ON THE WEDDERBURN NORM CONDITION FOR CYCLIC ALGEBRAS*

BY A. A. ALBERT

1. *Introduction.* Let F be any non-modular field, i a root of a cyclic equation in F of degree n and with roots $\theta^r(i)$. Suppose that A is a cyclic algebra with basis

$$i^r y^s, \qquad (r, s = 0, 1, \cdots, n-1),$$

where

$$y^r i = \theta^r(i) y^r, \; y^n = \gamma \text{ in } F.$$

J. H. M. Wedderburn has proved† that A is a division algebra if γ^r is not the norm, $N(a)$, of any a in $F(i)$ for every positive integer r less than n. It has never been shown, however, that this condition is a necessary one; but the problem of finding complete necessary and sufficient conditions has been reduced to the case n a power of a single prime. ‡

In the present paper cyclic algebras of order sixteen with the corresponding cyclic quartic in its canonical form §

$$\phi(\omega) \equiv \omega^4 + 2\nu(1 + \Delta^2)\omega^2 + \nu^2\Delta^2(1 + \Delta^2) = 0$$

such that ν and Δ are in F, and $\tau = 1 + \Delta^2$ is not the square of any quantity of F, are considered. The norm $N(a)$ of a polynomial in i is a rather complicated quartic form in four variables, yet we can secure the result that $\gamma^2 = N(a)$ if and only if $\gamma = \alpha^2 - \beta^2\tau$ for α and β in F, a curious property of cyclic quartic fields. When the above equation is satisfied the algebra A is expressible as a direct product of two generalized quaternion algebras. Necessary and sufficient conditions are secured that our algebras A of order sixteen be division algebras, and it is shown that for the particularly interesting case where F is *the field of all rational numbers* the Wedderburn condition is *necessary as well as sufficient.*

* Presented to the Society, December 30, 1930.

† Transactions of this Society, vol. 15 (1914), pp. 162–166.

‡ See a paper by the author, *On direct products, cyclic algebras, and pure Riemann matrices,* to appear in the Transactions of this Society, January, 1931.

§ See R. Garver, *Quartic equations with certain groups,* Annals of Mathematics, vol. 29 (1928), pp. 47–51.

2. *The Basic Theorem.* Let $F(x)$ be a cyclic quartic field. Then it is known (loc. cit.) that $F(x)=F(i)$, where i satisfies the equation

$$(1) \qquad \phi(\omega) \equiv \omega^4 + 2\nu\tau\omega^2 + \nu^2\Delta^2\tau = 0,$$

with $\tau = 1+\Delta^2$ not the square of any quantity of F and

$$(2) \qquad \nu \neq 0, \ \tau, \ \Delta \neq 0$$

all in F. Moreover if we define u by the equation

$$(3) \qquad i^2 = \nu(u-\tau),$$

then

$$(4) \qquad u^2 = \tau, \qquad \theta(i) = \frac{i}{\Delta}(u+1),$$

is the polynomial whose iteratives $i=\theta^0(i)=\theta^4(i), \theta(i), \theta^2(i)=-i$, $\theta^3(i)=\theta(-i)=-\theta(i)$ give the four roots in $F(i)$ of $\phi(\omega)=0$. Every quantity of $F(i)$ is expressible in the form

$$(5) \qquad a = a_1 + a_2 i, \qquad (a_1 \text{ and } a_2 \text{ in } F(u)),$$

and $a=0$ if and only if $a_1=a_2=0$. A quantity

$$(6) \qquad a_1 = \alpha_1 + \alpha_2 u, \qquad (\alpha_1 \text{ and } \alpha_2 \text{ in } F),$$

is zero if and only if $\alpha_1=\alpha_2=0$; and similarly

$$(7) \qquad \alpha_1^2 - \alpha_2^2\tau$$

vanishes if and only if $\alpha_1=\alpha_2=0$ by our restriction on τ.

We shall use repeatedly the following simple lemma.

LEMMA 1. *Every product of a finite number of scalars of the forms*

$$(8) \qquad \lambda^2 - \mu^2\tau,$$

$$(8') \qquad (\lambda^2 - \mu^2\tau)^{-1}, \qquad \lambda^2 - \mu^2\tau \neq 0,$$

with λ and μ in F, is expressible in the form (8) *for λ and μ in F.*

The truth of this is evident since

$$(\lambda_1 + \mu_1 u)(\lambda_2 + \mu_2 u) = (\lambda_1\mu_1 + \lambda_2\mu_2\tau) + (\lambda_1\mu_2 + \lambda_2\mu_1)u,$$

and hence

(9) $(\lambda_1^2 - \mu_1^2\tau)(\lambda_2^2 - \mu_2^2\tau) = (\lambda_1\mu_1 + \lambda_2\mu_2\tau)^2 - (\lambda_1\mu_2 + \lambda_2\mu_1)^2\tau;$

while if $\epsilon = \lambda^2 - \mu^2\tau \neq 0$, then

$$\epsilon^{-1} = \epsilon^{-2}\epsilon = \epsilon^{-2}(\lambda^2 - \mu^2\tau) = (\lambda\epsilon^{-1})^2 - (\mu\epsilon^{-1})^2\tau. \tag{10}$$

Let us now assume that $\gamma \neq 0$ is a scalar in F, such that $\gamma^2 = N(a)$, where a is in the cyclic field $F(i)$. We may write $a^{(r)} = a[\theta^r(i)]$, $(r=0, 1, \cdots)$, whence $a'' = a(-i)$. Then $u' = -u$; and if a_1 is in $F(u)$ so that a_1 has the form $a_1 = \alpha_1 + \alpha_2 u$, we have $a_1 = a_1''$ and

$$N(a_1) = a_1\, a_1'\, a_1''\, a_1''' = (a_1\, a_1')^2 = (\alpha_1^2 - \alpha_2^2\tau)^2. \tag{11}$$

Let us write $\gamma^2 = N(a)$, where

$$a = a_2 + a_3 i, \qquad (a_2 \text{ and } a_3 \text{ in } F(u)). \tag{12}$$

We shall first consider the case $a_3 = 0$. Then $a = a_2 = \alpha_3 + \alpha_4 u$, and

$$\gamma^2 = (\alpha_3^2 - \alpha_4^2\tau)^2. \tag{13}$$

This equation in a field F implies that

$$\gamma = \pm (\alpha_3^2 - \alpha_4^2\tau). \tag{14}$$

If $\gamma = \alpha_3^2 - \alpha_4^2\tau$, we have expressed γ in the form

$$\gamma = \alpha^2 - \beta^2\tau \tag{15}$$

with α and β in F, the result desired. Since $\tau = 1 + \Delta^2$, we have

$$-1 = \Delta^2 - \tau. \tag{16}$$

Hence if $\gamma = -(\alpha_3^2 - \alpha_4^2\tau)$, then $\gamma = (\Delta^2 - \tau)\ (\alpha_3^2 - \alpha_4^2\tau)$; and, by Lemma 1, γ has again the desired form (15).

Next let $a_3 \neq 0$. Then, if $a_3 = \lambda_3 + \lambda_4 u$, $a_1 = a_3^{-1}a_2$, we have

$$N(a) = N[a_3(a_1 + i)] = (\lambda_3^2 - \lambda_4^2\tau)^2 N(a_1 + i). \tag{17}$$

Let $\delta = \gamma(\lambda_3^2 - \lambda_4^2\tau)^{-1}$. Then

$$\delta^2 = \gamma^2(\lambda_3^2 - \lambda_4^2\tau)^{-2} = N(a_1 + i). \tag{18}$$

But if $b = a_1 + i$, then $\delta^2 = (bb'')\ (bb'')'$ so that if $w = \delta[(bb'')']^{-1}$, then $\delta = \delta' = w'bb''$. It follows that $\delta^2 = w\,w'N(b) = w\,w'\delta^2$. Hence

$$ww' = 1, \quad w = bb''\delta^{-1}, \quad bb'' = \delta w, \tag{19}$$

where $w = bb''\delta^{-1} = \xi_1 + \xi_2 u$ is in $F(u)$. If $a_1 = \alpha_1 + \alpha_2 u$, α_1 and α_2 in F, we have, by (3),

$$\begin{aligned} bb'' &= a_1^2 - i^2 = \alpha_1^2 + \alpha_2^2\tau + 2\alpha_1\alpha_2 u - \nu(u - \tau) \\ &= (\alpha_1^2 + \alpha_2^2\tau + \nu\tau) + (2\alpha_1\alpha_2 - \nu)u. \end{aligned}$$

From the linear independence of 1 and u this implies

$$\alpha_1^2 + \alpha_2^2\tau + \nu\tau = \delta\xi_1, \quad 2\alpha_1\alpha_2 - \nu = \delta\xi_2. \tag{20}$$

We obtain $2\alpha_1\alpha_2\tau - \nu\tau = \delta\xi_2\tau$, and by addition

$$\alpha_1^2 + 2\alpha_1\alpha_2\tau + \alpha_2^2\tau = \delta(\xi_1 + \xi_2\tau). \tag{21}$$

Since $1 - \tau = -\Delta^2$, if we complete the square in (21), it becomes

$$\begin{aligned} (\alpha_1 + \alpha_2\tau)^2 + \alpha_2^2(\tau - \tau^2) &= (\alpha_1 + \alpha_2\tau)^2 - (\alpha_2\Delta)^2\tau \\ &= \delta(\xi_1 + \xi_2\tau). \end{aligned} \tag{22}$$

Consider now the equation $ww' = 1$, or

$$\xi_1^2 - \xi_2^2\tau = 1, \quad \xi_2^2\tau = (\xi_1 + 1)(\xi_1 - 1). \tag{23}$$

Let $\xi_1 - 1 = 2\pi$, $\xi_1 + 1 = 2\sigma$. Then

$$4\sigma\pi = \xi_2^2\tau. \tag{24}$$

Suppose first that $\xi_1 + 1 = 0$ so that $\sigma = 0$ and $\xi_2 = 0$. Then $\xi_1 + \xi_2\tau = \xi_1 = -1 = \Delta_1^2 - \tau$. Hence in this case we have

$$\xi_1 + \xi_2\tau = \lambda_5^2 - \lambda_6^2\tau, \qquad (\lambda_5 \text{ and } \lambda_6 \text{ in } F). \tag{25}$$

Next let $\xi_1 + 1 \neq 0$, so that $\sigma \neq 0$; and let us define ϵ by the equation

$$2\sigma\epsilon = \xi_2. \tag{26}$$

Then (24) gives $4\sigma\pi = 4\sigma^2\epsilon^2\tau$, whence

$$\pi = \epsilon^2\sigma\tau. \tag{27}$$

But $2(\sigma - \pi) = \xi_1 + 1 - (\xi_1 - 1) = 2$, whence

$$1 = \sigma - \pi = \sigma - \epsilon^2\sigma\tau = \sigma(1 - \epsilon^2\tau). \tag{28}$$

Since $1 - \epsilon^2\tau \neq 0$, using Lemma 1, we have

$$\sigma = \beta_1^2 - \beta_2^2\tau, \qquad (\beta_1 \text{ and } \beta_2 \text{ in } F), \tag{29}$$

so that $\xi_1 = \pi + \sigma = \sigma(1 + \epsilon^2\tau)$, and

$$\begin{aligned} \xi_1 + \xi_2\tau &= \sigma[(1 + \epsilon^2\tau) + 2\epsilon\tau] = \sigma[(1 + \epsilon\tau)^2 - (\epsilon\Delta)^2\tau] \\ &= (\beta_1^2 - \beta_2^2\tau)[(1 + \epsilon\tau)^2 - (\epsilon\Delta)^2\tau] = \lambda_5^2 - \lambda_6^2\tau, \end{aligned} \tag{30}$$

for λ_5 and λ_6 in F, by Lemma 1. Hence *in all cases* (25) *is satisfied.*

If we now put $\beta_3 = \alpha_1 + \tau\alpha_2$, $\beta_4 = \Delta\alpha_2$, (22) becomes

$$\delta(\lambda_5^2 - \lambda_6^2\tau) = \beta_3^2 - \beta_4^2\tau. \tag{31}$$

Suppose first that $\beta_3^2 - \beta_4^2\tau = 0$, whence $\beta_3 = \beta_4 = 0$. Then our definitions above of β_3 and β_4 evidently give $\alpha_1 = \alpha_2 = 0$, and (20) take the form $\nu\tau = \delta\xi_1$, $-\nu = \delta\xi_2$. Squaring each side of both these, we may write $\nu^2\tau^2 = \delta^2\xi_1^2$, $\nu^2\tau = \delta^2\xi_2^2\tau$, whence, by subtraction and the use of the relations $1 = \xi_1^2 - \xi_2^2\tau$, $\tau = 1 + \Delta^2$, we obtain

$$\nu^2\tau^2 - \nu^2\tau = \tau(\nu^2\Delta^2) = \delta^2(\xi_1^2 - \xi_2^2\tau) = \delta^2. \tag{32}$$

Then $\tau = (\delta\nu^{-1}\Delta^{-1})^2$, which is a contradiction since τ is not the square of any quantity of F. Hence $\beta_3^2 - \beta_4^2\tau \neq 0$. Thus $\lambda_5^2 - \lambda_6^2\tau \neq 0$ has an inverse in F which has the form $\lambda_7^2 - \lambda_8^2\tau$ by Lemma 1, and we may write

$$\begin{aligned} \gamma &= \delta(\lambda_3^2 - \lambda_4^2\tau) = (\lambda_3^2 - \lambda_4^2\tau)(\lambda_7^2 - \lambda_8^2\tau)(\beta_3^2 - \beta_4^2\tau) \\ &= (\alpha^2 - \beta^2\tau), \end{aligned} \tag{33}$$

again using Lemma 1. We have proved in all cases the first part of the following statement.

THEOREM 1. *A scalar* $\gamma \neq 0$ *in* F *has the property*

$$\gamma^2 = N(a) \tag{34}$$

for a *in* $F(i)$, *a cyclic quartic field, if and only if*

$$\gamma = \alpha^2 - \beta^2\tau, \qquad (\alpha \text{ and } \beta \text{ in } F), \tag{35}$$

where $F(u)$ *is the quadratic subfield of* $F(i)$ *defined by* (1) *and* (3), *and* $u^2 = \tau$.

Moreover, when $\gamma = \alpha^2 - \beta^2\tau$, we have $N(\alpha + \beta\mu) = (\alpha^2 - \beta^2\tau)^2 = \gamma^2$, which is the converse in the preceding theorem.

Suppose now that $\gamma=\alpha^2-\beta^2\tau$ and $\gamma^2=N(b)$. If $a=\alpha+\beta u$, so that $\gamma=aa'$, we have $\gamma^2=N(a)=N(b)$. It follows that $b\neq 0$ and $N(ab^{-1})=1$, $a=wb$, where $N(w)=1$. Thus we have the following corollary.

COROLLARY 1. *Let $\gamma=aa'$, where a is in $F(u)$. Then $\gamma^2=N(b)$ for b in $F(i)$ if and only if b is the product of a by a unit of $F(i)$.*

Since $-1=dd'$, where d is given in (16) and is in $F(u)$, we have also the following result.

COROLLARY 2. *The scalar $\gamma^2=N(b)$ for b in $F(i)$ if and only if $-\gamma=ee'$ for e in $F(u)$.*

3. *The Wedderburn Norm Condition.* For a cyclic algebra of order sixteen Wedderburn's condition becomes

$$\gamma^r \neq N(a), \qquad (r = 1, 2, 3).$$

It is easily shown* that if γ or γ^3 were a norm then A would not be a division algebra. Hence the only possible case is $\gamma^2=N(a)$. By Theorem 1 this implies that $\gamma=\alpha^2-\beta^2\tau$. Consider the sub-algebra

$$\sum = (y^r, uy^r), \qquad (r = 0, 1, 2, 3),$$

an algebra of order eight with $yu=-uy$, $y^4=\gamma$, $u^2=\tau$ in F, $y^2u=uy^2$. We shall write

$$s = (e + y^2)y, \quad t = i(a_1 + y^2), \quad a_1 = \beta_1 q - \beta_2 u, \tag{36}$$

where we have used Corollary 2 to write

$$-\gamma = ee', \quad e = \beta_1 + \beta_2 u, \qquad (\beta_1 \text{ and } \beta_2 \text{ in } F), \tag{37}$$

and have

$$yi = \theta(i)y, \quad \theta(i) = qi, \quad q = \Delta^{-1}(u + 1), \quad qq' = -1, \tag{38}$$

since $\Delta^2 qq'=(u+1)(-u+1)=-(1+\Delta^2)+1=-\Delta^2$. We shall compute

$$\begin{aligned} st &= [(e + y^2)y][i(a_1 + y^2)] = (e + y^2)qi(a_1' + y^2)y \\ &= iq(e - y^2)(a_1' + y^2)y = iq[(ea' - \gamma) + (e - a_1')qy^2]y, \end{aligned}$$

since $ya=a'y$ for every a of $F(i)$ and $y^2 i=-iy^2$. Now

* See the author's paper *On direct products, etc.*, loc. cit.

$$q(ea' - \gamma) = q(ea' + ee') = eq(a_1' + e')$$
$$= eq[\beta_1 q' + \beta_2 u + \beta_1 - \beta_2 u] = \beta_1 e[qq' + q] = \beta_1 e(q - 1).$$

Also

$$q(e - a_1') = q[(\beta_1 + \beta_2 u) - (\beta_1 q' + \beta_2 u)] = \beta_1(q+1).$$

It follows that

$$st = \beta_1 i[e(q - 1) + (q + 1)y^2]y. \tag{39}$$

We have similarly

$$ts = [i(a_1 + y^2)][(e + y^2)y] = i[(a_1 e + \gamma) + (a_1 + e)y^2]y,$$
$$a_1 e + \gamma = a_1 e - ee' = e[(\beta_1 q - \beta_2 u) - (\beta_1 - \beta_2 u)] = \beta_1 e(q - 1),$$

while $a_1 + e = \beta_1 q - \beta_2 u + \beta_1 + \beta_2 u = \beta_1(q+1)$. We then obtain immediately from (39)

$$st = ts. \tag{40}$$

Consider the linear sets

$$B = (1, u, s, us), \qquad C = (1, y^2, t, y^2 t), \tag{41}$$

over F. We have the relations

$$su = - us, ty^2 = - y^2 t; uy^2 = y^2 u, ut = tu, sy^2 = y^2 s, st = ts, \tag{42}$$

so that every quantity of B is commutative with every quantity of C. We now show that

$$s^2 = (e + y^2)(e' + y^2)y^2 = [(ee' + \gamma) + (e + e')y^2]y^2 = 2\beta_1\gamma, \tag{43}$$

since $e + e' = 2\beta_1$, $ee' = -\gamma$. Also

$$t^2 = i^2(a_1 - y^2)(a_1 + y^2) = i^2(a_1^2 - \gamma)$$
$$= i^2[\beta_1^2 q^2 - 2\beta_1\beta_2 qu + \beta_2^2\tau + \beta_1^2 - \beta_2^2\tau]$$
$$= i^2\beta_1^2(q^2 + 1) - 2\beta_1\beta_2 qui^2,$$

since $\gamma = -ee'$. We have also $i^2 = \nu(u - \tau)$, so that

$$i^2 q = \nu\Delta^{-1}(u - \tau)\ (u + 1) = \Delta^{-1}\nu(\tau - \tau + u - u\tau)$$
$$= \Delta^{-1}\nu u(1 - \tau) = \Delta^{-1}\nu u(-\Delta^2) = -\Delta\nu u.$$

Moreover, we know that

$$i^2(q^2 + 1) = i^2[\Delta^{-2}(\tau + 2u + 1) + 1] = \Delta^{-2} i^2[2u + \tau + (1 + \Delta^2)]$$
$$= 2\nu\Delta^{-2}(u - \tau)(u + \tau) = 2\nu\Delta^{-2}(\tau - \tau^2) = - 2\nu\tau.$$

Hence

$$t^2 = 2\nu\tau\beta_1(\beta_2\Delta - \beta_1). \tag{44}$$

We shall assume at this point that

$$\beta_1 \neq 0, \ \beta_2\Delta - \beta_1 \neq 0, \tag{45}$$

for otherwise either $s^2=0$ or $t^2=0$, and A is evidently not a division algebra since from their form neither s nor t is zero. As a consequence, $a_1^2 - \gamma \neq 0$ has an inverse in $F(u)$ and $e^2 - \gamma \neq 0$ has an inverse in $F(u)$ since $t^2 = i^2(a_1^2 - \gamma) \neq 0$, while if

$$e^2 - \gamma = e^2 - ee' = 0,$$

then $e(e-e') = 2\beta_1 e = 0$, contrary to the hypothesis that $\beta_1 \neq 0$, so that $e \neq 0$ has an inverse in $F(u)$. The sets B and C are generalized quaternion algebras over F, since in B

$$u^2 = \tau, \ s^2 = 2\beta_1\gamma, \ su = -us,$$

while in C

$$(y^2)^2 = \gamma, \ t^2 = 2\nu\tau\beta_1(\beta_2\Delta - \beta_1), \ y^2 t = -ty^2,$$

and evidently from the form of s and t the quantities $1, u, s, us$ are linearly independent in F, and the quantities $1, y^2, t, y^2 t$ are linearly independent in F, when $i^\alpha y^\beta$ $(\alpha, \beta = 0, 1, 2, 3)$ form a basis of A. The linear set $BC = CB$ of all sums of all products of quantities of B and quantities of C is an algebra, since a product

$$\left(\sum_\lambda b_{1\lambda}c_{1\lambda}\right)\left(\sum_\mu b_{2\mu}c_{2\mu}\right) = \sum_{\lambda,\mu}(b_{1\lambda}b_{2\mu})(c_{1\lambda}c_{2\mu})$$

is in BC because for every λ and μ the quantities $b_{1\lambda}b_{2\mu}$ are in B and $C_{1\lambda}C_{2\mu}$ are in C. Now BC contains $F(u)$ and hence $(\gamma - a_1^2)^{-1}$, $(\gamma - e^2)^{-1}$. Since BC contains s, t, e, a_1, y^2, and is an algebra, it contains

$$\begin{aligned}(\gamma - a_1^2)^{-1}(ty^2 - a_1 t) &= (\gamma - a_1^2)^{-1} i(a_1 y^2 + \gamma - a_1^2 - a_1 y^2) \\ &= (\gamma - a_1^2)^{-1}(\gamma - a_1^2) i = i,\end{aligned}$$

and

$$\begin{aligned}(\gamma - e^2)^{-1}(y^2 s - es) &= (\gamma - e^2)^{-1}[(y^2 e + \gamma) - ey^2 - e^2]y \\ &= (\gamma - e^2)^{-1}(\gamma - e^2)y = y.\end{aligned}$$

But then BC contains the basis of A and has order sixteen. It follows that A is the *direct product* of B and C.

THEOREM 2. *Let $\gamma^2=N(a)$ for some a of $F(i)$ so that $-\gamma=ee'$, where $e=\beta_1+\beta_2 u$ and β_1 and β_2 are in F. Let $\beta_1\neq 0$, $\beta_2\Delta\neq\beta_1$, a set of necessary conditions that A be a division algebra. Then the cyclic algebra A is the direct product of two generalized quaternion algebras $B=(1, u, s, us)$, $C=(1, j, t, jt)$, with $y^2=j$, $su=-us$, $tj=-jt$, and*

$$(46)\quad u^2=\tau,\quad s^2=2\beta_1\gamma=\sigma,\quad j^2=\gamma,\quad t^2=\rho=2\nu\beta_1\tau(\beta_2\Delta-\beta_1).$$

Consider now the direct product of *any two generalized quaternion algebras B and C*. It is known that d in B has the property that d^2 is in F if and only if

$$(47)\quad d=\lambda_1 u+\lambda_2 s+\lambda_3 us,\quad d^2=Q_1=\lambda_1^2\tau+\lambda_2^2\sigma-\lambda_3^2\sigma\tau,$$

with λ_1, λ_2 and λ_3 in F. Similarly if f is in C then f^2 is in F if and only if

$$(48)\quad f=\lambda_4 j+\lambda_5 t+\lambda_6 jt,\quad f^2=Q_2=\lambda_4^2\gamma+\lambda_5^2\rho-\lambda_6^2\gamma\rho$$

for λ_4, λ_5, and λ_6 in F. *Suppose first that $Q\equiv Q_1-Q_2$ is a null form*, that is, that we can make $Q=0$ for values of $\lambda_1, \cdots, \lambda_6$ in F not all zero. Define d by (47) and f by (48) for the particular λ_i we have used to make Q vanish. Since A is the *direct* product of B and C, the quantities $d-f$ and $d+f$ are both not zero when the λ_i are not all zero. But $(d-f)(d+f)=d^2-f^2=Q_1-Q_2=Q=0$. Hence in A a product of two non-zero quantities is zero and A is not a division algebra.

Conversely, let Q not be a null form. Then, in particular, Q_1 and Q_2 are not null forms and B and C are known* to be division algebras. The algebra Γ whose quantities have the form $X=x_1+x_2u$, where x_1 and x_2 are in C, has a division sub-algebra C and the property that if we define $x'=x$ for every x of C, then $u^2=\tau$ in C, $x''=(x')'=u^2xu^{-2}=x$ for every x of C. But then Γ is known† to be a division algebra if and only if $\tau\neq x'x=x^2$ for any x of C. But τ is in F and if $\tau=x^2$ then, since x is an f of (48), and u is a d of (47), we have $Q=0$ for $\lambda_1=1$, a contradiction of our hypothesis that Q was not a null form.

Define $X'=x_1-x_2u$, for every X of Γ, and we will have $X'=sXs^{-1}$, $X''=s^2Xs^{-2}=X$, $s^2=\sigma$ in F. Then it is known

---

* See L. E. Dickson, *Algebren und ihre Zahlentheorie*, p. 47, for the condition $\sigma\neq\xi_1^2-\xi_2^2\tau$, equivalent to the condition we have stated.

† A theorem of L. E. Dickson, ibid., pp. 63–64.

(Dickson, loc. cit.) that A, whose quantities have the form $X+Ys$, is a division algebra when Γ is one if and only if

$$s^2=X'X \text{ for any } X \text{ of } \Gamma.$$

But if $s^2=X'X$, $(x_1-x_2u)(x_1+x_2u)=x_1^2-x_2^2\tau+(x_1x_2-x_2x_1)u=\sigma$ we have

$$\sigma = x_1^2 - x_2^2\tau, \quad x_1x_2 = x_2x_1. \tag{49}$$

First let x_1 and x_2 be in F. Then Q is a null form when we take $\lambda_1=\sigma$, $\lambda_2=\tau x_2$, $\lambda_3=x_1$, $\lambda_4=\lambda_5=\lambda_6=0$, since $0=\sigma\tau(\sigma+x_2^2\tau-x_1^2)$ $=\sigma^2\tau+(\tau x_2)^2\sigma-x_1^2\sigma\tau$, a contradiction. Next let x_1 be in F but x_2 not in F. Then $x_2^2\tau=x_1^2-\sigma$ is in F and $x_2\tau$ is an f of (48) while $(x_2\tau)^2=Q_2=x_1^2\tau-\sigma\tau$ so that Q is a null form for $Q_2=(x_2\tau)^2$, $\lambda_1=x_1$, $\lambda_2=0$, $\lambda_3=1$. The only remaining case is where x_1 is not in F. If x_1^2 were in F so that x_1 would be an f of (48), then x_1x_2 $=x_2x_1$ implies that $x_2=\xi+\eta x_1$, ξ and η in F, since in a generalized quaternion division algebra the only quantities commutative with a non-scalar quantity x are scalar coefficient polynomials in x. But x_2^2 is in F so that $\eta=0$ or $\xi=0$. When $\eta=0$, then $x_1^2=\xi^2\tau+\sigma$ and $Q_2=Q_1=\xi^2\tau+1^2\sigma-O\sigma\tau$, a contradiction of our hypothesis. When $\xi=0$ then $x_2=\eta x_1$ and $x_1^2-x_2^2\tau$ $=x_1^2(1-\eta^2\tau)$. But by Lemma 1 we have $(1-\eta^2\tau)^{-1}=\delta_1^2-\delta_2^2\tau$ and $x_1^2=Q_2=\sigma\delta_1^2-\sigma\tau\delta_2^2=Q_1$, a contradiction. We have finally come to the case where neither x_1 nor its square is in F. We then have, where f is given by (47) and $f^2=Q_2$, that $x_1=\lambda_7+f$ with $\lambda_7\neq 0$ in F. As before the relation $x_1x_2=x_2x_1$ implies that x_2 is a polynomial in x_1. But now we may write $x_2=\xi+\eta f$. Now

$$x_1^2 - x_2^2\tau = \lambda_7^2 + 2\lambda_7 f + Q_2 - (\xi^2 + 2\xi\eta f + \eta^2 Q_2)\tau = \sigma.$$

It follows that $2\lambda_7-2\xi\eta\tau=0$, so that $\lambda_7=\xi\eta\tau$ and

$$\sigma = \xi^2\eta^2\tau^2 - \xi^2\tau + Q_2(1-\eta^2\tau) = (Q_2-\xi^2\tau)(1-\eta^2\tau).$$

The quantity $(1-\eta^2\tau)\neq 0$ has an inverse $\delta_1^2-\delta_2^2\tau$ with δ_1 and δ_2 in F by Lemma 1, and $Q_2-\xi^2\tau=\sigma(\delta_1^2-\delta_2^2\tau)$, so that we have $Q_2=\xi^2\tau+\sigma\delta_1^2-\sigma\tau\delta_2^2=Q_1$. We have again shown that if A were not a division algebra, then Q would be a null form, a contradiction of our hypothesis. Hence A is a division algebra and we have proved the following theorem

THEOREM 3. *A direct product $A=B\times C$ of two generalized quaternion algebras $B=(1, u, s, us)$, $C=(1, j, t, jt)$ with $u^2=\tau$, $s^2=\sigma$, $su=-us$, $j^2=\gamma$, $t^2=\rho$, $tj=-jt$, is a division algebra if and only if the quadratic form*

$$Q = (\lambda_1^2\tau + \lambda_2^2\sigma - \lambda_3^2\sigma\tau) - (\lambda_4^2\gamma + \lambda_5^2\rho - \lambda_6^2\gamma\rho) \tag{50}$$

in the variables $\lambda_1, \lambda_2, \cdots, \lambda_6$ in F, is not a null form.

We may now apply Theorem 3 and our previous results to obtain complete necessary and sufficient conditions that a cyclic algebra be a division algebra. We first assume that $\gamma^2=N(a)$ for some a in $F(i)$. If $\gamma=0$, then $-\gamma=\beta_1^2-\beta_2^2\tau$ with $\beta_1=\beta_2=0$, and the form Q may be defined. If $\gamma\neq 0$, then by Corollary 2 we can again define the form Q with

$$\sigma=2\beta_1\gamma, \rho=2\nu\tau\beta_1(\beta_2\Delta-\beta_1).$$

Suppose first that Q is a null form. If $\gamma=0$, then $y^4=0$ while y is not zero and A is not a division algebra. If $\gamma\neq 0$ but $\beta_1=0$ or $\beta_2\Delta-\beta_1=0$, then again, as we have seen, A is not a division algebra. The only other case is where Theorem 2 can be applied and, by Theorem 3, A is again not a division algebra. Conversely let Q be not a null form. Then obviously from our definition of Q as above and the fact that we have the coefficients of Q all not zero in a non-null form, $\gamma\neq 0$, $\beta_2\Delta\neq\beta_1$, $\beta_1\neq 0$, and again A is the direct product of B and C; we may again apply Theorem 3, and A is a division algebra.

THEOREM 4. *Let A be a cyclic algebra with basis $i^\lambda y^\mu$, $(\lambda, \mu=0, 1, 2, 3)$, where i is a root of the cyclic quartic*

$$\phi(\omega) \equiv \omega^4 + 2\nu\tau\omega^2 + \nu^2\Delta^2\tau = 0$$

with $\tau=1+\Delta^2$, $\nu\neq 0$, $\Delta\neq 0$ in F, and τ not the square of any element in F. Also

$$\theta(i) = qi, q\Delta = 1 + u, i^2 = \nu(u-\tau), yi = \theta(i)y, y^4 = \gamma \text{ in } F.$$

Suppose that γ^2 is the norm of a quantity of $F(i)$ so that we have $-\gamma=\beta_1^2-\beta_2^2\tau$ with β_1 and β_2 in F. Then A is a division algebra if and only if the form

$$Q = \lambda_1^2\tau + \lambda_2^2\sigma - \lambda_3^2\sigma\tau - \lambda_4^2\gamma - \lambda_5^2\rho + \lambda_6^2\gamma\rho$$

with $\sigma=2\beta_1\gamma$, $\rho=2\beta_1\nu\tau(\beta_2\Delta-\beta_1)$ does not vanish for any $\lambda_1, \cdots, \lambda_6$ not all zero and in F.

The only other case is $\gamma^2 \neq N(a)$. Then obviously $\gamma \neq N(a)$ since otherwise $\gamma^2 = N(a^2)$, a contradiction. If $\gamma^3 = N(a)$, then either $\gamma = 0$, whence $\gamma^2 = N(0)$, a contradiction, or else $\gamma \neq 0$, $\gamma^6 = \gamma^2\gamma^4 = N(a^2)$, $\gamma^2 = N(a\gamma^{-1})$, again a contradiction. Hence the condition $\gamma^2 \neq N(a)$ is equivalent to the Wedderburn norm condition. We have also shown the former condition equivalent to the condition $\gamma \neq -ee'$ for any e of $F(u)$. We thus have proved the following theorem

THEOREM 5. *Let all the hypotheses of Theorem 4 be satisfied except that now $\gamma^2 \neq N(a)$ for any a of $F(i)$, or, what is the same thing, $-\gamma$ is not expressible in the form $\beta_1^2 - \beta_2^2\tau$, β_1 and β_2 in F. Then the cyclic algebra A is a division algebra.*

We shall finally pass to the case where F is the field R of all rational numbers. Quadratic forms have been studied in detail for this case and it has been shown that every indefinite quadratic form in five or more variables is a null form.* The numbers τ, σ, $-\sigma\tau$ all have the same sign only when all are negative. If they are all negative and γ, ρ, $-\gamma\rho$ are also all negative then τ and $-\gamma$ have opposite signs so that $Q = Q_1 - Q_2$ is an indefinite quadratic form. In the other cases obviously Q is indefinite, providing that its coefficients are all not zero. When some of the coefficients of Q are zero then, by making all the other variables zero and those with zero coefficients not zero, we can make Q zero so that Q is a null form. When none of the coefficients of Q is zero then Q is an indefinite quadratic form in six variables and hence is a null form. Hence in every case the cyclic algebra A is not a division algebra when the hypotheses of Theorem 4 are satisfied. We have† the following result.

THEOREM 6. *When $F = R$, the field of all rational numbers, the Wedderburn norm condition for cyclic algebras of order sixteen is necessary as well as sufficient.*

COLUMBIA UNIVERSITY

* For the first complete proof of this theorem see L. E. Dickson, *Studies in the Theory of Numbers.*

† We also have here a new short proof of the author's theorem that a direct product of two rational generalized quaternion division algebras is never a division algebra, by using the above proof that *when Q is a null form A is not a division algebra.* This theorem was first proved by the author and published in the Annals of Mathematics, vol. 30 (1929), pp. 621–625.