ON DIRECT PRODUCTS*

BY

A. ADRIAN ALBERT

1. **Introduction.** The principal contribution of this article is a set of theorems on the structure of the direct product of a normal division algebra A over F and an algebraic field $F(\eta)$, with applications of the Galois theory of equations. The theorems are useful new tools for research on normal division algebras. In particular it is shown that it is possible to extend the reference field F of any normal division algebra A of order p^2 over F, p a prime, such that $A'=A\times F(\eta)$ is a cyclic normal divison algebra over $F(\eta)$. A new proof is given of a little known theorem of R. Brauer† which reduces the problem of determinining all normal division algebras of order n^2 over F to the case where n is a power of a prime.

2. **Known theorems.** We shall repeatedly use the theorems given in the author's paper *On direct products, cyclic division algebras, and pure Riemann matrices*, and shall refer to it by the letter T. All our algebras A will be linear associative algebras with a modulus over any non-modular field F, and all sub-algebras of A will have the same modulus, 1, and the same zero quantity, 0, as A.

The symbol $\times$ shall mean direct product, $A\times B$ the direct product of an algebra A and an algebra B over the same field F. In $A\times B$ the algebras A and B will be taken, without loss of generality,to be sub-algebras of $A\times B$.

We shall require three well known theorems.

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

THEOREM 2. *Every simple algebra‡ A over F is expressible as a direct product $B\times M$ 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, and conversely.*

---

* Presented to the Society June 13, 1931; received by the editors April 17, 1931.

† This theorem seems to be almost unknown in America. It was obtained independently by the author, and this paper was, in fact, already received by the editors of these Transactions when the author discovered Brauer's priority. However, Brauer obtained his results in three memoirs using complicated theorems on linear groups going back fundamentally to two memoirs of I. Schur, and his papers are far from self-contained. The author's independent proof is a simple application of his new theorems on direct products. For references and Brauer's theorems, see his third paper in the Mathematische Zeitschrift, vol. 30 (1929), pp. 79–107.

‡ Not a zero algebra of order one, since we assume throughout that A has the modulus 1.

THEOREM 3. *Let A contain a normal simple sub-algebra B. Then A is the direct product of B and another sub-algebra C of A.*

We shall also use the author's theorems* T 3, 4, 7, 8, 13. They are respectively

THEOREM 4. *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.*

THEOREM 5. *Let $A = B \times C$ where B and C are normal simple algebras over F. Then A is a normal simple algebra over F.*

THEOREM 6. *Let $A = B \times C$ where A is a normal simple algebra. Then both B and C are normal simple algebras.*

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

THEOREM 8. *Let A be a normal division algebra of order m^2 over F and B bc a normal division algebra of order n^2 over F such that m and n are relatively prime integers. Then $A \times B$ is a normal division algebra of order m^2n^2 over F.*

3. **Extensions of the field F.** Let A be a normal divison algebra of order n^2 over F. We shall study what happens to A when we extend F by a quantity η which is commutative with all the quantities of A and is such that $F(\eta)$ is a algebraic field of order r over F. We shall thus consider the algebra A' which has the same basis and multiplication constants as A, but which is an algebra over $F(\eta)$. It is evident that A', considered as an algebra over F, is the direct product

$$A' = A \times F(\eta).$$

Let A be as above and let x in A have† $\phi(\omega) = 0$ as its minimum equation with respect to F. We shall say in this case that $\phi(\omega) = 0$ is an equation which *belongs to A*. It is well known that when A is a normal division algebra over F every equation belonging to A is irreducible in F.

Let x in A have $\phi(\omega) = 0$ as its minimum equation with respect to F so that, if m is the degree of $\phi(\omega)$, the quantities $1, x, x^2, \cdots, x^{m-1}$ are linearly independent with respect to F. Then in a *direct product* $A \times F(\eta)$ these quantities will be linearly independent with respect to $F(\eta)$. If $\phi(\omega)$ is reducible in $F(\eta)$, then $\phi(\omega) \equiv \phi_1(\omega)\phi_2(\omega)$ and $\phi_1(x) \cdot \phi_2(x) = 0$ where the $\phi_i(x)$ are each polynomials in x of degree less than m with coefficients not all zero in $F(\eta)$. But then $\phi_1(x) \neq 0$, and $\phi_2(x) \neq 0$ while their product is zero. This is impossible in a division algebra. We have

* These Transactions, vol. 33 (1931), pp. 235–243.

† We shall use the symbol ω to represent a scalar variable and $\phi(\omega)$, $\psi(\omega)$ as polynomials in ω with coefficients in F and leading coefficient unity.

THEOREM 9. *Let A be a normal division algebra over F and $F(\eta)$ an algebraic field over F. Then*

$$A' = A \times F(\eta)$$

is not a division algebra if some $\phi(\omega)=0$ which belongs to A is reducible in $F(\eta)$.

We continue with the following well known result.*

THEOREM 10. *There exist an infinity of irreducible equations $\phi(\omega)=0$ of degree n belonging to any normal division algebra A of order n^2 over F.*

We shall henceforth in general restrict our consideration of equations $\phi(\omega)=0$ belonging to A of order n^2 over F to equations of degree n, and shall say that such a $\phi(\omega)=0$ *properly belongs to A*.

Let $\phi(\omega)=0$ properly belong to A and let ξ be a quantity such that $\phi(\xi)=0$ so that $F(\xi)$ is an algebraic field of order n over F. Consider the algebra $A'=A\times F(\xi)$ where ξ is therefore taken to be a quantity which is *scalar* with respect to all quantities of A. J. H. M. Wedderburn has proved† that A, an algebra of order n^2 over F, is equivalent to an algebra of n-rowed square matrices with elements in $F(\xi)$. The n^2 basal quantities of A are equivalent to n^2 matrices which are linearly independent in $F(\xi)$ and hence form a basis of the set of all n-rowed square matrices with elements in $F(\xi)$. Thus $A'=A\times F(\xi)=M\times F(\xi)$, where M is a total matric algebra of order n^2 over F, for this latter algebra is evidently equivalent to the set of all n-rowed square matrices with elements in $F(\xi)$.

THEOREM 11. *Let A be a normal division algebra of order n^2 over F and let $\phi(\omega)=0$ be an equation which properly belongs to A. Consider the algebra $A'=A\times F(\xi)$ where $\phi(\xi)=0$. Then*

$$A' = A \times F(\xi) = M \times F(\xi), \tag{1}$$

where M is a total matric algebra of order n^2 over F.

Let $\phi(\omega)=0$ properly belong to A of order n^2 over F. Let B be a normal simple algebra of order n^2 over F and let B contain ξ satisfying $\phi(\xi)=0$. The direct product $A\times B$ has (1) as a sub-algebra, and hence M as a sub-algebra. By Theorem 3 we have

$$A \times B = M \times C,$$

where C is a sub-algebra of $A\times B$. By Theorem 5 the algebra $A\times B$ is a normal simple algebra, so that, by Theorem 6, C is a normal simple algebra. The

* Cf. the author's *Note on an important theorem on normal division algebras*, Bulletin of the American Mathematical Society, vol. 36 (1930), pp. 649–650.

† These Transactions, vol. 22 (1921), pp. 129–135; p. 133.

order of $A \times B$ is n^4, the order of M is n^2, so that the order of C is n^2. Algebra C is obviously the set of all quantities of $A \times B$ which are commutative with all the quantities of M. Hence C contains ξ.

THEOREM 12. *Let A be a normal division algebra of order n^2 over F and let $\phi(\omega)=0$ of degree n belong to A. Suppose that B is a normal simple algebra of order n^2 over F and that ξ in B is such that $\phi(\xi)=0$. Then*

$$A \times B = M \times C, \tag{2}$$

where M is a total matric algebra of order n^2 over F and C is a normal simple algebra of order n^2 over F and contains ξ.

We shall now study the general theory of the extension of F by η. In the author's proof of his Theorem $T4$ the following result was obtained.

THEOREM 13. *Let B be an algebra over F and let there exist an algebraic field $F(\xi)$ such that $B'=B\times F(\xi)$ is a total matric algebra over $F(\xi)$. Then B is a normal simple algebra over F.*

We shall apply the above result as follows. Let $F(\eta)$ be an algebraic field over F and consider the algebra $B=A\times F(\eta)$ over $F(\eta)$. The algebra $B'=B \times K(\xi)$ is an algebra over $K(\xi)$ where $K=F(\eta)$ and, when considered as an algebra over F, contains $A\times F(\xi)=M\times F(\xi)$ as a sub-algebra. It is thus evident that $B'=M\times F(\xi, \eta)=M'$, a total matric algebra over $K(\xi)$. By Theorem 13, algebra B is a normal simple algebra over $K=F(\eta)$.

LEMMA 1. *Let $A'=A\times F(\eta)$ where A is a normal division algebra. Then A' is a normal simple algebra over $F(\eta)$.*

By Theorem 4 algebra $A'=A\times F(\eta)$ is expressible in the form $A'=H'\times B$ where H' is a total matric algebra of order s^2 over $F(\eta)$ and B is a normal division algebra of order t^2 over its centrum $F(\eta)$. Evidently A' is a simple algebra over F and, when considered over F, $A'=H\times B$ where H is a total matric algebra of order s^2 over F and B is a division algebra of order t^2r over F such that r is the order of $F(\eta)$. Also, since A' has order n^2 over $F(\eta)$ we have $st=n$.

LEMMA 2. *Algebra $A'=A\times F(\eta)=H\times B$, where H is a total matric algebra of order s^2 over F and B is a division algebra of order t^2r over F which is a normal division algebra of order t^2 over its centrum $F(\eta)$ of order r over F such that $s^2t^2=n^2$, the order of the normal division algebra A over F.*

Consider the equation

$$\psi(\omega) \equiv \omega^r + \alpha_1\omega^{r-1} + \cdots + \alpha_r = 0 \;\; (\alpha_i \text{ in } F), \tag{3}$$

irreducible in F. It is well known that the r-rowed square matrix

$$\eta = \left\| \begin{matrix} 0 & 0 \cdots 0 & -\alpha_r \\ 1 & 0 \cdots 0 & -\alpha_{r-1} \\ 0 & 1 \cdots 0 & -\alpha_{r-2} \\ \cdot & \cdot \quad \cdot \quad \cdot & \cdot \\ 0 & 0 \cdots 0 & -\alpha_2 \\ 0 & 0 \cdots 1 & -\alpha_1 \end{matrix} \right\| \tag{4}$$

has $\psi(\omega)=0$ as its characteristic equation $|\omega I-\eta|=0$, where I is the r-rowed identity matrix. Hence if $F(\eta)$ is any algebraic field of order r we may assume that η is a quantity in a total matric algebra G of order r^2 over F.

Consider the normal simple algebra $A\times G$. By Lemma 2 this algebra has $A'=H\times B$ as a sub-algebra, where H is a total matric algebra of order s^2 over F. By Theorem 3, $A\times G=H\times C$, where C is a normal simple algebra. By Theorem 4 we may write $C=D\times K$ where D is a normal division algebra and K is a total matric algebra. Hence

$$A \times G = D \times (H \times K). \tag{5}$$

By Theorem 1 algebra $H\times K$ is a total matric algebra. By the uniqueness in Theorem 2 algebra A is equivalent to D and G to $H\times K$. If the order of K is e^2, then r^2, the order of G, is equal to s^2e^2. Hence s divides r as well as n.

THEOREM 14. *Let A be a normal division algebra of order n^2 over F, and let $F(\eta)$ be an algebraic field of order r over F. Then*

$$A \times F(\eta) = H \times B, \tag{6}$$

where H is a total matric algebra of order s^2 over F and B is a division algebra of order t^2r over F such that

$$n = st, \quad r = se, \tag{7}$$

and the integer s divides both r and n. Algebra B is a normal division algebra of order t^2 over $F(\eta)$.

We shall use the above theorem and its consequences repeatedly in our theory. In particular we have as immediate corollaries

THEOREM 15. *If $A\times F(\eta)=H\times F(\eta)$, then the order n^2 of A is a divisor of r^2.*

THEOREM 16. *If r and n are relatively prime, then $A\times F(\eta)$ is a division algebra.*

THEOREM 17. *If $A\times F(\eta)$ is a total matric algebra of order n^2 over $F(\eta)$ and r is prime to n, then $n=1$.*

We may now obtain two results of intrinsic interest but which will not be used in our later work. We have shown that $A\times G=H\times C$ where G is a total matric algebra of order $r^2=s^2e^2$. But then $G=H_1\times K_1$ where H_1 is equivalent to H and K_1 to K in (5), by Theorem 1. Since A is equivalent to D and K_1 to K, the algebra $A\times K_1$ is equivalent to $D\times K=C$. But C contains the sub-algebra B of Theorem 14, since C is the algebra of all quantities of $A\times G$ commutative with all the quantities of H, while $A\times F(\eta)=H\times B$. Hence we have

THEOREM 18. *Let A and $F(\eta)$ be as in Theorem 14, so that $r=es$. Then there exists a total matric algebra K of order e^2 over F such that $A\times K$ contains an algebra equivalent to B as a sub-algebra.*

In particular let $r=p$, a prime. If $A\times F(\eta)=A'$ is a division algebra, then, by Theorem 9, A contains no x whose minimum equation is that of η and hence reducible in $F(\eta)$. Conversely let A contain no x satisfying $\psi(\omega)=0$, the minimum equation of η. Since r is a prime, $s=1$ or p. If $s=p$ then $e=1$, and, by Theorem 18, A contains a sub-algebra equivalent to B and hence a quantity x satisfying $\psi(\omega)=0$, the minimum equation of η, a quantity of B. Hence $s=1$ and A' is a division algebra. As a corollary of Theorem 18 we thus have

COROLLARY. *Let A be a normal division algebra of order n^2 over F and $F(\eta)$ an algebraic field of order p, a prime. Then $A\times F(\eta)$ is a division algebra if and only if A contains no quantity satisfying the minimum equation of η with respect to F.*

4. **Applications of the Galois theory of equations.** We shall require the well known theorems*

LEMMA 1. *Every rational function η with coefficients in F of the roots of an equation having the group Γ for F belongs to a definite sub-group Δ of Γ. There exist functions belonging to any assigned sub-group of Γ.*

LEMMA 2. *If the rational function η with coefficients in F of the roots of an equation having the group Γ for F belongs to a sub-group Δ of index r under Γ, then the substitutions of Γ replace η by exactly r distinct functions called the conjugates of η under Γ. They are the roots of an equation $\psi(\omega)=0$ of degree r with coefficients in F which is irreducible in F.*

LEMMA 3. *Let Γ be the group for F of an equation $\phi(\omega)=0$ with coefficients in F. Let Δ be the sub-group to which belongs a rational function η with coefficients in F of the roots of $\phi(\omega)=0$. By the adjunction of η to F the group of $\phi(\omega)=0$ is reduced from Γ to Δ.*

* Cf. L. E. Dickson's *Modern Algebraic Theories*, Chicago, 1926, pp. 170–174, for these Lemmas.

We shall frequently use the very well known

SYLOW'S THEOREM. *If the order g of a substitution group Γ is divisible by a power p^ν of a prime p, then Γ has a sub-group Δ of order p^ν.*

Let Γ be a transitive group on p letters, where p is a prime. Then g is divisible by p and Γ has a sub-group Δ of order p. Every substitution s may be written as a product of cycles involving *different* letters and the order of s is the least common multiple of the number of letters in each cycle. If s is not the identity substitution and is in Δ of order p on p letters, the order of s is a divisor of p and must be p. Since p is the L.C.M. of the number of letters in the individual cycles of s, these cycles must all have p letters. But the letters in different cycles are different, and there are p letters altogether, so that s is a single cycle $(123 \cdots p)$. The group Δ contains the substitutions $1, s, s^2, \cdots, s^{p-1}$ and hence is composed solely of these substitutions. Thus Δ is the regular cyclic group of order p.

LEMMA 4. *Every transitive group Γ on p letters, p a prime, contains the regular cyclic group Δ of order p whose substitutions may be taken to be $1, s, s^2, \cdots, s^{p-1}$ where $s=(123 \cdots p)$.*

We may obviously apply Lemmas 1, 2, 3 to any equation belonging to A, a normal division algebra over F. In our environment they become

THEOREM 19. *Let $\phi(\omega)=0$ belong to a normal division algebra A over F and let Γ be the group for F of $\phi(\omega)=0$. Then if Δ is a sub-group of Γ of index r under Γ there exists an algebraic field $F(\eta)$ of order r over F such that in $A'=A\times F(\eta)$ over $F(\eta)$ the group of ϕ for $F(\eta)$ is Δ.*

We shall first apply this theorem to the case where A has order p^2, p a prime. Let $\phi(\omega)=0$ have degree p and belong to A, so that the group Γ of $\phi(\omega)=0$ for F is transitive and has order pr. By Lemma 4 the group Γ has a regular cyclic sub-group Δ of order p and index r. The order rp of Γ divides $p!$ so that r divides $(p-1)!$ and is prime to p. By Theorem 19 there exists an algebraic field $F(\eta)$ of order r such that the group of $\phi(\omega)=0$ for $F(\eta)$ is Δ. By Theorem 16 algebra $A'=A\times F(\eta)$ is a normal division algebra over $F(\eta)$. The quantity x in A whose minimum equation is $\phi(\omega)=0$ is in A' and satisfies an equation with cyclic regular group for $F(\eta)$. The equation $\phi(\omega)=0$ is a cyclic equation for $K=F(\eta)$, the field $K(x)$ is a cyclic normal field, and A' is a cyclic (Dickson) normal division algebra over K.

THEOREM 20. *Let A be a normal division algebra of order p^2 over F, p a prime. Then there exists an algebraic field $F(\eta)$ of order r over F such that r divides $(p-1)!$ and is prime to p and such that the algebra $A'=A\times F(\eta)$ is a cyclic (Dickson) normal division algebra of order p^2 over $F(\eta)$.*

We shall next obtain an important theorem for the case where n is not the power of a single prime. Let $n=p^eq$ where p is a prime, $e>0$, and $q>1$ is not divisible by p. Consider a normal division algebra A of order n^2 over F and let $\phi(\omega)=0$ belong properly to A, that is, have degree n and be the minimum equation for F of x in A. The group Γ of $\phi(\omega)=0$ has order g divisible by n since Γ is transitive. Hence g is divisible by p and we may write $g=p^\nu r_1$ where r_1 is prime to p. By Sylow's Theorem the group Γ has a sub-group Δ of order p^ν and, by Theorem 19, there exists a scalar η_1 of grade r_1 such that the group of $\phi(\omega)=0$ for $F(\eta)$ is Δ. By Theorem 14, $A\ =A\times F(\eta)=H_1\times B_1$ where H_1 is a total matric algebra of order s^2 over F and B_1 is a normal division algebra of order t^2 over $F(\eta)$ such that $n=st$, $r=se$. Since r is prime to p so is s_1. Also A' is not a division algebra, by Theorem 9, since $\phi(\omega)=0$ belongs to A, has degree n and group Δ of order $p^e<n$ for $F(\eta_1)$, an intransitive group. Since $s_1t_1=n$ and s_1 is prime to p, we may write $t_1=p^eq_1$ where q_1 is prime to p and $q_1<q$. If $q_1>1$ we apply the same process to B_1 over $F(\eta_1)=F_1$ to obtain a scalar η_2 such that $B_1\times F_1(\eta_2)=H_2\times B_2$ where H_2 is a total matric algebra of order s_2^2 over F_1 and B_2 is a normal division algebra of order t_2^2 such that $t_2=p^eq_2$ with $1\leqq q_2<q_1$. The field $F_1(\eta_2)=F(\eta_1, \eta_2)$ has order r_1r_2 prime to p with respect to F. We define in this way a sequence of scalars $\eta_1, \eta_2, \eta_3, \cdots$, a sequence of integers $r_1, r_2, \cdots$, and a decreasing sequence of integers $q>q_1>q_2>\cdots\geqq 1$. This latter sequence must terminate at some $q_k=1$, and if $F_k=F_{k-1}(\eta_k)=F(\eta_1, \eta_2, \cdots, \eta_k)$, then $F_k=F(\eta)$, an algebraic field of order $r=r_1r_2\cdots r_k$ over F such that $A\times F(\eta)=H\times B$, where H is a total matric algebra of order $s^2=s_1^2s_2^2\cdots s_k^2=q^2$ and B is a normal division algebra of order $p^{2e}q_k^2=p^{2e}$ over $F_k=F(\eta)$.

THEOREM 21. *Let A be a normal division algebra of order n^2 over F, where*

$$n = p^eq, \quad e > 0, \quad q > 1,$$

and p is a prime not dividing q. Then there exists an algebraic field $F(\eta)$ of order r over F such that r is prime to p and

$$A \times F(\eta) = H \times B,$$

where H is a total matric algebra of order q^2 over F and B is a normal division algebra of order p^{2e} over its centrum $F(\eta)$.

We shall also require the well known theorems

LEMMA 5. *Let η and ζ be rational functions with coefficients in F of the scalar roots of an equation whose group for F is Γ, and let both η and ζ belong to the same sub-group Δ of Γ. Then each of η and ζ is expressible as a rational function with coefficients in F of the other.*

LEMMA* 6. *Let* Γ *be a group of order* p^ν, p *a prime, and let* Γ_s *have order* p^s *and be contained in* Γ. *Then* Γ_s *is an invariant sub-group of index* p *of a sub-group* Δ *of* Γ.

Let now $\phi(\omega)=0$ have degree p^e, coefficients in F and a transitive group Γ of order p^ν for F. Let η be a scalar root of $\phi(\omega)=0$ and let Γ_s of order p^s be the sub-group of Γ to which η belongs. By Lemma 6 there exists a sub-group Δ of order p^{s+1} of Γ which contains Γ_s self-conjugately. The group Δ contains a substitution g not in Γ_s and the cycle of g containing η has order q a power of p, and replaces η by a root η_2 of $\phi(\omega)=0$, a conjugate to η under Δ. The root η_2 belongs to $g^{-1}\Gamma_s g=\Gamma_s$ since Γ_s is self-conjugate under Γ_s. Hence $\eta_2=\theta(\eta)$ by Lemma 5, where $\theta(\eta)$ is a polynomial in η with coefficients in F. The substitutions $I, g, g^2, \cdots, g^{q-1}$ are all in the group Δ and replace η by $\theta^i(\eta)$ respectively. These q polynomials are all conjugates to η under Δ, while there are exactly p such conjugates to η under Δ, since the index of Γ_s is p. Since q is a power of p, q is p and

$$\theta^p(\eta) = \theta^0(\eta) = \eta, \; \theta(\eta), \; \theta^2(\eta), \cdots, \theta^{p-1}(\eta)$$

are distinct and satisfy $\phi(\omega)=0$. They are all in $F(\eta)$. Passing to any field $F(x)$ equivalent to $F(\eta)$ we have

LEMMA 7. *Let* x *satisfy* $\phi(\omega)=0$ *whose group for* F *is a transitive group of order* p^e, p *a prime. Then* $F(x)$ *contains a quantity* $\theta(x)$ *such that*

$$\theta^p(x) = \theta^0(x) = x, \; \theta(x), \cdots, \theta^{p-1}(x)$$

are p *distinct roots of* $\phi(\omega)=0$.

Consider now the set of all quantities of $F(x)$ symmetric in the polynomials $\theta^i(x)$. This set evidently forms a sub-field $F(y)$ of $F(x)$. The equation

$$\psi(\omega) \equiv [\omega - \theta^{p-1}(x)] \cdots [\omega - \theta(x)][\omega - x]$$

evidently has coefficients in $F(y)$ and is also evidently not reducible in $F(y)$. Hence x has grade p with respect to $F(y)$ and $F(x)$ is a cyclic field of order p over $F(y)$.

THEOREM 22. *Let* $\phi(\omega)=0$ *have degree* p^e, *coefficients in* F, *and a transitive group of order a power of* p *with respect to* F *where* p *is a prime. Then if* x *is a quantity satisfying* $\phi(\omega)=0$ *the field* $F(x)$ *of order* p^e *over* F *contains a sub-field* $F(y)$ *of order* p^{e-1} *over* F *such that* $F(x)$ *is a cyclic field of order* p *over* $F(y)$.

Let now A be a normal division algebra of order p^{2e}, p a prime, and let x in A have grade p^e and $\phi(\omega)=0$ as its minimum equation for F. Let the group of

* Cf. Burnside, *The Theory of Groups*, Cambridge, 1897, pp. 64–65.

$\phi(\omega)=0$ have order $p^{\nu}r_1$ where r_1 is prime to p. As in the proof of Theorem 21 there exists an algebraic field $F_1=F(\eta_1)$ of order r_1 over F such that the group of $\phi=0$ for F_1 is a group Γ of order p^{ν}. By Theorem 14 the algebra $A'=A\times F(\eta_1)$ is a normal division algebra over $F(\eta_1)$, so that, by Theorem 9, the equation $\phi(\omega)=0$ is irreducible in $F(\eta_1)$, and Γ is a transitive group. We may therefore apply Theorem 22 and obtain the existence of a quantity y in $F_1(x)$ such that this field is a cyclic field of order p over $F_1(y)$ of order p^{e-1}. Apply this same process to the minimum equation of y with respect to F_1. We obtain the existence of a quantity η_2 of grade r_2 prime to p with respect to $F(\eta_1)=F_1$ such that the algebra $A''=A'\times F_1(\eta_2)$ is a normal division algebra over $F_2=F(\eta_1, \eta_2)=F_1(\eta_2)$ and the field $F_2(y)$ contains a sub-field $F_2(z)$ of order p^{e-2} with respect to F_2 and is a cyclic field of order p over this field. It is evident that the field $F_2(x)$ is a cyclic field over $F_2(y)$. Continuing in this fashion we obtain

THEOREM 23. *Let A be a normal division algebra of order p^{2e} over F, p a prime, and let x in A have grade p^e with respect to F. Then there exists an algebraic field $K=F(\eta)$ of order r prime to p with respect to F such that*

$$A' = A \times F(\eta)$$

is a normal division algebra over K, the algebraic field $K(x)$ has order p^e over K, and there exist quantities

$$x = x_e,\ x_{e-1}, \cdots, x_1$$

in $K(x)$ such that if

$$K_0 = K,\ K_i = K(x_i) \qquad (i = 1, 2, \cdots, e),$$

then K_i has order p^i with respect to K and is a cyclic field of order p over K_{i-1}. In particular A' contains a cyclic field $K(x_1)$ of order p over K.

5. **Cyclic algebras**. Let $\phi(\omega)=0$ have degree n, coefficients in F, and have the cyclic regular group for F. Then if x is a quantity satisfying $\phi(x)=0$ the algebraic field $F(x)$ is a normal cyclic field of order n over F, and there exists a quantity $\theta(x)$ in $F(x)$ such that if we define by induction

$$\theta^0(x) = x,\ \theta^k(x) = \theta[\theta^{k-1}(x)] \qquad (k = 1, \cdots),$$

then

$$\theta^n(x) = x,$$

and

$$\phi(\omega) \equiv [\omega - \theta^{n-1}(x)] \cdots [\omega - \theta(x)](\omega - x).$$

Consider an algebra A over F with the basis

(8) $$x^\alpha y^\beta \qquad (\alpha, \beta = 0, 1, \cdots, n-1),$$

and the multiplication table

$$(9)\qquad \phi(x) = 0,\ y^n = \gamma \text{ in } F,\ y^\beta f(x) = f[\theta^\beta(x)]y^\beta \qquad (\beta = 0, 1, \cdots),$$

for every $f(x)$ of $F(x)$. Such an algebra is always associative and is the *general Dickson algebra*. We shall say that a Dickson algebra is a *cyclic* algebra when it is a ***normal simple algebra***. The field F, the equation $\phi=0$, the particular polynomial $\theta(x)$ in (9), and the quantity γ in F formally define A, and we shall use the notation

$$A = F[\phi, \theta, \gamma].$$

Let $\gamma=0$ so that $y^n=0$ and $y\neq 0$ is a nilpotent quantity of A. If $a=\sum_{\alpha=0}^{n-1}a_\alpha(x)y^\alpha$ is any quantity of A then

$$(10)\qquad (ay)^n = by^n = 0.$$

For

$$y^\beta a = y^\beta \sum_{\alpha=0}^{n-1} a_\alpha(x)y^\alpha = \left(\sum_{\alpha=0}^{n-1} a_\alpha[\theta^\beta(x)]y^\alpha\right)y^\beta$$

and we may carry the n factors y in $(ay)^n$ to the right and obtain (10) with b in A. It follows that ay is nilpotent in A for every a of A. Hence y is ***properly*** nilpotent in A and A contains a ***radical***. Hence A is not even a semi-simple algebra and is not a cyclic algebra.

Let next $\gamma\neq 0$ and ξ be a scalar quantity with respect to quantities of A such that $\phi(\xi)=0$. Then Wedderburn has shown* that $A\times F(\xi)=M\times F(\xi)$ where M is a total matric algebra, so that, by Theorem 13, A is a normal simple algebra. We thus have

THEOREM 24. *A Dickson algebra is a cyclic algebra if and only if* $\gamma\neq 0$.

Professor Wedderburn in fact actually obtained formulas for the quantities of A in terms of those of M and conversely. He used a form of A reciprocal to ours and we shall use, instead, the form of L. E. Dickson.† Every quantity f of A has the form

$$f = f_0(x) + f_1(x)y + \cdots + f_{n-1}(x)y^{n-1}.$$

Let ξ be as above, and write

$$f_i \equiv f_i(\xi),\ f_i(\theta^\alpha) \equiv f_i[\theta^\alpha(\xi)].$$

Then if we let the quantities of $M\times F(\xi)$ be represented by matrices, the quantity f of A will be represented by

---

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

† *Algebren und ihre Zahlentheorie*, Zurich, 1927, p. 68, equation 54.

$$(11)\qquad \left\| \begin{array}{llll} f_0 & f_1 & f_2 & \cdots f_{n-1} \\ f_{n-1}(\theta)\gamma & f_0(\theta) & f_1(\theta) & \cdots f_{n-2}(\theta) \\ f_{n-2}(\theta^2)\gamma & f_{n-1}(\theta^2)\gamma & f_0(\theta^2) & \cdots f_{n-3}(\theta^2) \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot \\ f_1(\theta^{n-1})\gamma & f_2(\theta^{n-1})\gamma & f_3(\theta^{n-1})\gamma & \cdots f_0(\theta^{n-1}) \end{array} \right\| .$$

We require the representation of the basal quantities of M in terms of the quantities of $A \times F(\xi)$. Let then e_{ij} be the quantity of M which corresponds to the matrix with unity in the ith row and jth column and zeros elsewhere, so that the n^2 quantities e_{ij} are a basis of M with respect to F. The quantity x has the form above with $f_0(x)=1$ and all the other f's zero, while $y=0+y+0$. Hence (11) implies that

$$(12)\qquad x = \sum_{i=1}^{n} \xi_i e_{ii}, \quad y = e_{12} + e_{23} + \cdots + e_{n-1,n} + \gamma e_{n,1},$$

where we define

$$(13)\qquad \xi_i = \theta^{i-1}(\xi) \qquad (i = 1, \cdots, n).$$

By a very easy computation the quantity $(x-\xi_1)\ (x-\xi_2) \cdots (x-\xi_{i-1})$ $(x-\xi_{i+1}) \cdots (x-\xi_n)$ has zero for the coefficients of all the e_{kj} except e_{ii} itself, and, in fact,

$$(14)\qquad e_{ii} = \frac{(x - \xi_1)(x - \xi_2) \cdots (x - \xi_{i-1})(x - \xi_{i+1}) \cdots (x - \xi_n)}{(\xi_i - \xi_1)(\xi_i - \xi_2) \cdots (\xi_i - \xi_{i-1})(\xi_i - \xi_{i+1}) \cdots (\xi_i - \xi_n)} .$$

From (12) we obtain

$$(15)\qquad e_{ii} y = e_{i,i+1} = y e_{i+1,i+1} \qquad (i = 1, 2, \cdots),$$

under the assumption that subscripts are reduced modulo n when they exceed n. In particular

$$(16)\qquad e_{11} y = y e_{22},$$

where we shall require the form of

$$(17)\qquad \begin{aligned} e_{11} &= \frac{(x - \xi_2)(x - \xi_3) \cdots (x - \xi_n)}{(\xi_1 - \xi_2)(\xi_1 - \xi_3) \cdots (\xi_1 - \xi_n)}, \\ e_{22} &= \frac{(x - \xi_3)(x - \xi_4) \cdots (x - \xi_n)(x - \xi_1)}{(\xi_2 - \xi_3)(\xi_2 - \xi_4) \cdots (\xi_2 - \xi_n)(\xi_2 - \xi_1)} . \end{aligned}$$

From y^k in (11) we obtain

$$e_{11}y^k = e_{1k},\ \ \gamma e_{k1} = y^{n+1-k}e_{11}, \tag{18}$$

where we are using always

$$e_{ij}e_{jk} = e_{ik},\ \ e_{ij}e_{tk} = 0 \qquad (j \neq t;\ i, j, k, t = 1, 2, \cdots, n). \tag{19}$$

Since $\gamma \neq 0$ has an inverse γ^{-1} in F we have finally $e_{ij} = e_{i1}e_{1j}$ and, from (18),

$$e_{ij} = \gamma^{-1}y^{n+1-i}e_{ii}y^{j-1} \qquad (i, j = 1, \cdots, n). \tag{20}$$

We shall apply the form obtained in (20) as follows. Let $A = F[\phi, \theta, \gamma_1]$ and $B = F[\phi, \theta, \gamma_2]$ be two cyclic algebras differing only in their quantites γ. We shall use (8) as a notation for the basis of A with $y^n = \gamma$, and, correspondingly, for a basis and multiplication tables of B shall use

$$B = (\xi^\alpha \eta^\beta) \qquad (\alpha, \beta = 0, 1, \cdots, n-1), \tag{21}$$

$$\phi(\xi) = 0,\ \ \eta^n = \gamma_2,\ \ \eta^\beta f(\xi) = f[\theta^\beta(\xi)]\eta^\beta \qquad (\beta = 0, 1, \cdots), \tag{22}$$

so that if $\xi_i = \theta^{i-1}(\xi)$ then

$$\eta\xi_i = \xi_{i+1}\eta \qquad (i = 1, 2, \cdots, n), \tag{23}$$

where $\xi_{n+1} = \xi$. We shall consider the algebra

$$C = A \times B, \tag{24}$$

which contains $A \times F(\eta) = M \times F(\eta)$ as a sub-algebra, where M is the total matric algebra whose basis is given by (20), (17), with (16) holding. By Theorem 3 algebra C is expressible in the form

$$C = M \times D, \tag{25}$$

where D is the algebra of all quantities of C which are commutative with all the quantities of M and obviously contains $F(\xi)$. Also D contains

$$z = y\eta = \eta y. \tag{26}$$

For from (23) and (17) it is obvious that

$$\eta e_{11} = e_{22}\eta. \tag{27}$$

But (16) states that $ze_{11} = y(\eta e_{11}) = ye_{22}\eta = e_{11}z$. The quantity z is commutative with e_{11} and with y, and, since γ^{-1} is in F, with all of the quantities e_{ij} of (20), a basis of M. Hence z is in D.

We have thus shown that D contains ξ and z. Since D is an algebra over F it contains all the quantities

$$\xi^\alpha z^\beta \qquad (\alpha, \beta = 0, 1, \cdots, n-1), \tag{28}$$

where, since y is commutative with ξ and z, we have

$$(29) \qquad z^n = y^n\eta^n = \gamma_1\gamma_2, \quad z^\beta f(\xi) = f[\theta^\beta(\xi)]z^\beta \qquad (\beta = 0, 1, \cdots),$$

for every $f(\xi)$ in $F(\xi)$. The quantity z is merely a scalar multiple $y\eta$ of η, with respect to B, since y is scalar with respect to B. When (21) form a basis of B, the quantities (28) are thus linearly independent in F, and in fact in $F(y)$. Algebra D has order n^2 from Theorem 3 so that (28) form a basis of D, and the multiplication table of D is (29). Since $\gamma_1 \neq 0$, $\gamma_2 \neq 0$, the quantity $\gamma_1\gamma_2 \neq 0$ and D is the cyclic algebra $F[\phi, \theta, \gamma_1\gamma_2]$. We have proved

THEOREM 25. *Let $A = F[\phi, \theta, \gamma_1]$ and $B = F[\phi, \theta, \gamma_2]$ be cyclic algebras with the same ϕ, θ, and order n^2 and thus differing possibly only in their quantities γ. Then*

$$(30) \qquad A \times B = M \times C,$$

where M is a total matric algebra of order n^2 over F and C is the cyclic algebra $F[\phi, \theta, \gamma_1\gamma_2]$.

6. **Direct powers of normal simple algebras.** If A is any normal simple algebra over F and B is equivalent to A, then we can form the direct product $A \times B$ in such a fashion that A and B are sub-algebras of $A \times B$, by passing to equivalent algebras. We may evidently represent such a direct product symbolically by $A \times A$ where, in view of the direct product symbol, the two letters A mean merely *equivalent* algebras. As a generalization we may define the *direct power**

$$(31) \qquad A^{\alpha+1} = A \times A^\alpha = A^\alpha \times A \qquad (\alpha = 1, 2, \cdots),$$

by an obvious induction on α, where $A = A^1$. The powers here behave like ordinary powers of integers, as in a direct product we have commutativity and associativity of the symbols representing algebras, so that

$$(32) \qquad A^\alpha \times A^\beta = A^{\alpha+\beta}, \quad A^\alpha \times B^\alpha = (A \times B)^\alpha, \quad A \times B = B \times A,$$

for any normal simple algebras (in fact for any algebras) A and B. By Theorem 12 we have

$$A^2 = M \times B_1,$$

where M is as in (2) and B_1 is a normal simple algebra. By Theorem 12 algebra B_1 contains a quantity ξ whose minimum equation with respect to

* We shall use the notation of direct power so frequently in the following theory that to alter the above even slightly would make the work less clear and the printing too bulky. Hence although the symbol of (31) is customarily used in linear algebra theory to mean ordinary product, this meaning will not occur in the present paper. We shall then assume that the symbol of (31) represents throughout *direct power*.

F has degree n and belongs to A, a normal division algebra of order n^2 over F. Again by Theorem 12 we have $A^3 = M \times (A \times B_1) = M \times M \times B_2 = M^2 \times B_2$, where B_2 is a normal simple algebra of order n^2 over F and also contains ξ. In general we have

$$A^\alpha = M^{\alpha-1} \times B_{\alpha-1} \qquad (\alpha = 2, 3, \cdots). \tag{33}$$

But $B_{\alpha-1}$ is a normal simple algebra and we may write

$$B_{\alpha-1} = H_\alpha \times A_\alpha, \tag{34}$$

where A_α is a normal division algebra of order t_α^2 over F and H_α is a total matric algebra of order s_α^2 over F such that $s_\alpha t_\alpha = n$.

THEOREM 26. *Let A be a normal division algebra of order n^2 over F and M be a total matric algebra of order n^2 over F. Then the direct power*

$$A^\alpha = (M^{\alpha-1} \times H_\alpha) \times A_\alpha \qquad (\alpha = 2, 3, \cdots), \tag{35}$$

where H_α is a total matric algebra of order s_α^2 over F and A_α is a normal division algebra of order t_α^2 over F such that the relation

$$s_\alpha t_\alpha = n \tag{36}$$

holds.

Suppose that A were a normal division algebra for which $t_\alpha = 1$ for some integer* α. In this case $A^\alpha = M^\alpha$, a total matric algebra. We shall say that when such an integer α exists the least integer ρ for which A^ρ is a total matric algebra is the *exponent* of A.

7. **Algebras of order p^2, p a prime.** Let first A be any cyclic algebra of order p^2, p a prime, over F. The author has shown that a necessary and sufficient condition† that A be a division algebra is that γ be not the norm, $N(a)$, of any a in $F(x)$, and also that this condition was equivalent† to the condition that $\gamma^\alpha \neq N(a)$ $(\alpha = 1, 2, \cdots, p-1)$. Hence if $A = F[\phi, \theta, \gamma]$, then the algebras $F[\phi, \theta, \gamma^\alpha]$ $(\alpha = 1, 2, \cdots, p-1)$ are also normal division algebras. But in Theorem 23 we have $A \times A = A^2 = M \times A_2$ where $A_2 = F[\phi, \theta, \gamma^2]$ is a normal division algebra. Similarly $A^3 = M^2 \times A_3 = M^2 \times F[\phi, \theta, \gamma^3]$, and in general

$$A^\alpha = M^{\alpha-1} \times A_\alpha, \quad A^p = M^{p-1} \times B,$$

where $B = F[\phi, \theta, \gamma^p]$ is a cyclic algebra by Theorem 22, and $A_\alpha = F[\phi, \theta, \gamma^\alpha]$ is a normal division algebra for $\alpha = 1, \cdots, p-1$. Algebra B is not a division algebra since $\gamma^p = N(\gamma)$. Since B has order p^2, p a prime, Theorem 4 implies that $B = M$. We have proved the theorem

* We shall prove the existence of such an integer for any normal division algebra A in §8.

† These results are Theorems T 18, 19.

THEOREM 27. *Every cyclic division algebra A of order p^2 over F, p a prime, has p as its exponent ρ. Thus*

$$A^\alpha = M^{\alpha-1} \times A_\alpha, \quad A^p = M^p \quad (\alpha = 2, 3, \cdots, p-1), \tag{37}$$

where A has the direct product sequence

$$A_1 = A, A_2, \cdots, A_{p-1}, A_p = F, \tag{38}$$

of normal division algebras A_α of orders p^2 over F except for A_p which has order unity.

Let next A be any normal division algebra of order p^2 over F, p a prime. By Theorem 26 we have

$$A^p = (M^{p-1} \times H_p) \times A_p, \tag{39}$$

where A_p has order t^2 and $p = st$ so that $t = 1$ or p. By Theorem 20 there exists an algebraic field $F(\eta)$ of order r prime to p such that if $A' = A \times F(\eta)$ then A' is a cyclic normal division algebra over $F(\eta)$. By Theorem 27 we have $(A')^p = (M')^p$ where $M' = M \times F(\eta)$ is a total matric algebra of order p^2 over $F(\eta)$. Evidently

$$(A')^p = (M^{p-1} \times H_p)' \times (A_p)' = (M')^p$$

in algebras over $F(\eta)$, where the meaning of the symbols is clear. But then, by Theorem 7, algebra $(A_p)'$ is a total matric algebra over $F(\eta)$, since so are $(M^{p-1} \times H_p)'$ and $(M')^p$. Since r is prime to p and the order of A_p is unity or p^2, Theorem 17 implies that $t_p = 1$, and A^p is a total matric algebra. If $A^\alpha = M^\alpha$ with $\alpha < p$, then $(A')^\alpha = (M')^\alpha$ where A' is a cyclic normal division algebra over $F(\eta)$, contrary to the proved fact that p is the exponent of A'. Hence p is the exponent of A.

THEOREM 28. *Every normal division algebra of order p^2 over F, p a prime, has p as its exponent ρ, such that*

$$A^\alpha = M^{\alpha-1} \times A_\alpha, \quad A^p = M^p \quad (\alpha = 2, 3, \cdots, p-1), \tag{40}$$

and algebra A has the direct product sequence

$$A = A_1, A_2, \cdots, A_{p-1}, A_p = F, \tag{41}$$

of normal division algebras of orders $p^2, p^2, \cdots, p^2, 1$ respectively.

8. **The general case.** Let A be a normal division algebra of order n^2 over F. We shall first treat the case $n = p^e$, p a prime. For $e = 1$ we have proved

LEMMA 1. *Let A be a normal division algebra of order p^{2e} over F, p a prime. Then if $n = p^e$, the algebra $A^n = M^n$ is a total matric algebra over F.*

Assume, then, as the basis of an induction on e that the lemma is true for $e<f$. Let then A have order p^{2f} and set $n=p^f$, $t=p^{f-1}$. We may form, from (35),

$$A^t = M^{t-1} \times H_t \times A_t,$$

where M and H_t are total matric algebras and A_t is a normal division algebra over F whose order is a power of p. By Theorem 24 there exists an algebraic field $K=F(\eta)$ of order r prime to p over F such that $A'=A\times F(\eta)$ is a normal division algebra over K and contains a quantity x of grade p with respect to K. In algebras over K we have then

$$(A')^t = (M')^{t-1} \times (H_t)' \times (A_t)',$$

and $(A_t)'$ is also a normal division algebra over K. Let ξ be a scalar root of the minimum equation of x with respect to K so that the algebra $A''=A'\times K(\xi)$ is not a division algebra over $K(\xi)$, and by Theorem 14 we have

$$A'' = G \times B,$$

where G is a total matric algebra of order p^2 and B is a normal division algebra of order p^{2f-2} over $K(\xi)$. By the assumption of our induction B^t is a total matric algebra. Hence, in algebras over $K(\xi)$,

$$(A'')^t = G^t \times B^t = (M'')^t \times (H_t)'' \times (A_t)''$$

is a total matric algebra. It follows from Theorem 7 that $(A_t)''=(A_t)'\times K(\xi)$ is a total matric algebra over $K(\xi)$. By Theorem 15 the order of $(A_t)'$ is 1 or p^2. Hence the order of A_t is 1 or p^2 and, in either case,

$$(A^t)^p = A^n = M^{pt-p} \times (H_t)^p \times (A_t)^p$$

is a total matric algebra M^n, by Theorem 28. Our induction is complete and Lemma 1 is proved.

Let next A have order n^2 where $n=p^eq$ and p is a prime, q is prime to p. If $q=1$ then $A^n=M^n$ as we have proved. Let then $q>1$ be prime to p, an arbitrary prime factor of n. Form

$$A^n = M^{n-1} \times H_n \times A_n,$$

where A_n is a normal division algebra whose order divides n^2. By Theorem 21 there exists an algebraic field $F(\eta)$ of order r prime to p such that $A'=A\times F(\eta)$ $=H\times B$ where H is a total matric algebra of order q^2 over F and B is a normal division algebra of order $t^2=p^{2e}$ over F. Then

$$(A')^n = H^n \times B^n = H^n \times (B^t)^q$$

is a total matric algebra over $F(\eta)$, by Lemma 1. Hence $(A_n)'$ is a total matric algebra. By Theorem 15 the order of A_n is a divisor of r and is prime to p. But p was any prime factor of n and hence the order of A_n, a divisor of n^2, is prime to n and is unity. We have

LEMMA 2. *Let A be a normal division algebra of order n^2 over F. Then A^n is a total matric algebra.*

We have thus proved very simply the existence of an exponent ρ for any A where ρ is the *least* integer for which A^ρ is a total matric algebra. Let $A^\alpha = M^\alpha$ be a total matric algebra and write the positive integer α in its form

$$\alpha = \lambda\rho + \mu, \quad 0 \leqq \mu < \rho.$$

The integer $\lambda \neq 0$ since ρ is the least integer α. If $\mu \neq 0$, then $A^\alpha = M^{\lambda\rho} \times A^\mu$ is a total matric algebra and hence A^μ is a total matric algebra, a contradiction of the definition of ρ. Hence $A^\alpha = M^\alpha$ *if and only if α is divisible by ρ.*

In particular ρ divides n by Lemma 2. Let $n = tq$ where $t = p^e$, p a prime and $q > 1$ is prime to p. Then, as in the proof of Lemma 2, we have $A' = A \times F(\eta) = H \times B$ where B is a normal division algebra of order t^2 over $F(\eta)$ and H is a total matric algebra of order q^2. Then $(A')^\rho = H^\rho \times B^\rho$ is a total matric algebra since so is A^ρ. Hence B^ρ is a total matric algebra and ρ is divisible by the exponent of B, a power of p. Hence ρ is divisible by every prime factor p of n.

LEMMA 3. *Let A be a normal division algebra of order n^2 over F. Then A has an exponent ρ whose prime factors coincide with those of n and which is a divisor of n.*

Consider the sequence of algebras

$$A = A_1, A_2, \cdots, A_{\rho-1}, A_\rho = F, \tag{42}$$

a set of normal division algebras A_i of order t_i^2 over F such that t_i divides n. Let A_i and A_j be any two algebras of this sequence and let $i+j \equiv k \pmod{\rho}$, where $0 < k \leqq \rho$, $i+j = \lambda\rho + k$. Then since $A_i \times A_j$ is a normal simple algebra from Theorem 5,

$$A^{i+j} = M^{i-1} \times H_i \times A_i \times M^{j-1} \times H_j \times A_j = M^{i+j-2} \times H_i \times H_j \times H \times B,$$

where H is a total matric algebra and B is a normal division algebra as in Theorem 4. But

$$A^{i+j} = A^{\lambda\rho+k} = M^{\lambda\rho+k-1} \times H_k \times A_k.$$

From the uniqueness in Theorem 2 algebra B is equivalent to A_k. Hence, in the sense of equivalence,

$$A_i \times A_j = H_{i,j} \times A_k, \tag{43}$$

where $H_{i,j}$ is a total matric algebra. It is also obvious that if $\alpha = \lambda\rho + k$, where $0 < k \leqq \rho$, then

$$A^\alpha = M^{\alpha-1} \times H_k \times A_k,$$

since $A^{\lambda\rho} = M^{\lambda\rho}$ and does not affect the H and A with subscripts k. We have proved

THEOREM 29. *Every normal division algebra A of order n^2 over F has an exponent ρ which divides n and which is divisible by every prime factor of n.* For every integer $\alpha \geqq 2$ we have*

$$\alpha = \lambda\rho + k, \quad 0 < k < \rho, \quad \lambda \geqq 0, \tag{44}$$

and, in the sense of equivalence,

$$A^\alpha = M^{\alpha-1} \times H_k \times A_k, \tag{45}$$

where A_k is the kth member of the direct product sequence

$$A_1 = A, A_2, \cdots, A_{\rho-1}, A_\rho = F \tag{46}$$

of A. The sequence (46) *is a set of normal division algebras A_i of orders t_i^2 respectively dividing n^2. If A_i and A_j are any two members of* (46) *such that*

$$i + j \equiv k \pmod{\rho}, \tag{47}$$

then, in the sense of equivalence,

$$A_i \times A_j = A_k \times H_{i,j}, \tag{48}$$

where $H_{i,j}$ is a total matric algebra.

Let us assume for the moment that two of the algebras A_i and A_j in (46) were equivalent. We may take $i < j$. Since A is in (46) we have

$$A_{\rho-i} \times A_i = H_i,$$

a total matric algebra in view of the fact that $A_\rho = F$. But when A_i and A_j are equivalent we have then $A_{\rho-i} \times A_j$ a total matric algebra while $\rho + j - i \not\equiv 0 \pmod{\rho}$, a contradiction of Theorem 29. Hence the algebras of (46) are all non-equivalent.

THEOREM 30. *The direct product sequence of any normal division algebra is composed of non-equivalent algebras.*

9. **The fundamental theorem.** We shall now prove R. Brauer's principal result on normal division algebras. Let A be a normal division algebra of order n^2 and exponent ρ over F, and suppose that $n = p^e q$, where q is not divisible by the prime p and is not unity. Write $\rho = \sigma\tau$, where

* The theorem to this point was first proved by Brauer.

$$\tau = p^\beta, \quad \sigma > 1,$$

and σ is prime to p. There exists a positive integer λ such that

$$\lambda\sigma \equiv 1 \pmod{\tau},$$

since σ is prime to p. Also there exists a positive integer μ such that

$$\mu\tau \equiv 1 - \lambda\sigma \pmod{\rho}$$

since the greatest common divisor τ of ρ and τ divides $1-\lambda\sigma$. Then

$$\lambda\sigma + \mu\tau = 1 + \nu\rho$$

where evidently $\nu > 0$. We form

$$A^{1+\nu\rho} = M^{\nu\rho} \times A = A^{\lambda\sigma} \times A^{\mu\tau}.$$

But if $\delta = \lambda\sigma$, then

$$A^{\lambda\sigma} = M^{\delta-1} \times H_\delta \times A_\delta,$$

where A_δ is a normal division algebra whose order divides n^2. But $A^{\delta\tau} = A^{\lambda\rho}$ is a total matric algebra so that $(A_\delta)^\tau$ is a total matric algebra and the exponent of A_δ is a divisor of $p^\beta = \tau$ and is a power of p. By Theorem 29 the order of A_δ is also a power of p, $p^{2\alpha}$. Similarly, if $\epsilon = \mu\tau$, then

$$A^{\mu\tau} = A^\epsilon = M^{\epsilon-1} \times H_\epsilon \times A_\epsilon,$$

where A_ϵ is a normal division algebra. As before $(A_\epsilon)^\sigma$ is a total matric algebra, the exponent of A_ϵ divides σ and is prime to p, and the order of A_ϵ is s^2, a divisor of q^2. Now

$$A^{1+\nu\rho} = M^{\nu\rho} \times A = M^{\delta+\epsilon-2} \times H_\delta \times H_\epsilon \times (A_\delta \times A_\epsilon).$$

By Theorem 8 the algebra $A_\delta \times A_\epsilon$ is a normal division algebra. By Theorem 2 algebra A is equivalent to the direct product $A_\delta \times A_\epsilon$. Since n is then equal to $p^\alpha s$, we have $\alpha = e$ and $s = q$. Using Theorem 8 we obtain

LEMMA 1. *Let A be a normal division algebra of order n^2 over F, $n = p^e q$, where p is a prime and $q > 1$ is prime to p. Then*

$$A = B \times C,$$

where B is a normal division algebra of order p^{2e} over F and C is a normal division algebra of order q^2 over F, and conversely.

Suppose that $A = B \times C = D \times E$ where B and D have the same order s^2 and C and E have the same order t^2 such that s and t are relatively prime integers. By Theorem T 12, there exists a normal division algebra B_0 of order s^2 over

F such that $B\times B_0$ is a total matric algebra.* Similarly there exists an algebra E_0 of order t^2 over F such that $E\times E_0$ is a total matric algebra. Then

$$A \times B_0 \times E_0 = (B \times B_0) \times (C \times E_0) = (D \times B_0) \times (E \times E_0).$$

But $C\times E_0 = H\times G$, where H is a total matric algebra and G is a normal division algebra whose order divides t^4, the order of $C\times E_0$. Similarly $D\times B_0 = Q\times S$, where Q is a total matric algebra and S is a normal division algebra whose order divides s^4. Since

$$(B \times B_0) \times H \times G = (E \times E_0) \times Q \times S,$$

it follows from Theorems 1 and 2 that G and S are equivalent and have the same order, a divisor of both s^4 and t^4. But s is prime to t so that this order is unity. Hence

$$C \times E_0 = H,\ \ D \times B_0 = Q,\ \ C \times (E_0 \times E) = H \times E,$$

where H and $E\times E_0$ are total matric algebras. By Theorem 2 algebra C is equivalent to E. Similarly algebra D is equivalent to B.

LEMMA 2. *Let A have order n^2 over F and let $n = st$ where s and t are relatively prime integers. Then A is expressible as a direct product $B\times C$ of a normal division algebra B of order s^2 and a normal division algebra C of order t^2 in only one way in the sense of equivalence.*

We now apply our two lemmas as follows. Let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} = p_1^{e_1} n_1,\ \ n_1 = p_2^{e_2} n_2,\ \ \cdots,\ \ n_{m-1} = p_{m-1}^{e_{m-1}} \cdot p_m^{e_m},$$

where the p_i are distinct primes. By Lemmas 1 and 2 we have $A = B_1\times C_1$ where B_1 has order $p_1^{2e_1}$ and C_1 has order n_1^2 in one and only one way in the sense of equivalence, and conversely. Also $C_1 = B_2\times C_2$, where B_2 has order $p_2^{2e_2}$ and C_2 has order n_2^2. Again this expression is unique, so that the expression $A = B_1\times B_2\times C_2$ is also unique. Finally we evidently obtain $C_{m-1} = B_{m-1}\times B_m$ in one and only one way in the sense of equivalence and $A = B_1\times B_2\times \cdots \times B_m$, a direct product of normal division algebras B_i of orders $p_i^{2e_i}$ respectively in one and only one way in the sense of equivalence, and conversely, by Theorem 8, every such direct product is a normal division algebra of order n^2.

FUNDAMENTAL THEOREM. *Write any positive integer n in its unique factored form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

* In fact if ρ is the exponent of B then B_0 is $B_{\rho-1}$.

where the p_i are distinct primes. Every normal division algebra A of order n^2 over F is expressible as a direct product

$$A = B_1 \times B_2 \times \cdots \times B_m$$

*of normal division algebras B_i of orders $p_i^{2e_i}$ respectively in one and only one way in the sense of equivalence, and conversely.**

This completely reduces the problem of the determination of all normal division algebras of order n^2 to the case where n is a power of a prime. In particular it furnishes a determination of all normal division algebras of orders 36 and 144 over F since all normal division algebras of order 16, 9, 4 are known.†

* Brauer did not obtain the converse of the above, an immediate consequence of our Theorem 8.

† Cf. the author's *A determination of all normal division algebras of order sixteen*, these Transactions, vol. 31 (1929), pp. 253–260. The above result for the case of algebras of order 36 over F evidently replaces completely the author's partial results on *Algebras of type R_2 in thirty-six units*, American Journal of Mathematics, vol. 52 (1930), pp. 283–292, and *On normal division algebras of type R in thirty-six units*, these Transactions, vol. 33 (1931), pp. 235–243.

University of Chicago,
Chicago, Ill.