# CONSTRUCTION OF DIVISION ALGEBRAS*

BY

L. E. DICKSON

1. **Introduction.** The main outstanding problem in the theory of linear associative algebras is the determination of all division algebras. We shall make a noteworthy simplification of the theory of the construction of a type of algebras $\Gamma$ which includes all known division algebras. The simplification is so great that it would require a hundred pages to obtain our results by the best earlier method.

The paper gives an elementary exposition from first principles of the simplified construction of algebras $\Gamma$. It can be easily read by those familiar with the concept of real quaternions with the basis $1, i, j, k=ij$, complex quaternions, and, in general, quaternions over any field $F$. The few further terms used will be defined. The paper is independent of earlier literature except that, after proving a result for 3-rowed matrices, we give references to the similar proof for $p$-rowed matrices.

The emphasis on simplicity of exposition is warranted by the importance of the subject and the fact that the theory has now reached its last stage of simplicity. The paper will serve as an introduction to the writer's article *New division algebras*, in these Transactions, vol. 28 (1926), pp. 207–34 (cited as I), and to current literature based on it. We postpone extensions to non-Abelian equations whose roots have four or more generators.

2. **The algebra $\Gamma$ derived from a given algebra $\Sigma$.** The general theory requires a special case, which serves well as an introductory example.

Note that if $i$ is one root of $x^2-sx+p=0$, the second root is $\theta(i)=s-i$, while $\theta[\theta(i)]=\theta(s-i)=s-(s-i)=i$.

But quadratic equations are only the simplest cases of cyclic equations $f(x)=0$ of degree $p$ which are irreducible in a field $F$ and whose roots are related as follows. If $i$ is one root, it has another root $\theta(i)$ which is a polynomial in $i$ with coefficients in $F$. Using the notation of iteratives (which are not powers), we write $\theta^2(i)$ for $\theta[\theta(i)]$, $\theta^3(i)$ for $\theta[\theta^2(i)]$, etc. Then the roots of the cyclic equation are $i, \theta(i), \theta^2(i), \cdots, \theta^{p-1}(i)$, and we have $\theta^p(i)=i$.

The field $F(i)$ is composed of all rational functions of $i$ with coefficients in $F$, while each such function is known to be equal to a polynomial in $i$ with coefficients in $F$. Hence $F(i)$ may be regarded as an algebra over $F$ having the basis $1, i, i^2, \cdots, i^{p-1}$.

* Presented to the Society, February 22, 1930; received by the editors in December, 1929.

For our introductory example, we take $F(i)$ as algebra $\Sigma$. Each element $A$ of $\Sigma$ is therefore a polynomial $A(i)$ in $i$ with coefficients in $F$. Since $i$ and $\theta$ are roots of the same equation $f(x)=0$, irreducible in $F$, $A(i)B(i)=C(i)$ implies $A(\theta)B(\theta)=C(\theta)$. To each $A=A(i)$, let correspond $A'=A(\theta)$. Hence

$$(1) \qquad (AB)' = A'B', \quad (A+B)' = A'+B' \quad \text{for all } A \text{ and } B \text{ in } \Sigma.$$

We denote $(A')'$ by either $A''$ or $A^{(2)}$. In general, let $A^{(k)}$ denote the element which corresponds to $A^{(k-1)}$. Here

$$A^{(2)} = A[\theta^2(i)], \cdots, A^{(p)} = A[\theta^p(i)] = A(i) = A.$$

Hence for every $\gamma$ in the present commutative algebra $\Sigma$, we have

$$(2) \qquad A^{(p)}\gamma = \gamma A \text{ for all } A \text{ in } \Sigma.$$

To simplify the notations, let $p=3$. If $A$, $B$, $C$ are any polynomials in $i$, consider the matrix

$$M(A,B,C) = \begin{pmatrix} A & B & C \\ C'\gamma & A' & B' \\ B''\gamma & C''\gamma & A'' \end{pmatrix}.$$

In case $\gamma=\gamma'$ (whence $\gamma$ is in $F$), we find that the product of any two matrices $M(A, B, C)$ is a third such matrix. Likewise for their sum and for the product of $M$ by any number in $F$. Hence the totality of such matrices $M$ is an associative algebra over $F$. Special cases of $M$ are

$$(A) = \begin{pmatrix} A & 0 & 0 \\ 0 & A' & 0 \\ 0 & 0 & A'' \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \gamma & 0 & 0 \end{pmatrix}, \quad T^2 = \begin{pmatrix} 0 & 0 & 1 \\ \gamma & 0 & 0 \\ 0 & \gamma & 0 \end{pmatrix}.$$

We see that

$$M(A,B,C) = (A) + (B)T + (C)T^2, \quad T(A) = (A')T, \quad T^3 = (\gamma).$$

The algebra whose elements are the matrices $(A)$ is evidently equivalent to the algebra with the elements $A$. It is now a simple step to infer that the algebra whose elements are the matrices $M(A, B, C)$ is equivalent to an algebra $\Gamma$ whose elements are $A+BE+CE^2$, with $E^3=\gamma$, $EA=A'E$.

We readily extend* our proof from 3-rowed to $p$-rowed matrices and obtain

* I, pp. 217–19. Simpler in *Algebren und ihre Zahlentheorie*, p. 59.

THEOREM 1. *Let $\Sigma$ be any given associative algebra of order $p$. To each element $A$ of $\Sigma$ let correspond an element $A'$ also in $\Sigma$ such that* (1) *and* (2) *hold, where $\gamma=\gamma'$ is a self-corresponding element of $\Sigma$. Then there exists an associative algebra $\Gamma$ whose elements are*

$$A_0 + A_1E + \cdots + A_{p-1}E^{p-1}, \tag{3}$$

*where the $A$'s range independently over $\Sigma$, such that*

$$E^p = \gamma, \quad E^rA = A^{(r)}E^r \qquad (r = 1,2, \cdots; \text{any } A \text{ in } \Sigma). \tag{4}$$

By means of (4), the product of any two elements (3) can evidently be expressed in the form (3).

If in our example of a cyclic equation we replace $p$, $\gamma$, $E$ by $q$, $g$, $j$, respectively, we obtain

THEOREM 2. *Let an equation be irreducible in a field $F$ and have the roots $i$, $\theta(i)$, $\theta^2(i)=\theta[\theta(i)]$, $\cdots$, $\theta^{q-1}(i)$, where $\theta(i)$ is a polynomial in $i$ with coefficients in $F$ whose $q$th iterative $\theta^q(i)$ is equal to $i$. Then the algebra over $F$ with the basis* $i^mj^n(m, n=0, 1, \cdots, q-1)$, where*

$$j^q = g(i), \quad j^rP(i) = P[\theta^r(i)]j^r \qquad (r = 1,2, \cdots) \tag{5}$$

*for every polynomial $P(i)$, is associative if and only if*

$$g(i) = g(\theta). \tag{6}$$

**3. Algebras defined by an equation whose roots have two generators.** The roots of $\xi^4+c\xi^2+1=0$ are $i$, $-i$, $1/i$, $-1/i$. Write $\theta(i)=-i$, $\phi(i)=1/i=-i^3-ci$. Then the roots are $i$, $\theta(i)$, $\phi(i)$ and $\theta[\phi(i)]=\phi[\theta(i)]$. As a generalization, let $f(\xi)=0$ be an equation of degree $pq$ which is irreducible in a field $F$ and has the roots

$$\phi^r[\theta^s(i)] \qquad (r = 0,1, \cdots, p-1; s = 0,1, \cdots, q-1), \tag{7}$$

where $r$ and $s$ denote iteratives and not exponents, while $\phi(\xi)$ and $\theta(\xi)$ are polynomials with coefficients in $F$. Further, let

$$\begin{gathered} \theta^q(i) = i, \quad \phi^p(i) = \theta^e(i), \\ \theta[\phi(i)] = \phi[\theta^z(i)], \end{gathered} \tag{8}$$

where $q$ and $p$ are the least positive integers for which relations of type $(8_1)$ and $(8_2)$ hold.

Let $\Sigma$ be the algebra over $F$ having the basis $i^mj^n(m=0, 1, \cdots, pq-1; n=0, 1, \cdots, q-1)$ such that (5) and $f(i)=0$ hold. This $\Sigma$ may be obtained from Theorem 2 by replacing $F$ by the field $F_1$ derived by adjoining to $F$

* Before the associative law is proved $j^3, j^4, \cdots$ are to be replaced by $j_3, j_4, \cdots$.

all the elementary symmetric functions of $i$, $\theta(i), \cdots, \theta^{q-1}(i)$. Hence the latter are roots of an equation of degree $q$ with coefficients in $F_1$, which is irreducible in $F_1$ by I, §6. Since any polynomial in $i$ over $F_1$ is equal to a polynomial in $i$ over $F$, the algebra over $F_1$ in Theorem 2 may be regarded as our algebra $\Sigma$ over $F$. We assume (6). Then $\Sigma$ is associative.

We shall construct an algebra $\Gamma$ by means of Theorem 1. Each element of $\Sigma$ is of the form

$$A = \sum_{k=0}^{q-1} f_k(i) j^k, \tag{9}$$

where the $f_k(i)$ are polynomials in $i$ of degrees $\leqq pq-1$ with coefficients in $F$. To $A$ we let correspond*

$$A' = \sum_{k=0}^{q-1} f_k(\phi) j'^k, \quad j' = \alpha j^x. \tag{10}$$

In particular, $i' = \phi(i)$. By means of the relations

$$j^q = g(i), \; ji = \theta(i) j, \; f(i) = 0, \tag{11}$$

we can evidently reduce any product $AB$ to $C$, where also $B$ and $C$ are of type (9). Performing the same operations on $i'$ and $j'$ that we did on $i$ and $j$, we conclude that $A'B'$ can be reduced to $C'$ by means of the relations

$$j'^q = g(\phi), \; j'\phi(i) = \theta[\phi(i)] j', \; f(\phi) = 0. \tag{12}$$

In other words, (12) imply the desired property $(1_1)$.

When do relations (12) hold? In $(12_2)$ we insert the value (10) of $j'$, apply (5) for $r = x$, and obtain a relation which follows at once from $(8_3)$. We shall next prove by induction on $m$ that

$$\begin{aligned} j'^m &= \pi_m j^{mx}, \\ \pi_m(i) &= \alpha\alpha(\theta^x)\alpha(\theta^{2x}) \cdots \alpha(\theta^{(m-1)x}). \end{aligned} \tag{13}$$

For, if we multiply the second member of $(13_1)$ on the right by $\alpha j^x$ (or $j'$) and note that $j^{mx}\alpha = \alpha(\theta^{mx}) j^{mx}$ by (5), we get $\pi_{m+1} j^{(m+1)x}$. Hence (13) holds also when $m$ is replaced by $m+1$. The case $m = q$ of (13) shows that $(12_1)$ is equivalent to

$$\pi_q g^x = g(\phi). \tag{14}$$

* We desire that $\Sigma$ be enlarged to $\Gamma$ by an extender $E = k$ such that $kA = A'k$ by (4) and such that (32) shall hold. Hence $i' = \phi(i), j' = \alpha j^x$.

In §2 we require a self-corresponding element $\gamma=\gamma'$ of $\Sigma$. Let* $\gamma=\beta(i)j^e$. By (13),

$$\gamma' = \beta(\phi)j'^e = \beta(\phi)\pi_e j^{ex}.$$

By $(8_3)$ we see by induction that $\theta^k(\phi)=\phi(\theta^{kx})$. Take $k=e$ and note that $(8_2)$ implies $\theta^e(\phi)=\phi^p(\phi)=\phi(\phi^p)=\phi(\theta^e)$. Hence $\theta^{ex}=\theta^e$, $ex=e+c_1q$, where $c_1$ is an integer.† Hence $\gamma'=\gamma$ if and only if

$$\beta(\phi)\pi_e g^{c_1} = \beta, \quad c_1 = (ex-e)/q = \text{integer}. \tag{15}$$

It remains only to satisfy condition (2). If it holds for $A=B$ and for $A=C$, (1) gives

$$\begin{aligned}(BC)^{(p)}\gamma &= B^{(p)}C^{(p)}\gamma \\ &= B^{(p)}\gamma C = \gamma BC,\end{aligned}$$

whence (2) holds also for $A=BC$, and likewise for $A=B+C$. By (9) it therefore suffices to prove (2) for the cases $A=j$ and $A=a(i)$, a polynomial in $i$. For the latter case,

$$a^{(p)}(i) = a(\phi^p) = a(\theta^e)$$

by $(8_2)$. By (5),

$$\begin{aligned}\gamma a &= \beta j^e a \\ &= \beta a(\theta^e)j^e = a^{(p)}(i)\gamma.\end{aligned}$$

Hence there remains only the case $A=j$ of (2), denoted by (2′). By induction on $r$, using (13) with $m=x^r$, we get

$$j^{(r)} = \alpha(\phi^{r-1})\pi_x(\phi^{r-2})\pi_{x^2}(\phi^{r-3})\cdots\pi_{x^{r-1}}j^{x^r}. \tag{16}$$

Take $r=p$. Then (2′) requires‡ that

$$x^p = qc_2 + 1, \quad c_2 \text{ an integer}. \tag{17}$$

Hence (2′) is equivalent to

$$\alpha(\phi^{p-1})\pi_x(\phi^{p-2})\pi_{x^2}(\phi^{p-3})\cdots\pi_{x^{p-2}}(\phi)\pi_{x^{p-1}}g^{c_2}\beta(\theta) = \beta. \tag{18}$$

---

* In this choice we are guided by $(4_1)$ and $(8_2)$, the fact that $j$ and $E$ are associated with the respective roots $\theta$ and $\phi$, and finally by Lemma 2 of I, p. 212.

† This follows also from $\gamma'=\gamma$ and the fact that $q$ is a minimum in $(11_1)$.

‡ Also by (8). To prove $\theta(\phi^s)=\phi^s(\theta^{x^s})$ by induction on $s$, replace $i$ by $\phi$ and apply the earlier result $\theta^k(\phi)=\phi(\theta^{kx})$ for $k=x^s$. Take $s=p$ and note that $\theta(\phi^p)=\theta(\theta^e)=\theta^e(\theta)=\phi^p(\theta)$. Hence $\theta^{x^p}=\theta$.

By Theorem 1 with $E$ replaced by $k$, we now have

THEOREM 3. *Let an equation $f(\xi)=0$ be of degree $pq$, be irreducible in a field $F$, and have the roots* (7) *satisfying relations* (8). *Consider the algebra over $F$ having the basis $i^m j^n k^t (m=0, 1, \cdots, pq-1; n=0, 1, \cdots, q-1; t=0, 1, \cdots, p-1)$ with $f(i)=0$,* (5), *and**

$$k^p = \beta(i) j^e, \quad k^r P(i) = P(\phi^r) k^r, \quad k^r j^s = [j^{(r)}]^s k^r, \tag{19}$$

*where $j^{(r)}$ has the value* (16). *This algebra is associative if and only if conditions*† (6), (14), (15), *and* (18) *hold.*

Simplifications and interpretations of these conditions will be given in §§7, 8. Theorem 3 is equivalent to that proved by J. Williamson in these Transactions, vol. 30 (1928), pp. 112–5, by the method used by the writer for the case $x=q-1$ in I, pp. 228–34. That method is much more complicated than the present one since it examined the conditions for (1) for all $A$ and $B$, whereas it suffices to treat the cases (12).

4. **Algebras defined by Abelian equations.** The cyclic equation in §2 and the quartic in §3 are examples of Abelian equations. The general one is defined in

THEOREM 4. *Let an Abelian equation $f(x)=0$ be of degree $d=p_1 p_2 \cdots p_n$, irreducible in a field $F$, and have the roots*

$$\psi_1^{e_1}\{\psi_2^{e_2}[\cdots \psi_n^{e_n}(i)]\} \qquad \begin{pmatrix} e_1 = 0,1, \cdots, p_1 - 1 \\ \cdots\cdots\cdots\cdots \\ e_n = 0,1, \cdots, p_n - 1 \end{pmatrix},$$

*where each $\psi_j(i)$ is a polynomial in $i$ with coefficients in $F$, $\psi^e(t)$ denotes the $e$th iterative of $\psi(t)$, such that the $p_r$th iterative of $\psi_r(i)$ is equal to $i$, and*

$$\psi_j[\psi_k(i)] = \psi_k[\psi_j(i)] \qquad (j,k = 1, \cdots, n).$$

*Consider the algebra $A_n$ over $F$ with the basis*

$$i^h j_1^{e_1} \cdots j_n^{e_n} \qquad (h = 0,1, \cdots, d-1; e_s = 0,1, \cdots, p_s - 1),$$

*such that, for every polynomial $P(i)$,*

$$j_r^{p_r} = g_r(i), \quad j_r^m P(i) = P[\psi_r^m(i)]\, j_r^m \qquad (r = 1, \cdots, n; \ m = 1, 2, \cdots), \tag{20}$$

$$j_s^k j_r^m = T_m(i) T_m(\psi_s) \cdots T_m(\psi_s^{k-1}) j_r^m j_s^k \qquad (s,r = 1, \cdots, n; s > r), \tag{21}$$

* After the theorem is proved, we may replace (5) and (19) by their special cases (11) and (32), which with the associative law imply the former.

† We do not include the facts that $c_1$ and $c_2$ in (15) and (17) are integers, since they follow from the hypotheses (8).

$$(22) \qquad T_m(i) = T_{m,s,r} = \alpha(i)\alpha(\psi_r)\alpha(\psi_r^2)\cdots\alpha(\psi_r^{m-1}), \quad \alpha \equiv \alpha_{s,r}.$$

*Then $A_n$ is associative if and only if*

$$\alpha_{t,s}\alpha_{s,r}\alpha_{t,r}(\psi_s) = \alpha_{t,s}(\psi_r)\alpha_{s,r}(\psi_t)\alpha_{t,r} \qquad (t > s > r),$$

$$T_{p_r,t,r}g_r(i) = g_r(\psi_t), \quad \alpha_{t,r}\alpha_{t,r}(\psi_t)\cdots\alpha_{t,r}(\psi_t^{p_t-1})g_t(\psi_r) = g_t \qquad (t > r),$$

*and $g_t(i) = g_t(\psi_t)$, for $r, s, t = 1, \cdots, n$.*

After the theorem is proved, we may replace $(20_2)$ and (21) by the special cases

$$j_r i = \psi_r(i)j_r, \quad j_s j_r = \alpha_{s,r}(i)j_r j_s$$

of them, since these and the associative law imply the former.

We shall prove Theorem 4 by induction on $n$, assuming* that $\Sigma = A_{n-1}$ is associative. Let $R$ denote the relations (20) and (21) with subscripts restricted to $1, \cdots, n-1$. Let $R'$ denote the relations derived from $R$ by replacing $i$ and $j_r$ by

$$(23) \qquad i' = \psi_n(i), \quad j_r' = \alpha_{n,r}(i)j_r.$$

By means of relations $R$ we can evidently express any element of $\Sigma$ in the form

$$(24) \qquad A = \sum_{e_1=0}^{p_1-1} \cdots \sum_{e_{n-1}=0}^{p_{n-1}-1} a_{e_1,\cdots,e_{n-1}}(i)j_1^{e_1}\cdots j_{n-1}^{e_{n-1}}.$$

Similarly, by means of $R$, we can reduce any product $AB$ to $C$, where $B$ and $C$ are of type (24) with $a$'s replaced by $b$'s and $c$'s, respectively. Let $A'$ denote the sum (24) with $i$ and $j_r$ replaced by (23). Hence $A'B'$ can be reduced to $C'$ by means of relations $R'$ (since the operations on the accented letters are the same as those used on unaccented letters). In other words, $R'$ imply property (1).

By the remark below the theorem, $R'$ follow from the special cases

$$(25) \qquad j_r'^{p_r} = g_r(\psi_n), \quad j_r'\psi_n = \psi_r(\psi_n)j_r', \quad j_s'j_r' = \alpha_{s,r}(\psi_n)j_r'j_s' \qquad (s,r = 1, \cdots, n-1; s > r)$$

of them, in which the values of the $j'$ in (23) are to be inserted. From $(25_2)$ and $(20_2)$ with $m = 1$, we get

$$\alpha_{n,r}\psi_n[\psi_r(i)]j_r = \psi_r[\psi_n(i)]\alpha_{n,r}j_r$$

which is true by the assumption in the theorem. Similarly, $(25_3)$ becomes

* And employing the analog of the paragraph following (8). Compare the second paragraph of §5.

$$\alpha_{n,s}\alpha_{n,r}(\psi_s)j_sj_r = \alpha_{s,r}(\psi_n)\alpha_{n,r}\alpha_{n,s}(\psi_r)j_rj_s.$$

By the relation below the theorem, this holds if and only if

$$\alpha_{n,s}\alpha_{n,r}(\psi_s)\alpha_{s,r} = \alpha_{s,r}(\psi_n)\alpha_{n,r}\alpha_{n,s}(\psi_r) \qquad (r,s = 1, \cdots, n-1; s > r). \tag{26}$$

By induction on $m$

$$j_r'^m = T_{m,n,r}j_r^m.$$

Hence $(25_1)$ is equivalent to

$$T_{p_r,n,r}g_r(i) = g_r(\psi_n). \tag{27}$$

Since the desired formula $(4_1)$ is here $(20_1)$ with $r=n$, we must choose $\gamma=g_n(i)$. Then $\gamma=\gamma'$ becomes

$$g_n(i) = g_n(\psi_n). \tag{28}$$

Also, $p=p_n$ in (2), which requires proof only when $\gamma=g_n\neq 0$. If $A$ is a polynomial $a(i)$ in $i$, (2) holds since

$$\psi_n^{p_n}(i) = i, \quad g_nag_n^{-1} = a(i) = a(\psi_n^{p_n}) = a^{(p_n)}.$$

As below (15), it remains only to consider (2) for $A=j_r$, $r<n$. By (20), $j_rg_n=g_n(\psi_r)j_r$. Hence shall

$$g_nj_rg_n^{-1} = \frac{g_n}{g_n(\psi_r)}j_r = j_r^{(p)}$$

for $p=p_n$. By induction on $p$,

$$j_r^{(p)} = \alpha\alpha(\psi_n)\cdots\alpha(\psi_n^{p-1})j_r, \quad \alpha \equiv \alpha_{n,r}.$$

Hence (2) holds for $A=j_r$ if and only if

$$\alpha(i)\alpha(\psi_n)\cdots\alpha(\psi_n^{p_n-1}) = \frac{g_n}{g_n(\psi_r)}, \quad \alpha \equiv \alpha_{n,r} \quad (r = 1, \cdots, n-1). \tag{29}$$

Under the assumption that $A_{n-1}$ is associative, we have now proved that $A_n$ is associative if and only if conditions (26)-(29) hold. But $A_1$ is of the type in Theorem 2 and hence is associative if and only if $g_1(i)=g_1(\psi_1)$. This completes the proof of Theorem 4. It was first proved (in manuscript) two years ago by J. S. Georges after very long reductions of all conditions arising from (1).

5. **Algebras defined by an equation whose roots have three generators.** Let $f(\xi)=0$ be an equation of degree $pqs$ which is irreducible in $F$ and has the roots

$$\psi^m\{\phi^n[\theta^r(i)]\} \qquad (m < s, n < p, r < q). \tag{30}$$

Let the roots satisfy relations (8) and

$$\psi^s = \phi^s(\theta^q),\ \theta(\psi) = \psi[\phi^v(\theta^v)],\ \phi(\psi) = \psi[\phi^z(\theta^w)], \tag{31}$$

from which the argument $i$ has been suppressed, while $s$ is a minimum.

Let $\Sigma$ be the algebra over $F$ having the basis $i^m j^n k^t$ ($m \leqq pqs-1$, $n \leqq q-1$, $t \leqq p-1$) such that (5), (19), and $f(i)=0$ hold. As in the paragraph below (8), $\Sigma$ may be obtained from Theorem 3 by replacing $F$ by the field derived by adjoining to $F$ all elementary symmetric functions of the roots (7). We assume (6), (14), (15), and (18). Then $\Sigma$ is associative. We see that (5) and (19) are consequences of the associative law and the set $R$ of relations given by (11) and the following cases of (19):

$$k^p = \beta(i)j^e,\ ki = \phi(i)k,\ kj = \alpha(i)j^x k. \tag{32}$$

Let $R'$ denote the set of like relations (11′) and (32′) with $i, j, k$ replaced by $i', j', k'$, which are defined, in accord with (4) and (31), to be

$$i' = \psi(i),\ J \equiv j' = \epsilon(i)j^v k^v,\ K \equiv k' = \delta(i)j^w k^z. \tag{33}$$

By the usual argument, relations $R'$ imply property (1). We insert the values (33) into the five relations $R'$. By $(5_2)$ and $(19_2)$, we see that $(11_2')$ becomes

$$\epsilon\psi[\phi^v(\theta^v)]j^v k^v = \epsilon\theta(\psi)j^v k^v,$$

which is true by $(31_2)$. Similarly, $(32_2')$ follows from $(31_3)$.

Using $\pi_m$ in (13), we see by induction on $n$ that

$$kj^n = \pi_n(i)j^{x^n}k. \tag{34}$$

By induction on $m$,

$$k^m j^n = B_{m,n}j^{x^m n}k^m, \tag{35}$$

$$B_{m,n}(i) = \pi_n(\phi^{m-1})\pi_{xn}(\phi^{m-2})\pi_{x^2 n}(\phi^{m-3})\cdots\pi_{x^{m-1}n}(i). \tag{36}$$

By $(5_2)$ and $(19_2)$,

$$KJ = \delta\epsilon[\phi^z(\theta^w)]j^w k^z j^v k^v.$$

Applying (35) with $m=z$, $n=y$, and then $(5_2)$, we get

$$KJ = \delta\epsilon[\phi^z(\theta^w)]B_{z,y}(\theta^w)j^{w+x^z y}k^{z+v}. \tag{37}$$

We employ the abbreviations

$$h(t) = y + x^v y + x^{2v}y + \cdots + x^{(t-1)v}y,\ h(0) = 0, \tag{38}$$

$$C_d(i) = \epsilon\epsilon(\phi^v\theta^v)\epsilon(\phi^{2v}\theta^{h(2)})\epsilon(\phi^{3v}\theta^{h(3)})\cdots\epsilon(\phi^{(d-1)v}\theta^{h(d-1)}) \times B_{v,y}(\theta^v)B_{2v,y}(\theta^{h(2)})B_{3v,y}(\theta^{h(3)})\cdots B_{(d-1)v,y}(\theta^{h(d-1)}), \tag{39}$$

whence $C_1=\epsilon$. Hence if $d=1$,

$$J^d = C_d j^{h(d)} k^{dv}. \tag{40}$$

Assuming (40), we obtain the like result with $d$ replaced by $d+1$ by using (37) with $\delta$, $w$, $z$ replaced by $C_d$, $h(d)$, $dv$, respectively, whence $K$ is replaced by $J^d$. This proves (40) by induction.

The case $d=q$ of (40) shows that $(11_1')$ is equivalent to

$$C_q j^{h(q)} k^{qv} = g(\psi). \tag{41}$$

From $(19_1)$ by induction on $n$, we get

$$k^{np} = \beta_n j^{en},\ \beta_n(i) = \beta\beta(\theta^e)\cdots\beta(\theta^{e(n-1)}). \tag{42}$$

Since no lower than the $p$th power of $k$ is a polynomial in $i$ and $j$, (41) requires that

$$qv = c_3 p,\quad c_3 \text{ an integer}. \tag{43}$$

Replacing $k^{qv}$ by its value (42), and using (5), we see that the new form of (41) involves $j$ with the exponent

$$h(q) + ec_3 = c_4 q,\ c_4 \text{ an integer}, \tag{44}$$

and hence that (41) is equivalent to

$$C_q \beta_{c_3}(\theta^{h(q)}) g^{c_4} = g(\psi). \tag{45}$$

By a change of notation in (37) we see by (40) that

$$J^z K = C_x \delta(\phi^{xv}\theta^{h(x)}) B_{xv,w}(\theta^{h(x)}) j^{\xi} k^{xv+z},$$

$$\xi = h(x) + wx^{xv}. \tag{46}$$

Thus $\xi$ is $t(x, 1)$ in the notation (58). By $(32_3')$, $\alpha(\psi)J^z K = KJ$. By the exponents of $k$, we have

$$xv - v = c_5 p. \tag{47}$$

We apply (42) with $n$ replaced by $c_5$. By the resulting terms in $j$,

$$\xi + ec_5 - w - x^z y = c_6 q. \tag{48}$$

The resulting condition is

$$\alpha(\psi) C_x \delta(\phi^{xv}\theta^{h(x)}) B_{xv,w}(\theta^{h(x)}) \beta_{c_5}(\theta^{\xi}) g^{c_6} = \delta\epsilon(\phi^z\theta^w) B_{z,y}(\theta^w). \tag{49}$$

We obtain $K^d$ from $J^d$ by the replacement in (51). Let

$$H(t) = w + x^z w + x^{2z} w + \cdots + x^{(t-1)z} w,\quad H(0) = 0, \tag{50}$$

(51) $D_d(i)$ be derived from (39) by replacing $\epsilon$, $y$, $v$, $h$ by $\delta$, $w$, $z$, $H$.

In these notations, we have

(52) $$K^d = D_d j^{H(d)} k^{dz}.$$

Hence $(32_1')$ becomes

$$D_p j^{H(p)} k^{pz} = \beta(\psi) C_e j^{h(e)} k^{ev}.$$

By the terms in $k$ and those in $j$ after reductions by (42), we must have

(53) $$ev = c_7 p, \quad H(p) + ez - h(e) - ec_7 = c_8 q,$$

(54) $$D_p \beta_z(\theta^{H(p)}) g^{c_8} = \beta(\psi) C_e \beta_{c_7}(\theta^{h(e)}).$$

We have now examined all the relations (11′) and (32′).

A comparison of $(4_1)$ with $(31_1)$ leads us to choose

(55) $$\gamma = \sigma(i) j^a k^b,$$

and later to identify the $p$ in $(4_1)$ with our $s$. By (40), (52), and (37) in changed notations, we get

(56) $$J^m K^n = F_{m,n} j^{t(m,n)} k^{mv+nz},$$

(57) $$F_{m,n}(i) = C_m D_n [\phi^{mv}(\theta^{h(m)})] B_{mv, H(n)}(\theta^{h(m)}),$$

(58) $$t(m,n) = h(m) + x^{mv} H(n).$$

We take $m=a$, $n=b$. Comparing the exponents of $k$ in $\gamma'=\gamma$, we get

(59) $$av + bz - b = c_9 p.$$

By (42),

$$k^{av+bz} = \beta_{c_9} j^{ec_9} k^b.$$

Comparing the exponents of $j$ in $\gamma'=\gamma$, we get

(60) $$t(a,b) + ec_9 - a = c_{10} q.$$

Hence the conditions for $\gamma'=\gamma$ are (59), (60), and

(61) $$\sigma(\psi) F_{a,b} \beta_{c_9}(\theta^{t(a,b)}) g^{c_{10}} = \sigma(i).$$

Finally, we consider (2), viz.,

(62) $$A^{(s)}\gamma = \gamma A \text{ for all } A \text{ in } \Sigma.$$

This holds if $A$ is any polynomial $P(i)$ in $i$. For, by $(19_2)$, $(5_2)$, and $(31_1)$,

$$\gamma P = \sigma j^a P(\phi^b) k^b = \sigma P[\phi^b(\theta^a)] j^a k^b = \sigma P(\psi^s) j^a k^b = P^{(s)}\gamma.$$

By the remarks below (15), it remains only to find the conditions that (62) shall hold for the values $j$ and $k$ of $A$. By (33),

$$j'' = \epsilon(\psi)J^v K^v, \qquad k'' = \delta(\psi)J^w K^z. \tag{63}$$

Hence for two sets of values of $m$ and $n$ we need a formula of type

$$(J^m K^n)^{(r)} = G_{m,n,r}(i)j^{f(m,n,r)}k^{l(m,n,r)}. \tag{64}$$

Accenting each member and applying (33) and (56), we get a relation which is an identity in $j$ and $k$ if

$$l(m,n,r+1) = vf + zl, \quad f(m,n,r+1) = t(f,l), \tag{65}$$

$$G_{m,n,r+1} = G_{m,n,r}(\psi)F_{f,l}, \tag{66}$$

in which the arguments of $f$ and $l$ in the second members are $m$, $n$, $r$. Since we may identify (64) for $r=0$ with (56),

$$G_{m,n,0} = F_{m,n}, \quad f(m,n,0) = t(m,n), \quad l(m,n,0) = mv + nz. \tag{67}$$

For these initial values, (65) and (66) serve as recursion formulas to determine the $f$, $l$, $G$ uniquely.

By $(63_1)$ and (64) with $r=s-2$ we get $j^{(s)}$. Its product on the right by $\gamma$ in (55) is found by the rule (37). Hence for $V$ in (70),

$$j^{(s)}\gamma = Vj^{f+x^l a}k^{l+b}, \quad \gamma j = \sigma B_{b,1}(\theta^a)j^{a+x^b}k^b,$$

the second from (35). These shall be equal by (62) with $A=j$. Comparing exponents of $k$ and, after using (42), exponents of $j$, we get

$$l = c_{11}p, \quad f + x^l a + ec_{11} - a - x^b = c_{12}q, \tag{68}$$

$$V\beta_{c_{11}}(\theta^{f+x^l a})g^{c_{12}} = \sigma B_{b,1}(\theta^a), \tag{69}$$

$$V = \epsilon(\psi^{s-1})G\sigma(\phi^l\theta^f)B_{l,a}(\theta^f), \tag{70}$$

where the arguments of $f$ and $l$ and the subscripts of $G$ are $y$, $v$, $s-2$.

Similarly, starting with $(63_2)$, we find that (62) holds with $A=k$ if and only if

$$l - 1 = c_{13}p, \quad f + x^l a + ec_{13} - a = c_{14}q, \tag{71}$$

$$W\beta_{c_{13}}(\theta^{f+x^l a})g^{c_{14}} = \sigma, \tag{72}$$

where $W$ is derived from (70) by replacing $\epsilon$ by $\delta$, and the arguments of $f$ and $l$ and the subscripts of $G$ are now $w$, $z$, $s-2$.

By Theorem 1 with $p$ replaced by $s$, we now have

THEOREM 5. *Let an equation* $f(\xi)=0$ *be of degree* $pqs$, *be irreducible in a field* $F$, *and have the roots* (30) *satisfying relations* (8) *and* (31). *Consider the algebra over* $F$ *having the basis* $i^m j^n k^t E^c (m=0, \cdots, pqs-1;\ n=0, \cdots, q-1;\ t=0, \cdots, p-1;\ c=0, \cdots, s-1)$ *with* $f(i)=0$, (5), (19), *and**

$$
\begin{aligned}
E^s &= \sigma(i) j^a k^b, & E^r P(i) &= P(\psi^r) E^r, \\
E^r j^s &= [j^{(r)}]^s E^r, & E^r k^s &= [k^{(r)}]^s E^r,
\end{aligned} \tag{73}
$$

*where*

$$
j^{(r)} = \epsilon(\psi^{r-1})(J^v K^v)^{(r-2)}, \quad k^{(r)} = \delta(\psi^{r-1})(J^w K^s)^{(r-2)}
$$

*are found by* (64), *while their* $s$*th powers may be found by* (40) *with altered parameters. This algebra is associative if and only if conditions* (6), (14), (15), (18), (45), (49), (54), (61), (69), *and* (72) *hold.*

We do not include as conditions the facts that $c_1, \cdots, c_{14}$ are integers in (15), (17), (43), (44), (47), (48), (53), (59), (60), (68), and (71), since we shall prove in §6 that they follow from the hypotheses (8) and (31).

6. **Groups.** Let $r_1(i), \cdots, r_d(i)$ denote the $d$ roots† (30) arranged in an arbitrarily chosen order. Let $j$ and $k$ be any of the numbers $1, \cdots, d$. By means of (8) and (31), we can evidently reduce the function $r_k[r_j(i)]$ to the form (30) and hence obtain a certain root $r_l(i)$. If $j$ is fixed, but $k$ takes the values $1, \cdots, d$, then $l$ takes the same values rearranged. Hence we obtain a substitution $S_j$ on the $d$ roots which is said to replace $r_k$ by $r_l$.

Similarly, if $t$ is fixed and $r_l[r_t(i)]=r_f$, we obtain a substitution $S_t$ which replaces $r_l$ by $r_f$. Let $r_j[r_t(i)]=r_c$. Then

$$
r_k(r_c) = r_k[r_j(r_t)] = r_l(r_t) = r_f,
$$

which defines a substitution $S_c$ replacing $r_k$ by $r_f$. It is called the product of $S_j$ by $S_t$ and denoted by $S_j S_t$.

We therefore have a group of $d$ substitutions $S$ such that

$$
S_j S_t = S_c \quad \text{if} \quad r_j[r_t(i)] = r_c(i), \tag{75}
$$

while $S_j$ is uniquely determined by the root $r_j(i)$.

We return to the notation (30) for the roots. Let $\Theta$, $\Phi$, $\Psi$ denote the

---

* After the theorem is proved, we may replace (5), (19), and the last three of (73) by their special cases (11), (32) and

$$
Ei=\psi(i)E, \quad Ej=j'E, \quad Ek=k'E, \quad j' \text{ and } k' \text{ in (33).} \tag{74}
$$

In fact, the latter and the associative law imply the former.

† The same discussion applies to (7), to the Abelian equation in Theorem 4, and to any equation whose roots are all rational functions of one root.

substitutions determined by the roots $\theta(i)$, $\phi(i)$, $\psi(i)$, respectively. By (8), (31), and (75), we get*

$$\begin{aligned} &\Theta^q = 1, \quad \Phi^p = \Theta^e, \quad \Phi^{-1}\Theta\Phi = \Theta^x, \\ &\Psi^s = \Phi^b\Theta^a, \quad \Psi^{-1}\Theta\Psi = \Phi^v\Theta^y, \quad \Psi^{-1}\Phi\Psi = \Phi^z\Theta^w, \end{aligned} \tag{76}$$

in which $q$, $p$, $s$ cannot be replaced by smaller positive integers.

Write $j$, $k$, $E$ for the inverses of $\Theta$, $\Phi$, $\Psi$, respectively, and define $J$, $K$. Taking the inverse of each equation (76), we get

$$\begin{aligned} &j^q = 1, \qquad k^p = j^e, \qquad kj = j^x k, \qquad E^s = j^a k^b, \\ &Ej = JE, \quad Ek = KE, \quad J = j^y k^v, \quad K = j^w k^z. \end{aligned} \tag{77}$$

We evidently have the same relation between the parameters $q, p, e, x, \cdots$ for (77) as for (76).

The developments in §5 were based on (11), (32), and (73) as simplified in (74). If we suppress all factors which are polynomials in $i$, we obtain (77) and conclude that all resulting relations in §5 become consequences of (77). The fact that $c_3, \cdots, c_{14}$ in (43), $\cdots$, (71) are all integers is therefore a consequence of (77) and hence of (76) and therefore of (8) and (31).

THEOREM 6. *That $c_1, \cdots, c_{14}$ in (15), $\cdots$, (71) are integers are conditions for the existence of the group.*

While the proof applies also to $c_1$ and $c_2$ in (15) and (17), our former verification was more elementary.

7. **Simplifications.** Our conditions involve the product $\pi_m$ in (13). When $m$ is large, the number $m$ of factors may be reduced. Since $\theta^q(i) = i$, evidently $\pi_{n+q} = \pi_n\pi_q$. By induction on $y$,

$$\pi_{n+yq} = \pi_n\pi_q{}^y. \tag{78}$$

Here we may replace $\pi_q$ by its simple value from (14). Hence we may materially reduce the number of factors in condition (18). To this end we write

$$x^2 = x_2 + qy_2, \quad xx_2 = x_3 + qy_3, \quad \cdots, \quad xx_{p-1} = x_p + qy_p \quad (0 \leqq x_k < q). \tag{79}$$

Evidently $x_k \equiv x^k \pmod q$. Thus $x_p = 1$ by (17). Write

$$\alpha_{x_k} = \pi_{x_k}\theta^{y_{k+1}} \tag{80}$$

* We do not use the illuminating fact that if we start with an equation irreducible in $F$ whose roots are rational functions of one root $i$ with coefficients in $F$, and whose Galois group for $F$ is generated by $\Theta$, $\Phi$, $\Psi$ subject to (76), then the roots are (30) and satisfy relations (8) and (31). Similarly for the first line of (76) and the roots (75) satisfying (8).

also when $k=1$, taking $x_1=x$. Then (18) is equivalent to*

$$\alpha(\phi^{p-1})\alpha_{x_1}(\phi^{p-2})\alpha_{x_2}(\phi^{p-3})\cdots\alpha_{x_{p-2}}(\phi)\alpha_{x_{p-1}}=\beta\beta^{-1}(\theta). \tag{81}$$

In §5 we may again simplify $\pi_n$ in (34) by use of (78) and (14) and reduce the exponent $xn$ of $j$ below $q$. The new (35) is automatically simplified. After writing this paper, the author suggested to Miss Dora McFarland that she simplify the further formulas in §5. To do this she reduced at every stage all exponents of $j$ and $k$ below $q$ and $p$, respectively (see the preceding footnote). But the work became far more complicated and the formulas exceedingly complex.

8. **Example, interpretations.** Let $x=q-1$ in §3. We exclude the case $q=2$, since the equation is then Abelian and falls under §4. Then $p$ is even by (17). By the last part of (15), $2e\equiv 0 \pmod q$. But $0\leqq e<q$. Hence

$$\text{either } e=0, \text{ or } q \text{ is even and } e=\tfrac{1}{2}q. \tag{82}$$

Since $x, 2x, \cdots, (q-1)x$ are congruent to $q-1, q-2, \cdots, 1$, modulo $q$,

$$\pi_q=\alpha\alpha(\theta)\alpha(\theta^2)\cdots\alpha(\theta^{q-1}). \tag{83}$$

From (79), (80), and $x^2=1+q(q-2)$, we see that if $k$ is even,

$$x_k=1,\quad y_k=q-2,\quad \alpha_{x_k}=\alpha;$$

if $k$ is odd,

$$x_k=x,\quad y_k=0,\qquad \alpha_{x_k}=\pi_{q-1}g^{q-2}\equiv\chi,$$

$$\chi(i)=\alpha\cdot\alpha(\theta^2)\alpha(\theta^3)\cdots\alpha(\theta^{q-1})g^{q-2}. \tag{84}$$

Hence (81) becomes

$$\alpha(\phi^{p-1})\chi(\phi^{p-2})\alpha(\phi^{p-3})\chi(\phi^{p-4})\cdots\alpha(\phi)\chi(i)=\beta\beta^{-1}(\theta). \tag{85}$$

Now (15) becomes

$$\beta(\phi)=\beta \text{ if } e=0;\ \beta(\phi)\pi_e g^{e-1}=\beta \text{ if } e=\tfrac{1}{2}q. \tag{86}$$

THEOREM 7. *When $x=q-1$ in Theorem 3, the conditions that the algebra be associative are* (6), (14), (85), *and* (86).

A long proof of Theorem 7 was given in I, pp. 228–34.

We shall now simplify (85) and interpret it. Multiply (84) by $\alpha(\theta)g$ and apply (14) and (83); we get

$$\alpha(\theta)g\chi=g(\phi). \tag{87}$$

* We may prove (81) independently of (18). By induction on $r$, $j^{(r)}$ is the product of the left member of (81) with $p$ changed to $r$ by $j^{z_r}$. The case $r=p$ shows that (2) with $A=j$ becomes (81).

In (85) we insert the resulting fractional expression for $\chi$, clear of denominators, and obtain $M\beta(\theta)=L\beta$, where

$$M = \alpha(\phi^{p-1})\alpha(\phi^{p-3})\cdots\alpha(\phi)g(\phi^{p-1})g(\phi^{p-3})\cdots g(\phi),$$
$$L = \alpha(\theta\phi^{p-2})\alpha(\theta\phi^{p-4})\cdots\alpha(\theta)g(\phi^{p-2})g(\phi^{p-4})\cdots g,$$

in which consecutive superior letters differ by 2.

Since $\Phi$ transforms $\Theta$ into its inverse, $\Phi^s$ is commutative with $\Theta$ if $s$ is even. Then $\phi^s$ is commutative with $\theta$ and $\theta^{-1}$. If in $L$ we replace $i$ by $\theta^{-1}\phi$, and apply (6), we get $M$. Hence we may replace (85) by

$$L(i)\beta = L(\theta^{-1}\phi)\beta(\theta). \tag{88}$$

In $(8_3)$ replace $i$ by $\theta$. Hence $\theta[\phi(\theta)]=\phi$, $\phi(\theta)=\theta^{-1}(\phi)$.

Let $e=0$ and write $B(i)$ for $L(i)\beta$. In $(86_1)$ replace $i$ by $\theta$; we get $\beta[\theta^{-1}(\phi)]=\beta(\theta)$. Then (88) gives

$$B(\theta^{-1}\phi) = B(i) \text{ or } B(\theta^{-1}) = B(\phi^{-1}). \tag{89}$$

9. **Normalization of groups with two generators.** Let the generators $\Theta$ and $\Phi$ satisfy the relations in the first line of (76). We may write $e=\epsilon f$, where $f$ is prime to $q$, and all prime factors of $\epsilon$ divide $q$. Some of those primes are denoted by $r_i$ and the others by $s_i$, as follows. We may write $\epsilon=\sigma R$, where $\sigma$ is a product of powers of the $s_i$, and $R$ is a product of powers of the $r_i$, such that the exponent of the highest power of $r_i$ [or $s_i$] which divides $R$ [or $\sigma$] is $>$ [or $\leqq$] the exponent of its power which divides $q$. We may write $q=\rho Q$, where $\rho$ is a product of powers of the $r_i$, no one of which divides $Q$. Hence $\rho$ is a divisor of $R$, and $R/\rho$ is divisible by each $r_i$. Also, each $s_i$ divides $Q$, and $\sigma$ is a divisor of $Q$. Write $E=Q+R/\rho$. Since each $r_i$ divides $R/\rho$, but not $Q$, no $r_i$ divides $E$. If a prime divides $Q$, it is distinct from the $r_i$ and hence is not a factor of $R/\rho$ and therefore not of $E$. Hence $q=\rho Q$ is prime to $E$. Since $E$ and $f$ are both prime to $q$, $\Omega=\Theta^{Ef}$ generates all powers of $\Theta$. Now $E\rho=Q\rho+R\equiv R \pmod{\rho Q=q}$. Multiplication by $\sigma f$ shows that

$$\Omega^{\rho\sigma} = \Theta^{\rho\sigma Ef} = \Theta^{\sigma fR} = \Theta^{e}.$$

By $(76_2)$, $\Phi^p=\Omega^{\rho\sigma}$, and $\rho\sigma$ divides $\rho Q=q$.

THEOREM 8. *We may employ a power of $\Theta$ as a new generator in place of $\Theta$ such that the new e in* (76) *is a divisor of q.*

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.