CONDITIONS FOR ASSOCIATIVITY OF DIVISION ALGEBRAS CONNECTED WITH NON-ABELIAN GROUPS*

BY

JOHN WILLIAMSON

1. **Introduction.** The problem of the determination of division algebras has been successfully investigated by Professor L. E. Dickson, who was the first to discover a division algebra D of order n^2 over a field F, and who recently has shown† how to construct all algebras Γ of order $n^2 = Q^2q^2$ over a field F, corresponding to the Galois group G of order $n = Qq$ of an equation $f(x) = 0$ irreducible in F. In addition, he has determined the general conditions, called D_1, D_2, D_3, which must be satisfied by the algebra Γ if it is associative. He has also reduced these conditions in detail for an algebra Γ corresponding to a Galois group G of two generators, both when G is an abelian group, and when G is not abelian but of a special type. Based on his work, our problem is to reduce the associativity conditions, first when the group G is generated by two generators Θ_q and Θ_1, where Θ_q transforms Θ_1 into some power of Θ_1; and second when G is generated by three generators Θ_q, Θ_p, and Θ_1, where Θ_p transforms Θ_1 into some power of Θ_1 and Θ_q transforms Θ_1 and Θ_p into powers of Θ_1 and Θ_p respectively.

As this paper is a continuation of Dickson's paper (these Transactions, vol. 28 (1926), pp. 207–234), direct reference is made to it throughout. Numbered lemmas, numbered theorems and formulas in square brackets refer to lemmas, theorems and formulas in his paper. The notation is everywhere the same except that, for convenience in this paper, Q has been used for p, and δ for β. It is assumed that the reader has Dickson's paper before him.

The conditions D_1, D_2, and D_3 are the formulas [53], [55], and [58] of Theorem 10:

$$D_1 \qquad \delta = \delta(\theta_q)\alpha_e,$$

$$D_2 \qquad \alpha_k\alpha_r(\theta_{k_0})c_{k_0r_0} = c_{kr}(\theta_q)\alpha_u \qquad (k,r = 1, \cdots, q-1;\ \alpha_0 = 1),$$

$$D_3 \qquad \delta d_k = \alpha_k(\theta_q^{Q-1})\alpha_{k_0}(\theta_q^{Q-2})\alpha_{k_{00}}(\theta_q^{Q-3}) \cdots \alpha_{k_0 \cdots 0}\delta(\theta_{k_0 \cdots 0}) \qquad (k = 1, 2, \cdots, q-1),$$

* Presented to the Society, December 31, 1926; received by the editors January 28, 1927.

† L. E. Dickson, *New division algebras*, these Transactions, vol. 28 (1926).

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

Part 1. Algebras Γ connected with a non-abelian group generated by two generators

2. **The group G.** Let G_q be the cyclic group generated by Θ_1 of order q, and let G_q be extended to G by Θ_q where G_q is of index Q under G. Then the Qth, but no lower than the Qth power of Θ_q, is a substitution of G_q. If also Θ_q transforms Θ_1 into some power x of Θ_1, then

$$\Theta_q^Q = \Theta_1, \quad \Theta_q^{-1}\Theta_1\Theta_q = \Theta_1^x$$

where e and x are integers less than q.

Since G_q is cyclic we may denote $\Theta_1{}^k$ by $\Theta_k (k<q)$ and hence

$$\Theta_q^{-s}\Theta_k\Theta_q{}^s = \Theta_1{}^{kx^s} \text{ for all integers } s > 0. \tag{1}$$

But $\Theta_e=\Theta_q^Q$ and is commutative with Θ_q, hence it follows from (1) with $k=e$ and $s=1$ that

$$e(x-1) \equiv 0 \pmod{q}. \tag{2}$$

For the same reason replacing s by Q and k by 1 in (1), we see that

$$x^Q \equiv 1 \pmod{q} \tag{3}$$

and that x is relatively prime to q. Groups of this type exist; one such is a transitive group of order 16 with $Q=2$, $q=8$, $x=5$ and $e=4$.

3. **Algebra Σ.** The units j may be given the notation

$$j_1{}^k = j_k, \quad j_q^s = j_{sq}, \quad j_kj_{sq} = j_{sq+k} \quad (k<q, \quad s<Q), \tag{4}$$

$$j_1{}^q = g, \quad j_q^Q = \delta_{i_e}, \tag{5}$$

where g and δ are numbers $\neq 0$ of $F(i)$. We also see that

$$k_0 \equiv kx \pmod{q}, \quad k_{0\cdots 0} \equiv kx^s \pmod{q} \quad (k_0<q, \quad k_{0\cdots 0}<q)$$

where there are s zeros as subscript to k. Throughout this part of the paper α_{kx^s} will denote $\alpha_{k_{0\cdots 0}}$ where there are s zeros subscript to k.

The subgroup G_q is now cyclic. Hence by Theorem 1 the algebra Σ may be regarded as an algebra of order q^2 over the field F_1, derived from F by adjoining all the symmetric functions of i, $\theta_1(i)$, $\cdots$, $\theta_{q-1}(i)$. This algebra is associative if $g=g(\theta_1)$.* Consequently, by Theorem 10, Γ is associative, if the conditions D_1, D_2 and D_3 all hold and $g=g(\theta_1)$.

---

* Loc. cit., §4.

4. **Associativity conditions for Γ.** Equation [6] gives the following formulas:

$$(6)\qquad \begin{aligned} j_k j_r &= j_u, \quad u = k + r, \quad c_{kr} = 1 &&(r + k < q),\\ j_{kr} &= g j_u, \quad u = k + r - q, \quad c_{kr} = g &&(r + k \geqq q,\ r < q,\ k < q). \end{aligned}$$

The condition D_1 gives

$$(7)\qquad \delta = \delta(\theta_q)\alpha_e.$$

Let us now consider the condition D_2. For any integer $m > 0$, there exists an integer a_m, $0 \leqq a_m < q$, and an integer $t_m > 0$ such that $t_m x = mq + a_m$ and $(t_m - 1)x < mq$. We define t_0 to be 1. Hence a_m is the value of t_{m_0}, which is written for $(t_m)_0$. If $t_{m+1} > k \geqq t_m$, then $k = t_m + s$, $kx = mq + a_m + sx$ and $k_0 = a_m + sx$. In the same way, if $t_{n+1} > r \geqq t_n$, $r = t_n + v$ and $r_0 = a_n + vx$.

If $k + r < q$, $c_{kr} = 1$ by (6) and, if $k_0 + r_0 < q$, $c_{k_0 r_0} = 1$ and $(k+r)x = (m+n)q + r_0 + k_0$. Consequently $u = t_{m+n} + b$ and D_2 becomes

$$(8)\qquad \alpha_{t_m+s}\alpha_{t_n+v}(\theta_1^{kx}) = \alpha_{t_{m+n}+b}.$$

But, if $k_0 + r_0 \geqq q$, $u = t_{m+n+1} + b$, and D_2 becomes

$$(9)\qquad \alpha_{t_m+s}\alpha_{t_n+v}(\theta_1^{kx})g = \alpha_{t_{m+n+1}+b}.$$

If we write $k = 1$, that is $m = 0$ and $s = 1$, in (8) and (9) we get

$$(10)\qquad \alpha\,\alpha_{t_n+v}(\theta_1^{x}) = \alpha_{t_n+v+1} \qquad (v + 1 < t_{n+1} - t_n),$$

$$(11)\qquad \alpha\,\alpha_{t_n+v}(\theta_1^{x})g = \alpha_{t_{n+1}} \qquad (v + 1 = t_{n+1} - t_n),$$

and (12) follows by induction from (10) and (11):

$$(12)\qquad \alpha_r = \alpha_{t_n+v} = g^n \alpha\alpha(\theta_1^{x}) \cdots \alpha(\theta_1^{(r-1)x}) \qquad (r = 1, 2, \cdots, q-1).$$

It is easily verified that equations (9) and (10) are satisfied identically, when the values for α_k, α_r and α_u from (12) are substituted into them.

When $k + r = q$, $k_0 + r_0 = q$ and so $c_{kr} = c_{k_0 r_0} = g$, while $u = 0$. Hence D_2 becomes $\alpha_k \alpha_r(\theta_1^{kx})g = g(\theta_q)$, or on substitution for α_k and α_r from (12)

$$(13)\qquad \alpha\alpha(\theta_1^{x})\alpha(\theta_1^{2x}) \cdots \alpha(\theta_1^{(q-1)x})g^x = g(\theta_q).$$

That g occurs on the left hand side to the power of x is easily seen. For

$$(k + r)x = (m + n)q + k_0 + r_0 = (m + n + 1)q,$$

$$m + n + 1 = x.$$

If $k+r>q$, $c_{kr}=g$ and $u=k+r-q$. Then, as in the previous cases,

$$c_{k_0r_0} = 1, \quad k + r = t_{m+n} + b, \quad u = t_{m+n-s} + b;$$
$$= g, \quad k + r = t_{m+n+1} + b, \quad u = t_{m+n+1-s} + b.$$

On substituting for α_k, α_r and α_u their values from (12) into D_2 and cancelling the terms common to both sides, we see that, when $k+r>q$, D_2 reduces to (13). Hence we have the following lemma:

LEMMA A. *The condition D_2 reduces for all values of $k, r<q$, to* (12) *or* (13), *where* (12) *merely serves to express $\alpha_r(r=2, \cdots, q-1)$ in terms of α.*

Next, let us consider the condition D_3. Since $X^Q \equiv 1 \pmod q$, $j_{k_0\ldots_0}=j_k$ (where there are Q subscripts 0) and, since j_0 and j_k are commutative, d_k in D_3 is equal to 1. Condition D_3 becomes

$$(14) \qquad \delta = \alpha_k(\theta_q^{Q-1})\alpha_{kx}(\theta_q^{Q-2}) \cdots \alpha_{kx^{Q-1}}\delta(\theta_1^k) \qquad (k = 1,2, \cdots ,q-1).$$

LEMMA B. *The condition* (14) *follows for all values of $k<q$ from*

$$(15) \qquad \delta = \alpha(\theta_q^{Q-1})\alpha_x(\theta_q^{Q-2})\alpha_{x^2}(\theta_q^{Q-3}) \cdots \alpha_{x^{Q-1}}\delta(\theta_1).$$

To prove this lemma by induction, we assume that (14) holds for all values of $k \leqq k$ and, writing θ_1^k for i in (15), combine the equation thus obtained with (14). Since by [8] and (1)

$$\theta_q^{Q-s}\theta_1^k = \theta_1^{kx^s}\theta_q^{Q-s},$$
$$\delta\, \delta(\theta_1^k) = \prod_{s=1}^{s=Q} \alpha_{kx^{s-1}}(\theta_q^{Q-s})\alpha_{x^{s-1}}(\theta_1^{kx^s}\theta_q^{Q-s})\delta(\theta_1^k)\delta(\theta_1^{k+1}).$$

But by the general formula D_2 this becomes

$$(16) \qquad \delta = \delta(\theta_1^{k+1}) \prod_{s=1}^{s=Q} \alpha_{(k+1)x^{s-1}}(\theta_q^{Q-s}) \frac{c_{kx^{s-1},x^{s-1}}(\theta_q^{Q-s+1})}{c_{kx^s,x^s}(\theta_q^{Q-s})},$$

(Since $\Theta_1^{kx^s}=\Theta_{k_0\ldots_0}$, c_{kx^s,x^s} is used to denote $c_{k_0\ldots_0,1_0\ldots_0}$, where there are s subscripts 0.). All the c's in this product cancel except the first of the numerator and the last of the denominator, namely $c_{k,1}(\theta_q^Q)$ and c_{kx^Q,x^Q}, each of which is equal to 1, since for the induction $k<q-1$. Hence (16) is simply (14) with k replaced by $k+1$. As (14) holds for $k=1$ the proof of the lemma is complete.

We have now proved the following theorem:

THEOREM A. *Let $f(x)=0$ be an equation of degree Qq irreducible in F whose Galois group G is generated by Θ_1 and Θ_q, such that Θ_1 is of order q and Θ_q transforms Θ_1 into Θ_1^x and $\Theta_q{}^Q=\Theta_1{}^e$, while no lower than the Qth 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 x, e, q and Q must satisfy (2) *and* (3). *The roots of $f(x)=0$ are*

$$\theta_1^k(\theta_q^r(i)) = \theta_q^r(\theta_1^{kx^r}(i)) \qquad \begin{pmatrix} r = 0,1,\cdots,Q-1 \\ k = 0,1,\cdots,q-1 \end{pmatrix},$$

where $\theta_1^q(i)=i$, $\theta_q^Q(i)=\theta_1^e(i)$, and θ_1 and θ_q are rational functions of i with coefficients in F. There exists an associative algebra Σ whose elements are

$$A = f_0 + f_1 j_1 + f_2 j_1^2 + \cdots + f_{q-1} j_1^{q-1},$$

where the f_k are polynomials in i of degree less than Qq with coefficients in F, while

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

so that the product of any two elements of Σ is another element of Σ. Let

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

where α_k is defined by (12). *Then under multiplication defined by* [20] *the totality of polynomials in j_q with coefficients in Σ form an algebra of order Q^2q^2 over F, which is associative if and only if $g=g(\theta_1)$, $\delta=\delta(\theta_q)\alpha_e$, and* (13) *and* (15) *hold.*

PART 2. ALGEBRAS Γ CONNECTED WITH A GROUP GENERATED BY THREE GENERATORS

5. **The group G.** Let the group G have the invariant subgroup G_q, which is of the same type as the group G considered in §2, where G_q has the invariant cyclic subgroup G_p generated by Θ_1 of order p, and G_p is of index P under G_q and is extended to G_q by the substitution Θ_p. Further, let G_q be of index Q under G so that the Qth, but no lower than the Qth, power of Θ_q is a substitution of G_q. Then, if Θ_q transforms Θ_1 into Θ_1^y and Θ_p into Θ_p^z, while Θ_p transforms Θ_1 into Θ_1^x, we have

$$(17) \qquad \Theta_q^Q = \Theta_{e'} = \Theta_p^{e_2}\Theta_1^{e_1}, \qquad \Theta_p^P = \Theta_e = \Theta_1^e \qquad (e < p,\ e_1 < p,\ e_2 < P),$$

$$(18) \qquad \Theta_p^{-s}\Theta_1^a\Theta_p^s = \Theta_1^{ax^s}.$$

$$(19) \qquad \Theta_q^{-s}\Theta_1^a\Theta_q^s = \Theta_1^{ay^s},$$

$$(20) \qquad \Theta_q^{-s}\Theta_p^b\Theta_q^s = \Theta_p^{bz^s},$$

where a, b and s are integers >0.

It follows from §2 that the substitutions of G_q are represented uniquely in the form $\Theta_k=\Theta_{bp+a}=\Theta_p{}^b\Theta_1{}^a$ $(b<P,\ a<p)$ and if $q=Pp$ the substitutions of G in the form $\Theta_{rq+k}=\Theta_q{}^r\Theta_k(r<Q,\ k<q)$. As in §2 we see that

(21) $$x^P\equiv 1 \pmod{p},$$

(22) $$(x-1)e\equiv 0 \pmod{p}.$$

If we write $s=Q$, $a=1$ in (19), it follows from (17) that

(23) $$x^{e_2}\equiv y^Q \pmod{p}.$$

Similarly, from (17) and (20) with $s=Q$, we find that

(24) $$b(z^Q-1)=bmP,\ \ emb+e_1(x^b-1)\equiv 0 \pmod{p}(b=1,\cdots,P-1).$$

But (24) is satisfied if

(25) $$z^Q-1=mP,\ \ em+e_1(x-1)\equiv 0 \qquad \pmod{p}(m \text{ integer} > 0).$$

In addition the transforms of Θ_q^Q and $\Theta_p^{e_2}\Theta_1^{e_1}$ by Θ_q must be equal and also the transforms of Θ_p^P and Θ_e by Θ_p. Hence we have

(26) $$e_2(z-1)=np,\ \ e(z-y)\equiv 0 \qquad \pmod{p}(n \text{ integer} > 0).$$

Finally, since

$$\Theta_q^{-1}(\Theta_p^{-1}\Theta_1\Theta_p)\Theta_q=(\Theta_q^{-1}\Theta_p^{-1})\Theta_1(\Theta_p\Theta_q),$$
$$\Theta_1{}^{zy}=\Theta_1{}^{yz^s},$$

and, as x is relatively prime to p, y is relatively prime to p by (23). Hence

(27) $$x^{z-1}\equiv 1 \pmod{p}.$$

Other conditions to be satisfied by the parameters e, e_1, e_2, x, y, and z may be deduced, but these are all that will be required. It is sufficient for our purpose that groups of this type do exist. For example, there is a transitive group of order 32 in which $p=4$, $P=4$, $Q=2$, $e=2$, $e_1=2$, $e_2=0$ and $x=y=z=3$.

If $k=a+bp(a=0,1,\cdots,p-1;b=0,1,\cdots,P-1)$, then $k_{00\cdots0}=a_{00\cdots0}+b_{00\cdots0}p$ where $a_{00\cdots0}<p$ and $\equiv ay^s \pmod{p}$, $b_{00\cdots0}<P$ and $\equiv bz^s \pmod{P}$ and there are s subscripts 0. With these values of k and k_0, the units and constants of multiplication of Γ are given by formulas [49], [50] and [52], where p, e and β are replaced by Q, e' and δ respectively.

6. **The algebra Σ.** The subgroup G_q being now of the type G considered in §2, the algebra Σ, which by Theorem 1 may be regarded as an algebra of order q^2 over the field F_1, derived from F by adjoining all the symmetric functions of i, $\theta_1(i),\cdots,\theta_{q-1}(i)$, is of the type Γ considered in Part 1. If

we substitute p, P, β and ρ for q, Q, α and δ respectively, all the formulas of Part 1 hold. Hence Σ is associative if, and only if,

$$
\begin{aligned}
&g = g(\theta_1),\\
&\rho = \rho(\theta_p)\beta_e,\\
(28)\qquad &\beta\,\beta(\theta_1{}^x)\beta(\theta_1^{2x})\cdots\beta(\theta_1{}^{(p-1)x})g^x = g(\theta_p),\\
&\rho = \beta(\theta_p{}^{P-1})\beta_x(\theta_p{}^{P-2})\beta_{x^2}(\theta_p{}^{P-3})\cdots\beta_{x^{p+1}}\rho(\theta_1).
\end{aligned}
$$

By Theorem 10, if (28) holds, Γ is associative if and only if the conditions D_1, D_2, and D_3 all hold. In these conditions, as quoted in the introduction, we must now write e' for e.

7. **Associativity conditions for Γ.** Condition D_1 gives

$$
(29)\qquad \delta = \delta(\theta_q)\alpha_{e'} \qquad (e' = e_1 + e_2 p).
$$

In the consideration of condition D_2, let

$$
\begin{aligned}
k &= bp + a\\
r &= sp + t
\end{aligned}
\qquad
\begin{pmatrix} a,\ t = 0,1,\cdots,p-1\\ b,\ s = 0,1,\cdots,P-1 \end{pmatrix}.
$$

If $b = s = 0$, we see as in §4 that D_2 reduces to (30) and (31):

$$
(30)\qquad \alpha_a = \alpha_{t_n+v} = g^n\alpha\alpha(\theta_1{}^v)\cdots\alpha(\theta_1{}^{(a-1)v}) \qquad (a = 1,2,\cdots,p-1),
$$

$$
(31)\qquad g(\theta_q) = \alpha\alpha(\theta_1{}^v)\cdots\alpha(\theta_1{}^{(p-1)v})g^v,
$$

where $yt_n = np + a_n$ and $(t_n - 1)y < np$, while $t_{n+1} > a \geqq t_n$.*

Now, let $a = t = 0$ so that k and r are multiples of p and may be taken as kp and rp respectively. Hence we must consider the condition

$$
(32)\qquad \alpha_{kp}\alpha_{rp}(\theta_{kp_0})c_{kp_0,rp_0} = c_{kp,rp}(\theta_q)\alpha_u.
$$

If $zt_m = mP + a_m, z(t_m - 1) < mP (m = 0,1,\cdots,z-1)(a_m < P)$,* and $t_{m+1} > k \geqq t_m$, then $k = t_m + s$ and $kz = mP + b$, where $b = sz + a_m < P$.

Since, by the second of (17), $\Theta_p^{kz} = \Theta_p^b\Theta_1^{me}$,† we must consider the value of em. As at the beginning of §4 we can find integers f_μ and $a_\mu \geqq 0$, such that $ef_\mu = \mu p + a_\mu$ and $e(f_\mu - 1) < p$ where $a_\mu < p$. Then, if $f_{\mu+1} > m = f_\mu + h \geqq f_\mu$, $\Theta_p^{kz} = \Theta_p^b\Theta_1^{a_\mu + he}$. Hence $kp_0 = bp + a_\mu + he$. Similarly, if $r = t_n + v$, $n = f_\nu + w$,

---

* See the definition of t_m and a_m at the beginning of §4.

† If $e = 0$ the work is exactly similar to that in §4.

then $rp_0=dp+a_\nu+we$, where $d=vz+a_n<P$. We now require to consider the value of c_{kp_0,rp_0}. Since

$$j_{kp_0}j_{rp_0} = c_{kp_0,rp_0}j_{u_0}$$
$$= j_1^{a_\mu+he}j_p^{b}j_1^{a_\nu+we}j_p^{d},$$

then

$$c_{kp_0,rp_0}j_{u_0} = c_{bp,ne}(\theta_1^{me})j_1^{\sigma}j_p^{d+b}, \tag{33}$$

where $\sigma=a_\mu+a_\nu+(h+w)e$.

For, since

$$a_\nu + we \equiv ne \pmod p,$$
$$(a_\nu + we)x^b \equiv nex^b \pmod p$$

and so by (22)

$$nex^b \equiv ne \equiv a_\nu + we \pmod p.$$

In (33), $c_{bp,ne}$ denotes $c_{bp,f}$, where $ne\equiv f \pmod p$ and $f<p$, and later, to simplify the formulas, $c_{bp+a,sp+t}$ is often written for c_{kr}, if $\Theta_q^b\Theta_1^a=\Theta_k$ and $\Theta_q^s\Theta_1^t=\Theta_r$, even when a and t are greater than p, and b and s greater than P. When $b+d<P$, $j_p^{b+d}=j_{(b+d)p}$ and, if $\sigma<p$, $m+n$ is of the form $f_{\mu+\nu}+t$ and $c_{kp_0,rp_0}=c_{bp,ne}(\theta_1^{me})$; but, if $\sigma\geqq p$, then $m+n$ is of the form $f_{\mu+\nu+1}+t$ and $c_{kp_0,rp_0}=gc_{bp,ne}(\theta_1^{me})$.

When $b+d\geqq P$, $j_p^{b+d}=\rho j_1^{e}j_p^{b+d-P}$, and from (33) we see that a factor g or g^2 occurs in c_{kp_0,rp_0}, according as $\sigma+e\geqq p$ or $\geqq 2p$; that is, according as $m+n+1$ is of the form $f_{\mu+\nu+1}+t$ or $f_{\mu+\nu+2}+t$. Hence the complete values of c_{kp_0,rp_0} as obtained from (33) are given by

$$c_{kp_0,rp_0} = Xc_{bp,ne}(\theta_1^{me}) \tag{34}$$

where

$$\begin{aligned} X &= 1, \text{ if } k+r=t_{m+n}+s,\ m+n=f_{\mu+\nu}+t,\\ &= g, \text{ if } k+r=t_{m+n}+s,\ m+n=f_{\mu+\nu+1}+t,\\ &= \rho(\theta_1^{(m+n)e}), \text{ if } k+r=t_{m+n+1}+s,\ m+n+1=f_{\mu+\nu}+t,\\ &= \rho(\theta_1^{(m+n)e})g, \text{ if } k+r=t_{m+n+1}+s,\ m+n+1=f_{\mu+\nu+1}+t,\\ &= \rho(\theta_1^{(m+n)e})g^2, \text{ if } k+r=t_{m+n+1}+s,\ m+n+1=f_{\mu+\nu+2}+t. \end{aligned}$$

Now, since $j_pj_e=\beta_ej_ej_p$, we have

$$c_{bp,ne} = \beta_{ne}\beta_{ne}(\theta_p)\cdots\beta_{ne}(\theta_p^{b-1}), \tag{35}$$

and by (10) and (11)

$$
\begin{aligned}
(36) \qquad & \beta_{re} = \beta_e \beta_{(r-1)}(\theta_1^e) & (r \neq f_\nu), \\
& \beta_{re} = \frac{g}{g(\theta_p)} \beta_e \beta_{(r-1)e}(\theta_1^e) & (r = f_\nu).
\end{aligned}
$$

For $ex \equiv e \pmod{p}$ and accordingly $c_{e,(r-1)e} = c_{e_0,(r-1)e_0}$.

Hence, by (17), the second of (28), (35), and (36),

$$
(37) \qquad c_{bp,ne} = \frac{G_n}{G_n(\theta_p^b)} \left(\frac{g}{g(\theta_p^b)} \right),
$$

where $G_n = \rho\, \rho(\theta_e) \cdots \rho(\theta_e^{n-1})$, and $n = f_\nu + w$.

When $k+r<P$, $c_{kp,rp}=1$ and $u=(k+r)p$, and if we take $k=1$, D_2 by means of (34) and (37) becomes

$$
(38) \qquad Y \alpha_p \alpha_{rp}(\theta_p^s) \frac{G_n}{G_n(\theta_p^s)} \left(\frac{g}{g(\theta_p^s)} \right)^\nu = \alpha_{(r+1)p}
$$

where

$$
\begin{aligned}
Y &= 1, \quad r \neq t_{n+1} - 1, \\
&= \rho(\theta_e^{n+m}), \quad r + 1 = t_{n+1}, \quad n + 1 \neq f_{\nu+1}, \\
&= g\rho(\theta_e^{n+m}), \quad r + 1 = t_{n+1}, \quad n + 1 = f_{\nu+1}.
\end{aligned}
$$

From successive applications of (38) we get*

$$
(39) \qquad \alpha_{rp} = \alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{(r-1)s}) \rho\rho(\theta_e) \cdots \rho(\theta_e^{n-1}) g^\nu,
$$

where $r=1, 2, \cdots, P-1$; $r=t_n+v$; $n=f_\nu+w$.

By means of (34) and the formula $\theta_p^b \theta_1^{me} = \theta_p^{ks} = \theta_{kp_0}$, it can be shown that D_2 is satisfied identically when the values of α_{kp}, α_{rp} and α_u are substituted from (39) into (32), for all values of k and r for which $k+r<P$.

But, if $k+r=P$, $c_{kp,rp}=\rho$ and $u=e$. Hence

$$
(k + r)z = Pz, \quad k + r = t_z,
$$

and, since $kz \not\equiv 0 \pmod{P}$ $(k \leqq P-1)$, $z=m+n+1$. If

$$
(40) \qquad z = f_\lambda + h \qquad (a_\lambda + he < p),
$$

$\lambda = \mu+\nu$ or $\mu+\nu+1$ or $\mu+\nu+2$, and in all cases by (34) and (39) D_2 reduces to†

$$
(41) \qquad \alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{s(P-1)}) \rho\rho(\theta_e) \cdots \rho(\theta_e^{z-1}) g^\lambda = \rho(\theta_q) \alpha_e.
$$

---

* If $e=0$, $\nu \equiv 0$ and $\alpha_{rp} \equiv \alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{(r-1)s}) \rho^n$.

† If $e=0$, $\lambda=0$, $\alpha_e=1$ and (41) becomes $\alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{s(P-1)})\, \rho^z = \rho(\theta_q)$.

Similarly, if $k+r>P$, D_2 reduces to (41) for all values of $k<P$, $r<P$. For, when $k+r>P$, $c_{kp,rp}=\rho$ and $u=e+(k+r-P)p$. Now

$$\alpha_e\alpha_{(k+r-P)p}(\theta_e^y)c_{e_0,(k+r-P)p_0} = \alpha_{e+(k+r-P)p},$$

and by (26) D_2 becomes

$$\alpha_{kp}\alpha_{rp}(\theta_p^{ks})c_{kp_0,rp_0} = \rho(\theta_q)c_{es,(k+r-P)sp}\alpha_e\alpha_{(k+r-P)p}(\theta_p^{Ps}), \tag{42}$$

and, if

$$k + r = t_e + a \qquad (a_e + az < P),$$

then

$$z(k + r) = sP + a_e + az, \quad k + r - P = t_{e-s} + a.$$

Hence, if $s=f_\sigma+n$, where $a_\sigma+ne<p$, the left hand side of (42) is equal to

$$\alpha_p\alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{(k+r-1)s})\rho\rho(\theta_e) \cdots \rho(\theta_e^{\sigma-1})g^\sigma.$$

Then, if

$$s - z = f_\mu + n' \qquad (a_\mu + n'e < p),$$

by (40)

$$s = f_{\lambda+\mu} + n'' \text{ or } f_{\lambda+\mu+1} + n'',$$

and so $\sigma=\lambda+\mu$ or $\lambda+\mu+1$, according as $c_{es,(k+r-P)s}=1$ or g. The right hand side of (42) then becomes

$$\rho(\theta_q)\alpha_e\alpha_p(\theta_p^{Ps})\alpha_p(\theta_p^{(P+1)s}) \cdots \alpha_p(\theta_p^{(k+r-1)s})X,$$

where

$$X = \rho(\theta_e^z)\rho(\theta_e^{z+1}) \cdots \rho(\theta_e^{\sigma-1})g^{\sigma-\lambda}.$$

On equating the two sides so obtained and cancelling the common factors, we get (41).

We must now consider the general case of D_2, where

$$k = a + bp \qquad r = t + sp \qquad \begin{pmatrix} a,\ t = 1,2,\cdots,p-1 \\ b,\ s = 1,2,\cdots,P-1 \end{pmatrix}.$$

For simplicity in writing let

$j_1^{a'}$ be defined as j_a when $\Theta_1^{a'} = \Theta_a$ and $a' > p > a$,

$j_p^{b'}$ be defined as j_{bp+d} when $\Theta_p^{b'} = \Theta_{bp+d}$ and $b' > P > b$.

Then

$$j_1^a j_p^b j_1^t j_p^s = c_{bt}(\theta_1^a) j_1^a j_1^{tzb} j_p^b j_p^s,$$

$$j_k j_r = c_{bt}(\theta_1^a)c_{a,tzb}j_v c_{bp,sp}j_w.$$

Hence

(43) $$c_{kr} = c_{bt}(\theta_1^{a}) c_{a,txb} c_{bp,sp}(\theta_1^{v}) c_{vw}.$$

To get the value of $c_{k_0 r_0}$ we consider*

$$j_1^{ay} j_p^{bz} j_1^{ty} j_p^{sz}$$

which is equal to

(44) $$c_{ay,bzp} j_{k_0} c_{ty,szp} j_{r_0} = c_{ay,bzp} c_{ty,szp}(\theta_{k_0}) c_{k_0 r_0} j_{u_0}.$$

Since j_{bp_0} may be of the form $j_1^n j_p^m$ we have

$$c_{tyx^{bz},bzp} j_p^{bz} j_1^{ty} = c_{bzp,ty} j_1^{tyx^{bz}} j_p^{bz},$$

or, since $x^s \equiv x \pmod{p}$,

(45) $$c_{tyx^b,bzp} j_p^{bz} j_1^{ty} = c_{bzp,ty} j_1^{tyx^b} j_p^{bz}.$$

Hence

(46) $$c_{tyx^b,bzp}(\theta_1^{ay}) j_1^{ay} j_p^{bz} j_1^{ty} j_p^{sz}$$

$$= c_{bzp,ty}(\theta_1^{ay}) c_{ay,tyx^b} c_{bzp,szp}(\theta_{v_0}) c_{v_0 w_0} j_{u_0},$$

where

$$j_1^{ay} j_1^{tyx^b} = c_{ay,tyx^b} j_{v_0},$$

$$j_p^{bz} j_p^{sz} = c_{bzp,szp} j_{w_0}.$$

We get as special cases of D_2,

$$\alpha_v \alpha_w(\theta_{v_0}) c_{v_0 w_0} = c_{vw}(\theta_q) \alpha_u,$$

(47) $$\alpha_a \alpha_{tx^b}(\theta_{a_0}) c_{ay,tx^b y} = c_{a,tx^b}(\theta_q) \alpha_v,$$

$$\alpha_{bp} \alpha_{sp}(\theta_{bp_0}) c_{bzp,szp} = c_{bp,sp}(\theta_q) \alpha_w,$$

and

(48) $$\alpha_k = \alpha_{a+bp} = \alpha_a \alpha_{bp}(\theta_{a_0}) c_{ay,bzp}$$

$$(a = 0, 1, \cdots, p-1;\ b = 0, 1, \cdots, P-1),$$

where (48) combined with (30) and (39) defines α_k in terms of α and α_p, and $c_{ay,bzp} = 1$ or g according as $a_m + s_\mu < p$ or $\geqq p$, where

$$ay = mp + a_m \quad (a_m < p), \quad bz = sP + b_s \quad (b_s < P), \quad se = \mu p + s_\mu \quad (s_\mu < p).$$

---

* If $e = 0$, $c_{ny,mzp} = 1$ for all values of n and m.

Making use of (47) and (48), and substituting for c_{kr} and $c_{k_s r_s}$ their values obtained from (44), (45) and (46) in D_2, we get

$$\alpha_{bp}\alpha_t(\theta_p^{b^s})c_{bsp,ty} = c_{tyx^b,bsp}c_{bp,t}(\theta_q)\alpha_{tx^b}\alpha_{bp}(\theta_1^{tyx^b}). \tag{49}$$

The w in the first of (47) may be of the form $t+sp$ and so the first of (47) is a case of D_2 that we are considering. But by writing $a=v$, $b=0$, and proceeding as in the general case, we reduce it to (49), where since $b=0$ the formula corresponding to the first of (47) is now of the type (48). The second and third of (47) have been treated earlier.

We now prove the following lemma:

LEMMA A. *The formula* (49) *may be deduced for all values of* $b<P$ *and* $t<p$ *from*

$$\alpha_p\alpha(\theta_p^{s})c_{sp,y} = c_{yx,sp}c_{p,1}(\theta_q)\alpha_x\alpha_p(\theta_1^{xv}). \tag{50}$$

Assume that (49) holds for all values of $b\leqq b$ and $t\leqq t$, and consider (49) with $t=1$; that is

$$\alpha_{bp}\alpha(\theta_p^{b^s})c_{bsp,y} = c_{yx^b,bsp}c_{bp,1}(\theta_q)\alpha_{x^b}\alpha_{bp}(\theta_1^{yx^b}). \tag{51}$$

If we now write $\theta_1^{tyx^b}$ for i in (51) and multiply the left members of (51) and (49) together and equate the result to the product of the right members, we get

$$\begin{aligned}\alpha_{bp}\alpha_{t+1}(\theta_p^{b^s})c_{bsp,ty}c_{bsp,y}(\theta_1^{tyx^b})c_{tx^by,yx^b}\\ =Y\alpha_{(t+1)x^b}\alpha_{bp}(\theta_1^{(t+1)yx^b})\end{aligned} \tag{52}$$

where

$$Y = c_{ty,y}(\theta_p^{b^s})c_{bp,1}(\theta_1^{x^b}\theta_q)c_{tyx^b,bps}c_{yx^b,bsp}(\theta_1^{tyx^b})c_{tx^b,x^b}(\theta_q).$$

Now,

$$\begin{aligned}c_{ty,y}(\theta_p^{b^s})c_{bsp,(t+1)y}c_{tyx^b,bsp}c_{yx^b,bsp}(\theta_1^{tyx^b})\\ = c_{bsp,ty}c_{bsp,y}(\theta_1^{tyx^b})c_{tyx^b,yx^b}c_{(t+1)yx^b,bsp},\end{aligned}$$

and

$$c_{bp,t+1} = c_{bp,1}(\theta_1^{tx^b})c_{bp,t}c_{tx^b,x^b}.$$

Making use of these two results, we see that (52) becomes (49) with t replaced by $t+1$, and so by induction (49) may be deduced from (51).

Now, (49) with $t=x$ becomes

$$\alpha_{bp}\alpha_x(\theta_p^{b^s})c_{bsp,xy} = c_{yx^{b+1},bsp}c_{bp,x}(\theta_q)T, \tag{53}$$

where

$$T = \alpha_{x^{b+1}}\alpha_{bp}(\theta_1^{yx^{b+1}}).$$

Since

$$c_{(b+1)p,1} = c_{p,1}(\theta_p{}^b)c_{bp,x}$$

and

$$c_{bzp,zp}\,c_{(b+1)zp,y}\,c_{yx,zp}(\theta_p{}^{bz})c_{yx^{b+1},bpz}$$
$$= c_{zp,y}(\theta_p{}^{bz})c_{bzp,xy}\,c_{bzp,zp}(\theta_1{}^{yx^{b+1}})c_{yx^{b+1},(b+1)zp},$$

when we combine (53) with (50), where θ_p^{bz} is written for i in (50), we get (49) with b replaced by $b+1$ and our lemma is proved. Since $z<P$, $c_{yz,zp}=1$ and (50) becomes

(54) $$\alpha_p\alpha(\theta_p{}^z)c_{zp,y} = c_{p,1}(\theta_q)\alpha_z\alpha_p(\theta_1{}^{xy}),$$

where

$$c_{p1} = \beta,\ c_{zp,y} = \beta_y(\theta_p{}^{z-1})\beta_{yz}(\theta_p{}^{z-2}) \cdots \beta_{yz^{z-1}}.$$

We have now shown that the condition D_2 reduces for all values of $k<q$, $r<q$ to (30), (31), (39), (41), (48), and (54) where (30), (39), and (48) merely express $\alpha_k(k<q)$ in terms of α and α_p.

It remains to consider the condition D_3. If $j_{e'}j_k=d_kj_{k'}j_{e'}$, where $j_{k'}=j_{k_0}\cdots_e$ and there are Q subscripts 0, $k'=a'+b'p$, where $a'=ay^Q\equiv ax^{e_2}$ (mod p) by (26), and $b'=bz^Q=bmP+b$ by (24), and accordingly

$$j_p{}^{b'} = j_1{}^{me}j_p{}^b.$$

Also $c_{e'k}=d_kc_{k'e'}$ and D_3 becomes

(55) $$c_{e'k}\delta = c_{k'e'}\alpha_{a+bp}(\theta_q{}^{Q-1}) \cdots \alpha_{y^{Q-1}+bz^{Q-1}p}\delta(\theta_{k'}).$$

We shall now prove the following lemma:

Lemma B. *Condition D_3 follows for all values of $k<q$ from* (56) *and* (57):

(56) $$c_{e',1}\delta = c_{x^{e_2},e'}\alpha(\theta_q{}^{Q-1})\alpha_y(\theta_q{}^{Q-2}) \cdots \alpha_{y^{Q-1}}\delta(\theta_1{}^{x^{e_2}}),$$

(57) $$c_{e',p}\delta = c_{z^Qp,e'}\alpha_p(\theta_q{}^{Q-1})\alpha_{zp}(\theta_q{}^{Q-2}) \cdots \alpha_{z^{Q-1}p}\delta(\theta_p{}^{z^Q}).$$

Since (55) holds for all values of $k<q$, it is true in particular for the two cases $b=0$ and $a=0$ respectively:

(58) $$c_{e',a}\delta = c_{ax^{e_2},e'}\alpha_a(\theta_q{}^{Q-1})\alpha_{ay}(\theta_q{}^{Q-2}) \cdots \alpha_{ay^{Q-1}}\delta(\theta_1{}^{ax^{e_2}}),$$

(59) $$c_{e',bp}\delta = c_{b'p,e'}\alpha_{bp}(\theta_q{}^{Q-1})\alpha_{bzp}(\theta_q{}^{Q-2}) \cdots \alpha_{bz^{Q-1}p}\delta(\theta_p{}^{b'}).$$

If we write

$$\theta_1^{ay^Q} = \theta_1^{ax^{e_2}}$$

for i in (59), since

$$\theta_1^{ay^s}\theta_q{}^{Q-s} = \theta_q{}^{Q-s}\theta_1^{ay^Q},$$

we have from (58) and (59)

$$c_{e',a}c_{e',bp}(\theta_1^{ay^Q})\delta = c_{ax^{e_2},e'}c_{b'p,e'}(\theta_1^{ax^{e_2}})\delta(\theta_p{}^{b'}\theta_1^{ax^{e_2}})X, \tag{60}$$

where

$$X = \prod_{s=1}^{s=Q} \frac{\alpha_{ay^{s-1}+bx^{s-1}p}(\theta_q{}^{Q-s})c_{ay^{s-1},bx^{s-1}p}(\theta_q{}^{Q-s+1})}{c_{ay^s,bx^sp}(\theta_q{}^{Q-s})}$$

$$= c_{a,bp}(\theta_q{}^Q)\left[c_{ay^Q,bx^Qp}\right]^{-1}\prod_{s=1}^{s=Q}\alpha_{ay^{s-1}+bx^{s-1}p}(\theta_q{}^{Q-s}).$$

Now, since $meb+e_1(x^b-1)\equiv 0 \pmod{p}$ by (24),

$$j_p^{b'}j_{e'} = j_1^{meb}j_p^{b}j_1^{e_1}j_p^{e_2} = fj_1^{e_1}j_p^{b}j_p^{e_2} = fj_{e'}j_p^{b} \qquad (f\neq 0 \text{ and in } F(i)).$$

Hence,

$$j_1^{ax^{e_2}}j_p^{b'}j_{e'} = c_{ax^{e_2},b'p}c_{k'e'}j_u$$

$$= \frac{c_{b'p,e'}(\theta_1{}^{ax^{e_2}})c_{ax^{e_2},e'}c_{a,bp}(\theta_{e'})c_{e'k}j_u}{c_{e',bp}(\theta_1{}^{ax^{e_2}})c_{e'a}}.$$

From this result remembering that $ax^{e_2}\equiv ay^Q \pmod{p}$ and that $\Theta_p^Q=\Theta_{e'}$, we see that (60) becomes (55). By induction, in a manner similar to that used in Lemma B of §4, it can be shown that (58) and (59) are consequences of (56) and (57) respectively. In the proof we require the formulas

$$c_{e',a+1}c_{ax^{e_2},e'}c_{x^{e_2},e'}(\theta_1{}^{ax^{e_2}}) = c_{e'a}c_{e',1}(\theta_1{}^{ax^{e_2}})c_{ax^{e_2},x^{e_2}}c_{(a+1)x^{e_2},e'},$$

$$c_{bp,p}(\theta_{e'})c_{e',(b+1)p}c_{b'p,e'}c_{sQp,e'}(\theta_p{}^{b'})$$

$$= c_{e',bp}c_{e'p}(\theta_p{}^{b'})c_{b'p,sQp}c_{(b+1)'p,e'},$$

which can be deduced as in the previous cases. Since

$$c_{e'1} = c_{e_2p,1}(\theta_1{}^{e_1})c_{e_1,x^{e_2}} \text{ and } c_{e_1,x^{e_2}} = c_{x^{e_2},e_1} = c_{x^{e_2},e'},$$

(56) becomes

$$c_{e_2p,1}(\theta_1{}^{e_1})\delta = \alpha(\theta_q{}^{Q-1})\alpha_y(\theta_q{}^{Q-2})\cdots\alpha_{y^{Q-1}}\delta(\theta_1{}^{x^{e_2}}). \tag{61}$$

But $e_2\neq P-1$ by (26) and so $c_{e'p}=1$ and (57) becomes

$$\delta = c_{sQp,e'}\alpha_p(\theta_q{}^{Q-1})\alpha_{sp}(\theta_q{}^{Q-2})\cdots\alpha_{s^{Q-1}p}\delta(\theta_p{}^{sQ}). \tag{62}$$

In (61)

$$c_{e_2p,1} = \beta(\theta_p^{e_2-1})\beta_z(\theta_p^{e_2-2})\beta_{z^2}(\theta_p^{e_2-3}) \cdots \beta_{z^{e_2-1}},$$

and in (62), since $z^Q = mP+1$,

$$c_{zQp,e'} = \beta_{e'}(\theta_1^{me})c_{me,e_1x},$$

where $c_{me,e_1x} = 1$ or g, according as $t \leqq e_1$ or $> e_1$ and $e_1x \equiv t \pmod{p}$.

We have now proved

THEOREM B. *Let $f(x)=0$ be an equation of degree $n=QPp$, irreducible in a field F, whose group for F is generated by three generators Θ_1, Θ_p and Θ_q described in* §5. *Then the algebra Σ is associative if and only if conditions* (28) *hold. The totality of polynomials in j_q with coefficients in Σ form an algebra Γ of order n^2 over F which is associative if and only if conditions* (29), (31), (41), (54), (61), *and* (62) *all hold and Σ is associative.*

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.