ON DIVISION ALGEBRAS*

BY

O. C. HAZLETT

1. **Summary.** Linear algebras have been studied in great detail for many years, but they have usually been studied over a field F. In the papers by Dickson,[†] Cecioni,[‡] A. A. Albert[§] and others, a division algebra over a field F can be regarded as a division algebra defined over an algebra containing F. In the present paper, it is proved that every division algebra over a field F can be regarded as an algebra E_1 over a division algebra D_1, where D_1 is in its turn an algebra E_2 over an algebra D_2, etc. where each of the component algebras D_i is a division algebra defined over a field F_i contained in E_i of one of the three following types:

(1) fields,

(2) normal Dickson algebras,

(3) algebras which contain no Dickson subalgebras.

This paper does not determine whether there actually exist algebras of the third type, but the writer has the feeling that none such exist. This principle is applied to certain solvable algebras and it appears that under suitable conditions a solvable algebra is a direct product of solvable algebras.

2. **Relation to the literature; definitions.** We shall use the term *field* to denote a set of elements with two operations called addition and multiplication which is an abelian group with respect to addition and which, when we exclude the zero element (=the unit as to addition), is an abelian group with respect to multiplication. If, however, we do not insist on multiplication being commutative, then a set of numbers which is closed under the four rational operations (excluding division by zero) is said to form a *division* (*or primitive*) *algebra*, if it be always possible to solve for x in the algebra

* Presented to the Society, May 2, 1925; received by the editors in April, 1930.

[†] *Linear associative algebras and abelian equations*, these Transactions, vol. 15 (1914), pp. 31–46; *New division algebras*, ibid., vol. 28 (1926), pp. 207–234; *New division algebras*, Bulletin of the American Mathematical Society, vol. 34 (1928), pp. 555–560.

[‡] *Sopra un tipo di algebre prive di divisori dello zero*, Rendiconti del Circolo Matematico di Palermo, vol. 47 (1923), pp. 209–254.

[§] *On the structure of normal division algebras*, Annals of Mathematics, (2), vol. 30 (1929), pp. 322–338; *Normal division algebras in 4 p^2 units, p an odd prime*, ibid., pp. 583–590.

both of the equations $xy=z$ and $yx=z$ when y and z are any two numbers in the algebra. These are division algebras over any field F.*

When the field F is the field R of reals, it is well known that the only division algebras are (1) an algebra of one unit, the field R itself; (2) an algebra of two units, 1 and i, the field C of ordinary complex numbers; (3) an algebra of four units $(1, i, j, k)$, real quaternions. When the field of definition is C, the only division algebra is C itself. But when F is any other field, the nature and number of types of division algebras has not yet been fully determined, although recently much work has been done.†

When F is any algebraic field, Dickson considered a general class of algebras that he called Type A. He defines an algebra of this type as any linear associative algebra A, the coördinates of whose numbers range over F and for which the following properties hold:

(a) There exists in A a number i satisfying an equation $\phi(x)=0$ of degree n with coefficients in F and irreducible in F.

(b) Any number of A which is commutative with i is in $F(i)$.

(c) There exists in A a number j, not in $F(i)$, such that $ji=\theta j+\sigma$, where θ and σ are in $F(i)$.

All three of these conditions are satisfied by real quaternions, and the first two by any linear associative division algebra D over F, where we take i so that the degree of the irreducible equation in F satisfied by i is a maximum. Dickson‡ showed that every algebra of type A over F has a subalgebra S over F which can be exhibited as an algebra L over a field K with units $i^s j^k (k, s=0, \cdots, r-1)$. Multiplication is defined by the relations $ji=\theta(i)j, j^r=g$ where i is an element of S satisfying in the field K a uniserial abelian equation of degree r, with the roots $i, \theta(i), \theta^2(i), \cdots, \theta^{r-1}(i)$, where $\theta^r(i)=i$ and where g is a number of K. Dickson showed for $r=2$, 3 that g could be so chosen that in the algebra L, division (except by zero) is always possible and unique. Wedderburn,§ a few months later, showed that, for

* Wedderburn, *On hypercomplex numbers*, Proceedings of the London Mathematical Society, (2), vol. 6 (1907), p. 91; *A type of primitive algebra*, these Transactions, vol. 15 (1914), pp. 162–166; *On division algebras*, ibid., vol. 22 (1921), pp. 129–135; Dickson, *Linear Algebras* (Cambridge Tract No. 16); *Linear associative algebras and abelian equations*, these Transactions, vol. 15 (1914), pp. 31–46; *Algebras and their Arithmetics*, chapter V, Appendices I, II; *Algebren und ihre Zahlentheorie*, Zürich, Füssli, 1927, chapter III, etc.; F. Cecioni, *Sopra un tipo di algebre prive di divisori dello zero*, Rendiconti del Circolo Matematico di Palermo, vol. 47 (1923), pp. 209–254; Hazlett, *On the theory of associative division algebras*, these Transactions, vol. 18 (1917), pp. 167–176.

† In addition to the papers cited above, see E. Artin, *Über einen Satz von Herrn J. H. Maclagan Wedderburn*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, vol. 5 (1927), pp. 245–250; *Zur Theorie der hyperkomplexen Zahlen*, ibid., pp. 251–260; R. Brauer, *Über Systeme hyperkomplexer Zahlen*, Mathematische Zeitschrift, vol. 30 (1929), pp. 79–107.

‡ These Transactions, vol. 15 (1914), p. 37.

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

general r, g can be so chosen that L (and hence S) is a division algebra. Wedderburn has called division algebras of the type of L *Dickson algebras.*[*]

A *quadrate* (*normal*) *division algebra* is any division algebra which contains no numbers other than scalars which are commutative with every number of the algebra. Any division algebra is the direct product of a field and a quadrate division algebra.[†]

Several years later, Wedderburn[‡] proved that every division algebra of order 9 is either a field or a Dickson algebra. In a footnote of this paper he says that, although he has been unable to construct a division algebra analogous to Dickson algebras, but corresponding to a non-cyclic abelian equation, yet "it appears probable that they exist." More recently, Cecioni[§] considered division algebras over any field K whose order is a perfect square, n^2, and which contain an element i whose reduced equation is an abelian equation of degree n with coefficients in K, and determined certain properties of them. In April 1926, Dickson published another beautiful paper[||] on division algebras, in which he proved that just as there is a Dickson algebra corresponding to any cyclic group, so there is a division algebra corresponding to any solvable group.

More recently, A. A. Albert[¶] considered normal division algebras of order n^2 over a non-modular field F of type R_k.[**] He proved (Theorem 21): Let $A=B\times C$, where B is an associative normal division algebra of order n^2 over F, of type R_n, and C is an associative normal division algebra of order m^2 over F, of type R_m. If A be an associative division algebra, then A is a normal division algebra of type R_{mn}.[††]

[*] These Transactions, vol. 22 (1921), p. 134.

[†] Wedderburn, these Transactions, vol. 22 (1921), p. 130.

[‡] *On division algebras*, these Transactions, vol. 22 (1921), pp. 129–135.

[§] Loc. cit.

[||] *New division algebras*, these Transactions, vol. 28 (1926), pp. 207–234.

[¶] Loc. cit. I, p. 322.

[**] A normal division algebra is said to be of *type* R_k if it contain an element x of grade n and type R_k. The element x is said to be of *grade* t if the degree of its minimum equation is t; and of *type* R_k if its minimum equation have a set of k ordinary complex roots which are polynomials in one of the set.

[††] In his proof that A is normal, he uses the assumption that B and C are of special types. If we define a normal algebra as any algebra A (not necessarily a division algebra) over F which is such that the only numbers commutative with every number of A are in F, then we easily prove

THEOREM 1. *If B and C be two normal algebras defined over the field F, then $A=B\times C$ is normal*

For let $a=\sum b_ic_i$ be a number of A commutative with every number of A where each $b_i<B$ and. each $c_i<C$. We may assume without loss of generality that the b_i are linearly independent with respect to F. Since a is commutative with every number $\gamma<C$, then $\sum b_i(c_i\gamma)=\sum b_i(\gamma c_i)$. By the definition of a direct product, the b_i are linearly independent with respect to C and thus $c_i\gamma=\gamma c_i$. Since C is normal, $c_i<F$ and $a<B$. Since a is commutative with every number of B, then $a<F$ and

In the second paper,[*] he shows that every normal division algebra of order $4p^2$, p an odd prime, of the special type considered by Dickson[†] is of type R_{2p} and hence is "known," as he calls it. A "known" algebra might be described as a division algebra Γ which is a Dickson algebra with respect to a proper subalgebra Σ which, in its turn, is a "known" algebra with respect to a proper subalgebra.[‡]

A is normal.

Similarly in his proof that A is of type R_{nm}, he uses the assumption that $F(i)$ and $F(k)$ are imbedded in division algebras of a special kind, but this is not necessary. In fact, it is easy to prove

THEOREM 2. *Let $F(i)$ be a field of order n defined by i of type R_n and let $F(k)$ be a field of order m defined by k of type R_m. Then any number t that defines $F(i, k)$, of order p, is of type R_p.*

For $F(i, k)$ is defined as an overfield of F by any number t satisfying an irreducible equation of degree p, say

$$t=t_{11}=\sum a_\beta(i)k^\beta \qquad (\beta=0,\cdots,m-1)$$

where $a_\beta(i)<F(i)$. Then

$$t_{rs}=\sum a_\beta(\theta_r)\phi_s{}^\beta \qquad (r=1,\cdots,n;\ s=1,\cdots,m),$$

where $\theta_1,\cdots,\theta_n$ is a complete set of conjugates of i with respect to F and $\phi_1,\cdots,\phi_m$ is a complete set of conjugates of k with respect to F, is in $F(i, k)$ and thus is a polynomial in t with coefficients in F. Hence t is a root of $\phi(\xi)=\pi(\xi-t_{rs})=0$ of degree mn and with coefficients in F. Since the minimum function of t is a factor of $\phi(\xi)$, then t is of type p.

[*] Loc. cit. II, p. 583.

[†] *New division algebras*, Bulletin of the American Mathematical Society, vol. 34, p. 555.

[‡] Several of his theorems assert that if x be a number of a normal division algebra A satisfying certain conditions, then A contains a number satisfying certain other conditions and the proof of each of these theorems (32, 34, 35) actually uses numbers of A outside of $F(x)$, although the theorem seems to be about $F(x)$ rather than about A. Theorem 32: *Let A be normal division algebra. Let $x<A$ have the property that $-x$ satisfies the minimum equation of x. Then the minimum equation of x has even powers only. Let x^2 be of grade p with $\phi(\omega)=0$ as its minimum equation. Then x has grade $2p$ and the minimum equation is $\phi(\omega^2)=0$.* We can readily prove

THEOREM 3. *Let x generate a field $F(x)$ and let x have the property that $-x$ satisfies the minimum equation of x. Then the minimum equation of x has even powers only; and if x^2 be of grade p with $\phi(\omega)=0$ as its minimum equation, then x has grade $2p$ and its minimum equation is $\phi(\omega^2)=0$.*

For if $\chi(\xi)=0$ be the minimum equation of x, then $-x$ is a root of $\chi(\xi)=0$ and thus x is a root of $\chi(-\xi)=0$. Since $\chi(-\xi)=0$ is of the same degree as $\chi(\xi)=0$, the minimum equation, they must be identical except for a change of sign throughout, and thus $\chi(\xi)=0$ contains only even powers of ξ. By hypothesis, $F(x^2)$ is of order p and, since x satisfies an equation of degree at most 2 with respect to $F(x^2)$, then $F(x)$ is of order p or $2p$. But, if the order were p, then x would equal a polynomial in x^2 of degree p. Transposing the term x, we have an equation $\psi(\xi)=0$ containing precisely one term of odd degree with non-zero coefficient. Since $\chi(\xi)$ is a factor of $\psi(\xi)$, then $-x$ must satisfy $\psi(\xi)=0$ which implies $x=-x$ and this is impossible. Hence $F(x)$ is of order $2p$ and thus its minimum equation is $\phi(\omega^2)=0$. Instead of his Theorem 34, we prove the stronger

THEOREM 4. *Let $F(x)$ be a field of order $2p$ and let x satisfy*

$$\phi(\omega)\equiv\omega^{2p}+\alpha_1\,\omega^{2(p-1)}+\cdots+\alpha_p=0\ (\alpha_i<F)$$

such that $\phi(\omega)\equiv\psi(\omega^2)$ where $\psi(\rho)=0$ is cyclic. Then $\phi(\omega)=0$ is solvable.

For since $\psi(\rho)=0$ is a cyclic resolvent equation of $\phi(\omega)=0$, then the adjunction of a root of the former reduces the group G of the latter to an invariant subgroup G_1 and the quotient group $H_1=G/G_1$ is cyclic of order p. Now G_1 is the group of

$$\phi(\omega)\equiv\pi(\omega^2-\rho_i)=0$$

for the enlarged field containing the ρ_i and hence is of order 2^k. Hence the group of $\phi(\omega)=0$ is of order 2^kp and has a series of composition $p, 2,\cdots, 2$. Thus the theorem.

3. **General division algebras.** Let D be a division algebra over any algebraic field F, and let it contain a number i whose reduced equation, $\phi(x)=0$ of degree r, has at least two roots in $F(i)$. Then this equation has a root in $F(i)$ distinct from i, say $\theta(i)$; and hence its distinct symbolic powers $\theta, \theta^2, \cdots, \theta^n=i$ are, also, roots of $\phi(x)=0$. By previous work,* there is a number $J\neq 0$ in D and a polynomial $\theta(i)$ with coefficients in F such that $Ji=\theta(i)J$ if and only if $\theta(i)$ is a root of $\phi(x)=0$. Moreover, corresponding to each root of $\phi(x)=0$ which is in $F(i)$ there corresponds a number $J\neq 0$ in D which is essentially unique in the sense that all such numbers J corresponding to the same root are products of a particular such J by some (any) number in $F(i)$.†

Accordingly, let $J_1, J_2, \cdots, J_l=1$ be a set of non-zero numbers of D such that $J_k i=\theta_k(i)J_k(k=1, \cdots, l)$ where each θ_k is a polynomial in i and (by the foregoing remarks) is a root of $\phi(x)=0$. Also let the set of $\theta_k(k=1, \cdots, l)$ be such that they form a closed cycle,‡ namely, such that if θ_a and θ_b be any two θ's of the set (coincident or distinct), then $\theta_a\theta_b$ is also in the set. Then we have

LEMMA 1. *Let A be any algebra over F of Dickson's type A (defined as above) and let i be any number $\neq 0$ of A whose reduced equation, of degree r, has at least two roots, i and $\theta(i)$, in $F(i)$. Then there is a number $j\neq 0$ of A such that $ji=\theta(i)j$. If $J_1, J_2, \cdots, J_l$ be any set of numbers of A such that $J_k\, i=\theta_k(i)J_k$ is a polynomial in i where the θ's form a closed cycle (defined above), then the totality of numbers of the form $B=\sum_k A_k(i)J_k$, where the A_k range over all polynomials in i with coefficients in F, form an algebra B of order rl.*

For the set of numbers B is closed under addition and subtraction. Also, $J_kJ_ti=J_k\theta_t(i)J_t=\theta_t(\theta_k)J_kJ_t=\theta_p(i)J_kJ_t$ where $\theta_p(i)$ is in the set of θ's since they form a closed cycle. Hence $J_kJ_t=X(i)J_t$ where $X(i)$ is a polynomial in i§ and the set B is an algebra over F. It is already known that the set is of order rl. Note that B contains i itself since if we let $\theta_1=i$ then $j_1=i$ and thus $j_1i=i$.

Dickson proved this lemma‖ for the case when the θ's are symbolic powers of one of them.

By this lemma, there is in the algebra D a subalgebra D_1 corresponding

* Dickson, these Transactions, vol. 15 (1914), p. 35.

† Hazlett, these Transactions, vol. 18 (1917), p. 171.

‡ This is equivalent to saying that the corresponding substitutions (H) of Dickson's paper in the Transactions for April, 1926, form a group.

§ Hazlett, these Transactions, vol. 18 (1917), p. 171.

‖ These Transactions, vol. 15 (1914), p. 36.

to each root of the reduced equation $\phi(x)=0$ of the number i which is in $F(i)$. Since D is an associative division algebra, so also is D_1. Moreover, since the algebra D_1 is an algebra of the type A discussed by Dickson, his results apply here. Thus a number x of D_1 is commutative with all numbers of D_1 if x is in the field K generated by the elementary symmetric functions of $\theta_1, \theta_2, \cdots, \theta_l$. Also, D_1, an algebra of order rl over F, can be regarded as a quadrate algebra Q_1 of order r^2 and rank r over K. Hence D over F contains a quadrate subalgebra Q_1 of order r^2 defined over K, where K is an overfield of F which lies in D.

Since D is a quadrate division algebra, there is some overfield F_1 of F such that D is equivalent in F_1 to a simple matric algebra, M. Also, Q_1, considered as an algebra over K, where K is an algebra over F_1, is equivalent to a simple matric algebra M_1 which is a subalgebra of M. Hence, by one of Wedderburn's theorems, M is the direct product of M_1 and a simple matric algebra M_2 of order p^2, where $(pl)^2$ is the order of D. By the foregoing, M_1, considered as an algebra over K, where K is an algebra over F_1, is equivalent in F_1 to Q_1 over K, where K is now an algebra over F; but, since M_2 contains all numbers of M commutative with every number of M_1, this means that the numbers of K come from M_2 and K is equivalent in F_1 to a subalgebra of M_2. Moreover, M_2 does not have a basis which, when expressed in terms of the numbers of D_1, is rational in F. For, if it did, then (by one of Wedderburn's theorems) M_2 would be equivalent in F_1 to a division algebra D_2 over F which is a subalgebra of D and thus* D would be the direct product of D_2 and another quadrate division algebra, D_3, which contains all numbers of D commutative with every number of D_2. Thus D_3 would be equivalent to M_1 and hence would be equivalent to D_1 in F_1; and, since D_1 and D_3 are both subalgebras of D, then they would be equivalent in F. But this last is impossible since M_1 does not have a basis which, when expressed in terms of numbers of D, is rational in F. Hence M_2 does not have a basis rational in F.†

Thus we have

Remark 1. *Let D be a division algebra over the field F and let D contain Q_1 when Q_1 is a quadrate division algebra defined over $F(x)$ where x is in D but not in F. Then D can be represented as a division algebra defined over Q_1.*

Applying this to our algebra D, we see that if D contain any Dickson algebra D_1 as a subalgebra, then D can be represented as a division algebra defined over a quadrate Dickson algebra Q_1, where Q_1 is defined over $F(\alpha)$, an over-field of F. From the foregoing paragraphs, there is such a quadrate algebra Q_1 determined by i and any set of polynomials $\theta_1(i), \cdots, \theta_l(i)$ which

* *On division algebras*, these Transactions, vol. 22 (1921), p. 132.

† I here want to thank Professor Wedderburn for pointing out a mistake in this part.

are roots of $\phi(x)=0$ provided the θ's form a closed cycle. Since the symbolic powers of any such θ form a closed cycle, we may take these symbolic powers of θ which are distinct; then they (including $\theta^n=i$) satisfy an equation $g(x)=0$ of degree n with coefficients in K (=the field of the symmetric functions of $\theta, \theta^2, \cdots, \theta^n=i$) which is, moreover, irreducible in K.* In this case, Q_1 is a quadrate Dickson algebra of order n^2 over K. If n is composite, let $n=pq$ where p is a prime. Then θ^q is a polynomial in i with coefficients in F such that its first p symbolic powers are distinct, form a closed cycle, to which the above results apply, and thus are the roots of an equation of degree p with coefficients in K^1(= field of the symmetric functions of the symbolic powers of θ^q) which is irreducible in K. The quadrate algebra, Q, defined by this closed cycle is accordingly a Dickson algebra of order p^2 over K. Applying Remark 1, we have

REMARK 2. *If the division algebra D has a Dickson proper subalgebra D_1, then D_1 is a quadrate Dickson algebra Q_1 over $F(\alpha)$, where $F(\alpha)$ is an overfield of F, and D can be represented as an algebra E_1, defined over D_1. In its turn, D_1 can be regarded as an algebra E_2 over an algebra D_2, etc., where each of the component algebras D_i is a division algebra (defined over a field F_i contained in E_i) of one of the three following types:*

(1) *algebraic fields,*

(2) *normal Dickson algebras,*

(3) *algebras which contain no Dickson subalgebra.*

4. **Solvable algebras.** We now turn our attention to the algebras of Dickson's two most recent papers on division algebras. The above argument applies here.

In the first of these papers,† he is concerned with any associative algebra Γ with modulus 1 over any field F with the following properties.

(I) Γ is of order n^2.

(II) Γ contains an element i which satisfies an equation $f(x)=0$ of degree n irreducible in F.

(III) The only elements of Γ which are commutative with i are polynomials in i with coefficients in F.

(IV) The roots of $f(x)=0$ are rational functions, $\theta_r(i)$, of i with coefficients in F.

(V) The group, G, of $f(x)=0$ is solvable.

(VI) Γ contains elements $j_r\neq 0 (r=1, \cdots, n)$ satisfying $j_r i=\theta_r(i)j_r$.

(VII) The product of any j_r and j_s of VI is not zero.

* These Transactions, vol. 15 (1914), p. 37.

† *New division algebras*, these Transactions, vol. 28 (1926), pp. 207–234.

Such an algebra he called of Type E. For convenience, we might call any algebra of this type a *solvable algebra*. Note that any solvable algebra whose order is the square of a prime is necessarily a Dickson algebra, and that all Cecioni and Dickson algebras are special cases of solvable algebras.

In the following discussion, we shall consider $f(x)=0$ as an ordinary algebraic equation and shall restrict attention to its roots θ in an overfield of $F(i)$. Let G be the Galois group of order n of the equation $f(x)=0$. If the elements of G be denoted by Θ_r, the notation may be so chosen that Θ_r is the only substitution that replaces i by $\theta_r(i)$, and also $\Theta_r\Theta_s=\Theta_t$ if and only if $\theta_r\theta_s=\theta_t$. Moreover, since G is solvable, it has an invariant subgroup G_1 of prime index p and order q, such that every substitution of G can be expressed in the form $\Phi\Theta_k(1\leqq k\leqq q;\ 0\leqq r\leqq p)$, where Θ_k ranges over the substitutions of G, and Φ is a substitution of G not in G_1 and such that the pth power of Φ is the lowest power of Φ in G_1.*

If Θ_r and Θ_s be any two substitutions of G_1, then Θ_t is in G, and we have $j_k i=\theta_k(i)j_k$ $(1\leqq k\leqq q)$ and $j_r j_s=c_{rs}j_t(c_{rs}<F(i)\ )$. Thus the totality of linear functions of $j_1=1, j_2, \cdots, j_q$ with coefficients in $F(i)$ is a subalgebra, A_1, of Γ of order $nq=pq^2$ over F. Moreover, each number of A_1 is commutative with every number of the field F_1 of the symmetric functions of $\theta_1=i$, $\theta_2, \cdots, \theta_q$. Since $F(i)$ is an algebraic field of order $n=pq$ with respect to F and of order q with respect to F_1, then F_1 is of order p with respect to F and is defined by an irreducible equation $g_1(x)=0$ of degree p, with coefficients in F. Thus A_1 is a subalgebra S_1 of order q^2 and rank q over F_1.

From this it follows that we can arrange the n roots of $f(x)=0$ in p rows of q each and arrange similarly the corresponding solutions $j\neq 0$ of the equations $ji=\theta j$ as in the accompanying array:

$$\text{I}\qquad\left\{\begin{array}{llll}
\phi_1(\theta_1)\ =\ i, & \phi_1(\theta_2)\ =\ \theta_2, & \cdots, & \phi_1(\theta_q)\ =\ \theta_q\\
j_1J_1\ =\ j_1\ =\ J_1\ =\ 1, & j_2J_1\ =\ j_2, & \cdots, & j_qJ_1\ =\ j_q\\
\phi_2(\theta_1)\ =\ \phi_2, & \phi_2(\theta_2), & \cdots, & \phi_2(\theta_q)\\
j_1J_2\ =\ J_2, & j_2J_2, & \cdots, & j_qJ_2\\
\cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\\
\phi_p(\theta_1)\ =\ \phi_p, & \phi_p(\theta_2), & \cdots, & \phi_p(\theta_q)\\
j_1J_p\ =\ J_p, & j_2J_p, & \cdots, & j_qJ_p
\end{array}\right\}$$

where we have placed each solution $j\neq 0$ directly below the corresponding θ. The q θ's in the first line are the roots of $f_1(x)=0$ of degree q, the q θ's in the second line are the roots of an equation $f_1'(x)=0$ obtained by replacing i in

* For details, see the paper by Dickson cited in the previous footnote.

the coefficients of $f_1(x)=0$ by $\phi_2(i)$; etc. Since $\Phi^p<G$, then ϕ^p is a root in the first row, but is not i unless $\Phi=1$.

Now G_1 is the group of $f_1(x)=0$ for the field F_1. For, if we adjoin to F a root of $g_1(x)=0$, this is equivalent to enlarging F to F_1 and the group is reduced to an invariant subgroup of G. Since any symmetric function of the roots of $f_1(x)=0$ is unaltered by every transformation of G_1, then the group contains G_1 and thus is precisely G_1.

From this, it follows that the group of $g_1(x)=0$ for the field F is the quotient group $G/G_1=H_1$ and $g_1(x)=0$ is a cyclic equation. Since $g_1(x)=0$ is completely solvable in $F(i)$, we may denote any of its roots by (i). Since $g_1(\psi(x))=0$ has the root i in common with the irreducible equation $f(x)=0$, then it has all the roots of the latter and thus $g_1(x)=0$ has $\psi(\theta)$ as a root where θ is any root of $f(x)=0$. If $h(x)=\pi(x-\psi(\theta_k))$ $(1\leqq k\leqq n)$, then every coefficient of $h(x)$ is a symmetric function of the roots of $f(x)=0$ and thus is in F. Moreover, every root of $h(x)=0$ is a root of the irreducible equation $g_1(x)=0$. Thus every root of $g_1(x)=0$ is of the form $\psi(\theta)$, and $h(x)$ is the qth power of $g_1(x)$.

From this relation of the roots of $g_1(x)=0$ to the roots of $f(x)=0$, we readily obtain a set of numbers j of the algebra Γ satisfying the equation $j\psi(i)=\chi(i)j$. For if θ be any root of $f(x)=0$ and $j\neq 0$ a solution of $ji=\theta j$, then $j\ \psi\ (i)=\psi(\theta)j$. Moreover, if $\chi(i)$ be any number of F such that there exists a number $J\neq 0$ satisfying $J\psi(i)=\chi(i)J$, then $0=Jg_1(\psi)=g_1(\chi)J$ and hence χ is a root of $g_1(x)=0$. Accordingly, all such polymonials χ are of the form $\psi(\theta)$, where θ is a root of $f(x)=0$; and we find a solution $J\neq 0$ in Γ of each possible equation $J\psi=\chi J$ by taking as χ in turn every polynomial of the form $\psi(\theta)$ and then a corresponding J is the j corresponding to θ in the equation to $ji=\theta j$.

It is to be noted that, although a number j in Γ such that $ji=\theta j$ is essentially unique* in the sense that any other j satisfying the equation is of the form $\beta(i)j$, yet a number j in Γ such that $j\psi(i)=\psi(\theta)j$ is not essentially unique. For, since $f(x)=0$ has n roots, there are $n=pq$ essentially distinct numbers j that satisfy in turn the p possible equations $j\psi=\chi j=\psi(\theta)j$. Since $h(x)$ is the qth power of $g_1(x)$, the roots $\psi(\theta)$ of $h(x)=0$ are equal in sets of q each but the q corresponding j's are not essentially equal. In fact, $\psi(i)$ is a polynomial in i which is a symmetric function of the roots θ in the first row of the array I and the distinct roots of $g_1(x)=0$ are respectively the ψ-functions of each of the roots in the first column, and thus each $\psi(\phi_k)$ is a symmetric function of the roots in the kth row. Thus we may choose as the numbers j corresponding to the roots of $g_1(x)=0$ any q numbers such that one

* Since, under the assumptions, Γ has the basis $i^k j_r (k, r=1, \cdots, n)$.

is chosen from each row. That is, we may choose the j's of the first column; and sometimes we may so choose them that the corresponding θ's form a closed cycle. In the latter case, these j's are closed under multiplication except, possibly, for multipliers in $F(i)$. In any case, denote the j's by $J_1=1, J_2, \cdots, J_q$. The totality of numbers

$$\sum_{l,t} a_{lt}[\psi]^l J_t \qquad (a < F;\ l, t = 1, \cdots, p)$$

will be denoted by Γ_1.

Then the set of numbers j corresponding to the roots of $f(x)=0$ is obtained by forming all possible products $J_k j_l (k=1, \cdots, p; l=1, \cdots, q)$ or, if we wish, by forming all possible products $j_l J_k$. Every number of Γ is of the form

$$\sum_{s,t} \beta_{st}(i) j_s J_t \qquad (s = 1, \cdots, q;\ t = 1, \cdots, p),$$

where each $\beta<F(i)$ and therefore is of the form

$$\sum_{k,l} \alpha_{kl} i^k [\psi]^l \qquad (k = 1, \cdots, q;\ l = 1, \cdots, p).$$

Hence every number of Γ is of the form

$$\sum \beta_{klst}(i^k j_s)([\psi]^l J_t),$$

where each $\beta<F$. Let A_1 denote the totality of numbers of the form

$$\sum_{k,s} b_{ks} i^k j^s \qquad (k, s, = 1, \cdots q).$$

Note that, although the foregoing was proved under the assumption that p is a prime, yet the same reasoning holds if G_1 be any invariant subgroup of index p under G, a solvable group, since a resolvent equation of a solvable equation is always solvable.

Since (1) every number linearly dependent with respect to F on the products $i^k j_s (k, s=1, \cdots, q)$ is a number of A_1 and conversely every number of A_1 can be expressed in one and only one way as such a linear combination; (2) every number linearly dependent with respect to F on the products $[\psi]^l J_t$ $(l, t=1, \cdots, p)$ is a number of Γ_1 and conversely, we shall say that Γ over F has been represented as the algebra Γ_1 over the algebra A_1, where A_1 is defined over F.

If the J's can be so chosen that the set is closed under multiplication except for multipliers in F_1, then Γ_1 is an algebra of order p^2 over F. Moreover, Γ_1 is a normal algebra, for if $x=\sum x_{kl}[\psi]^k J_l (x_{kl}<F)$ be any number of Γ_1 that is commutative with every number of Γ_1, then $x\psi=\psi x$ is equivalent to

$$\sum_{k,l} x_{kl}[\psi]^k \psi_l J_l = \sum_{k,l} x_{kl}[\psi]^{k+1} J_l,$$

where $J_l\psi = \psi_l J_l$, and this is equivalent to

$$\sum_{k} x_{kl}[\psi]^k(\psi_l - \psi) = 0.$$

For each value of l there are two possibilities: $\psi = \psi_l$ or $\sum_k x_{kl}[\psi]^k = 0$. But $\psi \neq \psi_l$ unless $l = 1$, and hence $\sum x_{kl}[\psi]^k = 0$ $(l \neq 1)$, so that $x < F(\psi) = F_1$. Furthermore, $x(\psi)J_r = J_r x(\psi)$ if and only if

$$\sum_{k} x_k([\psi]^k - [\psi_r]^k)J_r = 0, \quad x_k([\psi]^k - [\psi_r]^k) = 0,$$

which is equivalent to saying that $x_k = 0$ unless $[\psi]^k = [\psi_r]^k$ for every r. But $\psi \neq \psi_r (r \neq 1)$ and thus $x_k = 0 (k \neq 0)$, so that $x < F$.

Since Γ_1 is quadrate and is defined over the same field F as Γ, then, by by one of Wedderburn's theorems, Γ is the direct product of Γ_1 and another quadrate division algebra, Γ_2, over F. To determine Γ_2, we must determine the totality of numbers of Γ that are commutative with every number of Γ_1. Now every number of Γ is of the form $x = \sum_{st} x_{st}(i) j_s J_t$. Accordingly, $x\psi = \psi x$ is equivalent to

$$\sum_{st} x_{st}(i)\psi(\phi_t(\theta_s)) j_s J_t = \sum_{st} x_{st}(i)\psi j_s J_t,$$

$$x_{st}(i)\left[\psi(\phi_t(\theta_s)) - \psi\right] = 0.$$

Thus $x_{st} = 0$ unless $\psi(\phi_t(\theta_s)\ ) = \psi$, and this last is equivalent to $\psi_t \equiv \psi(\phi_t) = \psi(\theta_l) = \psi$, where $\theta_s(\theta_l) = i$. Thus $x_{st} = 0$ unless $t = 1$, so that $x = \sum_s x_s(i) j_s$.* But the totality of such numbers x contains all numbers of $F(i)$. Now if $x < F(i)$, then $xJ_r = J_r x$ if and only if $x(i)J_r = x(\phi_r)J_r$, and thus such an x is commutative with every J_r if and only if $x < F_2$, the field of symmetric functions of the ϕ_r. Just as we proved that F_1 is of order p, so we prove that F_2 is of order q.

Since Γ_2 is a quadrate division algebra of order q^2 containing the number χ defining F_2 which satisfies an irreducible solvable equation of degree q, then Γ_2 is a solvable algebra and contains a set of numbers $K_l (l = 1, \cdots, q)$ such that $K_l \chi = \rho_l(\chi) K_l$ where ρ_l is a polynomial in χ with coefficients in F, and such that every number of Γ_2 is of the form $\sum y_l K_l (l = 1, \cdots, q)$ where $y_l < F_2$. Since $\rho_l(\chi)$ is a conjugate of χ with respect to F, then each ρ is of the form $\chi(\theta)$, where θ is a conjugate of i with respect to F. But χ is a symmetric function of the roots of $f(x) = 0$ in the first column of I, and hence (by the argument used above for the conjugates of ψ) the conjugates of χ

* Note that, even if Γ_1 be not an algebra, the totality of such numbers x is precisely the totality of numbers of Γ commutative with the numbers of F_1.

are the same symmetric functions of the roots in the second column, in the third column, and so on. If $\chi \equiv \chi(i)$, then the conjugates of χ are $\chi(\theta_l)$ $(l=1, \cdots, q)$. Hence $K_l\chi(i)=\chi(\theta_l)K_l=\chi_l K_l$.

But $K_l=\sum_s x_s(i)j_s$, and this last is equivalent to

$$x_s\chi(\theta_s) = x_s\chi(\theta_l) \qquad (s = 1, \cdots, q)$$

which is equivalent to $\chi_s=\chi_l$ if $x_s\neq 0$. Since the q conjugates of χ are distinct, then $x_s=0$ unless $s=l$, and thus

$$K_l = x_l(i)j_l \qquad (l = 1, \cdots, q).$$

Since $K_l\neq 0$ and $K_l i=\theta_l K_l$, we may take K_l in place of the old j_l, and we shall assume henceforth that we have so done. With this choice of $j_1, \cdots, j_q$, Γ_2 is the totality of numbers of the form $\sum_s x_s j_s$, where $x_s<F_2$. Note that the new set of j's is closed under multiplication except for the multipliers in F_2.

Thus we have the

Theorem. *Let* Γ *be a solvable algebra of order* n^2 *over a field* F. *Let* i *be any number of* Γ *satisfying a solvable irreducible equation* $f(x)=0$ *of degree* n *with roots in* $F(i)$ *as given by the square array* I *and let the essentially unique number* $j\neq 0$ *of* Γ *satisfying the equation* $ji=\theta j$ *corresponding to each such root* θ *be as given directly below* θ *in* I. *Let* F_1 *be the field of symmetric functions of* $\theta_1, \cdots, \theta_q$ *of the first row, and let it be defined by* ψ *where* ψ *satisfies an irreducible equation in* F *of degree* p. *Assume that the set of numbers* $J_1, \cdots, J_p$ *corresponding to the roots of the first column is closed under multiplication except for multipliers in* F_1. *Then the totality of numbers* $\sum_{lt}a_{lt}[\psi]^l J_t (a<F)$ *form a solvable division algebra* Γ_1 *of order* p^2. *Also, the set of roots* ϕ *of the first column is closed under iteration and their symmetric functions determine a field* $F_2=F(\chi)$ *defined by an irreducible equation of degree* q. *If the set of numbers* $j_1, \cdots, j_q$ *is not closed under multiplication except for multipliers in* F_2, *then each* j_s *may be multiplied by a suitable number* $x_s(i)\neq 0$ *such that the set* $x_1j_1, \cdots, x_qj_q$ *is closed under multiplication except for multipliers in* F_2. *If we take these as a new set of* $j_1, \cdots, j_q$ *then the totality of numbers of the form* $\sum_{ks}b_{ks}[\chi]^k j_s$ *form a solvable division algebra* Γ_2 *of order* q^2. *The algebra* Γ *is the direct product of* Γ_1 *and* Γ_2.

It should be noted that the assumption that the set of numbers $J_1, \cdots, J_p$ corresponding to the roots of the first column is closed under multiplication except for multipliers in F_1, is not as strong as it may at first seem. For if the set of numbers $J_1, \cdots, J_p$ of the first column is not closed under multiplication, there may be p non-zero numbers in $F(i)$, $y_1, \cdots, y_p$, such that the set $y_1J_1, \cdots, y_pJ_p$ is closed under multiplication except for multipliers in F_1. Moreover, even if this be not possible it may be possible for another set of $J_1=1, \cdots, J_p$; for J_2 is any non-zero solution j of the equation $ji=\theta j$ where θ is any root of $f(x)=0$ not in the first row; J_3 is any non-zero solution when θ is any root not in the first two rows; etc.

Moreover, this assumption as to the closure of the set of J's is not incompatible with the assumption that Γ is an associative solvable algebra, as will be seen if we turn to Dickson's article.* In §1, he exhibits a class of solvable division algebras of order p^2q^2 over F with basal numbers $i^aj^bk^c$ $(a<pq,\ b<q,\ c<p)$, where i satisfies an irreducible equation of degree pq with roots $\theta^k[\psi^r(i)]=\psi^r[\theta^k(i)]$ $(k=0,\ 1, \cdots, q-1;\ r=0,\ 1, \cdots, p-1)$ where $\theta^q=i$, $\psi^p=i$. Multiplication is determined by the associative law in conjunction with $j^q=g$, $k^p=r$, $kj=\alpha jk$, $ji=\theta j$, $ki=\psi k$ where q, r, $\alpha<F(i)$. The conditions for associativity reduce to

$$g = g(\theta), \quad \alpha\alpha(\theta)\alpha(\theta^2) \cdots \alpha(\theta^{q-1})g = g(\psi),$$

$$r = r(\psi), \quad \alpha\alpha(\psi)\alpha(\psi^2) \cdots \alpha(\psi^{p-1})r(\theta) = r.$$

Here the powers of j play the rôles of $j_1, \cdots, j_q$ of the present paper and the powers of k play the rôles of $J_1, \cdots, J_p$. To see that our assumption as to the set of the J's is not inconsistent with the above condition for associativity, take g and r as numbers in F and then both the sets of j and those of J are closed under multiplication. From the work above, it follows that $kj=jk$ and therefore $\alpha=1$ and all conditions for associativity are satisfied.

Brauer† has proved that any quadrate division algebra of order p^2q^2 where p and q are relatively prime is the direct product of a division algebra of order p^2 and a division algebra of order q^2. In particular, any solvable algebra Γ of order p^2q^2 is a direct product of a division algebra Γ_1 of order p^2 and a division algebra Γ_2 of order q^2. If Γ_1 be solvable, then it contains a number i, which satisfies an irreducible solvable equation in F of degree p; and similarly with Γ_2. Applying Theorem 21 of A. A. Albert's first paper‡ or by Theorem 2 of our footnotes re his theorem (see our §2), it follows that the i specified above may be taken as any number defining $F(i_1, i_2)$. As the resolvent equation $g_1(x)=0$, we shall take any defining equation of $F(i_1)$. Using the notation of the proof of the theorem, we first have the numbers $J_1, \cdots, J_p$ given us in Γ_1, and thus we have $J_li=\alpha_l(i_1)J_l$. But i_l is a polynomial in i, say $\psi(i)$; and hence, by the proof of the theorem, $\alpha_l(i)=\psi(\phi_l)$

* These Transactions, vol. 28, p. 207.

† Loc. cit., p. 104.

‡ Loc. cit., p. 329.

where ϕ_l is some root of $f(x)=0$, the irreducible equation defining i. We may take the present $\phi_2, \phi_3, \phi_4, \cdots$ as the $\phi_2, \phi_3, \phi_4, \cdots$ of I. For the α_l combine under iteration in a manner that might be described as simply isomorphic with the manner in which the corresponding elements of the group H_1 of $g_1(x)=0$ combine under multiplication, and the corresponding J_l combine in the same manner, so to speak, except that the order of multiplication is reversed.* Since H_1 is the quotient group, there is an α_l corresponding to each row of I, this correspondence applying to multiplication; also, there is a J_l corresponding to each row of I and this J_l may be taken as one of the j's in that row of I. It is only a matter of rearranging the elements of one row to put this element first in the row. Hence the present $J_1, \cdots, J_p$ can be taken as the $J_1, \cdots, J_p$ of I and then the present $\phi_1, \cdots, \phi_p$ become the ϕ's of I. Since the set of J's is closed under multiplication except for multipliers in $F_1=F(i)=F(\psi)$, we see that the assumptions of our theorem are satisfied whenever Γ is the direct product of two solvable division algebras.

* For details, see array I.

University of Illinois,
Urbana, Ill.