NEW DIVISION ALGEBRAS*

BY

L. E. DICKSON

1. **Introduction.** The chief outstanding problem in the theory of linear algebras (or hypercomplex numbers) is the determination of all division algebras. We shall add here very greatly to the present meager knowledge of them, since we shall show how to construct one or more types of division algebras of order n^2 corresponding to every solvable group of order n.

While it was long thought that the theory of continuous groups furnishes an important tool for the study of linear algebras, the reverse position is now taken. But this memoir shows how vital a rôle the theory of finite groups plays in the theory of division algebras.

Fields and the algebra of real quaternions were the only known division algebras until the writer's discovery in 1905 of a division algebra D, over a field F, whose n^2 basal units are $i^a j^b$ $(a, b = 0, 1, \cdots, n-1)$, where i is a root of an irreducible cyclic equation of degree n for F. Recently, Cecioni† gave a further division algebra of order 16.

It is here shown that the algebras D form only the first of an infinitude of systems of division algebras. The next system is composed of algebras Γ of order p^2q^2 over F with the basal units $i^a j^b k^c$ $(a<pq,\ b<q,\ c<p)$. We start with an irreducible equation of degree pq, three of whose roots are i, and the rational functions $\theta(i)$ and $\psi(i)$ with coefficients in F, such that the qth iterative $\theta^q(i)$ of $\theta(i)$ is i, and likewise $\psi^p(i)=i$, while all the roots are given by

$$\theta^k[\psi^r(i)]=\psi^r[\theta^k(i)] \qquad (k=0,1,\cdots,q-1\ ;\ r=0,1,\cdots,p-1)\ .$$

The complete multiplication table of the units follows by means of the associative law from

$$i^q=g\ , \qquad k^p=\gamma\ , \qquad kj=\alpha jk\ , \qquad ji=\theta(i)j\ , \qquad ki=\psi(i)k\ ,$$

where g, γ and α are in the field $F(i)$. The conditions for associativity all reduce to

$$g=g(\theta)\ , \qquad \alpha\alpha(\theta)\alpha(\theta^2)\cdots\alpha(\theta^{q-1})g=g(\psi)\ ,$$
$$\gamma=\gamma(\psi)\ , \qquad \alpha\alpha(\psi)\alpha(\psi^2)\cdots\alpha(\psi^{p-1})\gamma(\theta)=\gamma\ .$$

* Presented to the Society, October 31, 1925; received by the editors in October, 1925.

† Rendiconti del Circolo Matematico di Palermo, vol. 47 (1923), pp. 209–54.

The subalgebra with the units $i^a j^b$ may be regarded as an algebra Σ of type D with q^2 units $i^d j^b$ ($d, b = 0, 1, \cdots, q-1$) over the field F_1 derived from F by the adjunction of all the elementary symmetric functions of i, $\theta(i)$, $\theta^2(i), \cdots, \theta^{q-1}(i)$. This Σ is a division algebra if and only if g (which is in F_1) is not the norm, relative to F_1, of any number of the field $F(i)$. For $p=2$ and $p=3$, it is shown that Γ is then a division algebra if and only if

$$\gamma \neq X^{(p-1)} X^{(p-2)} \cdots X'' X' X$$

for any X in Σ, where $X^{(r)}$ denotes $k^r X k^{-r}$, which is an element of Σ. This result indicates that we have investigated Γ as a quasi algebra over Σ, where Σ is an algebra over F. Such a treatment is far simpler than the more direct study of Γ as an algebra over F (see the end of §10). The former method accomplishes a factorization of the difficulties both as to the conditions for associativity and the conditions that Γ be a division algebra.

The preceding Γ was obtained from an equation whose Galois group G is an abelian group with two independent generators of orders p and q. There are treated the generalizations when G is an arbitrary abelian group, and when G is any solvable group.

If in the above relations $j^q = g$, etc., we replace each number of the field $F(i)$ by unity, we obtain the generating relations $j^q = 1$, $k^p = 1$, $kj = jk$ of G. Similarly for any Γ, provided we reverse the order of multiplication (i.e., pass to the reciprocal algebra) in case G is not abelian. While any Γ thus shows at once its G, it is a long story to construct Γ from G.

In §§2, 3 are recast and amplified some known proofs partly to make the paper elementary and self-contained and partly to emphasize the minimum assumptions involved. The paper presupposes only the simplest notions concerning linear algebras* and the elements of the theory of finite groups. Further developments of the paper will be given in Chicago theses.

2. **A class of division algebras.** Let A be any associative division algebra, with the modulus 1, over any field F such that†

(I) A is of order n^2;

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

---

* Cf. the writer's *Algebras and their Arithmetics*, University of Chicago Press, 1923.

† Assumptions I–III do not impose actual limitations on the generality of our study of division algebras A. For, any A may be regarded as an algebra over the field B composed of all those elements of A which are commutative with every element of A. Taking B as a new field F of reference, we call A a *normal* division algebra over F. By *Algebras and their Arithmetics*, pp. 227–28, this normal A is of order a square, say n^2. In the German translation to be published in 1926 by Orell Füssli Verlag, Zürich, I prove at the end of Chapter VIII that A is then of rank n and deduce II and III at once.

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

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

All rational functions of i with coefficients in F form a field $F(i)$, whose numbers are known to be expressible as polynomials of degree $<n$ in i with coefficients in F.

There exist elements $z_1=1, z_2, \cdots, z_n$ *of* A *such that every element of* A *can be expressed in one and only one way in the form* $\sum g_k z_k$, *where the* g_k *are in* $F(i)$. For, we may choose as z_2 any element of A not in $F(i)$. If $g_1+g_2z_2$ is equal to $h_1+h_2z_2$, then $g_1=h_1$, $g_2=h_2$. For, their difference $a+bz_2$ is zero. If $b=0$, then $a=0$ and the statement is proved. If $b\neq 0$, z_2 would be the element $-b^{-1}a$ of $F(i)$, contrary to hypothesis. Next, we may choose as z_3 any element not of the form $a+bz_2$, where a and b are in $F(i)$. As before, if $g_1+g_2z_2+g_3z_3$ is equal to $h_1+h_2z_2+h_3z_3$, then $g_k=h_k (k=1, 2, 3)$. In this manner we obtain elements $z_1=1, z_2, \cdots, z_m$ of A such that every element of A can be expressed in one and only one way in the form $\sum g_k z_k$. Hence A is an algebra over F with the nm basal units $i^r z_k$ $(r=0, 1, \cdots, n-1;\ k=1, \cdots, m)$. Since A is of order n^2, we have $nm=n^2$, $m=n$.

Applying this result to the particular element $z_s i$ of A, we have

$$z_s i=\sum_{k=1}^{n} g_{sk} z_k \qquad (s=1, \cdots, n), \tag{1}$$

where the g_{sk} are in $F(i)$. Let G be the matrix having the element g_{sk} in the sth row and kth column. Let Z be the matrix composed of a single column of elements z_1 (at the top), $z_2, \cdots, z_n$. Then equations (1) are equivalent to the single equation $Zi=GZ$ in matrices. By induction on r, we get $Zi^r=G^rZ$. Multiply this by the coefficient of i^r in any assigned polynomial $h(i)$ with coefficients in F and sum as to r. We get $Zh(i)=h(G)Z$. Thus $h(G)=0$ implies $z_1h=h(i)=0$. Next, take $h(i)=f(i)=0$. Then $f(G)Z=0$, which implies $f(G)=0$. For, if the element in the sth row and kth column of $f(G)$ is f_{sk}, then $f(G)Z$ is a matrix having a single column whose element in the sth row is $\sum_k f_{sk}z_k=0$. By the remark preceding (1), this implies that every $f_{sk}=0$. The two results show that *the minimum equation* $f(x)=0$ *of* i *for* F *is also the minimum equation of matrix* G *for* F.

Let the minimum equation of G for any field F' containing F be $h(x)=0$ of degree d. Write $f(x)=g(x)h(x)+r(x)$, where $r(x)$ is either identically zero or has a degree $<d$. Then $r(G)=0$, so that $r(x)\equiv 0$. Take F' to be the field $F(i)$ to which belong all elements of G. Thus each root of the minimum equation of G for $F(i)$ is a root of $f(x)=0$. The former has the same roots

apart from multiplicity as the characteristic equation of G (*Algebras*, p. 110). Hence *every root of* $|G-xI|=0$ *is a root of* $f(x)=0$.

Let θ be any root of $|G-xI|=0$. By IV, θ is a rational function $\theta(i)$ of i with coefficients in F. Write $\alpha=\sum a_s z_s$, where the $a_s (s=1, \cdots, n)$ are numbers of $F(i)$. By (1),

$$\alpha i=\sum_{s,k=1}^{n} a_s g_{sk} z_k \ .$$

Hence $\alpha i=\theta\alpha$ if and only if

$$\sum_{s=1}^{n} g_{sk}a_s-\theta a_k=0 \qquad (k=1, \cdots, n) \ .$$

The determinant of the coefficients of $a_1, \cdots, a_n$ is $|G-\theta I|$, which is zero. Hence there exist solutions $a_1, \cdots, a_n$, not all zero, which are rational functions of the g_{sk} and $\theta(i)$ with rational coefficients and hence are numbers of $F(i)$. Thus α is in algebra A and $\alpha\neq 0$.

We next prove that the assumption that θ is a multiple root of $|G-xI|=0$ leads to a contradiction. Take the α just found as a new z_1 and retain the notation (1). Then

$$z_1 i=\theta z_1 \ , \qquad g_{11}=\theta \ , \qquad g_{1k}=0 \qquad (k>1) \ .$$

We can find numbers $a_2, \cdots, a_n$, not all zero, and a number c, all in $F(i)$, such that

$$\alpha=\sum_{s=2}^{n} a_s z_s \ , \qquad \alpha i=\theta\alpha+cz_1 \ .$$

The conditions are

$$(2) \qquad c=\sum_{s=2}^{n} a_s g_{s1} \ , \qquad \sum_{s=2}^{n} a_s g_{sk}-\theta a_k=0 \qquad (k=2, \cdots, n) \ .$$

Let M_x be the minor of $g_{11}-x$ in $G-xI$. Since the remaining elements $g_{12}, \cdots, g_{1n}$ of the first row are zero, $|M_x|$ vanishes when $x=\theta$. The matrix of the coefficients of $a_2, \cdots, a_n$ in equations (2), other than the first, is derived from M_θ by interchanging rows and columns, whence its determinant is zero. Hence those equations can be satisfied by choice of numbers $a_2, \cdots, a_n$, not all zero, of $F(i)$. Thus α is in algebra A and $\alpha\neq 0$. Since α lacks z_1,

$$(2') \qquad g(i)z_1+h(i)\alpha=0 \qquad \text{implies } g=h=0 \ .$$

If $c=0$, $z_1 i=\theta z_1$ and $\alpha i=\theta\alpha$ imply

$$\alpha^{-1}z_1 i=\alpha^{-1}\theta z_1=i\alpha^{-1}z_1 \ ,$$

so that $\alpha^{-1}z_1$ is commutative with i and hence by III is a number $\phi(i)$ of $F(i)$. By induction on k, $\alpha i^k=\theta^k\alpha$. Multiply by the coefficient of i^k in $\phi(i)$ and sum as to k. Hence

$$\alpha\phi(i)=\phi(\theta)\alpha \ .$$

Then $z_1=\alpha\phi(i)=\phi(\theta)\alpha$ contradicts (2′).

Hence $c\neq 0$. Then $\beta=cz_1$ is not zero in the division algebra A, and

$$\beta i=cz_1 i=c\theta z_1=\theta cz_1=\theta\beta\ , \qquad \alpha i=\theta\alpha+\beta\ .$$

By induction on k,

$$\alpha i^k=\theta^k\alpha+k\theta^{k-1}\beta\ .$$

Multiply by the coefficient of i^k in $f(i)$ and sum as to k. We get

$$\alpha f(i)=f(\theta)\alpha+f'(\theta)\beta\ , \qquad 0=f'(\theta)\beta\ .$$

This is impossible in a division algebra since $\beta\neq 0$ and $f'(\theta)\neq 0$, there being no double root θ of the irreducible equation $f(x)=0$. Hence $|G-xI|=0$ has no multiple root, so that its n distinct roots coincide with the n roots $\theta_r(i)$ of $f(x)=0$.

We have now proved* that A contains elements $j_r(r=0, 1, \cdots, n-1)$, each not zero, where $j_0=1$, such that

$$j_r i=\theta_r(i)j_r \qquad (r=0,1, \cdots, n-1)\ , \tag{3}$$

$$j_r i^k=[\theta_r(i)]^k j_r\ , \tag{4}$$

$$j_r\phi(i)=\phi[\theta_r(i)]j_r \qquad (r=0,1, \cdots, n-1)\ . \tag{5}$$

3. **Algebras of types B and C.** Discarding the assumption that A is a division algebra, we shall say that an associative algebra A, having the modulus 1, over a field F, is of *type B* if it has properties I, II, IV, if it contains elements $j_r\neq 0(r=1, \cdots, n-1)$ satisfying (3), and finally if every c_{rs} in Lemma 2 is not zero.

LEMMA 1. *A has the basis* $i^k j_r$ $(k, r=0, 1, \cdots, n-1)$.

For, if these n^2 elements are linearly dependent with respect to F, there exist polynomials $\phi_r(i)$, not all zero, of degree $<n$ in i with coefficients in F such that

$$\sum_{r=0}^{n-1}\phi_r(i)j_r=0\ .$$

Multiply by i^k on the right and apply (4); we get

$$\sum_{r=0}^{n-1}\phi_r(i)[\theta_r(i)]^k j_r=0 \qquad (k=0,1, \cdots, n-1)\ .$$

The determinant Δ of the coefficients of the $\phi_r(i)j_r$ is equal to the product of the differences of the n distinct roots $\theta_r(i)$ of $f(x)=0$ and hence is not zero.

* Stated by Wedderburn, these Transactions, vol. 22 (1921), pp. 133–34 (§4). The proof is based on suggestions made by him to the writer.

Multiply* the displayed equation on the left by the cofactor of the element of Δ in the $(k+1)$th row and $(r+1)$th column and sum for k. We get $\Delta\phi_r(i)j_r=0$. If $\phi_r(i)$ is not zero, it has an inverse in $F(i)$, and $j_r=0$, contrary to its origin. Hence every $\phi_r(i)=0$.

Since $f[\theta_s(x)]=0$ is satisfied by the root i of the equation $f(x)=0$ irreducible in F, it is satisfied by the root $\theta_r(i)$ of the latter. Hence $\theta_s[\theta_r(i)]$ is a root $\theta_u(i)$ of $f(x)=0$.

LEMMA 2. *If r and s are any two equal or distinct integers $\leqq n-1$ and if u is the uniquely determined integer for which $\theta_s[\theta_r(i)]=\theta_u(i)$, then*

$$j_r j_s = c_{rs} j_u , \tag{6}$$

where c_{rs} is in $F(i)$.

For by Lemma 1, there exist numbers d_{rst} in $F(i)$ such that

$$j_r j_s = \sum_{t=0}^{n-1} d_{rst} j_t .$$

Multiply by i on the right and apply (3), (5); we get

$$\theta_u(i) j_r j_s = \sum_{t=0}^{n-1} d_{rst}\theta_t(i) j_t .$$

Eliminate $j_r j_s$ and apply Lemma 1. Hence

$$d_{rst}[\theta_u(i)-\theta_t(i)]=0 ,$$

whence $d_{rst}=0$ if $t\neq u$ and therefore $\theta_t(i)\neq\theta_u(i)$.

An algebra of type B shall be called of type C if it has the commutivity property

$$\theta_r[\theta_s(i)]=\theta_s[\theta_r(i)] \quad (r, s=0, 1, \cdots, n-1) . \tag{7}$$

4. **Algebras of type D.** Consider the case of an algebra of type C for which $f(x)=0$ is an irreducible cyclic equation, having therefore the roots

$$i , \quad \theta_1(i) , \quad \theta_2(i)=\theta_1[\theta_1(i)] , \cdots , \theta_{r+1}(i)=\theta_1[\theta_r(i)] , \cdots ,$$

while $\theta_n(i)=i$. By Lemma 2,

$$j_r j_1 = a_r j_{r+1} \qquad (r=1, \cdots, n-1 ; j_n=1) .$$

By induction on k, $j_1^k=a_1a_2\cdots a_{k-1}j_k$. Since each $a_r\neq 0$ by hypothesis, we may introduce a_1j_2, $a_1a_2j_3$, $\cdots$, $a_1\cdots a_{n-2}j_{n-1}$ as new units $j_2, j_3, \cdots, j_{n-1}$, and then have $j_1^k=j_k (k=2, \cdots, n-1)$, while $j_1^n=g$, where g is in $F(i)$. The associative law implies that j_1^k and j_1^n are commutative, whence

* This step is an improvement on the proof by Cecioni, from whom we borrow also Lemma 2.

$gj_k = j_k g = g(\theta_k) j_k$, by (5). Thus $g = g(\theta_k)$ for every k, so that g is a symmetric function of the roots of $f(x) = 0$ and hence is in F. Writing j for j_1, we obtain the algebra* D over F having the n^2 basal units $i^s j^k (s,k = 0, 1, \cdots, n-1)$, where $ji = \theta(i) j$, $j^n = g$. The condition that g is in F insures that the algebra is associative (§9). It will be shown incidentally in §§12, 13 that for $n = 2$ or 3 D is a division algebra if g is not the norm $\Pi\phi[\theta_k(i)]$ of any polynomial $\phi(i)$ in i with coefficients in F. For any n, it was proved by Wedderburn† that D is a division algebra if no power of g less than the nth is the norm of a number of $F(i)$.

5. **Galois group G.** Let G be the Galois group for the field F of the irreducible equation $f(x) = 0$ whose roots are rational functions $i_r = \theta_r(i)$ of i with coefficients in F for $r = 0, 1, \cdots, n-1$. If a substitution of G leaves i unaltered, it leaves each i_r unaltered and is the identity substitution. Since the equation is irreducible, its group G is transitive. Hence G is of order n and contains one and only one substitution Θ_r which replaces i by $\theta_r(i)$. When it is applied to the rational relation $i_l = \theta_l(i)$, we obtain a true relation. Hence Θ_r replaces i_l by $\theta_l[\theta_r(i)]$, which is a certain $i_v = \theta_v(i)$. Similarly, Θ_s replaces i_v by $\theta_v[\theta_s(i)]$. Hence the product $\Theta_r\Theta_s$ replaces i_l by

$$\theta_v[\theta_s i] = \theta_l[\theta_r(\theta_s i)] = \theta_l[\theta_t(i)] \ , \quad \text{if} \quad \theta_r[\theta_s(i)] = \theta_t(i) \ .$$

But Θ_t replaces i_l by $\theta_l[\theta_t(i)]$. Hence

$$\Theta_r\Theta_s = \Theta_t \quad \text{if and only if} \quad \theta_r[\theta_s(i)] = \theta_t(i) \ . \tag{8}$$

First, let $f(x) = 0$ be an abelian equation so that the roots have the commutivity property (7). Then $\Theta_r\Theta_s = \Theta_s\Theta_r$ by (8), and G is an abelian (commutative) group. It is well known that any abelian group G has a set of independent generators $g_1, \cdots, g_k$ such that every substitution of G can be expressed in one and only one way in the form $g_1^{e_1} \cdots g_k^{e_k}$ $(e_i = 0, 1, \cdots, h_i - 1)$, where h_i is the order of g_i. Select any one of the independent generators of G, denote its order by p, and write $q = n/p$. Adopting a new subscript notation for the n substitutions of G, we shall write Θ_q for the selected generator and write $\Theta_0 = 1, \Theta_1, \cdots, \Theta_{q-1}$ for the subsitutions of the subgroup G_q which is generated by the generators other than Θ_q of G. The substitutions of G are therefore

$$\Theta_q^r\Theta_k \qquad (r = 0,1, \cdots, p-1 \ ; \ k = 0,1, \cdots, q-1) \ .$$

---

* Discovered by the writer and announced as a division algebra in the Bulletin of the American Mathematical Society, vol. 22 (1905–06), p. 442; details in these Transactions, vol. 15 (1914), p. 31.

† These Transactions, vol. 15 (1914), p. 162. Amplified in Dickson's *Algebras and their Arithmetics*, 1923, p. 221.

Since we have defined Θ_s only when $s \leqq q$, we are at liberty to write

$$\Theta_{k+rq} = \Theta_q^r \Theta_k \ .$$

By (8) we see that the roots have now been assigned a subscript notation such that $\theta_q^p(i) = i$ and

$$\theta_{rq}(i) = \theta_q^r(i) \ , \qquad \theta_{k+rq}(i) = \theta_{rq}[\theta_k(i)] \qquad (r<p \ , \ k<q) \ , \tag{9}$$

where $\theta^r(i)$ is the rth iterative of the function $\theta(i)$.

Second, let G be not abelian. We assume that G has an invariant subgroup G_q which is extended to G by a substitution Θ_q (whose order may exceed the index p of G_q under G). Since Θ_q transforms each substitution Θ_k of G_q into a substitution Θ_{k_0} of G_q, we have $\Theta_k\Theta_q = \Theta_q\Theta_{k_0}$. Hence in any product of factors $\Theta_k (k<q)$ and Θ_q, we can move the factors Θ_q to the front. Thus every substitution of G can be expressed in the form $\Theta_q^r\Theta_k (k<q)$. If the sth, but no lower, power of Θ_q belongs to G_q, the preceding formula with $r = 0, 1, \cdots, s-1$; $k = 0, 1, \cdots, q-1$, gives all the pq substitutions of G without repetition, whence $s = p$. Hence we may assign a subscript notation to the roots such that (9) holds. We assume that G_q has an invariant subgroup $G_{q'}$ which is extended to G_q by a single substitution; similarly for $G_{q''}$, etc. These assumptions imply that G is a solvable group. For, let p be the product of the primes $a_1, \cdots, a_e$, not necessarily distinct. Then G_q is an invariant subgroup of index a_1 of the extension G_{a_1q} of G_q by Θ_q^{p/a_1}, the a_1th, but no lower, power of which is in G_q. Similarly, G_{a_1q} is an invariant subgroup of index a_2 of the extension $G_{a_1a_2q}$ of G_q by $\Theta_q^{p/(a_1a_2)}$, whose a_2th power is the former extender. Finally, if $\pi = a_1a_2 \cdots a_{e-1}$, $G_{\pi q}$ is an invariant subgroup of index a_e of $G = G_{pq}$. The same argument applies to $G_{q'}$, etc. Hence we may proceed from G to the identity group through a series of groups each an invariant subgroup of prime index of its predecessor. This is the definition of a solvable group.

Conversely, any solvable group serves as a G. For, it has an invariant subgroup G_q of prime index a. We may take $p = a$ and Θ_q to be any substitution of G which is not in G_q. If the sth, but no lower, power of Θ_q belongs to G_q, we see as above that Θ_q extends G_q to a group of order sq, which must divide pq, whence $s = p$.

Algebras which satisfy the present and earlier assumptions shall be said to be of type E.

6. **Algebra Σ.** Let Γ be an algebra over F of type E. We saw that the Θ_r $(0 \leqq r < q)$ form a group G_q. Hence if r and s belong to the set $0, 1, \cdots, q-1$, we can find an integer u of the same set such that $\Theta_s\Theta_r = \Theta_u$. By (8), we have

(6), whence the totality of linear functions of $1, j_1, \cdots, j_{q-1}$ with coefficients in $F(i)$ is a subalgebra Σ of Γ. Thus Σ is of order $nq = pq^2$ over F.

Each $j_s (s<q)$ is commutative with every elementary symmetric function E of $\theta_0(i)=i, \cdots, \theta_{q-1}(i)$. For by (5), $j_sE=Hj_s$, where H is the same elementary symmetric function of $\theta_0[\theta_s(i)], \cdots, \theta_{q-1}[\theta_s(i)]$, which by (8) are equal to $\theta_0(i), \cdots, \theta_{q-1}(i)$ in a new order.

Let F_1 be the field obtained by adjoining to F all these functions E. Then i is a root of the equation

$$f_1(x) = \prod_{k=0}^{q-1} [x-\theta_k(i)] = 0 ,$$

whose coefficients belong to F_1. *This equation is irreducible in* F_1. For, suppose that $f_1(x)$ has a factor $q(x)$ with coefficients in F_1 which vanishes for $x=i$, but not for $\theta_s(i)$. Let e be any elementary symmetric function of the roots of $q(x)=0$. Thus $\pm e$ is equal to a coefficient and belongs to F_1. Hence e is equal to a polynomial in the adjoined E's and hence is a symmetric function of $\theta_0(i), \cdots, \theta_{q-1}(i)$ with coefficients in F. Thus e is commutative with every $j_k (k<q)$. Also $j_se=hj_s$, where h is the same elementary symmetric function of the $\theta_k[\theta_s(i)]$, where the $\theta_k(i)$ are the roots of $q(x)=0$. Thus $ej_s = hj_s$, whence $e=h$. Since this is true for every e, the $\theta_k(i)$ coincide in some order with the $\theta_k[\theta_s(i)]$. But for $k=0$ the latter is $\theta_s(i)$, which is not one of the roots $\theta_k(i)$ of $q(x)=0$.

THEOREM 1. *Algebra* Σ *of order* pq^2 *over* F *may be regarded as an algebra of type* E *of order* q^2 *over* F_1 *obtained by means of an equation* $f_1(x)=0$ *of degree* q *which is irreducible in* F_1. *Here* F_1 *is the field derived from* F *by adjoining the elementary symmetric functions of the roots* $\theta_0(i)=i, \cdots, \theta_{q-1}(i)$ *of* $f_1(x)=0$.

ALGEBRAS WITH AN ABELIAN GROUP G, §§7–14

7. **Γ as an algebra over Σ.** By (9) and Lemma 2,

$$j_q^2 = c_2 j_{2q} , \quad j_q^3 = c_3 j_{3q} , \quad \cdots , \quad j_q^{p-1} = c_{p-1} j_{(p-1)q} ,$$

where each c_k is a number $\neq 0$ of $F(i)$. The second members may be introduced as new units $j_{2q}, j_{3q}, \cdots$. Then

$$j_q^r = j_{rq} \quad (r=2, \cdots, p-1) , \quad j_q^p = \gamma \neq 0 , \tag{10}$$

where γ is in $F(i)$. In the same manner,

$$_kj_{rq} = d_{kr} j_{k+rq} \qquad (k=1, \cdots, q-1 \; ; r=1, \cdots, p-1) ,$$

where each d_{kr} is a number $\neq 0$ of $F(i)$, and the second members may be introduced as new units j. Thus

$$(11)\quad j_k j_{rq}=j_{k+rq}\ ,\qquad j_q j_k=\alpha_k j_{q+k}\quad (k=1,\cdots,q-1\ ;\ r=1,\cdots,p-1)\ ,$$

where each α_k is a number $\neq 0$ of $F(i)$. By the first relations in (10) and (11), any $j_s (s\geqq q)$ may be expressed as a product of a certain $j_k (0\leqq k<q)$ by a certain j_q^r. Hence every element of algebra Γ is of the form

$$(12)\qquad \mathscr{A}=\sum_{k=0}^{p-1} A_k j_q^k\ ,$$

where each A_k is in Σ, being of the form

$$(13)\qquad A=\sum_{k=0}^{q-1} f_k j_k\ ,$$

where f_k is a polynomial $f_k(i)$ in i with coefficients in F.

By (5) and (11_2),

$$j_q A=f_0(\theta_q)j_q+\sum_{k=1}^{q-1} f_k(\theta_q)\alpha_k j_{q+k}\ .$$

The final j is equal to $j_k j_q$ by (11_1). Hence

$$(14)\qquad j_q A=A' j_q\ ,\qquad A'=f_0(\theta_q)+\sum_{k=1}^{q-1} f_k(\theta_q)\alpha_k j_k\quad \text{for } A \text{ in (13)}\ .$$

Thus j_k transforms any element A of Σ into an element of A' of Σ. Write A'' for $(A')'$, $\cdots$, $A^{(r+1)}$ for $(A^{(r)})'$. By induction,

$$(15)\qquad j_q^r A=A^{(r)} j_q^r\ .$$

In particular, since $\gamma=j_q^p$ is commutative with j_q,

$$(16)\qquad \gamma'=\gamma\neq 0\ .$$

By (15) for $r=p+s$ and (10_2),

$$A^{(p+s)}\gamma j_q^s=\gamma j_q^s A=\gamma A^{(s)} j_q^s\ ,$$

$$(17)\qquad A^{(p+s)}=\gamma A^{(s)}\gamma^{-1}\ .$$

For any elements A and B in Σ,

$$(AB)^{(r)} j_q^r=j_q^r AB=A^{(r)} j_q^r B=A^{(r)} B^{(r)} j_q^r\ ,$$

$$(18)\qquad (AB)^{(r)}=A^{(r)}B^{(r)}\ ,\qquad (A+B)^{(r)}=A^{(r)}+B^{(r)}\ .$$

Let

$$\mathscr{B}=\sum_{l=0}^{p-1} B_{ij}{}^{l}_{q}\,. \tag{19}$$

Then

$$\mathscr{A}\mathscr{B}=\mathscr{P}=\sum_{s=0}^{p-1} P_s j^{s}_{q}\,, \tag{20}$$

$$P_s=\sum_{k=0}^{s} A_k B^{(k)}_{s-k}+\sum_{k=s+1}^{p-1} A_k B^{(k)}_{p+s-k}\gamma\,.$$

This gives the product of any two elements of Γ as an element of Γ.

Heretofore we have assumed that Γ is associative and deduced various needed formulas. We shall now proceed conversely and abstractly and establish the following result.

THEOREM 2. *Let Σ be an associative algebra to every element A of which corresponds a unique element A' of Σ. Define $A''=(A')'$, $\cdots$, $A^{(r)}=(A^{(r-1)})'$, so that $(A^{(r)})^{(s)}=A^{(r+s)}$. Let Σ contain an element $\gamma=\gamma'\neq 0$. Let the $A^{(r)}$ have the properties* (17) *and* (18). *Consider the set Γ of elements $\mathscr{A}=(A_0, A_1, \cdots, A_{p-1})$ in which the A_k range independently over Σ. Define the product of $\mathscr{A}$ by $\mathscr{B}=(B_0, \cdots, B_{p-1})$ to be $\mathscr{P}=(P_0, \cdots, P_{p-1})$, where P_s is given by* (20). *Then this multiplication is associative.*

We shall now give a direct proof, and later an indirect proof (§8). Let $\mathscr{C}=(C_0, \cdots, C_{p-1})$ be any third element of Γ. Then $\mathscr{P}\mathscr{C}=\mathscr{D}$, where

$$D_r=\sum_{s=0}^{r} P_s C^{(s)}_{r-s}+\sum_{s=r+1}^{p-1} P_s C^{(s)}_{p+r-s}\gamma\,.$$

Inserting the value (20) of P_s, we get $D_r=d_1+d_2+d_3+d_4$, where

$$d_1=\sum_{s=0}^{r}\sum_{k=0}^{s} A_k B^{(k)}_{s-k} C^{(s)}_{r-s}\,, \qquad d_2=\sum_{s=0}^{r}\sum_{k=s+1}^{p-1} A_k B^{(k)}_{p+s-k}\gamma C^{(s)}_{r-s}\,,$$

$$d_3=\sum_{s=r+1}^{p-1}\sum_{k=0}^{s} A_k B^{(k)}_{s-k} C^{(s)}_{p+r-s}\gamma\,, \qquad d_4=\sum_{s=r+1}^{p-1}\sum_{k=s+1}^{p-1} A_k B^{(k)}_{p+s-k}\gamma C^{(s)}_{p-r-s}\gamma\,.$$

Next, $\mathscr{B}\mathscr{C}=\mathscr{Q}=(Q_0, \cdots)$, where

$$Q_s=\sum_{t=0}^{s} B_t C^{(t)}_{s-t}+\sum_{t=s+1}^{p-1} B_t C^{(t)}_{p+s-t}\gamma\,,$$

and $\mathscr{A}\mathscr{Q}=\mathscr{E}=(E_0, \cdots)$, where

$$E_r=\sum_{k=0}^{r} A_k Q^{(k)}_{r-k}+\sum_{k=r+1}^{p-1} A_k Q^{(k)}_{p+r-k}\gamma\,.$$

We insert the value of $Q_s^{(k)}$ found from Q_s by use of (18) and $\gamma^{(k)}=\gamma$. We get $E_r=M+R+S+T$, where

$$M=\sum_{k=0}^{r}\sum_{t=0}^{r-k}A_kB_t^{(k)}C_{r-k-t}^{(t+k)}, \qquad R=\sum_{k=0}^{r}\sum_{t=r-k+1}^{p-1}A_kB_t^{(k)}C_{p-t+r-k}^{(t+k)}\gamma,$$

$$S=\sum_{k=r+1}^{p-1}\sum_{t=0}^{p+r-k}A_kB_t^{(k)}C_{p+r-k-t}^{(t+k)}\gamma, \qquad T=\sum_{k=r+1}^{p-1}\sum_{t=p+r-k+1}^{p-1}A_kB_t^{(k)}C_{2p-t+r-k}^{(t+k)}\gamma\gamma.$$

In M write $s=t+k$; we get d_1. In T, $t+k\geqq p+r+1>p$; we write $s=t+k-p$, apply (17), and get

$$T=\sum_{k=r+1}^{p-1}\sum_{s=r+1}^{k-1}A_kB_{s-k+p}^{(k)}\gamma C_{p+r-s}^{(s)}\gamma=\sum_{s=r+1}^{p-2}\sum_{k=s+1}^{p-1}=d_4.$$

In the terms of R having $t+k<p$, we set $s=t+k$ and get R_1; in those having $t+k\geqq p$, we set $s=t+k-p$, apply (17), and get R_2:

$$R_1=\sum_{k=0}^{r}\sum_{s=r+1}^{p-1}A_kB_{s-k}^{(k)}C_{p+r-s}^{(s)}\gamma, \qquad R_2=\sum_{k=0}^{r}\sum_{s=0}^{k-1}A_kB_{p+s-k}^{(k)}\gamma C_{r-s}^{(s)}=\sum_{s=0}^{r}\sum_{k=s+1}^{r}.$$

Treating S as we did R, we get $S=S_1+S_2$,

$$S_1=\sum_{k=r+1}^{p-1}\sum_{s=k}^{p-1}A_kB_{s-k}^{(k)}C_{p+r-s}^{(s)}\gamma=\sum_{s=r+1}^{p-1}\sum_{k=r+1}^{s},$$

$$S_2=\sum_{k=r+1}^{p-1}\sum_{s=0}^{r}A_kB_{p+s-k}^{(k)}\gamma C_{r-s}^{(s)}.$$

In R_1 and S_2 we may interchange the summation signs since the limits are constants. We see that $R_1+S_1=d_3$, $R_2+S_2=d_2$. Hence $\mathscr{AB}\cdot\mathscr{C}=\mathscr{A}\cdot\mathscr{BC}$ for any three elements of Γ.

8. **Γ as an algebra of matrices with elements in Σ.** To $\mathscr{A}$ in (12) we make correspond the square matrix

$$(21)\quad \begin{Bmatrix} A_0 & A_1 & A_2 & \cdots & A_{p-3} & A_{p-2} & A_{p-1} \\ A'_{p-1}\gamma & A'_0 & A'_1 & \cdots & A'_{p-4} & A'_{p-3} & A'_{p-2} \\ A''_{p-2}\gamma & A''_{p-1}\gamma & A''_0 & \cdots & A''_{p-5} & A''_{p-4} & A''_{p-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ A_2^{(p-2)}\gamma & A_3^{(p-2)}\gamma & A_4^{(p-2)}\gamma & \cdots & A_{p-1}^{(p-2)}\gamma & A_0^{(p-2)} & A_1^{(p-2)} \\ A_1^{(p-1)}\gamma & A_2^{(p-1)}\gamma & A_3^{(p-1)}\gamma & \cdots & A_{p-2}^{(p-1)}\gamma & A_{p-1}^{(p-1)}\gamma & A_0^{(p-1)} \end{Bmatrix},$$

denoted by $[\mathscr{A}]$, in which any row is derived from the preceding row by permuting its elements cyclically, adding another accent, and multiplying the new first element by $\gamma=\gamma'$ on the right. Using $\gamma'=\gamma$, (18) and the case $A^{(p)}=\gamma A\gamma^{-1}$ of (17), we find that* $[\mathscr{A}][\mathscr{B}]=[\mathscr{P}]$, where the P_s are given by (20). However, it is sufficient to compute only the elements of the first row of the product in view of the corollary below.

THEOREM 3. *Let $M=(m_{ij})$ be any p-rowed square matrix and $M'=(m'_{ij})$. Let T be the p-rowed square matrix† whose elements one place to the right of the diagonal are all* 1, *whose first element in the last row is $\gamma=\gamma'\neq 0$, and whose further elements are all zero. Then $TMT^{-1}=M'$ if and only if M is of the form* (21) *and $A_i^{(p)}=\gamma A_i\gamma^{-1}(i=0,1,\cdots,p-1)$, where $A''=(A')',\cdots,A^{(k)}=A'^{(k-1)}$.*

For, if we multiply the first row of M on the left by γ and carry it to the new last row, we get TM. If we multiply the last column of M' by γ on the right and carry it to the new first column, we get $M'T$. Thus $TM=M'T$ if and only if the second row of M (which is the first row of TM) is the first row of $M'T$ and hence is derived from the first row of M' by permuting its elements cyclically and multiplying the new first element by γ on the right, and if the third row of M (second of TM) is derived as before from the second row of M' and hence is derived in the same way from the second row of M with the addition of another accent, . . ., and finally if we permute cyclically the elements of the last row of M, add an accent, and multiply the new first element by γ on the right we get the last row of TM (which is the product of the first row of M by γ on the left).

Let also a second matrix N have the property that $TNT^{-1}=N'$. For any two elements m and n of M and N, let $(mn)'=m'n'$. Then evidently $(MN)'=M'N'$. Thus

$$TMNT^{-1}=M'N'=(MN)'\ .$$

Hence by Theorem 3, MN is of the form (21).

COROLLARY. *Under the assumptions* (18), $\gamma'=\gamma\neq 0$, *and $A^{(p)}=\gamma A\gamma^{-1}$, the product of any two matrices of type* (21) *is of that type.*

9. **Associativity conditions.** We seek the conditions on the constants of multiplication of Γ that Γ be an associative algebra. For A' defined in (14),

---

* Under the usual rule of multiplication of matrices, provided an element of $[\mathscr{A}]$ is kept as a left factor and one of $[\mathscr{B}]$ as a right factor.

† For $p=3$, $T=\begin{pmatrix}0&1&0\\0&0&1\\\gamma&0&0\end{pmatrix}$.

we see that $(A+B)'=A'+B'$ is satisfied identically. Hence $(AB)'=A'B'$ for all A and B in Σ if and only if it holds for $A=fj_k$, $B=hj_r(k, r=0, 1, \cdots, q-1)$, where f and h are arbitrary numbers of $F(i)$. This property holds identically if $k=0$ or $r=0$. Hence let $k>0, r>0$. Then

$$A'=f(\theta_q)\alpha_k j_k\ , \qquad B'=h(\theta_q)\alpha_r j_r\ .$$

By Lemma 2, $j_k j_r=c_{kr}j_u$, where c_{kr} is in $F(i)$ and u is determined so that $\theta_r[\theta_k(i)]=\theta_u(i)$. Thus

$$A'B'=f(\theta_q)\alpha_k h[\theta_q(\theta_k i)]\alpha_r(\theta_k)c_{kr}j_u\ ,$$
$$(AB)'=f(\theta_q)h[\theta_k(\theta_q i)]c_{kr}(\theta_q)\alpha_u j_u\ ,$$

if we take $\alpha_0=1$. The two h's are equal by (7). Hence*

$$\alpha_k\alpha_r(\theta_k)c_{kr}=c_{kr}(\theta_q)\alpha_u \qquad (k, r=1, \cdots, q-1;\ \alpha_0=1). \tag{22}$$

It remains to consider $A^{(p)}=\gamma A\gamma^{-1}$. From (14) we get by induction

$$A^{(s)}=f_0(\theta_q^s)+\sum_{k=1}^{q-1} f_k(\theta_q^s)\alpha_k(\theta_q^{s-1})\alpha_k(\theta_q^{s-2})\cdots\alpha_k(\theta_q)\alpha_k j_k\ ,$$

where θ_q^s denotes the sth iterative of $\theta_q(i)$. By (9), $\theta_q^p=i$. Taking $s=p$, we get

$$\alpha_k\alpha_k(\theta_q)\alpha_k(\theta_q^2)\cdots\alpha_k(\theta_q^{p-1})=\gamma\gamma^{-1}(\theta_k) \quad (k=1, \cdots, q-1). \tag{23}$$

Finally, $\gamma=\gamma'$ if and only if

$$\gamma=\gamma(\theta_q)\ . \tag{24}$$

THEOREM 4. *If Σ is associative, algebra Γ with an abelian group is associative if and only if conditions* (22)–(24) *hold.*

If $q=1$, conditions (22) and (23) are satisfied vacuously, while Σ is the field $F(i)$ and Γ is of type D of §4.

COROLLARY. *An algebra of type D is associative if and only if $\gamma=\gamma(\theta_1)$, which implies that γ is in F.*

10. **Algebras Γ whose abelian group has two generators.** The subgroup G_q is now cyclic. Hence by Theorem 1, algebra Σ is now of type D of order q^2 over the field F_1 derived from F by adjoining all the symmetric functions of $i, \theta_1, \cdots, \theta_{q-1}$. By §4, we may take $j_k=j_1^k(k=2, \cdots, q-1)$, $j_1^q=g$, where g is in F_1, a necessary and sufficient condition for which is $g=g(\theta_1)$. In (6),

* Note that (22) is the condition that we obtain equal results when we express $j_q\cdot j_k j_r$ and $j_q j_k\cdot j^r$ in the form $(\ )j_q$. This interpretation is useful when we consider a Γ whose G has more than two generators.

$$j_r j_k = j_u , \quad u = r+k , \quad c_{rk} = 1 \qquad (r+k<q) ,$$

$$j_r j_k = g j_u , \quad u = r+k-q , \quad c_{rk} = g \qquad (r+k \geqq q , r<q , k<q) .$$

Hence associativity conditions (22) become

$$\alpha_k \alpha_r(\theta_1^k) = \alpha_{r+k} \qquad (r, k = 1, \cdots, q-1 ; r+k<q) , \tag{25}$$

$$\alpha_k \alpha_r(\theta_1^k) g = g(\theta_q)\alpha_{r+k-q} \qquad (r<q , k<q , r+k \geqq q) , \tag{26}$$

where $\alpha_0 = 1$. Write α for α_1. For $r = 1$, (25) gives by induction

$$\alpha_k = \alpha\alpha(\theta_1)\alpha(\theta_1^2) \cdots \alpha(\theta_1^{k-1}) \qquad (k = 1, \cdots, q-1) . \tag{27}$$

Then every (25) follows at once from (27). For $r+k=q$ in (26), we replace the α's by their values (27), note that the final α is $\alpha_0 = 1$, and get at once

$$\alpha\alpha(\theta_1)\alpha(\theta_1^2) \cdots \alpha(\theta_1^{q-1}) g = g(\theta_q) . \tag{28}$$

For $r+k>q$, the value from (27) of the final α in (26) cancels with part of the the left member, whence

$$\alpha(\theta_1^{r+k-q})\alpha(\theta_1^{r+k-q+1}) \cdots \alpha(\theta_1^{r+k-1}) g = g(\theta_q) .$$

The q exponents form an arithmetical progression with the common difference 1 and hence are congruent modulo q to $0, 1, \cdots, q-1$ in some order. Hence the relation is (28).

Relations (23) all follow from the case $k = 1$:

$$\alpha\alpha(\theta_q)\alpha(\theta_q^2) \cdots \alpha(\theta_q^{p-1}) = \gamma\gamma^{-1}(\theta_1) . \tag{29}$$

For, if in (29) we replace i by $i, \theta_1, \theta_1^2, \cdots, \theta_1^{k-1}$ in turn, multiply together the resulting equations and apply (27), we obtain (23). Hence Γ is associative if and only if $g = g(\theta_1)$, $\gamma = \gamma(\theta_q)$, and (27), (28), (29) hold. Of these, (27) serve merely to express the α_k in terms of α.

THEOREM 5. *Let $f(x) = 0$ be an equation of degree pq irreducible in a field F whose Galois group for F is abelian and has two independent generators Θ_1 and Θ_q of orders q and p respectively. Then its roots* are*

$$\theta_1^k[\theta_q^r(i)] = \theta_q^r[\theta_1^k(i)] \qquad (k = 0, 1, \cdots, q-1 ; r = 0, 1, \cdots, p-1) ,$$

where θ_1 and θ_q are rational functions of i with coefficients in F such that the

* We may ignore the group and start with any irreducible equation whose pq roots are of the specified type.

qth iterative $\theta_1^q(i)$ *of* $\theta_1(i)$ *is* i *and likewise* $\theta_q^p(i)=i$. *There exists an associative algebra* Σ *whose elements are*

$$f_0+f_1j_1+f_2j_1^2+\cdots+f_{q-1}j_1^{q-1}, \tag{30}$$

where the f_k *are polynomials in* i *of degree* $\leqq pq-1$ *with coefficients in* F, *while*

$$j_1^q=g(i)=g(\theta_1)\ , \qquad j_1^r\phi(i)=\phi[\theta_1^r(i)]j_1^r \qquad (r=1,\cdots,q-1)\ ,$$

so that the product of any two elements (30) *of* Σ *is another element* (30) *of* Σ. *Under multiplication defined by* (20), *the totality of polynomials in* j_q *with coefficients in* Σ *form an algebra* Γ *of order* p^2q^2 *over* F *which is associative if and only if the four conditions* (24), (28),(29), *and* $g=g(\theta_1)$ *hold between the parameters* g,γ,α *of* Γ.

The conditions for associativity are not inconsistent since they are satisfied when $\alpha=1$ and g and γ are both in F. In this case the constants of multiplication of Γ all belong to F. It follows by induction from (22)–(24) that the corresponding results hold when G is abelian and has any number of generators.

Note that Γ has the basis $i^rj_1^aj_q^b$ $(r<pq,\ a<q,\ b<p)$. The laws of multiplication follow readily by the associative law from

$$j_1^q=g\ , \quad j_q^p=\gamma\ , \quad j_qj_1=\alpha j_1j_q\ , \quad j_ti=\theta_t(i)j_t \qquad (t=1,q)\ . \tag{31}$$

We find by induction that

$$j_q^rj_1^k=A_{rk}j_1^kj_q^r\ , \quad A_{rk}=\alpha_k\alpha_k(\theta_q)\cdots\alpha_k(\theta_q^{r-1})\ , \tag{32}$$

while $\alpha_k=\alpha\alpha(\theta_1)\cdots\alpha(\theta_1^{k-1})$, in accord with (27). Then for any polynomials u and w in $F(i)$, we have

$$uj_1^aj_q^b\cdot wj_1^cj_q^d=uw(\theta_1^a\theta_q^b)A_{bc}(\theta_1^a)j_1^{a+c}j_q^{b+d}\ . \tag{33}$$

If $zj_1^fj_q^h$ is any third element of Γ, we find that the associative law holds if and only if*

$$A_{bc}A_{b+d,f}(\theta_1^c)=A_{b,c+f}A_{df}(\theta_1^c\theta_q^b)\ , \tag{34}$$

which is independent of a,h,u,w,z. Since (34) involves four indices b,c,d,f, whereas (25), etc., involved only two, the present direct method of finding the conditions for associativity is far more complicated than our earlier indirect method.

11. **Representation as a matric algebra.** We shall represent algebra

* The initial condition was (34) with i replaced by θ^a If $f=1$, (34) reduces to (25).

Γ of §10 as an algebra of matrices with elements in $F(i)$. First we give such a representation of its subalgebra Σ of elements (30). We make use of §8 with Γ and Σ replaced by our present Σ and $F(i)$, respectively, and $j_q A = A' j_q$ in (14) replaced by $j_1 a = a(\theta_1) j_1$, where a is in $F(i)$. Hence to the element f given by (30) we make correspond the matrix

$$(35)\quad \left\{ \begin{array}{cccccc} f_0 & f_1 & f_2 & \cdots & f_{q-1} \\ f_{q-1}(\theta_1)g & f_0(\theta_1) & f_1(\theta_1) & \cdots & f_{q-2}(\theta_1) \\ f_{q-2}(\theta_1^2)g & f_{q-1}(\theta_1^2)g & f_0(\theta_1^2) & \cdots & f_{q-3}(\theta_1^2) \\ \cdots\cdots\cdots\cdots & & \cdots & & \cdots\cdots \\ f_1(\theta_1^{q-1})g & f_2(\theta_1^{q-1})g & f_3(\theta_1^{q-1})g & \cdots & f_0(\theta_1^{q-1}) \end{array} \right\},$$

which we denote by (f). Since $g(\theta_1) = g$, and $\theta_1^q(i) = i$, it follows from §8 without further discussion that $fr = s$ implies $(f)(r) = (s)$. These results have been established otherwise,* since Σ is an algebra of type D of order q^2 over F_1.

In matrix (21) replace each entry f, which is an element of Σ, by its matric representation (f). Such a p-rowed matrix $[\mathscr{A}]$ whose elements are q-rowed matrices gives rise at once to a pq-rowed matrix $\{\mathscr{A}\}$, formed by erasing the parentheses which enclose the elements of the sub-matrices. For example, let $p = q = 2$, $A_0 = a + bj_1$, $A_1 = c + dj_1$, whence $A_0' = a_2 + b_2\alpha j_1$, where a_2 denotes $a(\theta_2)$. Writing a_k for $a(\theta_k)$, $\theta_3(i) = \theta_1[\theta_2(i)]$, we have from (35)

$$(A_0) = \begin{pmatrix} a & b \\ b_1 g & a_1 \end{pmatrix}, \qquad (A_1) = \begin{pmatrix} c & d \\ d_1 g & c_1 \end{pmatrix},$$

and then from (21)

$$(36)\quad \{\mathscr{A}\} = \left\{ \begin{array}{cccc} a & b & c & d \\ b_1 g & a_1 & d_1 g & c_1 \\ c_2\gamma & d_2\alpha\gamma_1 & a_2 & b_2\alpha \\ d_3\alpha_1\gamma g & c_3\gamma_1 & b_3\alpha_1 g & a_3 \end{array} \right\},$$

since $A_1'\gamma = c_2\gamma + d_2\alpha j_1\gamma$, $j_1\gamma = \gamma_1 j_1$, $\gamma_2 = \gamma$.

The matrices $\{\mathscr{A}\}$ give the desired matric representation of Γ since the equation $\mathscr{A}\mathscr{B} = \mathscr{P}$ between any three elements of Γ implies $[\mathscr{A}][\mathscr{B}] = [\mathscr{P}]$, by §8, which in turn implies $\{\mathscr{A}\}\{\mathscr{B}\} = \{\mathscr{P}\}$. This is due to the following general theorem. Let (a) be a pq-rowed square matrix having a_{ij} as the element in the ith row and jth column. Let $(a)(b) = (c)$. By grouping the

* *Algebras and their Arithmetics*, pp. 221–24.

successive rows of (a) in blocks of q each and its successive columns in blocks of q, we obtain a compound matrix

$$[A]=\begin{pmatrix} A_{q,q} & A_{q,2q} & \cdots & A_{q,pq} \\ \cdots & \cdots & \cdots & \cdots \\ A_{pq,q} & A_{pq,2q} & \cdots & A_{pq,pq} \end{pmatrix},$$

where $A_{r,s}$ is a q-rowed square matrix having a_{rs} as the last element of the last row. For example, if $p=q=2$,

$$A_{22}=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad A_{24}=\begin{pmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{pmatrix}, \quad A_{42}=\begin{pmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{pmatrix},$$

$$A_{44}=\begin{pmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{pmatrix}.$$

The element in the ith row and jth column of $[A][B]$ is

$$\sum_{s=1}^{p} A_{iq,sq}B_{sq,jq}=C_{iq,jq},$$

whence $[A][B]=[C]$. Conversely, this implies $(a)(b)=(c)$.

The present method evidently leads to a representation by matrices with elements in $F(i)$ of any algebra Γ whatever be the number of generators of its abelian group. The existence of such a representation was proved by Cecioni by means of various technical theorems on linear algebras and matrices.

12. **Division algebras Γ with $p=2$.** We assume that Σ is a division algebra. Multiplication (20) in Γ becomes for $p=2$

$$(37) \qquad (A_0+A_1j_q)(B_0+B_1j_q)=(A_0B_0+A_1B_1'\gamma)+(A_0B_1+A_1B_0')j_q.$$

Let this product be zero while neither factor is zero. If $B_1=0$, then $B_0\neq 0$, $B_0'\neq 0$, $A_0B_0=0$, $A_1B_0'=0$, $A_0=A_1=0$, contrary to hypothesis. Since $B_1\neq 0$ it has an inverse in Σ, and the product is equal to

$$[(A_0+A_1j_q)B_1][B_1^{-1}B_0+j_q].$$

Hence it suffices to treat the case $B_1=1$. Then

$$A_0B_0+A_1\gamma=0, \qquad A_0+A_1B_0'=0.$$

If $A_1=0$, then $A_0=0$, contrary to hypothesis. Elimination of A_0 gives $A_1(\gamma-B_0'B_0)=0$.

THEOREM 6. *If $p=2$ and if Σ is a division algebra, then Γ is a division algebra if and only if**

* Note that $X'X$ and XX' are usually distinct. If they are equal when $X=j_1$, then $\alpha(\theta_1)=\alpha$. Write χ_3 for $g\gamma\alpha(\theta_1)$ and χ_2 for γ. Then $g=g(\theta_1)$ implies $\chi_3(\theta_1):\chi_3=\chi_2(\theta_1):\chi_2$. But in Cecioni's example (his §24), $\chi_3(\theta_1)=-\chi_3$, while $\chi_2(\theta_1)$ is distinct from $-\chi_2$ since $g_2\neq 0$ by his (52).

$$\gamma \neq X'X \text{ for any } X \text{ in } \Sigma . \tag{38}$$

If $q=2$, but p is arbitrary, Theorem 1 shows that Σ is the algebra over F_1 with the basal units $1, i, j_1, ij_1$ and is of type D with $n=2$, where F_1 is derived from F by the adjunction of the sum and the product of i and $\theta_1(i)$. It is associative if and only if $j_1^2=g$ is in F_1, i.e., if $g=g(\theta_1)$. We may apply Theorem 6 with Γ replaced by Σ and Σ replaced by the division algebra $F_1(i)$. When Σ is regarded as an algebra Γ, its q is 1, whence X' is $X(\theta_1)$. Hence for $q=2$, Σ is a division algebra if and only if $g \neq X(\theta_1)X$ for any X in $F_1(i)$, or in other words if g is not the norm, relative to F_1, of any number of $F_1(i) = F(i)$.

Applying also Theorem 5 for $p=q=2$, we obtain

THEOREM 7. *Let a quartic equation irreducible in F have the roots i, $\theta_1(i)$, $\theta_2(i)$, $\theta_3(i)$, where the $\theta_k(i)$ are rational functions of i with coefficients in F such that*

$$\theta_1\theta_1=\theta_2\theta_2=\theta_3\theta_3=i , \quad \theta_1\theta_2=\theta_2\theta_1=\theta_3 , \quad \theta_1\theta_3=\theta_3\theta_1=\theta_2 , \quad \theta_2\theta_3=\theta_3\theta_2=\theta_1 ,$$

where $\theta_r\theta_s$ denotes $\theta_r[\theta_s(i)]$. Under the law of multiplication

$$(a+bj_1)(c+dj_1)=ac+gbd(\theta_1)+[ad+bc(\theta_1)]j_1 , \tag{39}$$

where a,b,c,d,g are in $F(i)$, the elements $a+bj_1$ form an associative division algebra Σ if and only if g is in the field $F_1=F(i+\theta_1, i\theta_1)$, but is not the norm, relative to F_1, of any number of $F_1(i)=F(i)$. For $A=a+bj_1$, write $A'=a(\theta_2)+b(\theta_2)\alpha j_1$, where α and γ are in $F(i)$. Under the law of multiplication (37), *where A_0, A_1, B_0, B_1 are in Σ, the elements $A_0+A_1j_2$ form an associative division algebra Γ, when Σ is one, if and only if* (38) *holds and*

$$\alpha\alpha(\theta_1)g=g(\theta_2) , \quad \alpha\alpha(\theta_2)\gamma(\theta_1)=\gamma=\gamma(\theta_2) . \tag{40}$$

This Γ is an algebra over F with the 16 basal units $i^rj_s (r,s=0,1,2,3)$, where $j_3=j_1j_2$. Special cases of our laws of multiplication give

$$\begin{gathered} j_1^2=g , \quad j_2^2=\gamma , \quad j_1j_2=j_3 , \quad j_2j_1=\alpha j_3 , \quad j_1j_3=gj_2 , \\ j_2j_3=\alpha\gamma(\theta_1)j_1 , \quad j_3j_1=g\alpha(\theta_1)j_2 , \quad j_3j_2=\gamma(\theta_1)j_1 , \quad j_3^2=g\gamma\alpha(\theta_1) , \end{gathered} \tag{41}$$

as well as $j_ri=\theta_r(i)j_r$ and its consequence (5).

Cecioni gave a special example of Γ in which are satisfied the conditions that it be an associative division algebra.

13. **Division algebras Γ with $p=3$.** We assume that Σ is a division algebra. Suppose that $\mathscr{P}\mathscr{Q}=0$, where $\mathscr{P}$ and $\mathscr{Q}=K+Lj_q+Mj_q^2$ are elements $\neq 0$ of Γ, K, L and M being in Σ. If $M\neq 0$, we have

$$\mathscr{R}=\mathscr{Q}(j_q^2-Z)=U+Vj_q+Wj_q^2 , \quad W=K-MZ'' ,$$

since $j_q^3=\gamma$ is in Σ. Then $W=0$ if $Z=(M'\gamma)^{-1}K'\gamma$. We postpone the subcase $\mathscr{R}=0$. But if $M=0$, write $\mathscr{R}=\mathscr{Q}$. In either case, we have $\mathscr{P}\mathscr{R}=0$, where $\mathscr{R}=C+Dj_q$, $\mathscr{P}\neq 0$, $\mathscr{R}\neq 0$. If $D=0$, then $C\neq 0$, $\mathscr{P}\mathscr{R}C^{-1}=\mathscr{P}=0$. Hence $D\neq 0$, $\mathscr{A}\mathscr{B}=0$, where $\mathscr{A}=\mathscr{P}D\neq 0$, $\mathscr{B}=D^{-1}C+j_q$. Employing the notations (12) and (19) for $\mathscr{A}$ and $\mathscr{B}$, we have $B_1=1$, $B_2=0$. For $p=3$, (20) gives

$$
\begin{aligned}
&P_0=A_0B_0+A_1B_2'\gamma+A_2B_1''\gamma\ ,\\
&P_1=A_0B_1+A_1B_0'+A_2B_2''\gamma\ ,\quad P_2=A_0B_2+A_1B_1'+A_2B_0''.
\end{aligned}
\tag{42}
$$

Since $B_1=1$, $B_2=0$, and each $P_k=0$, we have

$$A_0B_0+A_2\gamma=0\ ,\quad A_0+A_1B_0'=0\ ,\quad A_1+A_2B_0''=0\ .$$

Hence $A_2\neq 0$. Elimination of A_0 and A_1 gives

$$A_2(B_0''B_0'B_0+\gamma)=0\ .$$

Write $B_0=-X$. Thus $\gamma=X''X'X$. In the postponed case $\mathscr{R}=0$, we have $\mathscr{R}j_q=0$, or $\mathscr{Q}(\gamma-Zj_q)=0$, while neither factor is zero. But this is the case $\mathscr{A}\mathscr{B}=0$ just treated.

THEOREM 8. *If $p=3$ and if Σ is a division algebra, then Γ is a division algebra if and only if*

$$\gamma\neq X''X'X \text{ for any } X \text{ in } \Sigma\ . \tag{43}$$

If $q=3$, but p is arbitrary, and if F_1 is derived from F by the adjunction of the elementary symmetric functions of i, $\theta_1(i)$, $\theta_2(i)$, Theorem 1 shows that Σ is an algebra over F_1 of type D with the basal units $i^rj_s(r,s=0,1,2)$, where $j_2=j_1^2$. It is associative if and only if $j_1^3=g$ is in F_1. We may apply Theorem 8 with Γ and Σ replaced by Σ and $F_1(i)$ respectively. When Σ is regarded as an algebra Γ, its q is 1, whence X' is $X(\theta_1)$. Hence for $q=3$, Σ is a division algebra if and only if $g\neq X(\theta_2)X(\theta_1)X$ for any X in $F_1(i)$, or in other words if g is not the norm, relative to F_1, of any number of $F_1(i)=F(i)$.

Applying also Theorem 5 for $p=q=3$, we obtain

THEOREM 9. *Let an equation of degree 9 irreducible in F have the roots*

$$\theta_1^k[\theta_3^r(i)]=\theta_3^r[\theta_1^k(i)] \qquad (k,r=0,1,2)\ ,$$

where θ_1 and θ_3 are rational functions of i with coefficients in F such that $\theta_1^3(i)=i$, $\theta_3^3(i)=i$. Let F_1 be derived from F by adjoining the elementary symmetric functions of i, θ_1, $\theta_1^2(i)$. Let Σ be the set of all linear functions of $1, j_1, j_2=j_1^2$ with

coefficients in $F(i)$ and let multiplication be performed in Σ by means of (5) *and* $j_1^3=g$. *Then Σ is an associative division algebra if and only if g is in F_1, but is not the norm, relative to F_1, of any number of $F(i)$. Let*

$$A'=a(\theta_3)+b(\theta_3)\alpha j_1+c(\theta_3)\alpha\alpha(\theta_1)j_2 \quad \textit{for} \quad A=a+bj_1+cj_2 . \tag{44}$$

Under the law of multiplication

$$(A_0+A_1j_3+A_2j_3^2)(B_0+B_1j_3+B_2j_3^2)=P_0+P_1j_3+P_2j_3^2 ,$$

where the P_k are defined by (42), *with γ in $F(i)$, the elements $A_0+A_1j_3+A_2j_3^2$ in which the A_k range independently over Σ form an associative division algebra Γ if and only if $\gamma\neq X''X'X$ for any X in Σ and*

$$g=g(\theta_1) , \quad \gamma=\gamma(\theta_3) , \quad \alpha\alpha(\theta_1)\alpha(\theta_1^2)g=g(\theta_3) , \quad \alpha\alpha(\theta_3)\alpha(\theta_3^2)\gamma(\theta_1)=\gamma . \tag{45}$$

Evidently Γ is an algebra over F with the 81 basal units ij_s $(r,s=0,1,\cdots,8)$. For brevity write f_k for $f(\theta_k)$, and $C=\alpha\alpha_1\alpha_3\alpha_4$. Then the multiplication table of Γ is given by (5) and the following relations in which j_r is denoted by r:

$1^2=2$, $12=g$, $13=4$, $14=5$, $15=g3$, $16=7$, $17=8$, $18=g6$,
$21=g$, $2^2=g1$, $23=5$, $24=g3$, $25=g4$, $26=8$, $27=g6$, $28=g7$,
$31=\alpha4$, $32=\alpha\alpha_1 5$, $3^2=6$, $34=\alpha7$, $35=\alpha\alpha_1 8$, $36=\gamma$, $37=\alpha\gamma_1 1$, $38=\alpha\alpha_1\gamma_2 2$,
$41=\alpha_1 5$, $42=g\alpha_1\alpha_2 3$, $43=7$, $44=\alpha_1 8$, $45=g\alpha_1\alpha_2 6$, $46=\gamma_1 1$, $47=\alpha_1\gamma_2 2$,
$48=g\gamma\alpha_1\alpha_2$, $51=g\alpha_2 3$, $52=g\alpha\alpha_2 4$, $53=8$, $54=g\alpha_2 6$, $5^2=g\alpha\alpha_2 7$,
$56=\gamma_2 2$, $57=g\gamma\alpha_2$, $58=g\gamma_1\alpha\alpha_2 1$, $61=\alpha\alpha_3 7$, $62=C8$, $63=\gamma$,
$64=\alpha\alpha_3\gamma_1 1$, $65=C\gamma_2 2$, $6^2=\gamma 3$, $67=\alpha\alpha_3\gamma_1 4$, $68=C\gamma_2 5$,
$71=\alpha_1\alpha_4 8$, $72=gC_1 6$, $73=\gamma_1 1$, $74=\alpha_1\alpha_4\gamma_2 2$, $75=g\gamma C_1$, $76=\gamma_1 4$,
$7^2=\alpha_1\alpha_4\gamma_2 5$, $78=g\gamma C_1 3$, $81=g\alpha_2\alpha_5 6$, $82=gC_2 7$, $83=\gamma_2 2$,
$84=g\gamma\alpha_2\alpha_5$, $85=g\gamma_1 C_2 1$, $86=\gamma_2 5$, $87=g\gamma\alpha_2\alpha_5 3$, $8^2=g\gamma_1 C_2 4$.

14. **Division algebras Γ with $p>3$.** If Γ is a division algebra, then

$$\gamma\neq X^{(p-1)}X^{(p-2)}\cdots X'X \text{ for any } X \text{ in } \Sigma . \tag{46}$$

For, if $\gamma=X^{(p-1)}\cdots X$, then $\mathscr{A}(j_q-X)=0$, while neither factor is zero, if

$$\mathscr{A}=\sum_{k=0}^{p-2} X^{(p-1)}X^{(p-2)}\cdots X^{(k+1)}j_q^k+j_q^{p-1} .$$

For $p=2$ and $p=3$, we proved that conversely (46) implies that Γ is a division algebra. But for $p>3$ no attempt is made here to prove this con-

verse. We cited in §4 Wedderburn's proof for the case in which Γ is an algebra of type D; he employed the determinant of matrix (35) in the matric representation of D. But for the corresponding matrix (21) for Γ, the notion of a determinant is absent since the elements of (21) are not commutative. This particular difficulty is overcome if we use the representation in §11 of Γ as an algebra of matrices $\{\mathscr{A}\}$ with elements in $F(i)$, whence the elements are now commutative. While the constants of multiplication of D involve a single parameter g, those of Γ involve not only the corresponding parameters g and γ, but also a parameter α connected with them by relations (28) and (29). Waiving the difficulty* which thus arises in assuming that γ is an independent variable which may be made zero without altering the analogue of Wedderburn's δ, let us attempt to apply his proof to matrix (36). Since $\gamma=\gamma(\theta_2)$, also $\delta=\delta(\theta_2)$; otherwise $\gamma+\delta$ is not zero and has an inverse. Hence in matrix $\{\gamma+\delta\}$ the elements outside the diagonal are all zero, while those in the diagonal are $e=\gamma+\delta$ and $f=\gamma(\theta_1)+\delta(\theta_1)$ each taken twice. Since $A_1=1$, we have $c=1$, $d=0$ in (36), whose determinant is the sum of $\gamma\gamma_1$ and a linear function of γ and γ_1. This determinant must divide e^2f^2 and hence is equal to ef. For $\gamma=0$, it is seen by inspection to be the product of $\rho=aa_1-gbb_1$ by $\rho(\theta_2)=a_2a_3-gb_2b_3$ in view of (40_1). Taking $\gamma=0$, we get $\delta\delta(\theta_1)=\rho\rho(\theta_2)$. But $\gamma+\delta=0$. Hence the condition is that $\gamma\gamma(\theta_1)\neq\rho\rho(\theta_2)$ for any ρ in $F(i)$.

But this is not a necessary condition that Γ be a division algebra. For, in Cecioni's example (his §24), with $\gamma=\chi_2$, we find that $\gamma\gamma(\theta_1)=-k_1^2=\rho\rho(\theta_2)$ for $\rho=k_1i$. Hence no obvious modification of the method used for D will succeed for Γ.

For $p=2$, q arbitrary, the corresponding condition is

$$\gamma\gamma(\theta_1)\cdot\cdot\cdot\gamma(\theta_{q-1})\neq\sigma\sigma(\theta_q) \text{ for any } \sigma \text{ in } F(i) .$$

15. **Algebras Γ whose group G is not necessarily abelian.** As at the end of §5, let G have an invariant subgroup G_q composed of $\Theta_0=1, \Theta_1, \cdots, \Theta_{q-1}$ and let G_q be extended to G by Θ_q. If p is the index of G_q under G, then Θ_q^p is a substitution Θ_e of G_q, while no lower than the pth power of Θ_q belongs to G_q. Also,

$$\Theta_k\Theta_q=\Theta_q\Theta_{k0} \qquad (k<q) , \tag{47}$$

and the substitutions of G are given without repetition by

$$\Theta_{rq+k}=\Theta_q^r\Theta_k \qquad (r=0,1,\cdots,p-1\ ;\ k=0,1,\cdots,q-1) . \tag{48}$$

* We assume that $q=2$. In $(A+j_2)(B+j_2)=\gamma+AB+(A+B')j_2$, we have $A+B'=0$ by hypothesis. Then $\delta=AB=-B'B$ involves α and hence depends on γ.

Hence (9) holds. As in §7, we may take

$$(49)\quad j_q^r=j_{rq}\ ,\quad j_kj_{rq}=j_{k+rq}\qquad (r=1,\cdots,p-1\ ;\ k=1,\cdots,q-1)$$

and conclude that every element of Γ is of the form (12). By (47) and (6),

$$(50)\quad \theta_k[\theta_q(i)]=\theta_q[\theta_{k_0}(i)]\ ,\quad j_qj_k=\alpha_{kj}j_{k_0}j_q\qquad (k=1,\cdots,q-1)\ ,$$

where α_k is in $F(i)$. Thus

$$(51)\quad j_qA=A'j_q\ ,\quad A'=f_0(\theta_q)+\sum_{k=1}^{q-1}f_k(\theta_q)\alpha_{kj}j_{k_0}\quad \text{for } A \text{ in (13)}\ .$$

Since $\Theta_q^p=\Theta_e$,

$$(52)\quad \theta_q^p(i)=\theta_e(i)\ ,\qquad j_q^p=\gamma\equiv\beta j_e\ ,$$

where β is a number $\neq 0$ of $F(i)$, and $e<q$. Since j_q is commutative with j_q^p,

$$\beta j_{e+q}=\beta j_ej_q=j_q\beta j_e=\beta(\theta_q)j_qj_e=\beta(\theta_q)\alpha_ej_{e_0}j_q\ ,$$

and the final product of the j's is j_{e_0+q}. Hence $e_0=e$ and

$$(53)\quad \beta=\beta(\theta_q)\alpha_e\ ,$$

where $\alpha_e=1$ if $e=0$. Hence $\gamma'=\gamma$. We have (18) and

$$(54)\quad A^{(p)}\gamma=\gamma A\ .$$

By Theorem 2, these relations imply that Γ is associative. We now investigate the conditions for these relations. We require that $(AB)'=A'B'$ for $A=fj_k$, $B=hj_r$ for all f and h in $F(i)$ and for $k, r=0, 1, \cdots, q-1$. We may write $\theta_r[\theta_k(i)]=\theta_u(i)$, whence $j_kj_r=c_{kr}j_u$. Replace i by $\theta_q(i)$ and apply (50_1) three times; we get

$$\theta_r\theta_k\theta_q=\theta_r\theta_q\theta_{k_0}=\theta_q\theta_{r_0}\theta_{k_0}=\theta_u\theta_q=\theta_q\theta_{u_0}\ ,$$

whence

$$\theta_{r_0}\theta_{k_0}=\theta_{u_0}\ ,\qquad j_{k_0}j_{r_0}=c_{k_0r_0}j_{u_0}\ .$$

Then

$$A'=f(\theta_q)\alpha_kj_{k_0}\ ,\qquad B'=h(\theta_q)\alpha_rj_{r_0}\ ,\qquad AB=fh(\theta_k)c_{kr}j_u\ ,$$
$$A'B'=f(\theta_q)\alpha_kh[\theta_q\{\theta_{k_0}(i)\}]\alpha_r(\theta_{k_0})c_{k_0r_0}j_{u_0}\ ,$$
$$(AB)'=f(\theta_q)h[\theta_k\{\theta_q(i)\}]c_{kr}(\theta_q)\alpha_uj_{u_0}\ .$$

The two h's are equal by (50). Hence the conditions are

$$(55)\quad \alpha_k\alpha_r(\theta_{k_0})c_{k_0r_0}=c_{kr}(\theta_q)\alpha_u\qquad (k, r=1,\cdots,q-1\ ;\ \alpha_0=1)\ ,$$

being satisfied identically if $k=0$ or $r=0$.

We next seek the conditions for (54). Write k_{00} for $(k_0)_0$, etc. By (47) we find by induction that

$$\Theta_k\Theta_q^s=\Theta_q^s\Theta_{k0\cdots0}, \tag{56}$$

where the number of zeros is s. The case $s=p$ gives

$$\theta_k\theta_e=\theta_e\theta_{k0\cdots0}, \qquad j_ej_k=d_kj_{k0\cdots0}j_e, \tag{57}$$

where there are p subscripts 0 to k, and d_k is in $F(i)$. By induction on s,

$$A^{(s)}=f_0(\theta_q^s)+\sum_{k=1}^{q-1}f_k(\theta_q^s)\alpha_k(\theta_q^{s-1})\alpha_{k0}(\theta_q^{s-2})\alpha_{k00}(\theta_q^{s-3})\cdots\alpha_{k0\cdots0}j_{k0\cdots0},$$

where there are $s-1$ subscripts 0 to k under the final α, and s of them under j. Take $s=p$ and apply (52_1). We see that the desired conditions for (54) are

$$\beta d_k=\alpha_k(\theta_q^{p-1})\alpha_{k0}(\theta_q^{p-2})\alpha_{k00}(\theta_q^{p-3})\cdots\alpha_{k0\cdots0}\beta(\theta_{k0\cdots0}) \qquad (k=1,\cdots,q-1), \tag{58}$$

where there are $p-1$ subscripts 0 under the last α, and p under the final θ.

THEOREM 10. *If the subalgebra with the units $i'j_k$ $(r<pq, k<q)$ is associative, then Γ is associative if and only if conditions* (53), (55), (58) *hold.*

Consider the simplest non-abelian case in which G_q is a cyclic group generated by Θ_1 such that Θ_q transforms Θ_1 into its inverse. Since Θ_q transforms $\Theta_k=\Theta_1^k$ into Θ_{q-k} and into Θ_{k_0} by (47), the latter subscripts differ only by a multiple of q. Hence

$$\text{if } k=0, \quad k_0=0; \quad \text{if } k>0, \quad k_0=q-k. \tag{59}$$

We employ the values of c_{rk} and u given above ((25) in §10). In (55), $k_0=q-k$, $r_0=q-r$. If $r+k<q$, then $r_0+k_0>q$ and (55) becomes

$$\alpha_k\alpha_r(\theta_1^{q-k})g=\alpha_{k+r} \qquad (r,k=1,\cdots,q-1;\ r+k<q). \tag{60}$$

For $r=1$ this gives by induction on k

$$\alpha_k=\alpha\alpha(\theta_1^{q-1})\alpha(\theta_1^{q-2})\cdots\alpha(\theta_1^{q-k+1})g^{k-1} \qquad (k=1,\cdots,q-1), \tag{61}$$

where $\alpha=\alpha_1$. Then (60) is seen to be satisfied when we insert the values of α_k, α_r, α_{k+r} from (61) and apply $g(\theta_1)=g$, $\theta_1^{q+s}=\theta_1^s$.

For $r+k=q$, whence $r_0+k_0=q$, (55) becomes

$$\alpha_k\alpha_r(\theta_1^{q-k})g=g(\theta_q). \tag{62}$$

Inserting the values of α_k and α_r from (61), we get

$$\alpha\alpha(\theta_1)\alpha(\theta_1^2)\cdot\cdot\cdot\alpha(\theta_1^{q-1})g^{q-1}=g(\theta_q)\ . \tag{63}$$

Finally, for $r+k>q$, (55) becomes

$$\alpha_k\alpha_r(\theta_1^{q-k})=g(\theta_q)\alpha_{k+r-q}\ . \tag{64}$$

Inserting the values (61) of the three α's, we see that the α's from the third α all cancel a like number of α's in the new left member, and that the resulting relation is (63).

Since Θ_q transforms Θ_1 into its inverse and vice versa, Θ_q^s transforms Θ_1 into itself or its inverse according as s is even or odd. Take $s=p$ and note that $\Theta_q^p=\Theta_e=\Theta_1^e$ transforms Θ_1 into itself. We exclude the case $q=2$ since Θ_q then transforms Θ_1 into itself and G is abelian. Hence p is even.

By (59), $k_{00}=k$. Thus (57) becomes $j_e j_k=d_k j_k j_e$. But $j_e=j_1^e$, $j_k=j_1^k$. Hence $d_k=1$. Thus (58) is

$$\beta=\alpha_k(\theta_q^{p-1})\alpha_{q-k}(\theta_q^{p-2})\alpha_k(\theta_q^{p-3})\alpha_{q-k}(\theta_q^{p-4})\cdot\cdot\cdot\alpha_k(\theta_q)\alpha_{q-k}\beta(\theta_k)\ , \tag{65}$$

for $k=1,\cdots,q-1$. We need the formula

$$\alpha_{q-1}\alpha_{q-1}(\theta_1)\cdot\cdot\cdot\alpha_{q-1}(\theta_1^{t-1})=[g(\theta_q)]^{t-1}\alpha_{q-t}\ . \tag{66}$$

To prove it by induction on t, multiply it by $\alpha_{q-1}(\theta_1^t)$ and apply (64) for $k=q-t$, $r=q-1$. We shall prove that (65) follows from the case $k=1$ by replacing i by i, θ_1, $\cdots$, θ_1^{k-1} in turn and taking the product. It suffices to watch the product of the general pair of consecutive factors

$$\alpha_1(\theta_q^{p-2s+1})\alpha_{q-1}(\theta_q^{p-2s})\ .$$

Replace i by θ_1^c and apply

$$\theta_q^{p-2s+1}\theta_1^c=\theta_1^{q-c}\theta_q^{p-2s+1}\ ,\qquad \theta_q^{p-2s}\theta_1^c=\theta_1^c\theta_q^{p-2s}\ ,$$

which follows from (56) which states that $\theta_1^k\theta_q^s=\theta_q^s\theta_1^k$ or $\theta_q^s\theta_1^{q-k}$, according as s is even or odd. Hence we get

$$\prod_{c=0}^{k-1}\alpha_1(\theta_1^{q-c}\theta_q^{p-2s+1})\cdot\prod_{c=0}^{k-1}\alpha_{q-1}(\theta_1^c\theta_q^{p-2s})\ .$$

By (61), the first product is derived from α_k/g^{k-1} by replacing i by θ_q^{p-2s+1}. By (66) with $t=k$, the second product is derived from $[g(\theta_q)]^{k-1}\alpha_{q-k}$ by replacing i by θ_q^{p-2s}. Thus the g's cancel and we get

$$\alpha_k(\theta_q^{p-2s+1})\alpha_{q-k}(\theta_q^{p-2s})\ ,$$

which is the product of the corresponding pair of consecutive factors in (65). Hence all cases of (65) follow from the case $k=1$. We first state our results for the case $e=0$, whence $\beta=\gamma$.

THEOREM 11. *Let $f(x)=0$ be an equation of degree pq irreducible in F whose Galois group G for F is generated by two substitutions Θ_1 and Θ_q of respective orders q and p such that Θ_q transforms Θ_1 into its inverse, while no lower than the pth power of Θ_q is equal to a power of Θ_1. Excluding the case $q=2$, we see that G is not abelian and that p is even. Then the roots of $f(x)=0$ are*

$$\theta_q^r[\theta_1^k(i)]=\begin{cases}\theta_1^k[\theta_q^r(i)] & (r \text{ even})\\ \theta_1^{q-k}[\theta_q^r(i)] & (r \text{ odd})\end{cases}\qquad \begin{pmatrix} r=0,1,\cdots,p-1\\ k=0,1,\cdots,q-1\end{pmatrix}, \tag{67}$$

where θ_1 and θ_q are rational functions of i with coefficients in F such that the qth iterative $\theta_1^q(i)$ of $\theta_1(i)$ is i and likewise $\theta_q^p(i)=i$. There exists an associative algebra Σ whose elements are

$$A=f_0+f_1j_1+f_2j_1^2+\cdots+f_{q-1}j_1^{q-1}, \tag{68}$$

where the f_k are polynomials in i of degree $<pq$ with coefficients in F, while

$$j_1^q=g(i)=g(\theta_1), \qquad j_1^r\phi(i)=\phi[\theta_1^r(i)]j_1^r \quad (r=1,\cdots,q-1), \tag{69}$$

so that the product of any two elements (68) *of Σ is another element* (68) *of Σ. Let*

$$A'=f_0(\theta_q)+\sum_{k=1}^{q-1}f_k(\theta_q)\alpha_kj_{q-k},$$

where α_k is defined by (61). *Then under multiplication defined by* (20), *the totality of polynomials in j_q with coefficients in Σ form an algebra Γ of order p^2q^2 over F which is associative if and only if $\gamma=\gamma(\theta_q)$,*

$$\gamma=\alpha(\theta_q^{p-1})\alpha_{q-1}(\theta_q^{p-2})\alpha(\theta_q^{p-3})\alpha_{q-1}(\theta_q^{p-4})\cdots\alpha(\theta_q)\alpha_{q-1}\gamma(\theta_1), \tag{70}$$

and also (63) *holds. Hence there are only four conditions on the parameters g, γ, α of Γ.*

The associative conditions are not inconsistent, being all satisfied if γ is F, and $g(\theta_1)=g$, $g(\theta_q)=g^{-1}$, $\alpha=g^{-1}$, whence every $\alpha_k(\theta_q^s)$ is g or g^{-1} according as s is odd or even.

For example, let $p=2$, $q=3$, and let

$$\Theta_1=(0\ 1\ 2)(3\ 5\ 4), \qquad \Theta_3=(0\ 3)(1\ 4)(2\ 5).$$

Then the roots of the sextic are

$$i,\ \theta_1,\ \theta_2=\theta_1[\theta_1(i)], \quad \theta_3,\ \theta_4=\theta_3[\theta_1(i)]=\theta_2[\theta_3(i)], \quad \theta_5=\theta_3\theta_2=\theta_1\theta_3.$$

For brevity write f_k for $f(\theta_k)$ and $\beta=\alpha\alpha(\theta_2)g$ for our former α_2. Then the multiplication table of Γ is given by (69_2) and the following relations in which j_r is denoted by r:

$$\begin{array}{lllll} 1^2=2\ , & 12=g\ , & 13=4\ , & 14=5\ , & 15=g3\ , \\ 21=g\ , & 2^2=g1\ , & 23=5\ , & 24=g3\ , & 25=g4\ , \\ 31=\alpha 5\ , & 32=\beta 4\ , & 3^2=\gamma\ , & 34=\alpha\gamma_2 2\ , & 35=\beta\gamma_1 1\ , \\ 41=\alpha_1 g3\ , & 42=\beta_1 5\ , & 43=\gamma_1 1\ , & 4^2=\alpha_1\gamma g\ , & 45=\beta_1\gamma_2 2\ , \\ 51=\alpha_2 g4\ , & 52=\beta_2 g3\ , & 53=\gamma_2 2\ , & 54=\alpha_2\gamma_1 g1\ , & 5^2=\beta_2\gamma g\ . \end{array}$$

The conditions for associativity are

$$g_1=g\ ,\quad \gamma_3=\gamma\ ,\quad g_3=\alpha\alpha_1\alpha_2 g^2\ ,\quad \gamma=\alpha\alpha_2\alpha_3 g\gamma_1\ .$$

Let F_1 be the field obtained from F by adjoining the elementary symmetric functions of $1, \theta_1, \theta_2$. Then Γ is a division algebra if and only if g is not the norm, relative to F_1, of any number of $F(i)$, and if $\gamma\neq X'X$ for any $X=a+bj_1+cj_1^2$, a, b, c in $F(i)$. Here

$$X'=a_3+c_3\alpha\alpha_2 g j_1+b_3\alpha j_2\ .$$

For any p and q, p even, we readily exhibit the group G of Theorem 11 in the desired regular form. Take $\Theta_1=C_1C_2\cdots C_p$, where each C_i is a cycle of q letters, no two C's having a letter in common. Write $\Theta_1^{-1}=C_2^{-1}C_3^{-1}\cdots C_p^{-1}C_1^{-1}$, where the cycle C_i^{-1} starts with the same letter as C_i, so that its remaining letters are those of C_i taken in reverse order. Then Θ_q is the substitution which replaces each letter of Θ_1 by that in the corresponding position in Θ_1^{-1}.

For example, if $p=2$, take $C_1=(0\ 1\cdots q-1)$, $C_2=(q\ q+1\cdots 2q-1)$. Then

$$C_2^{-1}=(q\ \ 2q-1\ \ 2q-2\cdots q+2\ \ q+1)\ ,\qquad C_1^{-1}=(0\ \ q-1\ \ q-2\cdots 2\ \ 1)\ ,$$

$$\Theta_q=(0\ q)(1\ \ 2q-1)(2\ \ 2q-2)\cdots(q-1\ \ q+1)\ .$$

For $p=4$, $q=3$,

$$\Theta_1=(0\ 1\ 2)(3\ 4\ 5)(6\ 7\ 8)(9\ 10\ 11)\ ,$$

$$\Theta_1^{-1}=(3\ 5\ 4)(6\ 8\ 7)(9\ 11\ 10)(0\ 2\ 1)\ ,$$

$$\Theta_3=(0\ 3\ 6\ 9)(1\ 5\ 7\ 11)(2\ 4\ 8\ 10)\ .$$

Next, let $e>0$. Since $e_0=e$, we have $2e=q$ by (59). Thus p and q are now both even.

THEOREM 12. *Let $f(x)=0$ be an equation of degree pq irreducible in F whose Galois group G is generated by Θ_1 and Θ_q, such that Θ_1 is of order q, Θ_q*

transforms Θ_1 *into its inverse,* $\Theta_q^p=\Theta_1^{q/2}$, *while no lower than the pth power of* Θ_q *is equal to a power of* Θ_1. *Excluding the case* $q=2$, *we see that* G *is not abelian and that* p *and* q *are both even. The roots are given by* (67), *where* $\theta_1^q(i)=i$, $\theta_q^p(i)=\theta_1^{q/2}(i)$. *Consider the algebras* Σ *and* Γ *of Theorem* 11, *where now* $j_q^p=\gamma=\beta j_{q/2}$. *Then* Γ *is associative if and only if* $g=g(\theta_1), \beta=\beta(\theta_q)\alpha_{q/2}$, (63) *holds, and* (65) *holds when* $k=1$.

The associative conditions are not inconsistent, being all satisfied if β is in F, and $g(\theta_1)=g$, $g(\theta_q)=g^{-1}$, $\alpha=g^{-1}$.

The simplest example is given by $p=2$, $q=4$. We may take*

$$\Theta_1=(0\ 1\ 2\ 3)(4\ 5\ 6\ 7)\ , \qquad \Theta_4=(0\ 4\ 2\ 6)(1\ 7\ 3\ 5)\ .$$

For any even integers p and q, we readily exhibit the group of Theorem 12 in the desired regular form. The only modification to make in the method used under Theorem 11 is that we start the final cycle C_1^{-1} of Θ_1^{-1} with the first letter after the middle of C_1.

For example, if $p=q=4$, take $\Theta_1=C_1C_2C_3C_4$, $C_1=(0\ 1\ 2\ 3)$, $C_2=(4\ 5\ 6\ 7)$,

$$C_3=(8\ 9\ 10\ 11),\ C_4=(12\ 13\ 14\ 15),\ \Theta_1^{-1}=C_2^{-1}C_3^{-1}C_4^{-1}C_1^{-1},$$

$$\Theta_1^{-1}=(4\ 7\ 6\ 5)(8\ 11\ 10\ 9)(12\ 15\ 14\ 13)(2\ 1\ 0\ 3)\ .$$

The substitution which replaces each letter of Θ_1 by that in the corresponding position in Θ_1^{-1} is

$$\Theta_4=(0\ 4\ 8\ 12\ 2\ 6\ 10\ 14)(1\ 7\ 9\ 15\ 3\ 5\ 11\ 13)\ .$$

Then $\Theta_4^4=\Theta_1^2$. The groups with $p=2$ are called dicyclic.

---

* This group is the regular form of the group whose 8 elements are the quaternions ± 1, $\pm i$, $\pm j$, $\pm k$.

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILL.