NEW RESULTS IN THE THEORY OF NORMAL DIVISION ALGEBRAS[*]

BY

A. ADRIAN ALBERT

1. Introduction. In 1905 L. E. Dickson defined a set of normal division algebras of order n^2 which were based on cyclic n-ics and are called cyclic algebras.[†] No further division algebras were known until, in 1923, F. Cecioni constructed[‡] algebras based on a *non-cyclic* abelian equation of degree four and which were apparently new division algebras. Cecioni made no attempt to show that the algebras that he had constructed were non-cyclic, that is, not equivalent to the much simpler cyclic algebras. He had however found a type of algebras possibly containing non-cyclic algebras.

The present paper begins by a consideration of the necessary and sufficient conditions that a given algebra A of order sixteen of the Cecioni type be an associative division algebra. The associativity conditions are reduced to the question of finding the solutions in integers of

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

where ρ and σ are integers such that neither ρ, σ, nor $\sigma\rho$ is a rational square. This equation has been treated in great detail by R. G. Archibald.[§] The conditions that A be a division algebra are reduced by algebraic theorems to the conditions either (a) G is a quadratic non-residue of σ_1, or (b) σ is a quadratic non-residue of G_1, or (c) $-\sigma_1 G_1$ is a quadratic non-residue of π, where $\gamma_1^2 - \gamma_2^2\rho = \Gamma^2 G$, $\sigma = \sigma_1\pi$, the numbers Γ and G are integers such that G is a product of distinct primes, and π is the highest common factor of G and σ. But the author has shown that all normal division algebras of order 16 are of the Cecioni type.[||] We have therefore constructed, in terms of the single condition given by (a), (b), and (c) and in terms of the integer solutions of a single diophantine equation, all normal division algebras of order sixteen over the field of all rational numbers. For the special case of cyclic algebras the solution of the equation is known and G becomes ρ so that, since all of the

[*] Presented to the Society, December 27, 1929; received by the editors in December, 1929.

[†] *Algebras and their Arithmetics*, p. 65.

[‡] Rendiconti del Circolo Matematico di Palermo, vol. 47 (1923), pp. 209–254.

[§] These Transactions, vol. 30 (1928), pp. 819–837.

[||] These Transactions, vol. 31 (1929), pp. 253–260.

quadratic non-residues of any number are known, we have constructed all cyclic algebras of order sixteen over R.

The problem of discovering whether or not there exist any non-cyclic normal division algebras of order sixteen presents itself. An algebraic necessary and sufficient condition that an algebra A in sixteen units be cyclic is found and, by its use, *it is shown that all of the algebras constructed by Cecioni are cyclic*, and not new. An investigation is then made of the diophantine necessary and sufficient conditions that A be non-cyclic and it is proved that A is non-cyclic if and only if two quartic forms with coefficients polynomials in $\rho, \sigma, \gamma_1, \cdots, \gamma_6$ are not null forms.

2. **Linear associative normal algebras of order sixteen.** We shall consider linear algebras over R, the field of all rational numbers. The algebras will be constructed with a quartic equation with rational coefficients and Galois group G_4 as a foundation. As is well known every such equation may be reduced by a rational Tschirnhausen transformation to an equation

$$\omega^4 + p\omega^2 + n^2 = 0 \qquad (p \text{ and } n \text{ in } R), \tag{1}$$

where ω is a scalar variable and R is the field of all rational numbers. Suppose that i satisfies equation (1). If we write

$$2i^2 + p = w, \quad i + \frac{n}{i} = v, \quad u = \frac{w}{v}$$

then

$$w^2 = p^2 - 4n^2, \quad v^2 = 2n - p, \quad u^2 = -(p + 2n),$$

so that the algebraic field $R(i)$ is evidently the direct product of two quadratic fields $R(u)$ and $R(v)$, and every quantity of $R(i)$ is uniquely expressible in the form

$$a(i) = \alpha_1 + \alpha_2 u + \alpha_3 v + \alpha_4 uv \qquad (\alpha, \cdots, \alpha_4 \text{ in } R).$$

It is well known that the converse of this proposition is true and that

LEMMA 1. *Every field $R(i)$ generated by a root of a quartic* (1) *with Galois group G_4 is a direct product of two quadratic fields*

$$R(u), \quad R(v) \tag{2}$$

where

$$u^2 = \rho, \quad v^2 = \sigma, \quad \rho = \rho_1\pi, \quad \sigma = \sigma_1\pi \tag{3}$$

and ρ_1, σ_1, π are each products of distinct rational prime integers such that no two of ρ_1, σ_1, π have a factor in common. Conversely every such direct product of two quadratic fields defines a quartic field generated by a quantity i satisfying a quartic with group G_4.

Let us examine the quantity i of the above lemma, where we assume that u and v are given. Suppose that we define a quantity $i=(u+1)v$. Then $i^2=(\rho+1+2u)\sigma$, $2\sigma u=i^2-(\rho+1)\sigma$ and

$$\begin{aligned} i^4 &= \sigma^2[(\rho+1)^2+4(\rho+1)u+4\rho] \\ &= \sigma^2[2/\rho+(\rho+1)^2]+2\sigma(\rho+1)[i^2-(\rho+1)\sigma] \\ &= 2\sigma(\rho+1)i^2-\sigma^2(\rho-1)^2 \end{aligned}$$

so that i satisfies

$$\phi(\omega) \equiv \omega^4 - 2\sigma(\rho+1)\omega^2 + \sigma^2(\rho-1)^2 = 0, \tag{4}$$

with roots i, $-i$, $\sigma(\rho-1)/i$, $-\sigma(\rho-1)/i$. But if we write

$$\theta_1 = -i, \qquad \theta_2 = \frac{-\sigma(\rho-1)}{i}, \quad \theta_3 = -\theta_2, \tag{5}$$

then

$$\theta_2 = v(1-u), \quad \theta_1 = (u+1)(-v), \tag{6}$$

$$\theta_3 = uv - v, \tag{7}$$

so that θ_1 is obtained from i by replacing v by $-v$, θ_2 from i by replacing u by $-u$, and θ_3 from i by replacing both u by $-u$ and v by $-v$. We may write any polynomial $a(i)$ of $R(i)$ in the form

$$a = \alpha_1 + \alpha_2 u + \alpha_3 v + \alpha_4 uv \qquad (\alpha_1, \cdots, \alpha_4 \text{ in } R) \tag{8}$$

and shall utilize the notations

$$a(-u) = \alpha_1 - \alpha_2 u + \alpha_3 v - \alpha_4 uv, \tag{9}$$

$$a(-v) = \alpha_1 + \alpha_2 u - \alpha_3 v - \alpha_4 uv, \tag{10}$$

$$a(-u,-v) = \alpha_1 - \alpha_2 u - \alpha_3 v + \alpha_4 uv. \tag{11}$$

Consider the algebra A with sixteen units given by the basis

$$i^r j_s \qquad (r,s = 0,1,2,3; j_3 = j_1 j_2; j_0 = 1), \tag{12}$$

and the multiplication table given by $\phi(i)=0$,

$$(a+bj_1)(c+dj_1) = ac + g_1 bd(\theta_1) + [ad + bc(\theta_1)]j_1 \tag{13}$$

for any a, b, c, d of $R(i)$,

$$(U+Vj_2)(X+Yj_2) = (UX+VY'g_2)+(UY+VX')j_2 \tag{14}$$

for any quantities U, V, X, Y of the form

(15) $$X = a + bj_1, \quad X' = a(\theta_2) + b(\theta_2)\alpha j_1,$$

where

(16) $$g_1, \quad g_2, \quad \alpha$$

are fixed quantities of $R(i)$. Cecioni has shown that if we define g_3 by

(17) $$g_3 = g_1 g_2 \alpha(\theta_1),$$

so that

(18) $$\alpha = \frac{g_3(\theta_1)}{g_1(\theta_1)g_2(\theta_1)},$$

then the algebra A defined above is associative if and only if

(19) $$g_1 = g_1(\theta_1), \quad g_2 = g_2(\theta_2), \quad g_3 = g_3(\theta_3)$$

and if

(20) $$g_3 g_3(\theta_1) = g_1 g_1(\theta_2) g_2 g_2(\theta_1).$$

We may obviously choose as a new basis for A the quantities

(21) $$j_s, \quad uj_s, \quad vj_s, \quad uvj_s \qquad (s = 0,1,2,3)$$

and obtain the following properties:

(22) $$j_1 a = a(-v)j_1, \quad j_2 a = a(-u)j_2, \quad j_3 a = a(-u,-v)j_3,$$

since

(23) $$j_1 a(i) = a(\theta_1)j_1, \quad j_2 a(i) = a(\theta_2)j_2, \quad j_3 a(i) = a(\theta_3)j_3.$$

For, as we have seen, θ_1 is obtained from i by replacing v by $-v$ and leaving u unaltered, so that any polynomial in $-i$ is obtained from the same polynomial in i by replacing v in it by $-v$ and u by u, that is we obtain $a(-v)$. The other equations of (23) are obtained by symmetry. If we write

$$g_1 = \gamma_1 + \gamma_2 u + (\delta_1 + \delta_2 u)v \qquad (\gamma_1, \gamma_2, \delta_1, \delta_2 \text{ in } R),$$

then $g_1 = g_1(\theta_1) = g_1(-v)$ so that, by the linear independence of $1, u, v, uv$ with respect to R, we have

$$(\delta_1 + \delta_2 u)v = -(\delta_1 + \delta_2 u)v = 0.$$

Hence by symmetry

(24) $$g_1 = \gamma_1 + \gamma_2 u, \quad g_2 = \gamma_3 + \gamma_4 v, \quad g_3 = \gamma_5 + \gamma_6 uv,$$

and conversely any g_i in the form (24) satisfy conditions (19). Now (20) becomes

(25) $$\gamma_5^2 - \gamma_6^2 \sigma\rho = (\gamma_1^2 - \gamma_2^2 \rho)(\gamma_3^2 - \gamma_4^2 \sigma)$$

and all of the associative algebras given by (12), (13), (14), (15), (18), (24) will be found when we find all solutions of (25). This problem has been considered in great detail by R. G. Archibald (loc. cit.) and the conditions for the existence of solutions of (25) have been found. We shall leave the associativity conditions in terms of the solutions of this diophantine equation. Let us assume now that in all further work the $\gamma_1, \cdots, \gamma_6$ satisfy (25).

Definition. A linear algebra A over R is said to be a normal algebra if the only quantities of A commutative with every quantity of A are rational numbers.

The writers in the theory of normal division algebras have assumed the algebras they constructed normal algebras, without proof. The proof is usually easy to give and we shall give it for the case we are considering.

Theorem 1. *The algebra A defined by* (12), (13), (14), (15), (18), (24), (25) *is a normal algebra when* $g_3 \neq 0$, $g_2 \neq 0$, $g_1 \neq 0$.

For A contains a sub-algebra Σ whose quantities are composed of all quantities of the form

$$X = a + bj_1 \qquad (a \text{ and } b \text{ in } R(i))$$

of A and every quantity of A is expressible in the form

$$c = X + Yj_2 \qquad (X \text{ and } Y \text{ in } \Sigma).$$

Suppose that c were in A and were commutative with every quantity of A. Then in particular

$$cu = (X + Yj_2)u = u(X - Yj_2) = uc = u(X + Yj_2),$$

and since u has an inverse $(1/\rho)u$ in A we have

$$u^{-1}u(X - Yj_2) = X - Yj_2 = u^{-1}uc = X + Yj_2.$$

By the linearity of A we obtain $Yj_2 = -Yj_2 = 0$, $c = X = a + bj_1$. By using $vc = cv = v(a - bj_1)$ and the fact that v has an inverse $\sigma^{-1}v$ in A we obtain $b = 0$, $c = a_1 + a_2 v$ with a_1 and a_2 in $R(u)$. Now $j_1^2 = g_1 \neq 0$ so that, since g_1 is in $R(u)$ and has an inverse when it is not zero, j_1 has an inverse $g^{-1}j_1$. Then $cj_1 = j_1 c$ shows that $a_1 + a_2 v = a_1 - a_2 v$ and $a_2 = 0$, $c = a_1 = \alpha_1 + \alpha_2 U$, α_1 and α_2 in R. Finally j_2 has an inverse $g_2^{-1}j_2$ and $cj_2 = j_2 c$ gives $\alpha_2 = 0$ which proves that c is in R as was desired.

3. **New necessary and sufficient conditions that A be a division algebra.** We shall assume that ρ and σ are numbers satisfying the conditions of Lemma 1, that $\gamma_1, \cdots, \gamma_6$ satisfy (25), and that $g_1 \neq 0$, $g_2 \neq 0$, $g_3 \neq 0$. We seek to find what further restrictions it is necessary and sufficient to impose on the parameters in order that A be a division algebra. We shall first find

a new sufficient condition that Σ, the sub-algebra of A of order eight defined by its basis

$$i^r j_s \qquad (r = 0,1,2,3;\ s = 0,1),$$

be a division algebra. It is known* that a necessary and sufficient condition that Σ be a division algebra is that

$$g_1 \neq cc(-\,v)$$

for any c of $R(i)$. We shall prove

Lemma 2. *Algebra Σ is a division algebra if there exists no $a \neq 0$ in $R(i)$ for which*

$$aa(-\,v)g_1 = f_1 \text{ in } R. \tag{26}$$

For suppose that the hypothesis of Lemma 2 were satisfied and yet Σ were not a division algebra. Using the known necessary and sufficient condition, there would exist a polynomial c in $R(u, v)$ for which

$$g_1 = cc(-\,v).$$

If $c = 0$ then $g_1 = 0$ contrary to hypothesis. Hence $c \neq 0$ and has an inverse in the quartic field $R(i)$. Write $c^{-1} = a$ and thus $[c(-v)]^{-1} = a(-v)$. Hence

$$aa(-\,v)g_1 = 1.$$

But this is contrary to our hypothesis that $aa(-v)\ g_1$ is not in R for any a. Hence Σ is a division algebra. Write

$$a_1 = \alpha_1 + \alpha_2 u, \quad a_2 = \alpha_3 + \alpha_4 u \qquad (\alpha_1, \cdots, \alpha_4 \text{ in } R)$$

and

$$a = a_1 + a_2 v.$$

Then

$$aa(-\,v) = a_1^2 - a_2^2\sigma = \alpha_1^2 + \alpha_2^2\rho - \sigma(\alpha_3^2 + \alpha_4^2\rho) + 2(\alpha_1\alpha_2 - \sigma\alpha_3\alpha_4)u,$$

so that

$$aa(-\,v)g_1 = f_1 + f_2 u \tag{27}$$

where

$$f_1 = \gamma_1[(\alpha_1^2 + \alpha_2^2\rho) - \sigma(\alpha_3^2 + \alpha_4^2\rho)] + 2\gamma_2\rho(\alpha_1\alpha_2 - \sigma\alpha_3\alpha_4), \tag{28}$$

$$f_2 = \gamma_2[(\alpha_1^2 + \alpha_2^2\rho) - \sigma(\alpha_3^2 + \alpha_4^2\rho)] + 2\gamma_1(\alpha_1\alpha_2 - \sigma\alpha_3\alpha_4). \tag{29}$$

* Cf. L. E. Dickson, *Algebren und ihre Zahlentheorie*, p. 64.

Hence there exists a polynomial for which $aa(-v)g_1$ is in R if and only if the quaternary quadratic form f_2 is a null form. Now

$$\gamma_2 f_2 = (\alpha_1\gamma_2 + \gamma_1\alpha_2)^2 + (\gamma_2^2\rho - \gamma_1^2)\alpha_2^2 - \sigma(\gamma_2\alpha_3 + \gamma_1\alpha_4)^2 - \sigma(\gamma_2^2\rho-\gamma_1^2)\alpha_4^2$$

and if we write

$$\epsilon_1 = \alpha_1\gamma_2 + \gamma_1\alpha_2, \quad \epsilon_2 = \gamma_2\alpha_3 + \gamma_1\alpha_4, \quad \epsilon_3 = \alpha_2, \quad \epsilon_4 = \alpha_4,$$

then

$$\gamma_2 f_2 = (\epsilon_1^2 - \sigma\epsilon_2^2) - (\gamma_1^2 - \gamma_2^2\rho)(\epsilon_3^2 - \sigma\epsilon_4^2).$$

We say that f_2 is a null form if and only if $\gamma_2 f_2$ is a null form. For if γ_2 were zero then $g_1=\gamma_1$ and by taking $a=1=\alpha_1$, $\alpha_2=\alpha_3=\alpha_4=0$ we show that f_2 is a null form. When $\gamma_2\neq 0$ the form f_2 is zero if and only if the non-zero multiple $\gamma_2 f_2$ is zero. The variables in $\gamma_2 f_2$ are all zero when and only when the variables in f_2 are all zero and we have proved

LEMMA 3. *Algebra Σ is a division algebra if the quaternary quadratic form*

$$\epsilon_1^2 - \sigma\epsilon_2^2 - (\gamma_1^2 - \gamma_2^2\rho)(\epsilon_3^2 - \sigma\epsilon_4^2) \tag{30}$$

is not a null form. This is equivalent to stating that $R(i)$ contains no polynomial $a(i)$ for which $aa(-v)g_1$ is in R.

We shall next find a sufficient condition that A itself be a division algebra under the assumption that Σ is one. It is known (loc. cit.) that A is a division algebra when Σ is one if and only if

$$g_2 \neq X'X$$

for any X of Σ. We shall prove that

LEMMA 4. *Algebra A is a division algebra when Σ is one if there exist no polynomials $b\neq 0$ and $d\neq 0$ in $R(i)$ such that*

$$bb(-u)g_2 = f_3, \quad dd(-u, -v)g_3 = f_5$$

with f_3 and f_5 in R.

For suppose that the hypotheses of Lemma 4 were satisfied and yet A were not a division algebra. Then there must exist a quantity X in Σ for which $g_2=X'X$. We may write

$$X = b(-v) + dj_1$$

where b and d are in $R(i)$. Then

$$X' = b(-u, -v) + d(-u)\alpha j_1$$

and

$$X'X = [b(-u, -v)b(-v) + d(-u)d(-v)\alpha g_1] + [b(-u, -v)d + d(-u)b\alpha]j_1,$$

so that

$$g_2 = b(-v)b(-u, -v) + d(-v)d(-u)\alpha g_1. \tag{31}$$

Now we know that, from (18) and $g_1 = g_1(-v)$,

$$\alpha = \frac{g_3(-v)}{g_1 g_2(-v)},$$

so that if (31) is true then

$$g_2 g_2(-v) = b(-v)b(-u, -v)g_2(-v) + d(-v)d(-u)g_3(-v) \tag{32}$$

and by replacing i in (32) by θ_1 and hence v by $-v$ we have

$$\gamma_3^2 - \gamma_4^2\sigma = bb(-u)g_2 + dd(-u, -v)g_3. \tag{33}$$

But it is easily shown that if

$$b = \beta_1 + \beta_2 v + (\beta_3 + \beta_4 v)u, \tag{34}$$

$$d = \delta_1 + \delta_2 uv + (\delta_3 + \delta_4 uv)u, \tag{35}$$

then

$$bb(-u)g_2 = f_3 + f_4 v, \quad dd(-u, -v)g_3 = f_5 + f_6 uv,$$

where

$$f_3 = \gamma_3[\beta_1^2 + \beta_2^2\sigma - \rho(\beta_3^2 + \beta_4^2\sigma)] + 2\gamma_4\sigma(\beta_1\beta_2 - \rho\beta_3\beta_4), \tag{36}$$

$$f_4 = \gamma_4[\beta_1^2 + \beta_2^2\sigma - \rho(\beta_3^2 + \beta_4^2\sigma)] + 2\gamma_3(\beta_1\beta_2 - \rho\beta_3\beta_4), \tag{37}$$

$$f_5 = \gamma_5[\delta_1^2 + \delta_2^2\sigma\rho - \rho(\delta_3^2 + \delta_4^2\sigma\rho)] + 2\gamma_6\sigma\rho(\delta_1\delta_2 - \rho\delta_3\delta_4), \tag{38}$$

$$f_6 = \gamma_6[\delta_1^2 + \delta_2^2\sigma\rho - \rho(\delta_3^2 + \delta_4^2\sigma\rho)] + 2\gamma_5(\delta_1\delta_2 - \rho\delta_3\delta_4). \tag{39}$$

Hence when (33) is true

$$\gamma_3^2 - \gamma_4^2\sigma = f_3 + f_4 v + f_5 + f_6 uv. \tag{40}$$

But $f_4 \neq 0$ unless $b = 0$ and hence also $f_3 = 0$, by our hypothesis. Similarly $f_6 \neq 0$ unless $b = f_3 = 0$. But (40) implies that $f_4 = f_6 = 0$ since $1, u, v, uv$ are linearly independent with respect to R. We have thus secured a contradiction and Lemma 4 is true.

Exactly as we showed in the proof of Lemma 3 that the form (29) was a null form if and only if (30) was a null form, we may show here that the form (37) is a null form if and only if

$$\gamma_4 f_4 = \epsilon_1^2 - \epsilon_2^2\rho - (\gamma_3^2 - \gamma_4^2\sigma)(\epsilon_3^2 - \epsilon_4^2\rho) \tag{41}$$

is a null form and that the form (39) is a null form if and only if

$$\gamma_6 f_6 = \epsilon_1^2 - \epsilon_2^2\rho - (\gamma_5^2 - \gamma_6^2\sigma\rho)(\epsilon_3^2 - \epsilon_4^2\rho) \tag{42}$$

is a null form. Let us suppose that the form (41) is not a null form but that (42) is a null form. Then

$$\mu_1^2 - \mu_2^2\rho - (\gamma_5^2 - \gamma_6^2\sigma\rho)(\mu_3^2 - \mu_4^2\rho) = 0 \tag{43}$$

for $\mu_1, \cdots, \mu_4$ in R and not all zero. Using the value $\gamma_5^2 - \gamma_6^2\sigma\rho = (\gamma_1^2 - \gamma_2^2\rho) \cdot (\gamma_3^2 - \gamma_4^2\sigma)$ we have

$$\mu_1^2 - \mu_2^2\rho - (\gamma_3^2 - \gamma_4^2\sigma)(\gamma_1^2 - \gamma_2^2\rho)(\mu_3^2 - \mu_4^2\rho) = 0. \tag{44}$$

Let us assume that $\gamma_2\gamma_4 \neq 0$. If $\mu_1 = \mu_2 = 0$ then $\mu_3^2 - \mu_4^2\rho = 0$, and $\mu_3 = \mu_4 = 0$ since ρ is not a rational square. Hence μ_1 and μ_2 are not both zero. Write

$$\epsilon_1 = \mu_1, \quad \epsilon_2 = \mu_2, \quad \epsilon_3 = \gamma_1\mu_3 + \gamma_2\mu_4\rho, \quad \epsilon_4 = \gamma_1\mu_4 + \gamma_2\mu_3, \tag{45}$$

so that $\epsilon_3^2 - \epsilon_4^2\rho = (\gamma_1^2 - \gamma_2^2\rho)(\gamma_3^2 - \gamma_4^2\sigma)$. Then

$$\epsilon_1^2 - \epsilon_2^2\rho - (\gamma_3^2 - \gamma_4^2\sigma)(\epsilon_3^2 - \epsilon_4^2\rho) = 0 \tag{46}$$

for $\epsilon_1, \cdots, \epsilon_4$ in R and ϵ_1 and ϵ_2 not both zero. This contradicts the hypothesis that (41) is not a null form. Hence when (41) is not a null form and $\gamma_2\gamma_4 \neq 0$ the form (42) is not a null form.

In the form f_2 write $\alpha_3 = \alpha_6\rho$, $\alpha_4 = \alpha_5$. Then (29) becomes

$$f_2 = \gamma_2[\alpha_1^2 + \alpha_2^2\rho - \sigma\rho(\alpha_5^2 + \alpha_6^2\rho)] + 2\gamma_1(\alpha_1\alpha_2 - \sigma\rho\alpha_5\alpha_6), \tag{47}$$

whence

$$\gamma_2 f_2 = (\gamma_2\alpha_1 + \gamma_1\alpha_2)^2 - (\gamma_1^2 - \gamma_2^2\rho)\alpha_2^2 - \sigma\rho[(\gamma_2\alpha_5 + \gamma_1\alpha_6)^2 - (\gamma_1^2 - \gamma_2^2\rho)\alpha_6^2],$$

which is a null form if and only if

$$\epsilon_1^2 - \sigma\rho\epsilon_2^2 - (\gamma_1^2 - \gamma_2^2\rho)(\epsilon_3^2 - \sigma\rho\epsilon_4^2) \tag{48}$$

is a null form. Similarly write in (37) $\beta_3 \equiv \rho\beta_6$, $\beta_4 \equiv \beta_5$, and it becomes

$$f_4 = \gamma_4[(\beta_1^2 + \beta_2^2\sigma) - \sigma\rho(\beta_5^2 + \beta_6^2\sigma)] + 2\gamma_3(\beta_1\beta_2 - \sigma\rho\beta_3\beta_4),$$

which is a null form if and only if

$$\epsilon_1^2 - \sigma\rho\epsilon_2^2 - (\gamma_3^2 - \gamma_4^2\sigma)(\epsilon_3^2 - \sigma\rho\epsilon_4^2) \tag{49}$$

is a null form. Hence (30) is a null form if and only if (48) is a null form while (41) is a null form if and only if (49) is a null form. Suppose that (30) were not a null form and (41) were a null form. Then there would exist rational numbers $\mu_1, \cdots, \mu_4$ in R and not all zero such that

$$\mu_1^2 - \sigma\rho\mu_2^2 - (\gamma_3^2 - \gamma_4^2\sigma)(\mu_3^2 - \mu_4^2\sigma\rho) = 0.$$

As before we may state that in particular μ_1 and μ_2 are not both zero. But $\gamma_5^2-\gamma_6^2\sigma\rho=(\gamma_1^2-\gamma_2^2\rho)(\gamma_3^2-\gamma_4^2\sigma)$ and thus $\gamma_3^2-\gamma_4^2\sigma=\lambda^2(\gamma_5^2-\gamma_6^2\sigma\rho)(\gamma_1^2-\gamma_2^2\rho)$ where $1/\lambda=\gamma_1^2-\gamma_2^2\rho\neq 0$ since $\gamma_2\neq 0$, ρ is not a square. Then

$$\mu_1^2-\sigma\rho\mu_2^2-\lambda^2(\gamma_1^2-\gamma_2^2\rho)(\gamma_5^2-\gamma_6^2\sigma\rho)(\mu_3^2-\mu_4^2\sigma\rho)=0,$$

and, by letting $\epsilon_1=\mu_1$, $\epsilon_2=\mu_2$, $\epsilon_3=\lambda(\gamma_5\mu_3+\gamma_6\mu_4\sigma\rho)$, $\epsilon_4=\lambda(\gamma_5\mu_4+\gamma_6\mu_3)$, we have a contradiction of the fact that (30) and hence (48) is not a null form. We thus obtain

LEMMA 5. *Algebra A is a division algebra when it is associative, when $\gamma_2\neq 0$, $\gamma_4\neq 0$, and when the form*

$$(30)\qquad \epsilon_1^2-\sigma\epsilon_2^2-(\gamma_1^2-\gamma_2^2\rho)(\epsilon_3^2-\sigma\epsilon_4^2)$$

in the four rational variables $\epsilon_1,\cdots,\epsilon_4$ is not a null form. This form is a null form if and only if there exists a polynomial a in $R(i)$ such that

$$(50)\qquad (aj_1)^2=\mu,\quad \mu \textit{ in } R.$$

We shall consider in detail the form (30). Write

$$e_1=\epsilon_1+\epsilon_2 v,\quad e_2=\epsilon_3+\epsilon_4 v\qquad (\epsilon_1,\cdots,e_4 \text{ in } R).$$

Then

$$e_1e_1(-v)=\epsilon_1^2-\epsilon_2^2\sigma,\quad e_2e_2(-v)=\epsilon_3^2-\epsilon_4^2\sigma,$$

and $\epsilon_1^2-\epsilon_2^2\sigma=0$ if and only if $\epsilon_1=\epsilon_2=0$, that is, if and only if $e_1=0$. Similarly $e_2e_2(-v)=0$ if and only if $e_2=0$. Hence if (30) is a null form there exist quantities e_1 and e_2 both not zero and both in $R(v)$, such that if $e_3=e_1/e_2=\mu_1+\mu_2v$ then

$$\gamma_1^2-\gamma_2^2\rho=\mu_1^2-\mu_2^2\sigma$$

with μ_1 and μ_2 in R and not both zero. We may make $\gamma_1,\cdots,\gamma_6$ integers by replacing j_1 and j_2 by integer multiples of these quantities. It follows that (30) is a null form if and only if the indefinite ternary quadratic form (with integer variables $\lambda_1,\lambda_2,\lambda_3$)

$$\lambda_1^2-\lambda_2^2\sigma-(\gamma_1^2-\gamma_2^2\rho)\lambda_3^2$$

is a null form. Thus A is a division algebra when it is associative, when $\gamma_2\gamma_4\neq 0$, and when the above form is not a null form.

We have found a new sufficient condition that A be a division algebra. We shall prove this condition also a necessary condition. Suppose that A were an associative normal division algebra and that the form were not a null form so that A contained a polynomial $a(i)$ of $R(i)$ such that if $j=aj_1$ then $j^2=\mu$ in R. But the algebra

$$(1,v,j,vj)$$

is a generalized quaternion sub-algebra of A over R and has the multiplication table $v^2=\sigma, j^2=\mu, jv=-vj$. This is known to be impossible when A is a division algebra.* Similarly when $\gamma_2=0$ we may take $j=j_1$ and have a contradiction. When $\gamma_4=0$ we take the sub-algebra

$$(1, u, j_2, uj_2)$$

and show that A is not a division algebra. We have proved

THEOREM 2. *The set of all linear associative normal division algebras in sixteen units over R is obtained by letting $\rho, \sigma, \gamma_1, \cdots, \gamma_6$ range over all rational integers such that*
(a) *ρ is a product of distinct primes,*
(b) *σ is a product of distinct primes,*
(c) *neither ρ, σ nor $\sigma\rho$ is a rational square,*
(d) $\gamma_2\neq 0$, $\gamma_4\neq 0$,
(e) $\gamma_5^2-\gamma_6^2\sigma\rho=(\gamma_1^2-\gamma_2^2\rho)(\gamma_3^2-\gamma_4^2\sigma)$,
(f) *the ternary quadratic form in the variables $\lambda_1, \lambda_2, \lambda_3$*

$$\lambda_1^2 - \lambda_2^2\sigma - (\gamma_1^2 - \gamma_2^2\rho)\lambda_3^2$$

is not a null form.

But all ternary quadratic null forms are known.† We write $\gamma_1^2-\gamma_2^2\rho=\Gamma^2G$, $G=G_1\pi$ and $\sigma=\sigma_1\pi$ where $\Gamma, G_1, \pi, \sigma_1, G$ are integers, G is a product of distinct primes and π is the positive greatest common divisor of σ and G. Then the form (f) is known to be a null form if and only if

$$\pi\lambda_1^2 - \sigma\lambda_2^2 - G_1\lambda_3^2$$

is a null form and this is true if and only if

$$G \equiv E_1^2 \bmod \sigma_1, \qquad \sigma \equiv E_2^2 \bmod G_1, \qquad -\sigma_1 G_1 \equiv E_3^2 \bmod \pi.$$

Hence we have the alternative theorem

THEOREM 2′. *We may replace* (f) *of Theorem* 2 *by the statement that either G is a quadratic non-residue of σ_1, σ is a quadratic non-residue of G_1, or $-\sigma_1G_1$ is a quadratic non-residue of π.*

4. An algebraic necessary and sufficient condition that A be a cyclic algebra.

Consider the form

$$Q = a_1x_1^2 + \cdots + a_5x_5^2, \tag{51}$$

where $a_1, \cdots, a_5$ are non-zero integers not all having the same sign. It is

* The author's paper, Annals of Mathematics, 1929, on *The structure of direct products*, etc.

† Cf. P. Bachmann, *Arithmetik der Quadratischen Formen*, Chapter 8.

well known that there exist integers $x_1, \cdots, x_5$ not all zero for which $Q=0$, that is that Q is a null form. As an obvious consequence we have

LEMMA 6. *Consider the form*

$$Q = \delta_1\xi_1^2 + \cdots + \delta_6\xi_6^2 \tag{52}$$

where $\delta_1, \cdots, \delta_6$ are non-zero rational integers not all having the same sign. Then there exist rational integers $\xi_1, \cdots, \xi_6$ not all zero for which $Q=0$.

We shall consider the form in $\alpha_1, \alpha_2, \beta_1, \cdots, \beta_4$

$$\begin{aligned} R = {} & \sigma(\Delta_1\alpha_1^2 + \tau\Delta_1\alpha_2^2 + 2\tau\alpha_1\alpha_2) + (\lambda\Delta_1 + \tau\mu)[\beta_1^2 + \beta_2^2\tau - \sigma(\beta_3^2 + \beta_4^2\tau)] \\ & + 2\tau(\mu\Delta_1 + \lambda)(\beta_1\beta_2 - \sigma\beta_3\beta_4) \end{aligned} \tag{53}$$

where

$$\lambda,\ \sigma \neq 0,\ \mu \neq 0,\ \Delta_1 \neq 0,\ \Delta_2 \neq 0,\ \tau = \Delta_1^2 + \Delta_2^2$$

are integers and τ is not the square of any rational number. Now

$$\Delta_1(\Delta_1\alpha_1^2 + \tau\Delta_1\alpha_2^2 + 2\tau\alpha_1\alpha_2) = (\alpha_1\Delta_1 + \tau\alpha_2)^2 - \tau\Delta_2^2\alpha_2^2 .$$

Suppose first that $\lambda\Delta_1+\tau\mu=0$. Then, since $\mu\neq 0$, $\lambda\neq 0$, and $\tau(\mu\Delta_1+\lambda) = \Delta_1(\lambda\Delta_1+\mu\tau)+\lambda\Delta_2^2 = \lambda\Delta_2^2 \neq 0$, we may write $2\Delta_1 R$ in the form

$$\begin{aligned} 2\Delta_1 R = {} & 2(\alpha_1\Delta_1 + \alpha_2\tau)^2 - 2\tau\Delta_2^2\alpha_2^2 + \lambda\Delta_2^2(\beta_1 + \beta_2)^2 - \lambda\Delta_2^2(\beta_1 - \beta_2)^2 \\ & - \sigma\lambda\Delta_2^2(\beta_3 + \beta_4)^2 + \sigma\lambda\Delta_2^2(\beta_3 - \beta_4)^2, \end{aligned} \tag{54}$$

since $(\beta_1+\beta_2)^2-(\beta_1-\beta_2)^2=4\beta_1\beta_2$. But the right member of (54) satisfies the conditions of Lemma 6 and may be made zero for integers

$$(\alpha_1\Delta_1 + \alpha_2\tau),\quad \alpha_2,\quad (\beta_1 + \beta_2),\quad (\beta_1 - \beta_2),\quad (\beta_3 + \beta_4),\quad (\beta_3 - \beta_4)$$

not all zero and hence for rational numbers $\alpha_1, \alpha_2, \beta_1, \cdots, \beta_4$ not all zero. It follows that we may make the form (53) vanish for integers $\alpha_1, \alpha_2, \beta_1, \cdots, \beta_4$ not all zero since it is a homogeneous polynomial in $\alpha_1, \alpha_2, \beta_1, \cdots, \beta_4$. Next let $\lambda\Delta_1+\tau\mu=\pi\neq 0$. Then

$$\begin{aligned} \Delta_1\pi R = {} & \pi(\Delta_1\alpha + \alpha_2\tau)^2 - \pi\tau\Delta_2^2\alpha_2^2 + [\pi\beta_1 + \tau(\mu\Delta_1 + \lambda)\beta_2]^2 \\ & + \tau[\pi^2 - (\mu\Delta_1 + \lambda)^2\tau]\beta_2^2 - \sigma[\pi\beta_3 + \tau(\mu\Delta_1 + \lambda)\beta_4]^2 \\ & - \sigma\tau[\pi^2 - (\mu\Delta_1 + \lambda)^2\tau]\beta_4^2 . \end{aligned} \tag{55}$$

Now $\pi^2-(\mu\Delta_1+\lambda)^2\tau$ is not zero since τ is not a rational square. Obviously the signs of the coefficients of the squares $(\alpha_1\Delta_1+\alpha_2\tau)^2$ and α_2^2 are different and we again have a form satisfying the conditions of Lemma 6. Again we may make (53) vanish for integer values of $\alpha_1, \alpha_2, \beta_1, \cdots, \beta_4$ not all zero.

LEMMA 7. *We may choose integers $\alpha_1, \alpha_2, \beta_1, \cdots, \beta_4$ not all zero for which the form R given by* (53) *vanishes.*

We shall prove

LEMMA 8. *Suppose that u is a quantity such that*

$$u^2 = \tau = \Delta_1^2 + \Delta_2^2 \tag{56}$$

where Δ_1 and Δ_2 are relatively prime integers and τ is not a rational square. Let S be a division algebra which is a generalized quaternion algebra with the basis

$$1, y, z, yz \tag{57}$$

and the multiplication table

$$zy = -yz,\ y^2 = \sigma,\ z^2 = \lambda + \mu u,\ \mu \neq 0,\ \lambda, \mu, \sigma \text{ integers}, \tag{58}$$

over the field $R(u)$. Then S contains a quantity x satisfying a cyclic quartic equation with integer coefficients.

For we may choose integers $\alpha_1, \alpha_2, \beta_1, \cdots, \beta_4$ not all zero such that the form (53) vanishes. Then if

$$a_1 = \alpha_1 + \alpha_2 u,\quad b = b_1 + b_2 v,\quad b_1 = \beta_1 + \beta_2 u,\quad b_2 = \beta_3 + \beta_4 u,\quad x = a_1 y + bz$$

we know that $x \neq 0$ and hence $x^2 \neq 0$ since S is a division algebra. We have

$$\begin{aligned} x^2 &= (a_1 y + bz)(a_1 y + bz) = a_1^2 \sigma + bzbz + a_1 b(yz + zy) \\ &= a_1^2 \sigma + (b_1^2 - b_2^2 \sigma)(\lambda + \mu u) = \epsilon_1 + \epsilon_2 u, \end{aligned}$$

where

$$\begin{aligned} \epsilon_1 &= (\alpha_1^2 + \alpha_2^2 \tau)\sigma + \lambda(\beta_1^2 + \beta_2^2 \tau) - \sigma\lambda(\beta_3^2 + \beta_4^2 \tau) + 2\tau\mu(\beta_1\beta_2 - \sigma\beta_3\beta_4), \\ \epsilon_2 &= 2\sigma\alpha_1\alpha_2 + \mu(\beta_1^2 + \beta_2^2 \tau) - \sigma\mu(\beta_3^2 + \beta_4^2 \tau) + 2\lambda(\beta_1\beta_2 - \sigma\beta_3\beta_4). \end{aligned}$$

Consider the linear combination $R = \epsilon_1 \Delta_1 + \epsilon_2 \tau$. It is obviously the form (53) so that $\epsilon_1 \Delta_1 + \epsilon_2 \tau = 0$. As we have chosen the α_i, β_i integers, ϵ_1 is an integer divisible* by τ and we may write $\epsilon_1 = -\tau\nu$. Then $\epsilon_2 = \nu\Delta_1$ and we have

$$x^2 = \nu(\Delta_1 u - \tau). \tag{59}$$

But $x^2 \neq 0$ so that $\nu \neq 0$. But then

$$\begin{aligned} x^4 &= \nu^2(\Delta_1^2 \tau + \tau^2 - 2\tau\Delta_1 u) = \nu^2(\tau\Delta_1^2 + \tau^2) - 2\tau\nu(\nu\tau + x^2) \\ &= \nu^2\tau(\Delta_1^2 - \tau) - 2\tau\nu x^2 = -\nu^2\tau\Delta_2^2 - 2\nu\tau x^2 \end{aligned}$$

and

$$x^4 + 2\nu(\Delta_1^2 + \Delta_2^2)x^2 + \nu^2\Delta_2^2(\Delta_1^2 + \Delta_2^2) = 0. \tag{60}$$

* For when Δ_1 and Δ_2 are relatively prime so are τ and Δ_1.

The above equation is known to be a canonical form of the cyclic quartic equation with integer coefficients and it may be verified that it has the roots x, $\theta(x)$, $\theta^2(x)$, $\theta^3(x)$ with

$$\theta(x) = \frac{x}{\Delta_2}(u + \Delta_1), \quad \theta^4(x) = x.$$

Thus S contains the desired quantity x and our lemma is proved.

We wish next to prove

LEMMA 9. *Let A be a normal division algebra in sixteen units over R. Let A contain a quantity u not in R but such that $u^2=\tau$, an integer of R. Then the algebra S of all quantities of A which are commutative with u is an algebra of order eight over R and has a basis* (57) *and a multiplication table* (58).

For since every quantity of S is by definition commutative with u not in R and A is a normal division algebra, $A>S$. The order of S is then at most eight. The quantity $-u$ is a root of the minimum equation of u and is a transform wuw^{-1} of u by a quantity w of A. Hence $w^2u=w(-u)w=uw^2$ and w^2 is in S. If w^2 is in R the algebra $B=(1, u, w, uw)$ is a generalized quaternion sub-algebra of A which we know to be impossible when A is a division algebra (loc. cit.). Hence the order of $R(w^2)$ is not unity. If the order of $R(w^2)$ is four then the quantity w is in $R(w^2)$ since A has rank four, and w is commutative with u, a contradiction. But the order of $R(w^2)$ is a divisor of the order of $R(w)$ and necessarily is two, so that $R(w^2)$ contains a quantity y generating it such that $y^2=\sigma$, a rational integer. The field $R(u, y)$ is a direct product of two quadratic fields and the quantity $i=(u+1)y$ satisfies an irreducible quartic with Galois group G_4. Its minimum equation has $-i$ as a root and $-i$ is a transform of i by a quantity z of A. In fact z corresponds for this i to the j_1 of §2, and the proof there given shows that z is commutative with u and its square is a polynomial $z^2=\lambda+\mu u$ with λ and μ taken to be rational integers without loss of generality. The integer μ is not zero, for then A would contain a generalized quaternion sub-algebra over R. The quantity y corresponds to the v of §2 and $zy=-yz$. We have proved Lemma 9 and by combining it with Lemma 8 and $\tau=\Delta_1^2+\Delta_2^2$ we have shown that A contains a quantity with cyclic quartic minimum equation.

Conversely let A be a cyclic algebra of order sixteen, that is, let A be a linear associative division algebra containing a quantity x with cyclic quartic minimum equation. Since (60) is a canonical form for the cyclic quartic with integer coefficients we may take, by a rational Tschirnhausen transformation, the minimum equation of x in the form (60). By defining u by (59) the minimum equation of u is (56).

Theorem 3. *Let A be a normal division algebra of order sixteen over R. Then A is a cyclic algebra if and only if A contains a quantity u whose minimum equation is*

$$u^2 = \tau = \Delta_1^2 + \Delta_2^2 \tag{56}$$

where Δ_1 and Δ_2 are rational and τ is not a rational square.

For if Δ_1 and Δ_2 were integers but not relatively prime we would define a new quantity u' by $u' = \pi u$ where π is the greatest common divisor of Δ_1 and Δ_2 and would have a new τ with Δ_1 and Δ_2 relatively prime integers. If Δ_1 and Δ_2 were fractions we would reduce the fractions to lowest terms and multiply u by the least common denominator of the fractions and again would have Δ_1 and Δ_2 relatively prime integers by the above process.

We have seen that the constants in the above proof of Lemma 7 were all not merely rational numbers but integers. We may obtain an interesting corollary. Suppose that A contained a quantity t whose minimum equation was

$$\omega^4 + 2\nu_1\tau\omega^2 + \nu_1^2\tau\Delta_4^2 = 0, \quad \tau = \Delta_3^2 + \Delta_4 = \sigma^2\rho, \quad \rho = \Delta_1^2 + \Delta_2^2, \tag{61}$$

with τ not a product of distinct primes but where ρ is a product of distinct primes. Applying our proof we see that A contains a quantity x with minimum eqation

$$\omega^4 + 2\nu\rho\omega^2 + \nu^2\Delta_2^2\rho = 0, \qquad \rho = \Delta_1^2 + \Delta_2^2, \tag{62}$$

and with ν, ρ, Δ_1, Δ_2 all integers. It is easily shown that we may take ν a product of distinct primes and have

Theorem 4. *Every cyclic algebra of order sixteen over R contains a quantity x with minimum equation*

$$\phi(\omega) \equiv \omega^4 + 2\nu\rho\omega^2 + \nu^2\Delta_2^2\rho = 0 \tag{63}$$

where ν and ρ are each products of distinct primes, ρ is not a rational square, $\rho = \Delta_1^2 + \Delta_2^2$ is any desired representation of ρ as a sum of two integer squares.

5. **Cyclic algebras.** Every normal division algebra in sixteen units containing a quantity x with minimum equation (63) is known to have a basis

$$x^r y_s \qquad (r, s = 0, 1, 2, 3), \tag{64}$$

and a multiplication table

$$y^r f(x) = f[\theta^r(x)]y^r, \quad y^4 = \gamma \qquad (r = 0, 1, 2, 3) \tag{65}$$

with γ an integer of R, for every $f(x)$ of $R(x)$. We shall put the cyclic algebra in our form for algebras of order sixteen (the form of Cecioni). Define u by

$$x^2 = \nu(\Delta_1 u - \rho) \tag{66}$$

so that

$$u^2 = \rho = \Delta_1^2 + \Delta_2^2 \tag{67}$$

where ρ is a product of distinct rational primes and $\rho \neq 0$, $\rho \neq 1$. Obviously the prime factors of ρ have the form 2 or $4n+1$. Also

$$\theta(x) = \frac{-\nu}{\Delta_2}(u + \Delta_1), \; \theta^2(x) = -x, \; \theta^3(x) = -\theta(x), \; \theta^4(x) = x. \tag{68}$$

We have $y^4 = \gamma$, a rational integer having no fourth power as a factor. We may write $\gamma = \gamma_4^2\sigma$ where γ_4 and σ are each products of distinct primes, and $\gamma_4 \neq 0$, $\sigma \neq 0$, $\sigma \neq 1$. It is easily shown that our definition implies that

$$yu = -uy, \quad y^2 u = uy^2, \quad xy^2 = -y^2 x. \tag{69}$$

Define a quantity v by $v\gamma_4 = y^2$. Then

$$v^2 = \sigma, \quad y^2 = \gamma_4 v, \quad xv = -vx, \quad uv = vu. \tag{70}$$

If $\gamma_4 \equiv 0 \pmod{\rho}$ then y_1 defined by $uy_1 = y$ has the property that

$$y_1^2 = -\frac{\gamma_4}{\rho}v, \quad y_1 x = \theta(x) y,$$

so that, without loss of generality, we may take $\gamma_4 \not\equiv 0 \pmod{\rho}$. We then have an algebra of the kind constructed in §§2 and 3 and with

$$j_1 = x, \; j_2 = y, \; j_3 = xy, \tag{71}$$

so that

$$\begin{aligned} j_1^2 &= -\nu\rho + \nu\Delta_1 u, \quad j_2^2 = \gamma_4 v, \\ j_3^2 &= x\theta(x)y^2 = \nu\Delta_2\gamma_4 uv. \end{aligned} \tag{72}$$

Hence

$$\gamma_1 = -\nu\rho, \; \gamma_2 = \nu\Delta_1, \; \gamma_3 = \gamma_5 = 0, \; \gamma_6 = \nu\Delta_2\gamma_4, \tag{73}$$

and

$$\begin{aligned} \gamma_1^2 - \gamma_2^2\rho &= \nu^2\Delta_2^2\rho, \quad \gamma_3^2 - \gamma_4^2\sigma = -\gamma_4^2\sigma, \\ \gamma_5^2 - \gamma_6^2\sigma\rho &= (\gamma_1^2 - \gamma_2^2\rho)(\gamma_3^2 - \gamma_4^2\sigma). \end{aligned} \tag{74}$$

Conditions (a), (b), (c), (d), (e) of Theorem 2 are satisfied. We let $\rho = \rho_1\pi$, $\sigma = \sigma_1\pi$, where π is the greatest common divisor of ρ and σ. Then we have

THEOREM 5. *Let ρ_1, σ_1, π be each products of distinct primes, let these three numbers be relatively prime in pairs, let $\rho_1 > 1$, $\pi > 0$, $\sigma_1 \neq 0$, $\sigma_1 \neq 1$ and $\rho = \rho_1 \pi$ be a product of primes of the form* 2 *and* $4n+1$. *Write $\sigma = \sigma_1 \pi$ and let Δ_1 and Δ_2 be any particular choice of a pair of integers such that*

$$\rho = \Delta_1^2 + \Delta_2^2 . \tag{75}$$

Suppose that one of the congruences

$$\rho \equiv E_1^2 \pmod{\sigma_1}, \quad \sigma \equiv E_2^2 \pmod{\rho_1}, \quad -\sigma_1 \rho_1 \equiv E_3^2 \pmod{\pi}$$

does not hold for any E_i. Then the set of algebras given by the basis

$$x^r y^s \qquad (r,s = 0,1,2,3), \tag{76}$$

and the multiplication table

$$\begin{gathered} x^4 + 2\nu\rho x^2 + \nu^2 \Delta_2^2 \rho = 0, \quad \theta(x) = \frac{-x}{\Delta_2}(u + \Delta_1), \; x^2 = \nu(\Delta_1 u - \rho), \\ \theta^2(x) = -x, \; \theta^3(x) = -\theta(x), \; y^r a(x) = a[\theta(x)]y^r, \\ y^4 = \gamma_4^2 \sigma \qquad (a \text{ in } R(x); r = 0,1,2,3), \end{gathered} \tag{77}$$

where $\nu \neq 0$ and $\gamma_4 \equiv 0 \pmod{\rho}$ are each products of distinct primes, is a set of associative division algebras over R to one of which every cyclic division algebra of order sixteen over R is equivalent.

As when ρ_1, σ_1, or π is given we know all of its quadratic non-residues we have explicitly determined all cyclic division algebras of order sixteen over R.

6. **The algebras of Cecioni.** Cecioni in his Palermo Rendiconti paper constructed normal division algebras based on a non-cyclic abelian equation

$$\psi(\omega) \equiv \omega^4 + p\omega^2 + n^2 = 0.$$

He took $n = 1$, i a root of $\psi(\omega) = 0$, and had a basis

$$i^r j_s \qquad (r,s = 0,1,2,3; j_0 = 1),$$

where

$$\begin{gathered} g = j_1^2 = h_1(i^2 + 1), \; \gamma = j_2^2 = h_2(\theta_2 + i), \; \alpha = \frac{\pm h_1 k(\theta_2 - i)}{g\gamma(\theta_1)}, \\ g = g(\theta_1), \; j_3^2 = g\gamma\alpha(\theta_1), \; k^2 + c^2 + (p + 2)h_2^2 = 0 \end{gathered}$$

so that

$$j_3^2 = \mp h_1 k(\theta_2 - i).$$

Now $(\theta_2-i)^2=\theta_2^2+i^2-2=-(p+2)$, so that if we let $u=\theta_2-i$ then $u^2=-(p+2)$. But $h_2\neq 0$ since otherwise $c=0$ and $j_2^2=0$. Hence $-(p+2)$ is expressible as a sum of two rational squares and we may write

$$u^2 = \tau = \Delta_1^2 + \Delta_2^2 .$$

Our Theorem 3 then shows that A is a cyclic algebra so that *Cecioni's construction did not give any non-cyclic algebras in sixteen units.* We shall take a special case of the algebras, solve the equations necessary, and give the cyclic quantity. Write

$$x = (\theta_2 + i)(u + j_3),$$

and take $k=h_2=1$, $c=4$, $p=-19$, so that

$$-(p + 2) = 17 = 1 + 4^2,\ \Delta_1 = 1,\ \Delta_2 = 2.$$

Then, since $j_3(\theta_2+i)=-(\theta_2+i)j_3,\ j_3u=uj_3,\ j_3^2=u$,

$$x^2 = (\theta_2 + i)^2u^2 + [(\theta_2 + i)j_3]^2 = 21\cdot 17 - 21u,$$

and

$$x^2 = -21(u - 17).$$

It follows that

$$x^4 + 2(-21)\cdot 17x^2 + (21)^2\cdot(2)^2\cdot 17 = 0,$$

a cyclic quartic with

$$x^2 = -21(u - 17),\quad \theta(x) = (x/2)(u + 1).$$

The algebras of Cecioni have been shown to be cyclic algebras and no non-cyclic algebras are known to exist. Cecioni's choice of ρ, σ made his algebras cyclic immediately no matter what the $\gamma_1, \cdots, \gamma_6$ are. The conditions that A be an associative algebra may be satisfied for ρ, σ not so obviously making A a cyclic algebra. For example we may take $\rho=3$, $\sigma=-1$ so that neither ρ, σ nor $\sigma\rho$ is a sum of two rational squares. Then if $\gamma_1=3$, $\gamma_2=\gamma_3=\gamma_4=1$, $\gamma_5=0$, $\gamma_6=2$, we have

$$\gamma_1^2 - \gamma_2^2\rho = 6,\ \gamma_3^2 - \gamma_4^2\sigma = 1 + 1 = 2,\ \gamma_5^2 - \gamma_6^2\sigma\rho = 12,$$

and A is associative. But A is a division algebra since

$$6 \neq \mu_1^2 + \mu_2^2$$

for any rational μ_1 and μ_2. But, as we shall show later, even this algebra is a cyclic algebra. We are led to an investigation of the diophantine conditions on $\rho, \sigma, \gamma_1, \cdots, \gamma_6$ that A be a non-cyclic algebra.

7. **A set of diophantine necessary and sufficient conditions that A be a non-cyclic algebra.** We shall consider a normal division algebra in sixteen units over R, and shall assume that neither ρ, σ, nor $\sigma\rho$ is expressible rationally in the form $\Delta_1^2+\Delta_2^2$. Then it is true that no polynomial s of $R(i)$ which is not in R, that is, which is not merely a rational number, has the property that

$$s^2 = \Delta_1^2 + \Delta_2^2 \qquad (\Delta_1 \text{ and } \Delta_2 \text{ in } R). \tag{78}$$

For let s be a quantity of $R(i)$ which is not in R but whose square is in R. Then $s=s_1+s_2v$ and $s^2=s_1^2+s_2^2\sigma+2s_1s_2v$. If s^2 is in R then $s_1s_2=0$ and $s_1=0$ or $s_2=0$. If $s_2=0$ then $s_1=\lambda_1+\lambda_2u$ and $s^2=s_1^2=\lambda_1^2+\lambda_2^2\rho+2\lambda_1\lambda_2u$. But s is not in R so that when $\lambda_1\lambda_2=0$ then $\lambda_1=0$ and $s=\lambda_2u$. If $s_2\neq0$, $s_1=0$ and $s=(\lambda_3+\lambda_4u)v$, $s^2=(\lambda_3^2+\lambda_4^2\rho+2\lambda_3\lambda_4u)\sigma$. Hence $\lambda_3\lambda_4=0$. If $\lambda_4=0$ then $s=\lambda_3v$ while if $\lambda_3=0$ then $s=\lambda_4uv$. We have proved

LEMMA 10. *The only quantities of $R(i)$ which are not in R but are such that their squares are in R are those quantities of the form*

$$s = \lambda_2u,\ \lambda_3v,\ or\ \lambda_4uv, \tag{79}$$

so that

$$s^2 = \lambda_2^2\rho,\ \lambda_3^2\sigma,\ or\ \lambda_4^2\sigma\rho. \tag{80}$$

But by hypothesis neither ρ, σ nor $\sigma\rho$ is a sum of two rational squares and we have the desired result. As a corollary of Lemma 10 we have

LEMMA 11. *The only quantities of grade two in $R(i)$ are those quantities of the form*

$$t = \lambda_1+\lambda_2u,\ \lambda_1+\lambda_3v,\ or\ \lambda_1+\lambda_4uv. \tag{81}$$

We wish now to find necessary and sufficient conditions that the algebra Σ_1 of all quantities of the form

$$a + bj_1 \qquad (a,b \text{ in } R(i)) \tag{82}$$

contain a quantity s such that $s^2=\Delta_1^2+\Delta_2^2$. If this be true then $s=a+bj_1$, $b\neq0$,

$$s^2 = a^2 + (bj_1)^2 + b[a + a(-v)]j_1, \tag{83}$$

so that, by the linear independence of the basal units of A, we have

$$b[a + a(-v)]j_1 = 0.$$

But $b\neq0$ and thus $a=a_2+a_1v=-(a_2-a_1v)=a_1v$ with a_1 in $R(u)$. Also if

$$(84)\qquad b = \beta_1 + \beta_2 u + (\beta_3 + \beta_4 u)v \qquad (\beta_1, \cdots, \beta_4 \text{ in } R)$$

then

$$(85)\qquad (bj_1)^2 = f_1 + f_2 u,$$

where

$$(86)\qquad f_1 = \gamma_1[(\beta_1^2 + \beta_2^2\rho) - \sigma(\beta_3^2 + \beta_4^2\rho)] + 2\gamma_2\rho(\beta_1\beta_2 - \sigma\beta_3\beta_4),$$

$$(87)\qquad f_2 = \gamma_2[(\beta_1^2 + \beta_2^2\rho) - \sigma(\beta_3^2 + \beta_4^2\rho)] + 2\gamma_1(\beta_1\beta_2 - \sigma\beta_3\beta_4).$$

Then if $a_1 = \alpha_1 + \alpha_2 u$ we have

$$s^2 = (\alpha_1^2 + \alpha_2^2\rho + 2\alpha_1\alpha_2 u)\sigma + f_1 + f_2 u$$

and $s^2 = \Delta_1^2 + \Delta_2^2$ if and only if

$$(88)\qquad (\alpha_1^2 + \alpha_2^2\rho)\sigma + f_1 = \Delta_1^2 + \Delta_2^2,\ 2\alpha_1\alpha_2\sigma + f_2 = 0.$$

We may eliminate α_2 between the two equations of (81) and, using the fact that $R(i)$ contains no quantities s with the desired property, we know that $\beta_1, \cdots, \beta_4$ are not all zero. This gives Lemma 12.

LEMMA 12. *Let A be a normal division algebra of order sixteen. Then its sub-algebra Σ_1 whose quantities are of the form $a + bj_1$ contains a quantity s, not in R but such that $s^2 = \Delta_1^2 + \Delta_2^2$ with Δ_1 and Δ_2 rational, if and only if there exist rational integers $\alpha_1, \beta_1, \cdots, \beta_4, \Delta_1, \Delta_2$ such that $\beta_1, \cdots, \beta_4$ are not all zero and*

$$(89)\qquad f_2^2\rho + 4\alpha_1^4\sigma^2 + 4\alpha_1^2\sigma(f_1 - \Delta_1^2 - \Delta_2^2) = 0.$$

For if $\alpha_1 = 0$ and (82) is satisfied then $f_2 = 0$ contrary to the hypothesis that A is a division algebra. Hence $\alpha_1 \neq 0$ and (89) is equivalent to (88). Since (89) is a homogeneous polynomial in the variables, its solution in rational numbers is equivalent to its solution in integers.

By symmetry we have

LEMMA 13. *Sub-algebra Σ_2 of division algebra A, containing quantities $a + bj_2$ with a and b in $R(i)$, contains a quantity s not in R and yet such that $s^2 = \Delta_1^2 + \Delta_2^2$ if and only if*

$$(90)\qquad f_4^2\sigma + 4\alpha_1^4\rho^2 + 4\alpha_1^2\rho(f_3 - \Delta_1^2 - \Delta_2^2) = 0$$

for integers $\alpha_1, \Delta_1, \Delta_2$, and $\beta_1, \cdots, \beta_4$ not all zero, where f_3 is given by (36) *and f_4 by* (37).

LEMMA 14. *Sub-algebra Σ_3 of division algebra A, containing quantities $a+dj_3$ with a and d in $R(i)$, contains a quantity s not in R and yet such that $s^2=\Delta_1^2+\Delta_2^2$ if and only if*

$$f_6^2\sigma\rho + 4\alpha_1^4\rho^2 + 4\alpha_1^2\rho(f_5 - \Delta_1^2 - \Delta_2^2) = 0 \tag{91}$$

for integers α_1, Δ_1, Δ_2 and $\delta_1, \cdots, \delta_4$ not all zero, where f_5 is given by (38) *and f_6 by* (39).

We shall consider, at this point, the special example given at the end of §5. In that example we had $\sigma=-1$, $\rho=\gamma_1=3$, $\gamma_2=1$. In that case take $\beta_1=\beta_3=\beta_4=0$, $\beta_2=\alpha_1=2$ so that $f_2=3\beta_2^2$,

$$f_2^2\rho = 27\beta_2^4 = 27\alpha_1^4,\ 4\alpha_1^2\sigma f_1 = -36\alpha_1^4,$$

and

$$f_2^2\rho + 4\alpha_1^4\sigma^2 + 4\alpha_1^2\sigma f_1 = -5\alpha_1^4.$$

But then if $\Delta_1=1$, $\Delta_2=2$,

$$4\alpha_1^2\sigma(-\Delta_1^2 - \Delta_2^2) = 4, \quad 5\alpha_1^2 = 5\alpha_1^4,$$

and the form (89) vanishes so that algebra Σ_1 contains a quantity

$$s = (2+3u)v + 6uj_1, \quad s^2 = 5,$$

since $2\alpha_1\alpha_2\sigma = -f_2$, $\alpha_2=3$. Then algebra A is cyclic.

Let us now assume that neither Σ_1, Σ_2 nor Σ_3 contains a quantity s such that $s^2=\Delta_1^2+\Delta_2^2$. We wish to investigate the conditions that a quantity

$$s = T_1 + Tj_2 \qquad (T_1, T \neq 0 \text{ in } \Sigma_1) \tag{92}$$

be such that $s^2=\Delta_1^2+\Delta_2^2$ with Δ_1 and Δ_2 in R. If s^2 is in R, then since

$$s^2 = T_1^2 + (Tj_2)^2 + T_1(Tj_2) + (Tj_2)T_1$$

and since

$$(Tj_2)^2 = TT'g_2, \quad (Tj_2)T_1 = TT_1'j_2,$$

with T_1' and T' in Σ, we have

$$T_1(Tj_2) + (Tj_2)T_1 = 0, \quad T_1^2 + W = \Delta_1^2 + \Delta_2^2, \tag{93}$$

where

$$W = (Tj_2)^2 = TT'g_2. \tag{94}$$

Since W is in Σ_1 and Tj_2 is not in Σ_1 we know that Tj_2 is not a polynomial in W and the order of $R(W)$ is less than that of $R(Tj_2)$. But W is not in R since then $(Tj_2)^2$ would be in R and A would contain a generalized quaternion sub-algebra $(1, u, Tj_2, uTj_2)$. Hence W has grade two and $R(W)$ contains $T_1^2=-W+\Delta_1^2+\Delta_2^2$. The field $R(T_1)$ contains W. Since T_1 is in Σ_1 an algebra over $R(u)$, $T_1u=uT_1$. The field $R(u, W)$ has order four since u is not in $R(W)>R(Tj_2)$. Hence $R(T)=R(u, T_1^2)=R(u, W)$, for T must be in any field of order four with whose quantities it is commutative.* Then

$$T_1 = P_1(W) + P(W)u,$$

and since $(Tj_2)T_1=-T_1(Tj_2)$ we have $P_1(W)=0$ and $s=P(W)u+Tj_2$ with $P(W)=\lambda_1+\lambda_2W$, λ_1 and λ_2 in R, and T in Σ_1. Since W has grade two we may write

$$W^2 = 2\phi_1W + \phi_2, \qquad V = W - \phi_1, \qquad V^2 = \phi_2 + \phi_1^2 \equiv \psi,$$

and if $P(W)=\alpha_1+\alpha_2V$, $W=V+\phi_1$, then

$$s^2 = (\alpha_1^2 + \alpha_2^2\psi + 2\alpha_1\alpha_2V)\rho + V + \phi_1,$$

which equals $\Delta_1^2+\Delta_2^2$ if and only if

$$(\alpha_1^2 + \alpha_2^2\psi)\rho + \phi_1 = \Delta_1^2 + \Delta_2^2, \quad 2\alpha_1\alpha_2\rho = -1. \tag{95}$$

It now becomes necessary to compute ϕ_1 and ϕ_2. We may write

$$Tj_2 = (b + dj_1)j_2 = bj_2 + dj_3 \qquad\qquad (b, d \text{ in } R(i)).$$

If $d=0$ then bj_2 is in Σ_2 so that s is in Σ_2 contrary to our hypothesis that Σ_2 contains no quantities s such that s is not in R and yet $s^2=\Delta_1^2+\Delta_2^2$. Similarly $b\neq0$ and we shall now write

$$(Tj_2)^2 = W = (bj_2)^2 + (dj_3)^2 + bd(-u)j_2j_3 + db(-u, -v)j_3j_2.$$

We have taken A so that $j_2j_3=\alpha g_2(-v)j_1$, $j_3j_3=g_2(-v)g_1$ and

$$W = (bj_2)^2 + (dj_3)^2 + [b\alpha(-u) + db(-u, -v)]g_2(-v)j_1.$$

Write

$$(bj_2)^2 = f_3 + f_4v, \quad (dj_3)^2 = f_5 + f_6uv,$$

where, as we know, f_3, f_4, f_5 and f_6 are given respectively by (36), (37), (38), (39). Then

$$W = q_1 + q_2j_1, \tag{96}$$

with

$$q_1 = (f_3 + f_5) + f_4v + f_6uv, \quad q_2 = [bd(-u)\alpha + db(-u, -v)]g_2(-v) \tag{97}$$

and

* It is known that the only quantities of a normal division algebra of order n^2 over F which are commutative with a quantity x of grade n in the algebra, are polynomials in x with coefficients in F.

$$g_1g_2(-v)\alpha = g_3(-v). \tag{98}$$

Then

$$W^2 = q_1^2 + (q_2j_1)^2 + q_2[q_1 + q_1(-v)]j_1.$$

We shall prove

LEMMA 15. *The quantity q_2 is zero if and only if $b=0$ or $d=0$.*

For let $b=0$ or $d=0$. By its form q_2 vanishes. Let next $b\neq 0$ and $d\neq 0$. If $q_2=0$ then

$$W = f_3 + f_5 + (f_4 + f_6u)v \quad \text{in} \quad R(i).$$

But W has grade two with respect to R as we have shown. Also the only polynomials in i of grade two were proved in Lemma 11 to be quantities of the form $\lambda_1+\lambda_2u$, $\lambda_1+\lambda_3v$, $\lambda_1+\lambda_4uv$. If W has any of these three forms then $f_4=0$ or $f_6=0$. But when A is a division algebra $f_4=0$ if and only if $b=0$ and f_6 was shown to be zero if and only if $d=0$. This furnishes a contradiction and Lemma 15 is true.

We have assumed that $b\neq 0$ and $d\neq 0$. Then $q_2\neq 0$, and since

$$q_1^2 + (q_2j_1)^2 + q_2[q_1 + q_1(-v)]j_1 = 2\phi_1(q_1 + q_2j_1) + \phi_2,$$

we have

$$2\phi_1 = q_1 + q_1(-v) = 2(f_3 + f_5), \quad \phi_1 = f_3 + f_5, \tag{99}$$

while

$$\phi_2 = q_1^2 + (q_2j_1)^2\phi_1q_1 = (q_2j_1)^2 - q_1q_1(-v).$$

We may easily compute $q_1q_1(-v)$ and have

$$q_1q_1(-v) = (f_3 + f_5)^2 - \sigma(f_4^2 + f_6^2\rho + 2f_4f_6u). \tag{100}$$

To compute $(q_2j_1)^2$ replace α by its value and we have

$$g_1q_2 = bd(-u)g_3(-v) + db(-u, -v)g_1g_2(-v).$$

Also

$$g_1(q_2j_1)^2 = g_1q_2q_2(-v)g_1.$$

But

$$g_1q_2(-v) = b(-v)b(-u, -v)g_3 + d(-v)b(-u)g_1g_2$$

and

$$\begin{aligned} g_1(q_2j_1)^2 = {} & [bb(-v)d(-u)d(-u, -v)g_3g_3(-v) \\ & + dd(-v)b(-u)b(-u, -v)g_1^2g_2g_2(-v)] \\ & + g_1[bb(-u)d(-u)d(-v)g_2g_3(-v) \\ & + b(-v)b(-u, -v)dd(-u, -v)g_2(-v)g_3]. \end{aligned} \tag{101}$$

But $g_3g_3(-v)=g_1g_1(-u)g_2g_2(-v)$ so that the right member of (101) has a factor g_1. First

$$[bb(-u)g_2][d(-u)d(-v)g_3(-v)] = (f_3+f_4v)(f_5-f_6uv),$$

so that the second term in brackets of the right member of (101) is

$$2(f_3f_5-f_4f_6\sigma u)g_1. \tag{102}$$

The first term has a factor $g_1g_2g_2(-v)$, and apart from this factor is

$$g_1b(-u)b(-u,-v)dd(-v)+bb(-v)d(-u)d(-u,-v)g_1(-u). \tag{103}$$

Also since

$$b=\beta_1+\beta_2v+(\beta_3+\beta_4v)u=\beta_1+\beta_3u+(\beta_2+\beta_4u)v,$$

$$d=\delta_1+\delta_2uv+(\delta_3+\delta_4uv)u=\delta_1+\delta_3u+(\delta_4\rho+\delta_2u)v,$$

we havc

$$bb(-v)=\beta_1^2+\beta_3^2\rho-(\beta_2^2+\beta_4^2\rho)\sigma+2(\beta_1\beta_3-\sigma\beta_2\beta_4)u,$$

$$dd(-v)=\delta_1^2+\delta_3^2\rho-(\delta_2^2+\delta_4^2\rho)\sigma\rho+2(\delta_1\delta_3-\sigma\rho\delta_2\delta_4)u.$$

Let

$$\begin{aligned} h_3 &= \beta_1^2+\beta_3^2\rho-\sigma(\beta_2^2+\beta_4^2\rho),\\ h_4 &= -2(\beta_1\beta_3-\sigma\beta_2\beta_4),\\ h_5 &= \delta_1^2+\delta_3^2\rho-\sigma\rho(\delta_2^2+\delta_4^2\rho),\\ h_6 &= 2(\delta_1\delta_3-\sigma\rho\delta_2\delta_4). \end{aligned} \tag{104}$$

Then $b(-u)b(-u,-v)=h_3+h_4u$ and

$$g_1dd(-v)b(-u)b(-u,-v)=(h_3+h_4u)(h_5+h_6u)(\gamma_1+\gamma_2u).$$

But (103) is a polynomial in u added to the same polynomial in $-u$ and its value is

$$H=2[\gamma_1(h_3h_5+h_4h_6\rho)+\gamma_2\rho(h_3h_6+h_4h_5)], \tag{105}$$

so that

$$\phi_2=\sigma f_4^2+\sigma\rho f_6^2-f_3^2-f_5^2+(\gamma_3^2-\gamma_4^2\sigma)H.$$

But

$$\psi=\phi_2+\phi_1^2=\phi_2+f_3^2+f_5^2+2f_3f_5$$

so that

$$\psi=\sigma f_4^2+\sigma\rho f_6^2+2f_3f_5+(\gamma_3^2-\gamma_4^2\sigma)H. \tag{106}$$

The form (106) reduces to σf_4^2 when $d=0$ and to $\sigma\rho f_6^2$ when $b=0$. Also $s^2=\Delta_1^2+\Delta_2^2$ if and only if

$$(107)\qquad \psi + 4\alpha_1^4\rho^2 + 4\alpha_1^2\rho(\phi_1 - \Delta_1^2 - \Delta_2^2) = 0,$$

for if $\alpha_1=0$ then $V^2=\psi=0$ which is not true since, as we have shown, W is not in R. Hence (107) is equivalent to (95). But it reduces to (90) when $d=0$ since then $f_5=0$, $\phi_1=f_3$. Similarly (107) reduces to (91) for $b=0$. We then have (90) and (91) included in (107) and may omit them. Suppose that (107) were satisfied for values of the variables not all zero. If all of the β_i and δ_i were zero then we could, by taking the remaining variables not all zero, have a solution. But the resulting quantity s would be zero. We must therefore seek solutions with not all of the β_i and δ_i vanishing. The solution of (107) in rational numbers is equivalent to its solution in integers and we have

THEOREM 6. *A normal division algebra A in sixteen units over R with integer parameters ρ, σ, $\gamma_1, \cdots, \gamma_6$ satisfying the conditions of Theorem* 2, *and such that neither ρ, σ nor $\sigma\rho$ is a sum of two integer squares, is a non-cyclic algebra if and only if*

$$(a)\qquad f_2^2\rho + 4\alpha_1^4\sigma^2 + 4\alpha_1^2\sigma(f_1 - \Delta_1^2 - \Delta_2^2) \neq 0,$$

$$(b)\qquad \psi + 4\alpha_1^4\rho^2 + 4\alpha_1^2\rho(\phi_1 - \Delta_1^2 - \Delta_2^2) \neq 0,$$

for any integers α_1, Δ_1, Δ_2, $\beta_1, \cdots, \beta_4$, $\delta_1, \cdots, \delta_4$ such that $\beta_1, \cdots, \beta_4$, $\delta_1, \cdots, \delta_4$ are not all zero and f_1 is given by (86), *f_2 by* (87), *ϕ_1 by* (99), (36), *and* (38), *and ψ by* (106), (105), (104), (37), (39).

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.