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 $\Gamma$ of order $n^2 = q^n$ over a field $F$,
corresponding to the Galois group $G$ of order $n = q^n$ 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 $\Gamma$ if it is associative.
He has also reduced these conditions in detail for an algebra $\Gamma$ 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 $\Theta_0$ and $\Theta_1$, where $\Theta_0$ transforms $\Theta_1$ into some power of $\Theta_1$;
and second when $G$ is generated by three generators $\Theta_0$, $\Theta_1$, and $\Theta_2$, where $\Theta_0$
transforms $\Theta_1$ into some power of $\Theta_1$ and $\Theta_2$ transforms $\Theta_1$ and $\Theta_2$ into powers
of $\Theta_1$ and $\Theta_2$ 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 every-
where the same except that, for convenience in this paper, $Q$ has been used
for $p$, and $\delta$ for $\beta$. 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:

\[
D_1 \quad \delta = \delta(\theta_0)\alpha_s,
\]

\[
D_2 \quad \alpha_k\alpha_s(\theta_0\alpha) c_{k\theta_0} = c_{k\theta_0}(\theta_0\alpha) (k, r = 1, \ldots, q - 1; \alpha_0 = 1),
\]

\[
D_3 \quad \alpha_k\alpha_s(\theta_0\alpha) c_{k\theta_0} = c_{k\theta_0}(\theta_0\alpha) (k = 1, 2, \ldots, q - 1),
\]

* 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).

111
where there are $Q - 1$ subscripts 0 under the last $\alpha$ and $Q$ under the final $\theta$.

**Part 1. Algebras $\Gamma$ Connected with a Non-Abelian Group Generated by Two Generators**

2. The group $G$. Let $G_0$ be the cyclic group generated by $\Theta_1$ of order $q$, and let $G_0$ be extended to $G$ by $\Theta_q$ where $G_0$ is of index $Q$ under $G$. Then the $Q$th, but no lower than the $Q$th power of $\Theta_q$, is a substitution of $G_q$. If also $\Theta_q$ transforms $\Theta_1$ into some power $x$ of $\Theta_1$, then
\[
\Theta_q^2 = \Theta_1, \quad \Theta_q^{-1}\Theta_q\Theta_q = \Theta_1^x
\]
where $e$ and $x$ are integers less than $q$.

Since $G_q$ is cyclic we may denote $\Theta_1^x$ by $\Theta_s(k < q)$ and hence

\[
(1) \Theta_q^s = \Theta_1^x
\]

But $\Theta_0 = \Theta_q^0$ and is commutative with $\Theta_q$, hence it follows from (1) with $k = e$ and $s = 1$ that

\[
(2) e(x - 1) = 0 \quad (\text{mod } q).
\]

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

\[
(3) xQ = 1 \quad (\text{mod } q)
\]

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 $\Sigma$. The units $j$ may be given the notation

\[
(4) j^k = j_k, \quad j^s = j_s, \quad j_k j_m = j_{k+m} \quad (k < q, \ s < Q),
\]

\[
(5) j^k = g, \quad j^q = \delta_k,
\]

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

\[
k_0 = kx \quad (\text{mod } q), \quad k_0 \cdots k_s = kx^s \quad (\text{mod } q) \quad (k_0 < q, \ k_0 \cdots k_s < q)
\]

where there are $s$ zeros as subscript to $k$. Throughout this part of the paper $\alpha_{k,z}$ will denote $\alpha_{k,\ldots,z}$ where there are $s$ zeros subscript to $k$.

The subgroup $G_q$ is now cyclic. Hence by Theorem 1 the algebra $\Sigma$ may be regarded as an algebra of order $q^2$ over the field $F_{12}$ derived from $F$ by adjoining all the symmetric functions of $i, \theta_1(i), \ldots, \theta_{q-1}(i)$. This algebra is associative if $g = g(\theta_i)$. Consequently, by Theorem 10, $\Gamma$ is associative, if the conditions $D_1, D_2$ and $D_3$ all hold and $g = g(\theta_i)$.

4. Associativity conditions for $\Gamma$. Equation [6] gives the following formulas:

$$j_kj_r = j_u, \quad u = k + r, \quad c_{br} = 1 \quad (r + k < q),$$

$$j_k = gj_u, \quad u = k + r - q, \quad c_{br} = g \quad (r + k \geq q, \ r < q, \ k < q).$$

The condition $D_1$ gives

$$\delta = \delta(\theta_0)a_s.$$

Let us now consider the condition $D_2$. For any integer $m > 0$, there exists an integer $a_m$, $0 \leq a_m < q$, 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 $t_m$ which is written for $(t_m)_0$. If $t_{m+1} > k \geq t_m$, then $k = t_m + s$, $kx = mq + a_m + sx$ and $k_0 = a_m + sx$. In the same way, if $t_{n+1} > r \geq t_n$, $r = t_n + v$ and $r_0 = a_n + vx$.

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

$$\alpha_{t_{m+n} + t_{m+n} + (\theta_1^{k+r})} = \alpha_{t_{m+n} + b}.$$  

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

$$\alpha_{t_{m+n} + t_{m+n} + (\theta_1^{k+r})}g = \alpha_{t_{m+n+1} + b}.$$  

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

$$\alpha \alpha_{t_{n+1}}(\theta_1^s) = \alpha_{t_{n+1} + 1}, \quad (s + 1 < t_{n+1} - l_n),$$

$$\alpha \alpha_{t_{n+1}}(\theta_1^s)g = \alpha_{t_{n+1} + 1}, \quad (s + 1 = t_{n+1} - l_n),$$

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

$$\alpha_r = \alpha_{t_{n+r}} = g^r \alpha(\theta_1^s) \cdots \alpha(\theta_1^{(r-1)s}) \quad (r = 1, 2, \ldots, q - 1).$$

It is easily verified that equations (9) and (10) are satisfied identically, when the values for $\alpha$, $\alpha_r$, and $\alpha_u$ from (12) are substituted into them.

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

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

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,
\[
\begin{align*}
c_{kr} & = 1, \quad k + r = t_{m+n} + b, \quad u = t_{m+n-1} + b; \\
g & = k + r = t_{m+n+1} + b, \quad u = t_{m+n+1-1} + b.
\end{align*}
\]

On substituting for \( \alpha_k, \alpha_r \) and \( \alpha_u \) 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 \( \alpha_r(r = 2, \ldots, q-1) \) in terms of \( \alpha_0 \).

Next, let us consider the condition \( D_3 \). Since \( x^Q = 1 \mod q \), \( j_k, \ldots, j_k \) (where there are \( Q \) subscripts 0) and, since \( j_k \) and \( j_k \) are commutative, \( d_k \) in \( D_3 \) is equal to 1. Condition \( D_3 \) becomes

\[
\delta = \alpha_k(\theta_q^{-1})\alpha_k(\theta_q^{-2}) \cdots \alpha_k(\theta_q^{-q}) \quad (k = 1, 2, \ldots, q - 1).
\]

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

\[
\delta = \alpha(\theta_q^{-1})\alpha(\theta_q^{-2}) \cdots \alpha(\theta_q^{-q}) \delta(\theta_0).
\]

To prove this lemma by induction, we assume that (14) holds for all values of \( k \leq k \) and, writing \( \theta_0^k \) for \( i \) in (15), combine the equation thus obtained with (14). Since by [8] and (1)

\[
\delta(\theta_0^k) = \prod_{i=1}^{k} \alpha_k \delta(\theta_0^i) \delta(\theta_0^{i+1}).
\]

But by the general formula \( D_2 \) this becomes

\[
\delta(\theta_0^{k+1}) = \prod_{i=1}^{k} \alpha_{k+1} \delta(\theta_0^{i+1}) \frac{c_{k+1} \delta(\theta_0^{i+1})}{c_{k+1} \delta(\theta_0^{i+1})},
\]

(Since \( \Theta_0 = \Theta_{1, \ldots, q}, c_{k+1} \) is used to denote \( c_{k+1, \ldots, q} \), 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 \( c_{k+1} \delta(\theta_q^0) \) and \( c_{k+1} \delta(\theta_q^0) \), 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 \( \Theta_1 \) and \( \Theta_q \), such that \( \Theta_1 \) is of order \( q \) and \( \Theta_q \) transforms \( \Theta_1 \) into \( \Theta_1^q \) and \( \Theta_1^Q = \Theta_1^r \), while no lower than the \( Q \)th power of
\( \Theta_q \) is equal to a power of \( \Theta_1 \). 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

\[
\theta^r_i(\theta^r_1(i)) = \theta^r_0(\theta^r_1(i)) \quad \text{for} \quad r = 0, 1, \ldots, Q - 1 \quad (k = 0, 1, \ldots, q - 1),
\]

where \( \theta^r_0(i) = i, \theta^r_1(i) = \theta_1^r(i) \), and \( \theta_1 \) and \( \theta_q \) are rational functions of \( i \) with coefficients in \( F \). There exists an associative algebra \( \Sigma \) whose elements are

\[
A = f_0 + f_1j_1 + f_2j_2^2 + \cdots + f_{q-1}j_1^{q-1},
\]

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

\[
j_1^q = g(i) = g(\theta_1), \quad j_1^q = \phi(\theta_1^r(i))j_1^r \quad (r = 1, \ldots, q - 1),
\]

so that the product of any two elements of \( \Sigma \) is another element of \( \Sigma \). Let

\[
A' = f_0(\theta_0) + \sum_{k=1}^{q-1} f_k(\theta_0)\alpha_k j_k^s,
\]

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

**PART 2. ALGEBRAS \( \Gamma \) 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 \( \Theta_1 \) of order \( p \), and \( G_p \) is of index \( P \) under \( G_q \) and is extended to \( G_q \) by the substitution \( \Theta_s \). Further, let \( G_q \) be of index \( Q \) under \( G \) so that the \( Q \)th, but no lower than the \( Q \)th, power of \( \Theta_q \) is a substitution of \( G_q \). Then, if \( \Theta_q \) transforms \( \Theta_1 \) into \( \Theta_1^r \) and \( \Theta_p \) into \( \Theta_s^r \), while \( \Theta_p \) transforms \( \Theta_1 \) into \( \Theta_1^r \), we have

\[
\begin{align*}
\Theta_q^e \Theta_p^r &= \Theta_q^e \Theta_p^r \Theta_1^{{e}r}, & \Theta_q^r \Theta_p^e &= \Theta_q^r \Theta_p^e \Theta_1^{{e}r} \quad (e < p, e_1 < p, e_2 < P), \\
\Theta_p^r \Theta_q^e \Theta_p &= \Theta_q^e \Theta_1^{{e}r} \Theta_p^r, \\
\Theta_q^s \Theta_1 \Theta_q^e &= \Theta_1 \Theta_q^e, \\
\Theta_q^s \Theta_1 \Theta_q^e &= \Theta_1 \Theta_q^e.
\end{align*}
\]

where \( a, b \) and \( s \) are integers \( > 0 \).

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
It follows from §2 that the substitutions of $G_q$ are represented uniquely in the form $\Theta_\varepsilon=\Theta_0^a=\Theta_0^a\Theta_0^e (b < P, \ a < q)$ and if $q=P \varepsilon$ the substitutions of $G$ in the form $\Theta_{r_0}^a=\Theta_0^r\Theta_0^e (r < Q, \ k < q)$. As in §2 we see that

\begin{align}
(21) \quad x^p &= 1 \\
(22) \quad (x - 1)s &= 0
\end{align}

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

\begin{equation}
(23) \quad x^{**} = y^Q \quad (mod \ p).
\end{equation}

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

\begin{equation}
(24) \quad b(s^q - 1) = bmP, \ emb + e_1(x^q - 1) = 0 \quad (mod \ p)(b = 1, \cdots, P - 1).
\end{equation}

But (24) is satisfied if

\begin{equation}
(25) \quad s^q - 1 = mP, \ emb + e_1(x - 1) = 0 \quad (mod \ p)(m \ integer \ > 0).
\end{equation}

In addition the transforms of $\Theta_1^Q$ and $\Theta_2^Q\Theta_0^e$ by $\Theta_0$ must be equal and also the transforms of $\Theta_0^p$ and $\Theta_0$ by $\Theta_0$. Hence we have

\begin{equation}
(26) \quad e_1(x - 1) = nP, \ e(x - y) = 0 \quad (mod \ p)(n \ integer \ > 0).
\end{equation}

Finally, since

\begin{align}
\Theta_0^{-1}(\Theta_1^{-1}\Theta_1\Theta_0)\Theta_0 &= (\Theta_0^{-1}\Theta_1^{-1})\Theta_1(\Theta_0\Theta_0), \\
\Theta_1^v &= \Theta_1^{**},
\end{align}

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

\begin{equation}
(27) \quad x^{**} = 1 \quad (mod \ p).
\end{equation}

Other conditions to be satisfied by the parameters $c, \ e_1, \ e_2, \ x, \ y,$ 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 $k_0 \cdots 0 = a_0 \cdots 0 + b_0 \cdots 0 P$ where $a_0 \cdots 0 < p$ and $= a'y^t (mod \ p), \ b_0 \cdots 0 < P$ and $= bz^t (mod \ P)$ and there are $s$ subscripts 0. With these values of $k$ and $k_0$, the units and constants of multiplication of $\Gamma$ are given by formulas [49], [50] and [52], where $\varepsilon, \ e$ and $\beta$ are replaced by $Q, \ e'$ and $\delta$, respectively.

6. The algebra $\Sigma$. The subgroup $G_q$ being now of the type $G$ considered in §2, the algebra $\Sigma$, which by Theorem 1 may be regarded as an algebra of order $q^s$ over the field $F_1$, derived from $F$ by adjoining all the symmetric functions of $i, \ \theta(i), \cdots, \ \theta_{q-1}(i)$, is of the type $\Gamma$ considered in Part 1. If
we substitute $\phi, P, \beta$ and $\rho$ for $q, Q, \alpha$ and $\delta$ respectively, all the formulas of Part 1 hold. Hence $\Sigma$ is associative if, and only if,

$$g = g(\theta_1),$$
$$\rho = \rho(\theta_2)\beta,$$

(28)

$$\beta \beta(\theta_{s+2})\beta(\theta_{s+3}) \cdots \beta(\theta_{s+(p-1)})g^s = g(\theta_p),$$
$$\rho = \beta(\theta_p)\beta(\theta_{p+1})\beta(\theta_{p+2}) \cdots \beta_{s+p}(\theta_1).$$

By Theorem 10, if (28) holds, $\Gamma$ 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 $\Gamma$. Condition $D_1$ gives

(29)

$$\delta = \delta(\theta_e)\alpha_e, \quad (e' = e_1 + e_2p).$$

In the consideration of condition $D_2$, let

$$k = bP + a, \quad (a, t = 0, 1, \cdots, p - 1),$$
$$r = sP + t, \quad (b, s = 0, 1, \cdots, P - 1).$$

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

(30)

$$\alpha_s = \alpha_{s+t'p} = g^s\alpha(\theta_s^{e'}) \cdots \alpha(\theta_s^{(p-1)e'})$$

(a = 1, 2, \cdots, p - 1),

(31)

$$g(\theta_e) = \alpha\alpha(\theta_s^{e'}) \cdots \alpha(\theta_s^{(p-1)e'})g^e,$$

where $\gamma e = np + a_0$ and $(l_{n-1})y < np$, while $t_{n+1} > a \geq t_n$. *

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)

$$\alpha_{kp}\alpha_{rp}(\theta_{kp})\alpha_{kp,rp} = c_{kp,rp}(\theta_e)\alpha.$$
then \( r_{p_0} = d\theta + a_r + we \), where \( d = vz + a_n < P \). We now require to consider the value of \( c_{b_{p_0},r_{p_0}} \). Since

\[
j_{b_{p_0} j_{r_{p_0}}} = c_{b_{p_0},r_{p_0}} j_{u_0} = j_1^{\sigma a_+ w} j_{u_1}^{\sigma a_+ w} j_{f_{p_0}}^{d},
\]

then

(33) \( c_{b_{p_0},r_{p_0}} j_{u_0} = c_{b_{p,n}(\theta^{m*})} j_{f_{p}^{d+d^*}} j_{p} \),

where \( \sigma = a + a_r + (h+w)e \).

For, since

\[
(a_r + we)^x \equiv ne \pmod{p},
\]

and so by (22)

\[
ne^x \equiv ne \equiv a_r + we \pmod{p}.
\]

In (33), \( c_{b_{p,n}} \) denotes \( c_{b_{p},f} \), where \( ne = f \pmod{p} \) and \( f < p \), and later, to simplify the formulas, \( c_{b_{p+a},n+a} \) is often written for \( c_{kr} \), if \( \Theta_{\theta^*}^k = \Theta_{\theta^*} \) and \( \Theta_{\theta^*}^k = \Theta_r \), even when \( a \) and \( t \) are greater than \( p \), and \( b \) and \( s \) greater than \( P \). When \( b + d < P, j_{p}^{d+d^*} = j_{p}^{d+d} \), and from (33) we see that a factor \( g \) or \( g^2 \) occurs in \( c_{b_{p},r_{p}} \), according as \( \sigma + s \geq p \) or \( \geq 2p \); that is, according as \( m+n+1 \) is of the form \( f_{\mu+t+1} + t \) or \( f_{\mu+t+2} + t \). Hence the complete values of \( c_{b_{p},r_{p}} \) as obtained from (33) are given by

(34) \( c_{b_{p},r_{p}} = Xc_{b_{p},n}(\theta^{m*}) \)

where

\[
X = 1, \quad \text{if} \quad k + r = t_{m+n} + s, \quad m + n = f_{\mu+t} + t,
\]

\[
= g, \quad \text{if} \quad k + r = t_{m+n} + s, \quad m + n = f_{\mu+t+1} + t,
\]

\[
= \rho(\theta^t_{\mu+n+s}), \quad \text{if} \quad k + r = t_{m+n+1} + s, \quad m + n + 1 = f_{\mu+t} + t,
\]

\[
= \rho(\theta^t_{\mu+n+1})g, \quad \text{if} \quad k + r = t_{m+n+1} + s, \quad m + n + 1 = f_{\mu+t+1} + t,
\]

\[
= \rho(\theta^t_{\mu+n+1})g^2, \quad \text{if} \quad k + r = t_{m+n+1} + s, \quad m + n + 1 = f_{\mu+t+2} + t.
\]

Now, since \( j_{d^*} = \beta_j j_{f_{p}} \), we have

(35) \( c_{b_{p},n} = \beta_{n} \beta_{n}(\theta_{a}) \cdots \beta_{n}(\theta_{a}^{b-1}) \),
and by (10) and (11)

\[ \beta_{r+s} = \beta_s \beta_{r-1}(\theta_s^r) \quad (r \neq f_s), \]
\[ \beta_{r+s} = \frac{g}{g(\theta_p)} \beta_s \beta_{r-1}(\theta_s^r) \quad (r = f_s). \]

For \[ e \equiv e \pmod{p} \] and accordingly \( c_s(r-1)s = c_s(r-3)s. \)

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

\[ c_{bp, n} = \frac{G_n}{G_n(\theta_p^s)} \left( \frac{g}{g(\theta_p^s)} \right), \]

where \( G_n = \rho(\theta_s) \cdots \rho(\theta_s^{r-1}), \) and \( n = f_s + w. \)

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

\[ Y_{\alpha_p \alpha_p(\theta_p^s)} \frac{G_n}{G_n(\theta_p^s)} \left( \frac{g}{g(\theta_p^s)} \right) = \alpha_{(r+1)p}, \]

where

\[ Y = 1, \quad r \neq f_{n+1} - 1, \]
\[ = \rho(\theta_s^{r+n}), \quad r + 1 = f_{n+1}, \quad n + 1 \neq f_{n+1}, \]
\[ = \rho(\theta_s^{r+n}), \quad r + 1 = f_{n+1}, \quad n + 1 = f_{n+1}. \]

From successive applications of (38) we get*

\[ \alpha_{bp} = \alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{(r-1)s}) \rho(\theta_s) \cdots \rho(\theta_s^{r-1}) g^r, \]

where \( r = 1, 2, \cdots, P - 1; \ r = f_{n+1}; \ n = f_s + w. \)

By means of (34) and the formula \( \theta_p^{m+n} = \theta_p^n = \theta_{bp}, \) it can be shown that \( D_k \) is satisfied identically when the values of \( \alpha_{bp}, \alpha_{rp} \) and \( \alpha_a \) are substituted from (39) into (32), for all values of \( k \) and \( r \) for which \( k + r < P. \)

But, if \( k + r = P, \ c_{bp, rp} = \rho \) and \( u = e. \) Hence

\[ (k + r)z = Pz, \quad k + r = t_s, \]

and, since \( k + r \equiv 0 \pmod{P} \) \( (k \leq P - 1), z = m + n + 1. \) If

\[ z = f_\lambda + h \quad (a \lambda + he < p), \]

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

\[ \alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{(P-1)s}) \rho(\theta_s) \cdots \rho(\theta_s^{r-1}) g^\lambda = \rho(\theta_s) \alpha_s. \]

* If \( e = 0, v = 0 \) and \( \alpha_{rp} = \alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{(r-1)s}) \rho^v. \)
† If \( e = 0, \lambda = 0, \alpha_s = 1 \) and (41) becomes \( \alpha_p \alpha_p(\theta_p^s) \cdots \alpha_p(\theta_p^{(r-1)s}) \rho^v = \rho(\theta_s). \)
Similarly, if \( k+r>P \), \( D_t \) reduces to (41) for all values of \( k<P, r<P \). For, when \( k+r>P \), \( c_{b, r} = \rho \) and \( u = e+(k+r-P)\rho \). Now
\[
\alpha \alpha (k+r)_{b, (k+r-P)} = \alpha \alpha (k+r-P),
\]
and by (26) \( D_t \) becomes
\[
\alpha b \alpha (\theta ^{b}) c_{b, r} = \rho (\theta ^{b}) c_{a, (k+r-P)} s \alpha \alpha (k+r-P) \rho (\theta ^{b}),
\]
and, if
\[
k + r = t_o + a
\]
then
\[
s(k+r) = sP + a + as, \quad k + r - P = t_{s-o} + a.\]
Hence, if \( s = f_o + n \), where \( a + n e < P \), the left hand side of (42) is equal to
\[
\alpha \alpha (\theta ^{b}) \cdot \cdot \cdot \alpha \alpha (\theta ^{b})^{b} r \rho (\theta ^{b}) \cdot \cdot \cdot \rho (\theta ^{b})^{g}.\]
Then, if
\[
s = s = f_o + n'
\]
by (40)
\[
s = f_o + n''\text{ or } f_o + n''',\]
and so \( \sigma = \lambda + \mu \) or \( \lambda + \mu + 1 \), according as \( c_{a, (k+r-P)} \) is 1 or \( g \). The right hand side of (42) then becomes
\[
\rho (\theta ^{b}) \alpha \alpha (\theta ^{b})^{b} \rho (\theta ^{b})^{b+1} \cdot \cdot \cdot \alpha \alpha (\theta ^{b}) \rho (\theta ^{b})^{g}.\]
where
\[
X = \rho (\theta ^{b}) \rho (\theta ^{b+1}) \cdot \cdot \cdot \rho (\theta ^{b+1}) g^{e-l}.\]
On equating the two sides so obtained and cancelling the common factors, we get (41).

We must now consider the general case of \( D_t \), where
\[
k = a + b \rho \quad (a, t = 1, 2, \ldots, p - 1)\]
\[
r = t + s \rho \quad (b, s = 1, 2, \ldots, P - 1).\]
For simplicity in writing let
\[
j \cdot k' \text{ be defined as } j_o \text{ when } \Theta ^{t} = \Theta _a \text{ and } a' > \rho > a,
j \cdot b' \text{ be defined as } j_{b' + d} \text{ when } \Theta ^{b'} = \Theta _{b' + d} \text{ and } b' > P > b.\]
Then
\[
j \cdot k' j' = c_{b_{1}l}^{a} j'o^{j} j'_{i} j'_{i},
\]
\[
j \cdot k' j_o = c_{b_{1}l}^{a} c_{a} l j_{o} c_{b_{1}l}^{d} j_{o}.
\]
Hence

\( c_{kr} = c_{k, \theta^*} c_{\alpha_1, \ldots, \alpha_p} c_{\beta_1, \ldots, \beta_p} c_{\nu, \mu} \)  

To get the value of \( c_{k, \nu} \), we consider:

\( j_1^t j_2^w j_3^x j_4^y j_5^z \)

which is equal to

\( c_{ay, bsp} j_1^t j_2^w j_3^x j_4^y = c_{ay, bsp} c_{\nu, \mu} c_{\theta, \alpha} c_{\beta, \beta} j_5^z j_6^w \)

Since \( j_{bp} \), may be of the form \( j_1^t j_2^w \), we have

\( c_{ay, bsp} j_1^t j_2^w j_3^x j_4^y = c_{ay, bsp} c_{\nu, \mu} c_{\theta, \alpha} c_{\beta, \beta} j_5^z j_6^w \),

or, since \( x^2 = x \pmod{p} \),

\( c_{ay, bsp} j_1^t j_2^w j_3^x j_4^y = c_{ay, bsp} c_{\nu, \mu} c_{\theta, \alpha} c_{\beta, \beta} j_5^z j_6^w \).

Hence

\( c_{ay, bsp} (\theta^*)^t j_1^t j_2^w j_3^x j_4^y j_5^z \)

\( = c_{ay, bsp} (\theta^*)^t c_{ay, bsp} c_{\nu, \mu} c_{\theta, \alpha} c_{\beta, \beta} j_5^z j_6^w \),

where

\( j_1^t j_2^w = c_{ay, bsp} j_5^z \),

\( j_5^z j_6^w = c_{ay, bsp} j_6^z \).

We get as special cases of \( D_3 \),

\( \alpha_0 \alpha_0 (\theta_0) c_{\nu, \mu} = c_{\nu, \mu} (\theta_0) \alpha_0 \),

\( \alpha_0 \alpha_1 (\theta_0) c_{ay, bsp} = c_{ay, bsp} (\theta_0) \alpha_0 \),

\( \alpha_0 \alpha_p (\theta_0) c_{ay, bsp} = c_{ay, bsp} (\theta_0) \alpha_0 \),

and

\( \alpha_0 = \alpha_0 + \beta_p = \alpha_0 \alpha_p (\theta_0) c_{ay, bsp} \)

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

where (48) combined with (30) and (39) defines \( \alpha_0 \) in terms of \( \alpha \) and \( \alpha_p \), and \( c_{ay, bsp} = 1 \) or \( g \) according as \( a + b < p \) or \( \geq p \), where

\( ay = mp + a_m \ (a_m < p), \ bx = sP + b_s \ (b_s < P), \ se = \mu p + s_p \ (s_p < p) \).
Making use of (47) and (48), and substituting for $c_b$ and $c_{b^1}$ their values obtained from (44), (45) and (46) in $D_2$, we get

\[(49) \quad \alpha_{b^1} \alpha_{t^1} (\theta_b^1) c_{b^p, t^p} = c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) \alpha_{t^1} \alpha_{b^1} (\theta_b^1).\]

The $w$ in the first of (47) may be of the form $t + s^p$ 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

\[(50) \quad \alpha_{b^1} \alpha_{t^1} (\theta_b^1) c_{b^p, t^p} = c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) \alpha_{t^1} \alpha_{b^1} (\theta_b^1).\]

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

\[(51) \quad \alpha_{b^1} \alpha_{t^1} (\theta_b^1) c_{b^p, t^p} = c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) \alpha_{t^1} \alpha_{b^1} (\theta_b^1).\]

If we now write $\theta_i^1$ 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

\[(52) \quad \alpha_{b^1} \alpha_{t^1} (\theta_b^1) c_{b^p, t^p} c_{b^p, t^p} (\theta_t^1) c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) = Y \alpha_{t^1} \alpha_{b^1} (\theta_b^1)\]

where

\[Y = C_{t^1, b^1} (\theta_b^1) c_{b^p, t^p} (\theta_t^1) c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) c_{b^1, t^1} (\theta_b^1).\]

Now,

\[C_{t^1, b^1} (\theta_b^1) c_{b^p, t^p} (\theta_t^1) c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) = C_{b^p, t^1} c_{b^p, t^1} (\theta_t^1) c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) c_{b^1, t^1} (\theta_b^1),\]

and

\[C_{b^p, t^1} = C_{b^p, t^1} (\theta_t^1) c_{b^p, t^1} c_{t^1, b^1} (\theta_b^1).\]

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

\[(53) \quad \alpha_{b^1} \alpha_{x^1} (\theta_b^1) c_{b^p, x^p} = c_{t^1, b^1} c_{b^1, t^1} (\theta_t^1) T,\]

where

\[T = \alpha_{t^1} \alpha_{b^1} (\theta_b^1).\]
Since
\[ c_{(b+1)p,1} = c_{p,1}(\theta p^b)c_{b,p,a} \]
and
\[
\begin{align*}
&c_{b+1,p,s} c_{(b+1)s,p,1} c_{y,s} c_{y,(b+1)s,p,1} \\
&= c_{s,p,1}(\theta p^b)c_{b+1,p,s} c_{b,p,s} c_{(b+1)s,p,1} c_{(b+1)s,p,1}
\end{align*}
\]
when we combine (53) with (50), where \( \theta^6 \) is written for \( i \) in (50), we get (49) with \( b \) replaced by \( b+1 \) and our lemma is proved. Since \( z<P, c_{y,sp}=1 \) and (50) becomes
\[
\alpha_p \alpha(\theta p^b)c_{sp,1} = c_{p,1}(\theta p^b)\alpha \alpha(\theta p^b),
\]
where
\[
c_{p,1} = \beta, c_{sp,1} = \beta^0(\theta p^{-1})\beta^1(\theta p^{-2}) \cdots \beta^{y-1}.
\]

We have now shown that the condition \( D_3 \) 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 \( \alpha \) and \( \alpha_p \).

It remains to consider the condition \( D_3 \). If \( j=\delta j_k = d_{jk}j_k \), where \( j_k = j_{k+1} \), and there are \( Q \) subscripts 0, \( k = a+b_1 \), where \( a = ay(\bmod p) \) by (26), and \( b_1 = b_1^{Q-1} = b_1^{Q-1} \), and accordingly
\[
\begin{align*}
\delta_{j_k} &= \delta_{j_k} \delta_{j_k} \\
\delta_{j_k} &= \delta_{j_k} \delta_{j_k} \\
\delta_{j_k} &= \delta_{j_k} \delta_{j_k} \\
\delta_{j_k} &= \delta_{j_k} \delta_{j_k} \\
\delta_{j_k} &= \delta_{j_k} \delta_{j_k} \\
\delta_{j_k} &= \delta_{j_k} \delta_{j_k}
\end{align*}
\]

Also \( c_{j_k} = d_k c_{j_k} \) and \( c_{j_k} \) becomes
\[
\begin{align*}
c{j_k} &= e_{j_k} \alpha (\theta q^{Q-1}) \alpha (\theta q^{Q-2}) \cdots \alpha (\theta q^{Q-1}) \\
c{j_k} &= e_{j_k} \alpha (\theta q^{Q-1}) \alpha (\theta q^{Q-2}) \cdots \alpha (\theta q^{Q-1})
\end{align*}
\]

We shall now prove the following lemma:

**Lemma B.** Condition \( D_3 \) follows for all values of \( k<q \) from (56) and (57):
\[
\begin{align*}
&c_{j_k} = c_{j_k} (\theta q^{Q-1}) \alpha (\theta q^{Q-2}) \cdots \alpha (\theta q^{Q-1}) \\
&c_{j_k} = c_{j_k} (\theta q^{Q-1}) \alpha (\theta q^{Q-2}) \cdots \alpha (\theta q^{Q-1})
\end{align*}
\]

Since (55) holds for all values of \( k<q \), it is true in particular for the two cases \( b=0 \) and \( a=0 \) respectively:
\[
\begin{align*}
&c_{j_k} = c_{j_k} (\theta q^{Q-1}) \alpha (\theta q^{Q-2}) \cdots \alpha (\theta q^{Q-1}) \\
&c_{j_k} = c_{j_k} (\theta q^{Q-1}) \alpha (\theta q^{Q-2}) \cdots \alpha (\theta q^{Q-1})
\end{align*}
\]

If we write
\[
\gamma \gamma Q = \gamma \gamma Q
\]
for $i$ in (59), since
\[ \theta_i^a = \theta_i^{a-1}, \]
we have from (58) and (59)
\[ c_{o',o',b_p(a^{m})} \delta = c_{a,m},o'o'c_{b',p',o'}(\theta_{o'})^\delta(\theta_{b'}^{a+m})^X, \]
where
\[ X = \prod_{i=1}^{m} \frac{\alpha_{a_{i-1}+b_{i-1}p}(\theta_{b'^{i}}^a)}{\alpha_{a_{i},b_p}(\theta_{b'^{i}}^a)}. \]

Now, since $m b + e_i (x^b - 1) \equiv 0 \pmod{p}$ by (24),
\[ f_p^{j_i} = j_p^{m} j_p^{j_i} = f_j^{j_i} f_p^{j_i} = f_j^{j_i} f_p^{j_i} \quad (f \neq 0 \text{ and in } F(i)). \]
Hence,
\[ j_p^{m} j_i j_i = c_{a,m,b_p} c_{b,p} j_i. \]
From this result remembering that $a x^n = a y^d \pmod{p}$ and that $\Theta^{n} = \Theta^{d}$, 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
\[ c_{o',o',b_p}(a^{m},o')c_{a,m} = c_{o',o',b_p}(a^{m},o'), \]
which can be deduced as in the previous cases. Since
\[ c_{o',o',b_p}(a^{m},o')c_{a,m} = c_{o',o',b_p}(a^{m},o'), \]
(56) becomes
\[ c_{a,m} = c_{a,m} = c_{a,m} = c_{a,m}, \]
(61) becomes
\[ c_{a,m}(\theta_{o'}) = \alpha(\theta_{a}^{1-m}) \alpha_{a}^{1-m} \alpha_{a}^{1-m} \alpha_{a}^{1-m} \alpha_{a}^{1-m}. \]
But $e_a = P - 1$ by (26) and so $c_{o',p} = 1$ and (57) becomes
\[ d = c_{a,d}^e = c_{a,d}^e = c_{a,d}^e. \]
In (61)
\[ c_{mp,1} = \beta(\theta_p^{-1})\beta(\theta_p^{-2}) \beta(\theta_p^{-3}) \cdots \beta(\theta_p^{-n}), \]
and in (62), since \( e = mP + 1 \),
\[ c_{mp,m'} = \beta(\theta_e^{-m'})c_{m',q}, \]
where \( c_{m',q} = 1 \) or \( g \), according as \( t \leq e_1 \) or \( > e_1 \) and \( e_1 x \equiv t \pmod{p} \).

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 \( \Theta_1, \Theta_p \) and \( \Theta_q \) described in §5. Then the algebra \( \Sigma \) is associative if and only if conditions (28) hold. The totality of polynomials in \( \Sigma \) with coefficients in \( \Sigma \) form an algebra \( \Gamma \) of order \( n^3 \) over \( F \) which is associative if and only if conditions (29), (31), (41), (54), (61), and (62) all hold and \( \Sigma \) is associative.

**University of Chicago,**

**Chicago, ILL.**