R(z)$, we have already proved that D is a division algebra of exponent two. We therefore have the following theorem.

THEOREM 6. *There exist cyclic fields of degree eight over $K = R(z)$ with corresponding sub-fields Z of degree four over K such that K contains quantities γ in F for which $D = (Z, S, \gamma)$ is a division algebra of exponent two.*

The above theorem provides the first proof† of the existence of a non-primary normal division algebra of degree four over a function field $R(z)$, the simplest previous example being that of an algebra over $R(y, z)$, where y and z are two independent indeterminates.

7. *Primary Algebras of Degree Eight.* Let A be a normal division algebra of degree p^e over F, p a prime. I have proved‡ that

$$A^p = M_0^{p-1} \times M_p \times A_p = M \times A_p,$$

* This Bulletin, vol. 37 (1931), pp. 301–312, Theorems 3, 4.

† It is not difficult, however, to give a simpler proof for the case $\nu > 0$.

‡ See Theorem 7 of my paper *Algebras of degree 2^e*, etc., Annals of Mathematics, vol. 33 (1932), pp. 311–318.

where $M = M_0{}^{p-1} \times M_p$, M_0 is a total matric algebra of degree p^e, M_p is a total matric algebra of degree $p^f > 1$, A_p is a normal division algebra of degree $p^{e-f} \geqq 1$. Also the exponent ρ of A has the value $\rho = p^r$, where $r \leqq e$. Since $\rho = p\rho_1$, we have $\rho_1 = p^{r-1}$, $A^p = A^{p\rho_1} = M^{\rho_1} \times (A_p)^{\rho_1}$ is a total matric algebra. Hence $A_p{}^{\rho_1}$ is a total matric algebra. Conversely, if ρ_0 is the exponent of A_p, then $A^{p\rho_0} = M^{\rho_0} \times A_p{}^{\rho_0}$ is a total matric algebra. We thus have $\rho \leqq p\rho_0$, $p\rho_1 \leqq p\rho_0$, $\rho = p\rho_1 = p\rho_0$, and we have the following fact.

LEMMA 3. *The exponent ρ of A is $p\rho_0$, where ρ_0 is the exponent of A_p.*

Let $p = 2$, $e = 3$, so that $A^2 = (M_0 \times M_2) \times A_2$. If $A = B \times C$ is non-primary, where B may be taken to have degree four, C degree two, then $A^2 = B^2 \times C^2 = (L \times L_2 \times B_2) \times (K \times K_2 \times C_2)$. But K_2 has degree two, C_2 has degree unity, C^2 is a total matric algebra. Hence $A^2 = M_0 \times Q$, where M_0 is a total matric algebra and Q is a normal simple algebra of degree two.

LEMMA 4. *Let A be a non-primary normal division algebra of degree eight. Then $A^2 = M_0 \times Q$, where M_0 is a total matric algebra and Q is a normal simple algebra of degree two.*

We now let A be any normal division algebra of degree eight. Then $A^2 = M \times A_2$, where M is a total matric algebra and A_2 is a normal division algebra. If A_2 has degree unity or two, then A has exponent two or four by Lemma 3 and may or may not be primary. But, by Lemma 3, if A_2 has degree four then A is primary and has exponent $2s$ where s is the exponent of A_2.

THEOREM 7. *Let A be a normal division algebra of degree eight over F so that*

$$A^2 = M \times A_2,$$

where M is a total matric algebra and A_2 is a normal division algebra of degree $2^t \leqq 4$. Then A has exponent two or four according as $t = 0, 1$ and it is not yet known whether A may be primary. But if $t = 2$, then A is primary and has exponent $2s$, where s is the exponent of A_2.

By Theorems 6, 7 we have the following result.

THEOREM 8. *There exist primary normal division algebras of degree eight and exponent four.*

THE UNIVERSITY OF CHICAGO