ON DIRECT PRODUCTS, CYCLIC DIVISION ALGEBRAS, AND PURE RIEMANN MATRICES*

BY
A. ADRIAN ALBERT

1. **Introduction.** The present paper is the result of a consideration of several related topics in the theory of linear associative algebras and the application of the results obtained to the theory of Riemann matrices. We first consider a linear algebra problem of great importance in its application to Riemann matrix theory, the question as to when a normal division algebra of order n^2 over F is representable by an algebra of m-rowed square matrices with elements in F. It is shown that this is possible if and only if n^2 divides m and this is applied to prove that.

The multiplication index h of a pure Riemann matrix of genus p is a divisor† of $2p$.

The algebras called cyclic (Dickson) algebras are the simplest normal division algebras structurally. J. H. M. Wedderburn has given sufficient conditions that constructed cyclic algebras be division algebras but it seems to have been overlooked that these conditions have not been shown to be necessary. In the fundamental problem of the construction of all such division algebras necessary and sufficient conditions are of course needed. The question of the necessity of the Wedderburn conditions is considered here and the results applied to obtain what seems a remarkable restriction on the types of algebras which may be the multiplication algebras of pure Riemann matrices. Also certain general theorems on direct products of normal simple algebras are proved and the conclusions used to reduce the problem of the construction of cyclic division algebras to the case where the order of the algebra is a power of a single prime.

2. **Results presupposed and elementary theorems.** We shall assume that F is any non-modular field and shall use the definitions of direct product, division algebras, and other terms as in L. E. Dickson's *Algebren und ihre Zahlentheorie*. We shall assume

THEOREM 1. *The direct product A of two total matric algebras B and C of orders n^2 and m^2 respectively is a total matric algebra of order $(nm)^2$.*

---

* Presented to the Society, April 18, 1930; received by the editors in June, 1930.

† It was merely known until now that $h \leqq 2p$, a very much milder condition.

THEOREM 2. *Every simple algebra over F, which is not a zero algebra of order one, is expressible as a direct product of a division algebra B over F and a total matric algebra M over F in one and only one way in the sense of equivalence. Conversely every such direct product is simple.*

We shall henceforth restrict the algebras of this paper to be not zero algebras when they are simple. Moreover we shall study only associative algebras. If A is the direct product of B and C where B and C are simple, then, by the operation of passing to algebras equivalent to B and C, we may assume that the moduli of A, B, and C are all the same quantity and similarly for the zero quantities. We shall assume this operation performed in all cases and that $\times$ is the notation for direct product, while if M and P are linear sets that MP is their product.

Definition. An algebra A with a modulus e over a field F is called *normal* if the only quantities of A commutative with all quantities of A are multiples of e by scalars in F.

THEOREM 3. *Let A be a normal simple algebra. Then A is the direct product of a normal division algebra and a total matric algebra and conversely.*

For A is the direct product of a total matric algebra M and a division algebra B. If B were not normal then there would be a quantity x in B such that x is not a scalar multiple of the modulus e of A and yet $xb=bx$ for every b of B. But $xm=mx$ for every m of M since $A=B\times M$. The quantities of A are sums of multiples of quantities of B by quantities of M so that $xa=ax$ for every a of A, a contradiction of the hypothesis that A is normal.

Conversely if B is a normal division algebra and M is a total matric algebra, then $A=B\times M$ is simple. Let $M=(e_{ij})$, $e_{ij}e_{jk}=e_{ik}$, $e_{ij}e_{tk}=0$ $(j\neq t)$. Then if

$$x = \sum_{i,j} b_{ij}e_{ij} \qquad (b_{ij} \text{ in } B)$$

is commutative with all of the quantities of A we have

$$xe_{kt} = \sum_{i} b_{ik}e_{it} = e_{kt}x = \sum_{j} b_{kj}e_{kj}$$

for all k and t. It follows from the definition of direct product that $b_{ij}=0$ $(i\neq j)$, $b_{ii}=b_{11}$, and that x is in B. But the only quantities of B commutative with all quantities of B are scalar multiples of its modulus, the modulus of A, so that x is a multiple of the modulus by a scalar of F and A is normal.

THEOREM 4. *Let $A=B\times C$ where B and C are normal simple algebras over F. Then A is a normal simple algebra over F.*

For by adjoining a scalar ξ to F, the algebra B_1 with the same basal units

and constants of multiplication as B but over $F(\xi)=F'$ is a total matric algebra. Also ξ may be so chosen that C simultaneously reduces to a total matric algebra by the well known theorem on the adjunction of a finite number of scalars to a nonmodular field being equivalent to the adjunction of a single scalar. But A' over F' is a total matric algebra. By Theorem 3, A' is normal and if A were not normal obviously neither would be A', having the same basis and constants of multiplication as A. Hence A is normal. Moreover by a known* theorem A' is semi-simple if and only if A is simple. If A were reducible then so obviously would be A' so that, since A' is simple and not reducible, A is not reducible. A semi-simple algebra which is not reducible is simple and A is thus a normal simple algebra.

We shall assume a theorem† of J. H. M. Wedderburn.

THEOREM 5. *Let A be a linear associative algebra over a non-modular field F. Let e be the modulus of A and suppose that B, a normal simple sub-algebra of A, has the same modulus e as A. Then A is the direct product of B and another algebra C with the same modulus e.*

We also have for A an algebra with modulus the same as that of B, C_1, C

THEOREM 6. *Let $A=B\times C=B\times C_1$, where B is a normal simple algebra. Then $C_1=C$.*

For let c_1 be in C_1. Then c_1 is in A and is necessarily expressible in the form

$$c_1 = \sum_i b_i u_i,$$

where b_i are in B and the u_i are a basis of C, with $u_1=e$, the modulus of A. But if b is any quantity of B, then

$$bc_1 = c_1 b, \quad 0 = bc_1 - c_1 b = \sum_i (b_i b - b b_i) u_i.$$

By the definition of direct product this implies that $b_i b = b b_i$ for all b's of B, so that the b_i are in F and the quantities of C_1 are in C. Similarly the quantities of C are in C_1 and $C=C_1$.

THEOREM 7. *Let $A=B\times C$ where A is a normal simple algebra. Then both B and C are normal simple algebras.*

For it evidently suffices to prove the above true for C. Suppose that C were not simple so that C would contain an invariant proper sub-algebra N. Then $NC\leqq N$, $CN\leqq N$. But if $P=B\times N$, then $AP=(B\times C)\ (B\times N)=B^2\times(CN)\leqq P$, while $PA=(B\times N)\ (B\times C)=B^2\times(NC)\leqq P$, so that A would

* Dickson (loc. cit.) p. 110, Corollary to Theorem 18.

† Proceedings of the Edinburgh Mathematical Society, vol. 25 (1906–1907), pp. 1–3.

have the invariant proper sub-algebra P contrary to the hypothesis that A is simple. If C were not normal, then there would exist an x in C such that $xc=cx$ for every c of C while x is not a multiple of the modulus of C by a quantity of F. But then evidently $xa=ax$ for every a of A contrary to the hypothesis that A is a normal algebra. It follows that C is a normal simple algebra.

THEOREM 8. *Let $A=B\times C$ where A and B are total matric algebras. Then C is a total matric algebra.*

For A is a normal simple algebra, so that, by Theorem 7, so is C. Hence $C=M\times D$ where M is a total matric algebra and D is a normal division algebra. It follows that $A=B\times C=(B\times M)\times D$, where, by Theorem 1, $B\times M$ is a total matric algebra. By the uniqueness in Theorem 2 and the fact that A is a total matric algebra, algebra D has order one and $C=M$ is a total matric algebra.

3. **On direct products of normal division algebras.** The theory of the complex multiplications of pure Riemann matrices has been studied in detail by various authors.* Of utmost importance in this theory is the question as to what are necessary and sufficient conditions that a division algebra B of order h over F be expressible as an algebra of m-rowed square matrices with elements in F. The author has reduced this question to the case where B is a normal division algebra over F.† Using this reduction, and by a consideration of certain theorems on direct products of normal division algebras, we shall completely answer the above question. We shall also obtain a theorem on the direct products of normal division algebras of relatively prime orders for use in the next section.

THEOREM 9. *Let B be a normal division algebra of order n^2 over F. Then there exists a normal simple algebra B_1 of order n^2 over F such that $A=B\times B_1$ is a total matric algebra over F.*

For it is well known that every linear associative algebra with a modulus and having order t over F is equivalent to an algebra of t-rowed square matrices. Hence B is equivalent to an algebra C of n^2-rowed square matrices with elements in F and, if M is the algebra of all n^2-rowed square matrices with elements in F, then by Theorem 5, $M=C\times C_1$ where C_1 is a normal simple algebra. Let B_1 be an abstract algebra defined so that it is equivalent

* For references see the Bulletin of the National Research Council, No. 63, *Selected Topics in Algebraic Geometry*, chapters 15, 16, 17, 1928.

† In a paper *On the structure of pure Riemann matrices with non-commutative multiplication algebras*, to be published in the Rendiconti del Circolo Matematico di Palermo, probably in January, 1931.

to C_1. Since M has order n^4 and C has order n^2, algebra C_1 has order n^2. Hence B_1 has order n^2 and is a normal simple algebra. Let A be the direct product of B and B_1. Evidently A is equivalent to M and is a total matric algebra over F.

THEOREM 10. *Let $M=B\times C$ be a total matric algebra over F, where B and C are normal division algebras. Then B and C have the same order.*

For if the order of B is n^2 and that of C is r^2, then, without loss of generality, we may take $n\leqq r$. Let B_1 be the algebra of Theorem 9 such that $A=B\times B_1$ is a total matric algebra. By the associative law and $A=B_1\times B$, the algebra $G=B_1\times M$ may also be written $G=A\times C$. Now $B_1=D\times T$ where D is a normal division algebra of order $t^2\leqq n^2$ and T is a total matric algebra. Hence $G=B_1\times M=D\times(T\times M)$, where $T\times M$ is a total matric algebra. But, by Theorem 2, G is simple, $G=D\times(T\times M)=C\times A$, and C is equivalent to D. Hence $t=r$. But $t\leqq n\leqq r$. It follows that $r=n$ as desired.

We are now in a position to prove the fundamental theorem on the representation of a normal division algebra over F as an algebra of matrices with elements in F.

THEOREM 11. *A normal division algebra B of order n^2 over F is expressible as a sub-algebra of the algebra of all m-rowed square matrices with elements in F if and only if m is divisible by n^2.*

For if $m=n^2t$ then B can be expressed first as a sub-algebra of H, the algebra of all n^2-rowed square matrices with elements in F. Then if T is a t-rowed total matric algebra, the algebra $M=H\times T$ is an m-rowed total matric algebra by Theorem 1. Evidently B is a sub-algebra of M and its representation in M provides an expression for B as a sub-algebra of the algebra of all m-rowed square matrices with elements in F which is equivalent to M.

Conversely let B be a sub-algebra of M, an m-rowed total matric algebra over F. Then $M=B\times(D\times T)$ by Theorem 5, where D is a normal division algebra and T is a total matric algebra, so that $m=ndt$ where d^2 is the order of D and t^2 the order of T. By Theorem 8 the algebra $B\times D$ is a total matric algebra, so that, by Theorem 10, $d=n$, and $m=n^2t$.

As a corollary we have

THEOREM 12. *The algebra B_1 of Theorem 9 is a normal division algebra.*

For let $B_1=D\times T$, where T is a total matric algebra and D a normal division algebra. Then $A=B\times B_1=(B\times D)\times T$, so that, by Theorems 8 and 10, D has order n^2. But B_1 has order n^2. It follows that B_1 is D and is a normal division algebra.

We shall finally prove

THEOREM 13. *Let $A=B\times C$ where B and C are normal division algebras whose orders m^2 and n^2 respectively are relatively prime. Then A is a normal division algebra.*

For by Theorem 4 algebra A is a normal simple algebra and $A=H\times D$ where H is a total matric algebra of order h^2 and D a normal division algebra of order d^2. Hence $mn=hd$. Let B_1 be the normal division algebra of Theorems 9 and 12 so that $B\times B_1$ is a total matric algebra. The direct product $B_1\times D$ is a normal simple algebra by Theorem 4, and $B_1\times D=Q\times P$ where Q is a total matric algebra and P a normal division algebra. But $G=B_1\times A=B_1\times(H\times D)=H\times(B_1\times D)=H\times(Q\times P)=(H\times Q)\times P=(B_1\times B)\times C$. It follows that $H\times Q$ is equivalent to $B_1\times B$ from the uniqueness in Theorem 2. Hence if Q has order q^2, then $hq=m^2$. By forming the direct product $C_1\times A$ we prove similarly that h divides n^2. Hence all prime factors of h are factors of both m and n. But m and n are relatively prime so that $h=1$ and $A=D$ is a division algebra.

4. **Cyclic normal division algebras.** Let x satisfy an equation $\phi(\xi)=0$ of degree n, with leading coefficient unity and further coefficients in F, and with the cyclic group with respect to F. Then there exists a polynomial $\theta(x)$ such that if we define its iteratives $\theta^r(x)=\theta[\theta^{r-1}(x)]$, $\theta^0(x)=x(r=0,1,\cdots)$, then $\theta^n(x)=x$ and $\phi[\theta^r(x)]=0$. The algebra D with the basis

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

and the multiplication table

$$\phi(x) = 0,\ y^n = \gamma,\ y^r f(x) = f[\theta^r(x)]y^r \quad (r = 0, 1, \cdots, n-1),$$

for every $f(x)$ of $F(x)$, where γ is in F, is an associative normal algebra over F. For every $f=f(x)$ in $F(x)$ we write

$$N(f) = f[\theta^{n-1}(x)]\cdots f[\theta(x)]\cdot f(x),$$

a quantity in F, and call $N(f)$ the norm of f. J. H. M. Wedderburn has proved*

THEOREM 14. *Algebra D is a division algebra if no power $\gamma^r(r<n)$ is the norm of any f in $F(x)$.*

The above condition is a sufficient condition that D be a division algebra but is not known to be necessary. For $n=2$, 3 the above condition is also necessary but may be replaced by the simpler condition that $\gamma\neq N(f)$ for

* These Transactions, vol. 15 (1914), pp. 162–166.

any f of $F(x)$. We shall show that a like result holds *for n any prime* and shall reduce the problem of constructing all cyclic algebras to the *case n a power of a prime.*

THEOREM 15. *Let $F(x)$ be a cyclic field of order $r=nm$ where n and m are relatively prime integers. Then $F(x)$ is the direct product of two cyclic fields of orders m and n respectively, and conversely.*

For let G be the cyclic substitution group of order r which is the Galois group of the minimum equation of x. Then G will consist of the powers of a single substitution P such that $P^r=I$, the identity substitution. Since m and n are relatively prime there exist integers g and h such that $1=gm+hn$. Then for every $\alpha<r$ we have $g\alpha\equiv\beta(\text{mod } n)$ and $h\alpha\equiv\delta(\text{mod } m)$, where $0\leqq\beta<n$ and $0\leqq\delta<m$. But then

$$P^\alpha = (P^m)^{g\alpha}\cdot(P^n)^{h\beta} = P^{m\beta}\cdot P^{n\delta},$$

since $P^r=I$. Hence every substitution of G is expressible as a product of substitutions of the groups $G_1=(P^{m\beta})$ and $G_2=(P^{n\delta})$. It follows that G is the direct product of G_1 and G_2. It is known that there exists a quantity a in $F(x)$, which *belongs to the group* G_2 and hence has grade n with respect to F and G_1 as a representation of the Galois group of its minimum equation. Then this equation has the cyclic group with respect to F. Similarly there exists a quantity b in $F(x)$, *which belongs to* G_1 and has grade m with respect to F and G_2 as a representation of the Galois group of its minimum equation. The field $F(a, b)$ contains $F(a)$ and $F(b)$ as sub-fields and hence its order is divisible by both m and n. But m and n are relatively prime so that the order of $F(a, b)$ is divisible by mn. The order of $F(a, b)$, a sub-field of $F(x)$ of order mn, is at most mn, so that $F(a, b)$ has order mn and $F(a, b)=F(x)$. But when $F(a, b)$ has order mn, the product of the orders of $F(a)$ and $F(b)$, it is the direct product of $F(a)$ and $F(b)$ by the definition of direct product. It follows that $F(x)$ is the direct product of the two cyclic fields $F(a)$ and $F(b)$.

Conversely let X be the direct product of two cyclic fields $F(a)$ and $F(b)$ of relatively prime orders n and m respectively. Let ξ be a scalar root of the minimum equation of a and let η be a scalar root of the minimum equation of b. The field $F(\xi, \eta)$ has $F(\xi)$ and $F(\eta)$ as sub-fields and hence has order mn. It follows that $F(\xi, \eta)$ is the direct product of $F(\xi)$ and $F(\eta)$ and is equivalent to X. Thus $X=F(a, b)$ is a commutative division algebra or field. Let x generate X so that $X=F(x)$, $x=Q(a, b)$, a polynomial in a and b with coefficients in F. Let the roots of the minimum equation of a which are in $F(a)$ be denoted by $\lambda^\beta(a)$, $(\beta=0, 1, \cdots, n-1)$, and the roots of the minimum equation of b in $F(b)$ by $\mu^\delta(b)$, $(\delta=0, 1, \cdots, m-1)$. If $K=F(b)$ then any rational

function of the $\lambda^\beta(a)$ with coefficients in K which is symmetric in the $\lambda^\beta(a)$ is in K, since the minimum equation of a with respect to K is the same as its minimum equation with respect to F. The polynomial

$$\phi(\omega) \equiv \prod_{\beta,\gamma} \omega - Q[\lambda^\beta(a); \mu^\delta(b)]$$

has coefficients in K since they are symmetric in the $\lambda^\beta(a)$. But they are symmetric in the $\mu^\delta(b)$, so they are in F. The equation $\phi(\omega)=0$ has degree mn. It has leading coefficient unity, further coefficients in F and $\phi(x)=0$. Hence $\phi(\omega)=0$ is the minimum equation of x since x has grade mn. We may choose integers g and h such that

$$gm + hn = 1, \quad g\alpha \equiv \beta \pmod{n}, \quad h\alpha \equiv \delta \pmod{m},$$

so that every integer less than mn is expressible in the form

$$\alpha = \beta m + \delta n + \alpha_1 mn \qquad (0 \leqq \beta < n,\ 0 \leqq \delta < m).$$

Now if S is the substitution replacing a by $\lambda(a)$ and T is the substitution replacing b by $\mu(b)$ then the substitution P which is the substitution replacing x by

$$\theta(x) = Q[\lambda(x), \mu(x)]$$

is equivalent to the substitution product $S \cdot T$. Hence P^α replaces x by

$$\theta^\alpha(x) = Q[\lambda^\beta(x), \mu^\delta(x)] \qquad (\alpha = 0, 1, \cdots, r-1),$$

with β and δ determined as above. It follows that the Galois group of the minimum equation of x has a cyclic sub-group of order mn. But since the roots in $F(x)$ of the minimum equation of x are mn in number the group of this equation is actually the above cyclic group

$$(P^\alpha)\ (\alpha = 0, 1, \cdots, r-1),\ r = mn.$$

THEOREM 16. *Let A be a cyclic normal division algebra of order r^2 over F, and $r=mn$ where m and n are relatively prime integers. Then A is the direct product of a cyclic normal division algebra B of order n^2 and a cyclic normal division algebra C of order m^2, each having the same γ as A. Conversely the direct product A of two cyclic normal division algebras B and C of relatively prime orders n^2 and m^2 respectively is a cyclic normal division algebra whose γ may be taken to be the γ of B and C.*

Let A be a cyclic algebra of order r^2 over F so that A contains a quantity x whose minimum equation with respect to F has degree $r=mn$ and roots $\theta^\alpha(x)$ in $F(x)$. Moreover, A contains a quantity y such that

$$y^{\alpha}f(x) = f[\theta^{\alpha}(x)]y^{\alpha}, \quad y^{r} = \gamma \text{ in } F.$$

Let A be a normal division algebra. Let a and b be defined as in the proof of Theorem 15 so that a is unaltered by the substitutions of the group $G_2 = (P^{n\delta})$ where P generates the Galois group of the minimum equation of x, and $G_1 = (P^{m\beta})$ is a representation of the Galois group of the minimum equation of a. Then evidently $y^{n\delta}a = ay^{n\delta}$, while $(y^m)^n = \gamma$, $y^{m\beta}a = \lambda^{\beta}(a)y^{m\beta}$. Similarly $(y^n)^m = \gamma$, $y^{m\beta}b = by^{m\beta}$, $y^{n\delta}b = \mu^{\delta}(b)y^{n\delta}$. Let B be the algebra with the basis

$$a^{g}y^{m\beta} \qquad (g, \beta = 0, 1, \cdots, n-1),$$

and C be the algebra with the basis

$$b^{h}y^{n\delta} \qquad (h, \delta = 0, 1, \cdots, m-1).$$

The algebras B and C are cyclic algebras with the same γ as A. Moreover every quantity of B is commutative with every quantity of C. Every quantity of A is expressible in the form

$$\sum_{\alpha=0}^{r-1} f_{\alpha}(x)y^{\alpha} \qquad [f_{\alpha}(x) \text{ in } F(x)].$$

But any such quantity has the form

$$\sum g_{\beta\delta}y^{m\beta}y^{n\delta}$$

since we may find integers β, δ for which

$$y^{\alpha} = y^{m\beta} \cdot y^{n\delta} \cdot \gamma^{\alpha_1}$$

and express each $f_{\alpha}(x)$ in the form $g_{\beta\gamma}(a, b) \cdot \gamma^{-\alpha_1}$ since $F(x)$ is the direct product of $F(a)$ and $F(b)$. Hence the set A is a set whose quantities are sums of products of quantities of B and quantities of C and is contained in the set BC. But BC is a sub-set of A so that A is equal to BC. Since the quantities of B are commutative with the quantities of C, A is the direct product of B and C.

Conversely let B be a cyclic normal division algebra over F and have order n^2 so that B contains a quantity a such that the minimum equation of a with respect to F is cyclic with respect to F and with polynomial roots $\lambda^{\beta}(a)$ $(\beta = 0, 1, \cdots, n-1)$ such that $\lambda^{0}(a) = \lambda^{n}(a) = a$. Then B contains also a quantity y_1 such that

$$y_1^{n} = \gamma_1 \text{ in } F, \quad y_1^{\beta}g(a) = g[\lambda^{\beta}(a)]y_1^{\beta} \qquad (\beta = 0, 1, \cdots, n-1),$$

for every $g(a)$ in $F(a)$. Similarly let C have order m^2 where m and n are relatively prime, contain the cyclic m-ic field $F(b)$, and contain the quantity y_2 such that

$$y_2^m = \gamma_2 \text{ in } F, \quad y_2^\delta g(b) = g[\mu^\delta(b)]y_2^\delta \quad (\delta = 0, 1, \cdots, m-1).$$

If A is the direct product of B and C then A is a normal division algebra by Theorem 13. Moreover the direct product of $F(a)$ and $F(b)$ is a cyclic field $F(x)$ whose polynomial roots are

$$\theta^\alpha(x) = Q[\lambda^\beta(a), \mu^\delta(b)],$$

and if we let $y = y_1y_2$ then $y^\alpha x = \theta^\alpha(x)y^\alpha$ with β and δ properly chosen integers such that $\alpha = \beta m + \delta n + \alpha_1 mn$. We thus have

$$y^{nm} = y_1^{nm}y_2^{mn} = \gamma_1^m\gamma_2^n,$$

and A is a cyclic algebra whose γ is $\gamma_1^m\gamma_2^n$. If we let $y_{11} = \gamma_2 y_1^m$, $y_{22} = \gamma_1 y_2^n$, then

$$y_{11}^n = \gamma_2^n\gamma_1^m = \gamma, \quad y_{22}^m = \gamma_1^m\gamma_2^n = \gamma,$$

and we may replace y_1 in the basis of B by y_{11}, y_2 in the basis of C by y_{22}, and each of these algebras will have the same γ as A. In fact since m and n are relatively prime we may choose an integer s such that $ms \equiv 1 \pmod{n}$, so that y_{11}^s is a constant multiple of y_1 and we have a basis of B when we replace y_1 by y_{11}.

As an immediate corollary we have

THEOREM 17. *Let $r = p_1^{e_1} \cdot p_2^{e_2} \cdots p_t^{e_t}$ where the p_i are distinct primes. Every cyclic algebra of order r^2 over F which is a division algebra is a direct product of t cyclic division algebras of order $p_i^{2e_i}$, and conversely all such direct products are cyclic division algebras.*

We have thus reduced the problem of constructing all cyclic division algebras to the case where the order is a power $2e$ of a prime p. This latter problem is of great difficulty even in the case where $p = 2$, $e = 2$. When $e = 1$ we may make a simple discussion as follows.

THEOREM 18. *A cyclic algebra A of order p^2 over F, p a prime, is a division algebra if and only if γ is not the norm of any polynomial in x.*

For suppose that γ be not the norm of any polynomial in x but that A were not a division algebra. By the sufficient condition of Theorem 14 there must exist an integer $\alpha < p$, such that

$$\gamma^\alpha = N(g), \qquad g \text{ in } F(x).$$

Since p is a prime there exists an integer σ such that $\sigma\alpha \equiv 1 \pmod{p}$. Let then $\sigma\alpha = 1 + tp$, $\sigma > 0$, $t > 0$, so that

$$\gamma \cdot \gamma^{tp} = \gamma^{\sigma\alpha} = [N(g)]^\sigma = N(g^\sigma).$$

If $\gamma=0$ then $\gamma=N(0)$, a contradiction. Hence

$$\gamma = (\gamma^{-t})^p \cdot N(g^\sigma) = N(g^\sigma\gamma^{-t}),$$

a contradiction.

Conversely let $\gamma=N(f)$, where f is in $F(x)$. If $f=0$ then $y^p=0$ which is impossible in a division algebra when $y\neq 0$. But $1, y, \cdots, y^{p-1}$ are linearly independent with respect to F so that y is not zero and f is not zero. Then f has an inverse in $F(x)$, and if h is this inverse we have $(hy)^p=N(hf)=1$. But if $y_1=hy$ then $1, y_1, y_1^2, \cdots, y_1^{p-1}$ are linearly independent with respect to F, since the quantities $x^r y^s$ $(r, s=0, 1, \cdots, p-1)$ are linearly independent with respect to F. It follows that $y_1-1\neq 0$, and $y_1^{p-1}+y_1^{p-2}+\cdots+y_1+1\neq 0$. But y_1^p-1 is the product of the two aforesaid non-zero quantities and is zero, which is impossible in a division algebra.

We shall now obtain some simple but interesting limitations on the order of a cyclic division algebra A when the sufficient condition of Theorem 14 is not satisfied.

THEOREM 19. *Let A be a cyclic division algebra of order r^2 where $r=p_1^{e_1}\cdot p_2^{e_2}\cdots p_t^{e_t}$ and the p_i are distinct prime integers. Then if γ^s is the norm of a polynomial in x, the integer s is divisible by $p_1\cdot p_2\cdots p_t$.*

For suppose that s were not divisible by p, a factor of r. Then there would exist an integer α such that $\alpha s\equiv 1 \pmod{p^e}$. Let $\alpha s=1+tp^e$ and $r=p^e m$, so that we can express A as the direct product of a cyclic division algebra B of order p^{2e} and a cyclic division algebra C of order m^2 by Theorem 16. The norm of any polynomial in x may be written as the norm of a polynomial in a where a is the cyclic quantity of Theorem 16 for the algebra B. We have then that

$$\gamma^s = N_a(c)$$

where c is a polynomial in a so that

$$\gamma^{\alpha s} = \gamma\gamma^{tp^e} = N_a(c), \quad \gamma = N_a(c\gamma^{-t}).$$

If y_1 is the y of algebra B we have

$$(y_1)^{p^e} = N_a(c), \quad (c^{-1}y_1)^{p^e} - 1 = 0,$$

from which, as in the proof of Theorem 18, it quickly follows that B is not a division algebra. But this is impossible since B is a sub-algebra of the division algebra A.

As a corollary we have

THEOREM 20. *Let A be a cyclic division algebra of order r^2. Then if p is a prime and γ^p is the norm of a polynomial in x, the integer r is a power of p.*

For if r were not a power of p then it would contain a factor not dividing p.

For the case where B is a cyclic algebra of order p^2, p a prime, we may explicitly determine the structure of algebra B_1 of Theorem 9. We showed that B_1 was a normal division algebra of order p^2 in Theorem 12. We shall now prove

THEOREM 21. *A direct product $A=B\times C$ of a cyclic division algebra B of order p^2, p a prime, and a normal division algebra C of order p^2 is a total matric algebra if and only if C is equivalent to B.*

We use the form of the multiplication table of B which is reciprocal to our previous form, assuming that

$$y^s x^r \qquad (r, s = 0, 1, \cdots, p-1)$$

are a basis of B and that

$$y^p = \gamma, \quad xy^s = y^s\theta^s(x) \qquad (s = 0, 1, \cdots, p-1).$$

Assume first that C is equivalent to B and let X in C correspond to x in B and Y in C to y of B. Consider the quantities

$$e_{ii} = \frac{(x-X_1)(x-X_2)\cdots(x-X_{i-1})(x-X_{i+1})\cdots(x-X_p)}{(X_i-X_1)(X_i-X_2)\cdots(X_i-X_{i-1})(X_i-X_{i+1})\cdots(X_i-X_p)},$$

$$e_{1i} = y^{i-1}e_{ii}, \quad e_{i1} = \frac{1}{\gamma}y^{p+1-i}e_{11} \qquad (i = 2, \cdots, p),$$

$$e_{ij} = e_{i1}e_{1j} \qquad (i, j = 1, \cdots, p),$$

where $X_i=\theta^i(X)$. Then Wedderburn has shown* that, with the agreement that $e_{j+mp,\,i+mp}=e_{ji}$, we have

$$e_{ii}y^k = y^k e_{k+i,k+i}, \quad x = \sum_i X_i e_{ii},$$

$$y = e_{12} + e_{23} + \cdots + \gamma e_{p1},$$

for all integer values of k and i. In particular $e_{ii}y^{-1}=y^{-1}e_{i-1,i-1}$. Since $X_iY=YX_{i+1}$ we have obviously from the form of the e_{ii} that $e_{ii}Y=Ye_{i+1,i+1}$. Hence if $Z=Yy^{-1}$ then $e_{ii}Z=Ze_{ii}$. Also since $A=C\times B$ we have $Zy^k=y^kZ$ whence from the definitions of the e_{ij}, $Ze_{ij}=e_{ij}Z$. Wedderburn has also shown that the e_{ij} form a basis of an algebra M which is a total matric algebra of order p^2. The linear set $M_1=(Z^sX^r)$ $(r, s=0, 1, \cdots, p-1)$ is an algebra with

* These Transactions, vol. 15 (1914), pp. 162–166.

the multiplication table given by $XZ^k = Z^k\theta^k(X)$, $Z^p = Y^p y^{-p} = \gamma\gamma^{-1} = 1$. Since the quantities of M are commutative with those of M_1 and since both sets are algebras, the set MM_1 is an algebra. But MM_1 is contained in A. Also the quantities x, y, X, Y are all in MM_1 by the above displayed equations and hence all of the quantities of A are in MM_1. It follows that $A = MM_1$, and since the quantities of M are commutative with those of M_1, $A = M \times M_1$. Algebra $A = B \times C$ is a normal simple algebra by Theorem 4. Hence algebra M_1 is a normal simple algebra by Theorem 7. But algebra A has order p^4 and M has order p^2 so that M_1 has order p^2. Since p is a prime, M_1 is either a normal division algebra or a total matric algebra. But $Z^p = 1$ which is impossible in a normal division algebra when $1, Z, Z^2, \cdots, Z^{p-1}$ are linearly independent with respect to F. By our choice of the basis of M_1 and the fact that the order of M_1 is p^2 we have the independence of the above quantities so that M_1 is a total matric algebra. By Theorem 1, A is a total matric algebra.

Conversely let $A = B \times C$ be a total matric algebra, where B is a cyclic algebra of order p^2, p a prime. If B_1 is equivalent to B we have already shown that $G = B \times B_1$ is a total matric algebra. Consider the algebra $H = B_1 \times A = G \times C$. Now A and G are total matric algebras and B_1 and C are normal division algebras, so that, by Theorem 2, B_1 is equivalent to C. It follows that C is equivalent to B.

5. Applications to the theory of pure Riemann matrices. Let ω be a pure Riemann matrix over a real field K. It is known that the algebra of multiplications of ω is a division algebra D of order $h \leqq 2p$ over K and that D has a representation as an algebra of $2p$-rowed square matrices with elements in K. Let D be expressed as an algebra which is a normal division algebra of order n^2 over its central field $K(q)$ of order t, so that $h = n^2 t$. The minimum equation of q is irreducible in K since D is a division algebra and there exists a representation of q as a $2p$-rowed square matrix whose elements on the diagonal are the same t-rowed square matrix Q with elements in F and whose elements off the diagonal are zero matrices, while $2p = mt$. Any two representations of q as a $2p$-rowed square matrix with elements in K are similar in K so that we may take the representation of D such that q has the above representation. It follows that D has a representation as an algebra of m-rowed square matrices with elements in $K(Q)$, and by applying Theorem 11, with $F = K(Q)$, we have immediately m divisible by n^2. This gives $m = n^2 r$, $2p = hr$, and

THEOREM 22. *The multiplication index h of a pure Riemann matrix ω of genus p over a real field K is a divisor of $2p$.*

The only normal division algebras of order n^2 which are known are the so-called algebras of type R_n. By this we mean that the algebra A which is a normal division algebra in n^2 units over F contains a quantity a whose minimum equation $\phi(\xi)=0$ with respect to F has degree n and roots $\theta_j(a)$, where $\theta_1(a)=a$, $\theta_j(a)$ is in $F(a)$. Also $\theta_j[\theta_k(a)]$ is a root of $\phi(\xi)=0$ so that there exists a set of integers $t_{j,k}$ such that

$$\theta_j[\theta_k(a)] = \theta_{t_{j,k}}(a) \qquad (j, k = 1, \cdots, n).$$

Algebra A has a basis

$$a^{j-1}y_k \qquad (j, k = 1, \cdots, n),$$

where $y_1=1$ and

$$y_j a = \theta_j(a)y_j, \quad y_k y_j = g_{j,k}y_{t_{j,k}},$$

with the $g_{j,k}$ in $F(a)$. The author has studied the case where such algebras A are the multiplication algebras of pure Riemann matrices of genus p over a real field F in great detail. Assume first that the equation $\phi(\xi)=0$ has a real root α_1 so that all of its roots are real when F is a real field. The author has shown (loc. cit. *On the structure of pure Riemann matrices with non-commutative multiplication algebras*) that there must necessarily exist n numbers $\beta_j(\alpha_1)$ in $F(\alpha_1)$ and positive, such that if $\alpha_j=\theta_j(\alpha_1)$, then

$$\beta_j(\alpha_k)\beta_k(\alpha_1) = [g_{j,k}(\alpha_1)]^2\beta_{t_{j,k}}(\alpha_1).$$

We shall assume that n has an odd prime factor p. Then, since the Galois group of $\phi(\xi)=0$ has order n, it contains at least one substitution of order p, since it is known that if a prime divides the order of a group there is a sub-group G_1 of order the prime in the original group. This sub-group of order p is necessarily cyclical and generated by a single substitution of order p. Without loss of generality we may take $\theta_2(a)$ to be the quantity by which a is replaced by the above substitution, so that $y_2{}^r a=\theta_2{}^r(a)y_2{}^r$ $(r=0, 1, \cdots, p-1)$, and we may take $y_{r+1}=y_2{}^r$ $(r=0, 1, \cdots, p-1)$, $y_2{}^p=g(a)$. Let v be a polynomial in a belonging to the sub-group G_1. Then A contains a cyclic sub-algebra

$$H = (a^r y_2{}^s) \qquad (r, s = 0, 1, \cdots, p-1)$$

over the field $F(v)$ and, since $g(a)$ is a power of y_2, therefore commutative with y_2, therefore unaltered when we replace a by $\theta_2(a)$, $g(a)$ is in $F(v)$. Assume now that α_1, a root of the minimum equation of a, is real. Since $F(a)$ and $F(\alpha_1)$ are equivalent and $\alpha_j=\theta_j(\alpha_1)$ there must exist polynomials $\beta_j(a)$ in $F(a)$ such that

$$\beta_j[\theta_k(a)]\beta_k(a) = [g_{j,k}(a)]^2\beta_{t_{j,k}}(a).$$

We have taken

$$\theta_2^k(a) = \theta_{k+1}(a), \quad y_2^k = y_{k+1} \quad (k = 0, 1, \cdots, p-1)$$

whence

$$g_{j,2}(a) = 1\,(j < p), \quad t_{j,2} = j+1 \quad (j = 2, \cdots, p-1),$$
$$\beta_1(a) = t_{p,2} = 1, \quad g_{p,2} = g(a).$$

But then if $\theta(a) = \theta_2(a)$

$$\beta_j[\theta(a)]\beta_2(a) = \beta_{j+1}(a) \qquad (j = 2, \cdots, p-1),$$

so that

$$\begin{aligned}
\beta_3(a) &= \beta_2[\theta(a)]\beta_2(a), \\
\beta_4(a) &= \beta_3[\theta(a)]\beta_2(a) = \beta_2[\theta^2(a)]\beta_2[\theta(a)]\beta_2(a), \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\beta_p(a) &= \beta_{p-1}[\theta(a)]\beta_2(a) = \beta_2[\theta_2^{p-2}(a)] \cdots \beta_2[\theta(a)]\beta_2(a),
\end{aligned}$$

and we obtain

$$\beta_p[\theta(a)]\cdot\beta_2(a) = N_H[\beta_2(a)] = [g(a)]^2\cdot 1$$

where $N_H[\beta_2(a)]$ is the norm in the cyclic algebra H of the polynomial $\beta_2(a)$. But $g(a)$ is the γ of Theorem 20 and p is not a power of 2, a contradiction. Hence n contains no odd prime factor p and is a power of 2.

The only other case where it is possible to make a detailed study of the structure of the Riemann matrices is the case where the minimum equation of a has all imaginary roots but now such that the unique substitution replacing each root by its complex conjugate is commutative with all of the substitutions of the Galois group of this minimum equation. Let P_0 be this unique substitution, and as before assume that n has an odd prime factor p so that the Galois group G of the minimum equation $\phi(\xi) = 0$ of a has a cyclic substitution P of order p. Now $PP_0 = P_0P$ and $P_2 = PP_0$ obviously generates a cyclic substitution of order $2p$ such that $P_2^p = P_0$. We may rearrange the roots of $\phi(\xi) = 0$ so that $\theta_2(a)$ is the polynomial into which a is carried by P_2,

$$\theta_2^i(a) = \theta_{i+1}(a)\ (j = 0, 1, \cdots, 2p-1), \quad y_2^{2p} = g(a) = g_{2p,2}(a),$$
$$g_{j,2}(a) = 1 \quad (j < 2p), \quad t_{2p,2} = 1, \quad t_{j,2} = j+1 \quad (j = 2, \cdots, 2p-1).$$

The author has shown that there exist positive numbers β_j (α_1) such that if α_1 is an ordinary complex root of $\phi(\xi) = 0$ and $\alpha_j = \theta_j(\alpha_1)$, then $\beta_k = \beta_k(\alpha_1)$ in $F(\alpha_1)$ and $n = 2n_1$,

$$\beta_j[\alpha_k]\beta_k(\alpha_1) = g_{j,k}(\bar{\alpha}_1)\cdot g_{jk}(\alpha_1)\cdot\beta_{t_{j,k}}(\alpha_1).$$

The above equations were proved true under the assumptions that

$$\bar{\alpha}_1 = \theta_{1+n_1}(\alpha_1), \quad \bar{\alpha}_j = \theta_{1+n_1}(\alpha_j) = \theta_j[\theta_{1+n_1}(\alpha_1)],$$

but, since they hold for any subscripts, they will hold after our permutation of the subscripts which makes $\theta_2{}^k(a) = \theta_{k+1}(a)$ $(k = 0, 1, \cdots, 2p-1)$. Now $\theta_2{}^p(\alpha_j) = \bar{\alpha}_j$ and we have, from the correspondence between $F(a)$ and $F(\alpha_1)$,

$$\beta_j[\theta_k(a)]\beta_k(a) = g_{j,k}[\theta_2{}^p(a)] \cdot g_{j,k}(a) \cdot \beta_{t_{j,k}}(a) \qquad (j, k = 0, 1, \cdots, n).$$

But $g(a) = y_2{}^{2p}$ is unaltered by transforming by the quantity $y_2{}^p$, so that $g(a) = g[\theta_2{}^p(a)]$ and the above equations make the square of $g(a)$, as for the case of real α_1 but with p now replaced by $2p$, equal to the norm, with respect to the substitution P_2, of a polynomial in a. As before this would make a division sub-algebra of A not a division algebra unless $2p$ is a power of two. This contradicts our hypothesis that p is odd and we have

THEOREM 23. *Let ω be a pure Riemann matrix over a real field F and with D its multiplication algebra. Let D be a normal division algebra in n^2 units over F, and suppose that D contains a quantity a whose minimum equation has degree n, n complex roots all polynomials in one of them with coefficients in F, and the property that these roots are all real, or all imaginary such that the substitution carrying each root to its complex conjugate is commutative with all of the substitutions of the Galois group of the equation. Then n is a power of two.*

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.