A FUNDAMENTAL SYSTEM OF INVARIANTS OF THE GENERAL MODULAR LINEAR GROUP WITH A SOLUTION OF THE FORM PROBLEM*

BY

LEONARD EUGENE DICKSON

1. We shall determine m functions which form a fundamental system of invariants for the group G_m of all linear homogeneous transformations on m variables with coefficients in the Galois field of order p^n. In the so-called form problem for the group G_m, we seek all sets of values of the m variables for which the m fundamental absolute invariants take assigned values. It is shown in § 8 that all sets of solutions are linear combinations of the roots of an equation involving only the powers $p^{nm}, p^{n(m-1)}, \cdots, p^n, 1$ of a single variable. This fundamental equation has properties analogous to those of a linear differential equation of the m-th order. In §§ 10–16 we determine the degrees of the irreducible factors of the fundamental equation and, in particular, the smallest field in which it is completely solvable. We obtain a wide generalization of the theory of the equation $\xi^{p^{nm}} - \xi = 0$, which forms the basis of the theory of finite fields. The function defined by the left member of the fundamental equation includes the type of substitution quantics in one variable the theory of which is equivalent to, but preceded historically, the theory of linear modular substitutions on m variables. We here find that the latter theory necessitates a return to the earlier quantics in one variable. Finally, in §§ 17–22, we consider the interpretation of certain invariants.

It follows from the theorem concerning the product of two determinants that a transformation T of G_m replaces the function

$$[e_1, \cdots, e_m] = \begin{vmatrix} x_1^{p^{e_1 n}} & x_2^{p^{e_1 n}} & \cdots & x_m^{p^{e_1 n}} \\ x_1^{p^{e_2 n}} & x_2^{p^{e_2 n}} & \cdots & x_m^{p^{e_2 n}} \\ \cdot & \cdot & \cdot & \cdot \\ x_1^{p^{e_m n}} & x_2^{p^{e_m n}} & \cdots & x_m^{p^{e_m n}} \end{vmatrix}$$

by one which equals $|T|$ times the initial function. By § 2, each of these functions has the factor

$$L_m = [m-1, m-2, \cdots, 1, 0].$$

* Presented to the Society, September 6, 1910.

Certain of the quotients will be given a special notation:

$$Q_{ms} = [m, m-1, \cdots, s+1, s-1, \cdots, 1, 0]/L_m.$$

They are absolute invariants of G_m. We shall prove the

Theorem. *The m invariants L_m, Q_{m1}, $\cdots$, $Q_{m\,m-1}$ are independent and form a fundamental system of invariants of the group G_m.*

2. Consider the product P of all the linear functions

$$a_1 x_1 + a_2 x_2 + \cdots + a_m x_m$$

in which the a_i are elements not all zero of the $GF[p^n]$ and such that, of the coefficients a_i not zero, the one with smallest subscript is unity:

$$P = \prod_{k=1}^{m} \prod_{a} (x_k + a_{k+1} x_{k+1} + \cdots + a_m x_m),$$

where the inner product extends over the $p^{n(m-k)}$ sets $a_{k+1}, \cdots, a_m$ of $m-k$ elements of the field. Hence the term

$$\prod_{k=1}^{m} x_k^{p^{n(m-k)}} = x_1^{p^{n(m-1)}} \cdots x_{m-1}^{p^n} x_m$$

occurs once and but once in the expansion of P and has the coefficient unity. This term is the product of the elements in the main diagonal of the determinant L_m. Since L_m is invariant * under G_m and has the factor x_1, it follows that L_m is identical † with the product P.

Similarly, $[e_1, \cdots, e_m]$ has the factor L_m.

Theory of Ternary Invariants.

3. In the adjoint determinant of the nine first minors of

$$L_3 = (x^{p^{2n}} y^{p^n} z),$$

consider the three determinants formed of the elements in the first and third columns:

$$\begin{vmatrix} (y^{p^n} z) & (x^{p^n} y) \\ (y^{p^{2n}} z^{p^n}) & (x^{p^{2n}} y^{p^n}) \end{vmatrix}, \qquad \begin{vmatrix} (y^{p^{2n}} z) & (x^{p^{2n}} y) \\ (y^{p^{2n}} z^{p^n}) & (x^{p^{2n}} y^{p^n}) \end{vmatrix}, \qquad \begin{vmatrix} (y^{p^n} z) & (x^{p^n} y) \\ (y^{p^{2n}} z) & (x^{p^{2n}} y) \end{vmatrix}.$$

They equal $y^{p^n} L_3$, $y^{p^{2n}} L_3$, $y L_3$, respectively. Hence $L_3^{p^n-1}$ times the first determinant equals the p^n-th power of the third. Transposing the negative terms

* This fact appears to have been first noted by the writer. See his *Linear Groups*, p. 216.

† This theorem is due to Professor E. H. MOORE, Bulletin of the American Mathematical Society, vol. 2 (1896), p. 189. His three proofs differ from the above invariantive proof. His sequence of variables is the reverse of that employed here.

and dividing by $(x^{p^{2n}}y^{p^n})(y^{p^{2n}}z^{p^n})$, we get

$$\frac{(y^{p^n}z)L_3^{p^n-1}+(y^{p^{3n}}z^{p^n})}{(y^{p^{2n}}z^{p^n})}=\frac{(x^{p^n}y)L_3^{p^n-1}+(x^{p^{3n}}y^{p^n})}{(x^{p^{2n}}y^{p^n})}.$$

The second member is invariant under G_2 (§ 1) and is replaced by the first member by the transformation $x'=z$, $z'=-x$, which extends G_2 to G_3. Hence the second member is an invariant of G_3.

Similarly, from the first and second determinants, we get

$$\frac{(x^{p^{2n}}y)L_3^{p^n-1}+(x^{p^{3n}}y^{p^{2n}})}{(x^{p^{2n}}y^{p^n})}=\frac{(y^{p^{2n}}z)L_3^{p^n-1}+(y^{p^{3n}}z^{p^{2n}})}{(y^{p^{2n}}z^{p^n})},$$

so that the first member is an invariant of G_3.

If we employ the following integral invariants of G_2,

$$(1)\qquad L_2=(x^{p^n}y),\qquad Q_{21}=\frac{(x^{p^{2n}}y)}{L_2}=\frac{x^{p^{2n}-1}-y^{p^{2n}-1}}{x^{p^n-1}-y^{p^n-1}},$$

we may express our ternary invariants in the form

$$(2)\qquad L_3,\qquad Q_{32}=\left(\frac{L_3}{L_2}\right)^{p^n-1}+Q_{21}^{p^n},\qquad Q_{31}=Q_{21}\left(\frac{L_3}{L_2}\right)^{p^n-1}+L_2^{p^{2n}-p^n},$$

the identification of the last two with the quotients Q_{3i} (§ 1) being made in § 4. The fact that L_3 is divisible by L_2 follows from § 2; the quotient may be obtained from the expansion

$$(3)\qquad L_3=z^{p^{2n}}L_2-z^{p^n}L_2Q_{21}+zL_2^{p^n}.$$

We proceed to the proof that the three invariants (2) form a fundamental system. Let I be any homogeneous ternary invariant and let I_0 be the sum of the terms of I which lack z. Then I_0 and the coefficients of the various powers of z in I are invariants of the binary group G_2 on x, y, and hence* are integral functions of the invariants (1).

Let $cL_2^aQ_{21}^b$ be the term of I_0 in which a is a minimum. Then the term of I_0 of minimum degree in y is cx^ey^a, where

$$e=ap^n+bd,\qquad d=p^{2n}-p^n.$$

Since x^ey^a does not occur elsewhere in I_0, cx^ey^a and therefore also cz^ey^a is a term of I. Hence cy^a is a term of an invariant of G_2 and hence a term of kQ_{21}^a. Thus $a=\alpha d$.

Let $c'L_2^{a'}Q_{21}^{b'}$ be any term of I_0. By the homogeneity of I_0,

$$(a'-a)(p^n+1)+(b'-b)d=0.$$

Hence a' is divisible by p^n. We next show that a' is divisible by p^n-1, so that a' is divisible by $d=p^n(p^n-1)$.

* DICKSON, these Transactions, this volume, p. 1.

Apply to I_0 a transformation of determinant ρ, where ρ is a primitive root of the $GF[p^n]$. Since Q_{21} is an absolute invariant and L_2 takes the factor ρ (§ 1), it follows that $\rho^{a'} = \rho^a$, whence $a' \equiv a \pmod{p^n - 1}$. But a is divisible by d. Hence a' is divisible by $p^n - 1$.

Let $b = p^\beta B$, where B is prime to p. Let $f = p^\beta(p^n - 1)$. Then

$$Q_{21} = x^d + x^{d-p^n+1}y^{p^n-1} + \cdots, \qquad Q_{21}^{p^\beta} = x^{dp^\beta} + x^{dp^\beta - f}y^f + \cdots,$$

$$Q_{21}^b = x^{bd} + Bx^{bd-f}y^f + \cdots,$$

$$L_2^a = (x^{p^{2n}}y^{p^n} - x^{p^n}y^{p^{2n}})^{a(p^n-1)} = x^{ap^n}y^a + ax^{ap^n-d}y^{a+d} + \cdots.$$

Suppose that $\beta < n$. Then $f < d$ and

$$L_2^a Q_{21}^b = x^{\mu+f}y^a + Bx^\mu y^{a+f} + \cdots \qquad (\mu = ap^n + bd - f).$$

Neither of these terms occurs in another term $c' L_2^{a'} Q_{21}^{b'}$, for which therefore $a' > a$. In fact, $a' \geqq a + d > a + f$. Hence I contains the term $cBz^\mu y^{a+f}$. But $a + f$ is not a multiple of d and B is not zero in the field. Hence $\beta \geqq n$ and b is of the form $p^n b_1$. Hence by (2),

$$I' = I - cQ_{31}^a Q_{32}^{b_1}$$

is an invariant in which I'_0 lacks $cL_2^a Q_{21}^b$.

We can similarly delete one after another of the terms free of z and reach ultimately an invariant I_1 in which there are no terms free of z. Since I_1 has the factor z, it has the factor L_3. Thus $I_1 = L_3^e I_2$, where I_2 is either a constant or else is a function having terms free of z. In the latter case we repeat the above process on I_2. It follows that *any integral invariant of G_3 is an integral function of the three invariants* (2).

4. For $m = 3$, the invariants Q_{ms} of § 1 are

$$Q_{32} = (x^{p^{3n}}y^{p^n}z)/L_3, \qquad Q_{31} = (x^{p^{3n}}y^{p^{2n}}z)/L_3.$$

Their degrees $p^{3n} - p^{2n}$ and $p^{3n} - p^n$ equal the degrees of the second and third invariants (2), respectively. Hence by the theorem of § 4 the corresponding invariants differ only by a constant factor. We now prove that the factor is unity in each case.

The terms free of z in the quotient Q_{3i} are given by the quotient of the coefficient of z in the numerator by the coefficient of z in the denominator L_3. For $i = 2, 1$, we get respectively

$$(x^{p^{3n}}y^{p^n})/(x^{p^{2n}}y^{p^n}) = Q_{21}^{p^n}, \qquad (x^{p^{3n}}y^{p^{2n}})/(x^{p^{2n}}y^{p^n}) = L_2^{p^{2n}-p^n}.$$

Hence the relations (2) are proved. For another proof by means of a vanishing determinant of the fifth order, see § 6.

Expressions for the Quotients Q_{ms}.

5. The process which led so naturally to invariants (2) can be readily applied also when $m > 3$. For example, if $m = 4$,

$$\begin{vmatrix} (x^{p^{2n}} y^{p^n} w) & (x^{p^{2n}} y^{p^n} z) \\ (x^{p^{3n}} y^{p^n} w) & (x^{p^{3n}} y^{p^n} z) \end{vmatrix} = L_4 \begin{vmatrix} x^{p^n} & y^{p^n} \\ x & y \end{vmatrix},$$

$$\begin{vmatrix} (x^{p^{2n}} y^{p^n} w) & (x^{p^{2n}} y^{p^n} z) \\ (x^{p^{3n}} y^{p^{2n}} w^{p^n}) & (x^{p^{3n}} y^{p^{2n}} z^{p^n}) \end{vmatrix} = L_4 \begin{vmatrix} x^{p^{2n}} & y^{p^{2n}} \\ x^{p^n} & y^{p^n} \end{vmatrix}.$$

Equating the p^n-th power of the upper to $L_4^{p^n-1}$ times the lower, transposing the negative terms, and dividing by $(x^{p^{3n}} y^{p^{2n}} w^{p^n})(x^{p^{3n}} y^{p^{2n}} z^{p^n})$, we get

$$\frac{(x^{p^{2n}} y^{p^n} z) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{2n}} z^{p^n})}{(x^{p^{3n}} y^{p^{2n}} z^{p^n})} = \frac{(x^{p^{2n}} y^{p^n} w) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{2n}} w^{p^n})}{(x^{p^{3n}} y^{p^{2n}} w^{p^n})}.$$

It follows that the left member is an invariant of G_4 (later identified with Q_{43}). We are led in a similar manner to the invariants

$$\frac{(x^{p^{3n}} y^{p^n} z) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{3n}} z^{p^n})}{(x^{p^{3n}} y^{p^{2n}} z^{p^n})}, \qquad \frac{(x^{p^{3n}} y^{p^{2n}} z) L_4^{p^n-1} + (x^{p^{4n}} y^{p^{3n}} z^{p^{2n}})}{(x^{p^{3n}} y^{p^{2n}} z^{p^n})},$$

which will be identified with Q_{42} and Q_{41}, respectively.

6. For general m, we obtain the desired expressions for Q_{ms} by means of the following determinant, which vanishes identically:

$$D_s = \begin{vmatrix} A & A' \\ O & B \end{vmatrix},$$

where O is a matrix of $m - 2$ rows and m columns all of whose elements are zero, A' is derived from A by deleting the last column, and*

$$A = \begin{vmatrix} x_1^{p^{nm}} & \cdots & x_m^{p^{nm}} \\ x_1^{p^{n(m-1)}} & \cdots & x_m^{p^{n(m-1)}} \\ \cdot & \cdots & \cdot \\ x_1^{p^n} & \cdots & x_m^{p^n} \\ x_1 & \cdots & x_m \end{vmatrix}, \qquad B = \begin{vmatrix} x_1^{p^{n(m-1)}} & \cdots & x_{m-1}^{p^{n(m-1)}} \\ \cdot & \cdots & \cdot \\ x_1^{p^{n(s+1)}} & \cdots & x_{m-1}^{p^{n(s+1)}} \\ x_1^{p^{n(s-1)}} & \cdots & x_{m-1}^{p^{n(s-1)}} \\ \cdot & \cdots & \cdot \\ x_1^{p^n} & \cdots & x_{m-1}^{p^n} \end{vmatrix}.$$

By Laplace's development of D_s we get

$$\begin{aligned}(-1)^{m-2}[m, \cdots, 1][m-1, \cdots, s+1, s-1, \cdots, 1, 0] \\ + (-1)^s(-1)^{m-s-1}[m, \cdots, s+1, s-1, \cdots, 0][m-1, \cdots, 1] \\ + (-1)^m[m-1, \cdots, 0][m, \cdots, s+1, s-1, \cdots, 1] = 0.\end{aligned}$$

* If $s = 1$, the exponents in the last row of B are p^{2n}; if $s = m - 1$, the exponents in the first row are $p^{n(m-2)}$.

Let the factor $(-1)^m$ be removed. For $1 < s < m-1$, we get

$$L_m^{p^n} \cdot Q_{m-1\,s} L_{m-1} - Q_{ms} L_m \cdot L_{m-1}^{p^n} + L_m (Q_{m-1\,s-1} L_{m-1})^{p^n} = 0,$$

$$(4) \qquad Q_{ms} = Q_{m-1\,s} \left(\frac{L_m}{L_{m-1}} \right)^{p^n-1} + Q_{m-1\,s-1}^{p^n} \qquad (1<s<m-1).$$

For $s=1$ and $s=m-1$, we obtain respectively

$$L_m^{p^n} \cdot Q_{m-1\,1} L_{m-1} - Q_{m1} L_m \cdot L_{m-1}^{p^n} + L_m \cdot L_{m-1}^{p^{2n}} = 0,$$

$$L_m^{p^n} \cdot L_{m-1} - Q_{m\,m-1} L_m \cdot L_{m-1}^{p^n} + L_m (Q_{m-1\,m-2} L_{m-1})^{p^n} = 0,$$

$$(5) \quad Q_{m1} = Q_{m-1\,1} \left(\frac{L_m}{L_{m-1}} \right)^{p^n-1} + L_{m-1}^{p^{2n}-p^n}, \qquad Q_{m\,m-1} = \left(\frac{L_m}{L_{m-1}} \right)^{p^n-1} + Q_{m-1\,m-2}^{p^n}.$$

As a check, we observe that the terms free of x_m, namely the final terms in (4) and (5), equal the quotient of the coefficients of z in the numerator and denominator of Q_{mi}. We note that

$$(6) \quad p^{nm} - p^{ns} = \text{degree of } Q_{ms}, \qquad p^{n(m-1)} + \cdots + p^n + 1 = \text{degree of } L_m.$$

Expanding L_m according to the last column and introducing the Q_{ms} of § 1, we get

$$(7) \quad L_m = x_m L_{m-1}^{p^n} + L_{m-1} \sum_{s=1}^{m-2} (-1)^s x_m^{p^{ns}} Q_{m-1\,s} + (-1)^{m-1} x_m^{p^{n(m-1)}} L_{m-1}.$$

Hence (4) and (5) may be given an integral form.

Fundamental System of Invariants of G_m.

7. **Theorem.** *The functions L_μ, $Q_{\mu 1}, \cdots, Q_{\mu\,\mu-1}$ are independent and form a fundamental system of invariants for G_μ.*

We assume that the theorem is true for $\mu \leqq m$, where $m \geqq 2$, and prove that it is true for $\mu = m+1$.

Let I be any homogeneous integral invariant of G_{m+1}. The coefficients of the various powers of x_{m+1} in I are invariants of G_m and hence by hypothesis are integral functions of L_m, $Q_{m1}, \cdots, Q_{m\,m-1}$. In particular, the sum I_0 of the terms of I free of x_{m+1} is an aggregate of terms

$$t' = c' L_m^{a'} Q_{m1}^{b'_1} \cdots Q_{m\,m-1}^{b'_{m-1}} \qquad (c' \neq 0).$$

Consider the set of terms t' in which a' has the minimum value a, the subset in which b'_1 has the minimum value b_1, etc. In the resulting unique term

$$t = c L_m^a Q_{m1}^{b_1} \cdots Q_{m\,m-1}^{b_{m-1}},$$

the term of minimum degree in x_m is, by (4), (5), (7), $x_m^a t_1$, where

$$t_1 = c L_{m-1}^{a_1} \prod_{s=2}^{m-1} Q_{m-1\,s-1}^{p^n b_s} \qquad (a_1 = ap^n + b_1 d).$$

Similarly, the term of t_1 of minimum degree in x_{m-1} is $x_{m-1}^{a_1} t_2$,

$$t_2 = cL_{m-2}^{a_1} \prod_{s=3}^{m-1} Q_{m-2\,s-2}^{p^{2n}b_s} \qquad (a_2 = a_1 p^n + p^n b_2 d).$$

Proceeding in this manner, we see that t contains a term

$$\tau = cx_m^a x_{m-1}^{a_1} x_{m-2}^{a_2} \cdots x_{m-i}^{a_i} \cdots x_1^{a_{m-1}} \quad (a_i = a_{i-1} p^n + p^{n(i-1)} b_i d),$$

where $a_0 = a$. Evidently τ occurs but once in the product t. Further, τ does not occur in a product t' distinct from t. For, if so, $a' = a$ and hence (by a_1) $b_1' = b_1$, then (by a_2) $b_2' = b_2$, etc., so that $t' \equiv t$. Hence I has the isolated term τ and therefore also

$$x_{m+1}^{a_1} \tau_1, \qquad \tau_1 \equiv cx_{m-1}^a x_{m-2}^{a_2} \cdots x_1^{a_{m-1}}.$$

Hence τ_1 is a term of an invariant of G_m. The latter invariant has the term

$$x_m^{a_2} \tau_2, \qquad \tau_2 \equiv cx_{m-2}^a x_{m-3}^{a_3} \cdots x_1^{a_{m-1}}.$$

Hence τ_2 is a term of an invariant of G_{m-1}. Proceeding in this manner, we see that $\tau_m = cx_1^a$ is a term of an invariant of G_2. Hence cx_1^a is a term of kQ_{21}^a, whence $a = \alpha d$.

By (6_1) the degree of Q_{ms} is a multiple of p^n. Since a is a multiple of p^n, it follows that t is of degree a multiple of p^n. Since this is therefore true of t, and since the degree of L_m is prime to p, by (6_2), it follows that a' is a multiple of p^n. As in § 3, a' is a multiple of $p^n - 1$. Hence *in every term t' of I_0, a' is a multiple of $d = p^n(p^n - 1)$.*

By (4), (5), (7), we have

$$Q_{m1} = L_{m-1}^d + x_m^r L_{m-1}^{r^2} Q_{m-1\,1} + \cdots, \qquad Q_{ms} = Q_{m-1\,s-1}^{pn} + x_m^r L_{m-1}^{r^2} Q_{m-1\,s} + \cdots \quad (s > 1),$$

the final Q being suppressed if $s = m - 1$. In these series the exponents of x_m differ by multiples of $r = p^n - 1$. Let $b_s = p^{\beta_s} B_s$, where B_s is prime to p. To obtain the power p^β of a sum in a field having modulus p, we have only to multiply every exponent by p^β. Hence we get

$$(8) \qquad L_m^a = (L_m^{vn})^{\alpha r} = x_m^a L_{m-1}^{ap^n} - \alpha r x_m^{a+d} L_{m-1}^{ap^n - d} Q_{m-1\,1}^{p^n} + \cdots,$$

$$(9) \qquad Q_{m1}^{b_1} = L_{m-1}^{db_1} + B_1 x_m^{rp^{\beta_1}} L_{m-1}^{e} Q_{m-1\,1}^{p^{\beta_1}} + \cdots \qquad (e = db_1 - rp^{\beta_1}),$$

$$(10) \qquad Q_{ms}^{b_s} = Q_{m-1\,s-1}^{p^n b_s} + B_s x_m^{rp^{\beta_s}} L_{m-1}^{r^2 p^{\beta_s}} Q_{m-1\,s-1}^{e_s} Q_{m-1\,s}^{p^{\beta_s}} + \cdots \quad (e_s = b_s p^n - p^{n+\beta_s}),$$

where in the last series $s > 1$ and the term $Q_{m-1\,s}$ is to be suppressed if $s = m - 1$. Hence t/c contains the terms

$$T_1 = B_1 x_m^{a + rp^{\beta_1}} L_{m-1}^{e + ap^n} Q_{m-1\,1}^{p^{\beta_1}} \prod_{s=2}^{m-1} Q_{m-1\,s-1}^{p^n \beta_s},$$

$$T_\sigma = B_\sigma x_m^{a + rp^{\beta_\sigma}} L_{m-1}^{h_\sigma} Q_{m-1\,\sigma-1}^{e_\sigma} Q_{m-1\,\sigma}^{p^{\beta_\sigma}} \prod Q_{m-1\,s-1}^{p^n b_s} \qquad (h_\sigma = ap^n + db_1 + r^2 p^{\beta_\sigma}),$$

where $\sigma > 1$ and $Q_{m-1\,\sigma}$ is to be suppressed if $\sigma = m-1$, and where in the final product s has the values $2, \cdots, \sigma-1, \sigma+1, \cdots, m-1$.

First, let $\beta_1 < n$. Then $rp^{\beta_1} < d$. The product t contains but one term with the same set of exponents as T_1. For, if we employ a term of (9) after the second, the exponent of x_m exceeds that in T_1; if we employ the second term in (9), we must use the first terms in (8) and (10) and hence get T_1 itself; if we employ the first term of (9), we must use the first term of (8), and obtain as the exponent of L_{m-1} in the product of the two

$$ap^n + db_1 > e + ap^n.$$

Suppose that T_1 is a term of a product t' distinct from t. If $a' > a$, then $a' \geqq a + d$, since a' and a are multiples of d. Thus the minimum exponent a' of x_m in t' would exceed the exponent of x_m in T_1. Hence $a' = a$. Hence by (6) and the homogeneity of our invariant,

$$\sum_{s=1}^{m-1} (b'_s - b_s)(p^{nm} - p^{ns}) = 0. \tag{11}$$

Hence $(b'_1 - b_1)p^n$ is a multiple of p^{2n}, so that

$$b'_1 \equiv a_1 \pmod{p^n} \qquad \text{when} \qquad a' = a. \tag{12}$$

Thus in $b'_1 = p^{\beta_1'}B'_1$, we have $\beta'_1 = \beta_1$. Hence T_1 cannot occur in terms of t' other than

$$x_m^a L_{m-1}^{ap^n} (L_{m-1}^{db_1'} + B'_1 x_m^{rp^{\beta_1}} L_{m-1}^{e'} Q_{m-1\,1}^{p^{\beta_1}}) \prod_{s=2}^{m-1} Q_{ms}^{b_s'}. \tag{13}$$

If we employ the second term in the parenthesis, we must take the term of each Q_{ms} free of x_m. Then $b'_1 = b_1$, from the exponents of L_{m-1}, and $b'_s = b_s$ $(s = 2, \cdots, m-1)$, from the exponents of $Q_{m-1\,s-1}$. But $t' \neq t$. If we employ the first term in the parenthesis in (13), we obtain as the exponent of L_{m-1} in the product of the first two factors

$$ap^n + db'_1 > e + ap^n,$$

since $b'_1 \geqq b_1$ when $a' = a$. Hence the assumption is false.

We have now shown that T_1 occurs as an isolated term of the invariant. But the exponent of x_m is not a multiple of d and the coefficient B_1 is not zero in the field. Hence this case $\beta < n$ is excluded. Thus b_1 is a multiple of p^n.

Of the numbers $b_1, \cdots, b_{m-1}$ not multiples of p^n, let b_σ be the one with smallest subscript. Then $\sigma > 1$. A term of t with the same set of exponents as T_σ can be obtained only by taking the first terms of (8), (9), (10), for $s < \sigma$. If we use the second term of (10) for $s = \sigma$, we must take the first term of (10) for $s > \sigma$ and then obtain T_σ. If we use the first term of (10) for $s = \sigma$, the exponent of $Q_{m-1\,\sigma-1}$ in the product is $p^n b_\sigma$, which exceeds its exponent e_σ in T_σ.

Next, if T_σ occurs in t', distinct from t, then $a' = a$. From (12) it now follows that b_1' is a multiple of p^n. Analogous to (9),

$$(14) \qquad Q_{m1}^{b_1'} = L_{m-1}^{db_1'} + x_m^d K.$$

Hence we must take the first terms of (8) and (14). In the product of these two, the exponent of L_{m-1} is $ap^n + db_1' > h_\sigma$ if $b_1' \geqq b_1 + p^n$. Hence* must $b_1' = b_1$. If $\sigma > 2$, b_2 is by hypothesis a multiple of p^n. Then by (11), b_2' is a multiple of p^n. Hence we must take the first term $Q_{m-11}^{p^n b_2'}$ of $Q_{m2}^{b_2'}$. Since Q_{m-11} does not occur in the expansion of Q_{ms} for $s > 2$, and occurs in T_σ with the exponent $p^n b_2$, we conclude that $b_2' = b_2$. In this manner we may show that we must take the first term of $Q_{ms}^{b_s'}$ $(s < \sigma)$ and that $b_s' = b_s$ $(s = 2, \cdots, \sigma - 1)$. Then by (11), $b_\sigma' \equiv b_\sigma \pmod{p^n}$, whence $\beta_\sigma' = \beta_\sigma$. If we employ the second term in $Q_{m\sigma}^{b_\sigma'}$, we must use the first term in $Q_{ms}^{b_s'}$ $(s > \sigma)$ and we obtain the term T_σ if and only if $b_s' = b_s$ $(s = \sigma, \cdots, m-1)$, as shown by comparing the exponents of Q_{m-1s} $(s \geqq \sigma)$. But then $t' \equiv t$. If we employ the first term in $Q_{m\sigma}^{b_\sigma'}$, the total exponent of $Q_{m-1\sigma-1}$ in t' is $p^n b_\sigma'$ which exceeds its exponent e_σ in T_σ since $b_\sigma' \geqq b_\sigma$, in view of our definition of t.

We have now shown that τ_σ occurs as an isolated term of the invariant. But the exponent of x_m is not a multiple of d and the coefficient B_σ is not zero in the field. Hence our assumption on b_σ is false, so that $b_1, \cdots, b_{m-1}$ are all multiples of p^n. Set $b_s = p^n c_s$. Then

$$I' = I - c\,Q_{m+11}^{\sigma} \prod_{s=1}^{m-1} Q_{m+1s+1}^{c_s}$$

is an invariant of G_{m+1} in which I_0' lacks t. As at the end of § 3, it follows that I is an integral function of L_{m+1}, $Q_{m+1i}(i = 1, \cdots, m)$.

It remains to prove that the latter invariants are independent.† Any rational integral relation between them can be given the form

$$AL_{m+1} + B(Q_{m+11}, \cdots, Q_{m+1m}) = 0.$$

Let $x_{m+1} = 0$. Then by (4) and (5) with m replaced by $m+1$, we get

$$B(L_m^d, Q_{m1}^{p^n}, \cdots, Q_{mm-1}^{p^n}) = 0.$$

But L_m and the Q_{ms} are independent by hypothesis. Hence $B \equiv 0$. Thus the initial relation has the factor L_{m+1}. Since the relation cannot reduce to $L_{m+1}^\lambda \equiv 0$, it may be given the form $A'L_{m+1} + B' = 0$. As before $B' \equiv 0$. A repetition of this argument shows that no relation exists between the L_{m+1}, Q_{m+1i}.

As a basis for our induction, we note that there is no relation $AL_2 + cQ_{21}^e = 0$

* For $m = 3$, (11) gives $b_2' = b_2$, whence $t' \equiv t$.

† Another proof follows from the existence of solutions of the form problem (§ 8), whatever values be assigned to the fundamental invariants.

between the invariants of G_2. For, by setting $y=0$, we get $cx^{ed}=0$, whence $c=0$. Proceeding similarly with $A=A'L_2+c'Q_{21}^{e'}=0$, we prove that $A\equiv 0$.

The Form Problem.

8. In discussing the solution of a set of equations with coefficients in a finite field having modulus p, it is convenient to introduce the infinite field F_p composed of all the roots of all rational integral equations with integral coefficients taken modulo p. Then F_p, like the field of all complex numbers, has the property that any algebraic equation of degree k with coefficients in the field has k roots in the field.

In the form problem for the group G_m, we seek the sets of values of the m variables x_i for which the m fundamental absolute invariants L_m^r, Q_{ms} $(s=1,\cdots,m-1)$ take assigned values λ, q_s in F_p. Here $r=p^n-1$. If l is a particular r-th root of λ, the problem * consists in the solution of

$$L_m(x_i)=l, \qquad Q_{ms}(x_i)=q_s \qquad (s=1,\cdots,m-1). \tag{15}$$

Let $x_1,\cdots,x_m$ be a set of solutions of (15). Since the determinant L_{m+1} vanishes when x_{m+1} equals one of the x_i $(i\leqq m)$, it follows from (7), with m replaced by $m+1$, that $x_1,\cdots,x_m$ are roots of

$$l\xi^{p^{nm}}+\sum_{s=1}^{m-1}(-1)^{m-s}lq_s\xi^{p^{ns}}+(-1)^m l^{p^n}\xi=0. \tag{16}$$

Suppose for the present that $l\neq 0$. The preceding equation gives

$$\xi^{p^{nm}}+\sum_{s=1}^{m-1}(-1)^{m-s}q_s\xi^{p^{ns}}+(-1)^m\lambda\xi=0. \tag{17}$$

This equation has no double root and hence has p^{nm} distinct roots in F_p. If ξ_1 and ξ_2 are roots, then are also $\xi_1+\xi_2$, $c_1\xi_1$, where c_1 is an element of the $GF[p^n]$. Indeed, in that field,

$$(\xi_1+\xi_2)^{p^{ns}}=\xi_1^{p^{ns}}+\xi_2^{p^{ns}}, \qquad (c_1\xi_1)^{p^{ns}}=c_1\xi_1^{p^{ns}}.$$

Hence there exist m solutions $\xi_1,\cdots,\xi_m$ of (17), linearly independent with respect to the $GF[p^n]$, while ξ is a solution if and only if

$$\xi=c_1\xi_1+\cdots+c_m\xi_m \qquad (c\text{'s in } GF[p^n]). \tag{18}$$

Since the x_i are solutions, we have

$$x_i=c_{i1}\xi_1+\cdots+c_{im}\xi_m \qquad (i=1,\cdots,m), \tag{19}$$

in which the c_{ij} are elements of non-vanishing determinant of the $GF[p^n]$. Indeed, by § 1,

$$l=L_m(x_i)=|c_{ij}|\cdot L_m(\xi_i). \tag{20}$$

* This problem is the form problem for the subgroup G'_m of all the transformations of determinant unity.

To show conversely that any such set of values (19) satisfy equations (15), let $\xi_1, \cdots, \xi_m$ be any set of roots of (17) linearly independent with respect to the $GF[p^n]$. Then by § 2, $L_m(\xi_i) \neq 0$. Define the x_i by (19), where $|c_{ij}| \neq 0$. Then $l \neq 0$ by (20). By § 2, the p^{nm} expressions (18) are the roots of

$$L_{m+1}(\xi_1, \cdots, \xi_m, \xi) = 0,$$

in which the coefficient of $\xi^{p^{nm}}$ is $\pm L_m(\xi_i) \neq 0$, and hence are the roots of

$$\xi^{p^{nm}} + \sum_{s=1}^{m-1} (-1)^{m-s} Q_{ms}(\xi_i) \xi^{p^{ns}} + (-1)^m [L_m(\xi_i)]^r \xi = 0.$$

Since this equation and (17) have in common the p^{nm} distinct roots (18), they are identical. In view of the absolute invariance of L_m^r and Q_{ms}, we conclude that the expressions (19) satisfy equations (15), in which $l^r = \lambda$.

Theorem. *For $\lambda \neq 0$, $x_1, \cdots, x_m$ is a set of solutions of*

$$(21) \qquad L_m^{p^n-1} = \lambda, \qquad Q_{ms} = q_s \qquad (s = 1, \cdots, m-1)$$

if and only if $x_i = c_{i1}\xi_1 + \cdots + c_{im}\xi_m$ $(i = 1, \cdots, m)$, where the c_{ij} are elements of non-vanishing determinant of the $GF[p^n]$, and $\xi_1, \cdots, \xi_m$ is any set of roots of equation (17) linearly independent with respect to the $GF[p^n]$.

To obtain the sets of solutions of (15), we restrict the c_{ij} to be of determinant unity and hence, by (20), the ξ_i to be linearly independent roots of (17) for which $L_m(\xi_i) = l$.

Next, let $\lambda = 0$, $q_1 \neq 0$. If the minors of the elements of the first row of L_m all vanished, there would exist (§ 2) a linear relation between each set of $m-1$ of the x's. Applying a linear transformation, we would obtain $x_m = x_{m-1} = 0$. By (7) the quotient L_m/L_{m-1} would vanish and, by (5_1), $Q_{m1} = 0$, in contradiction with $q_1 \neq 0$. Hence the above minors are not all zero. After permuting the variables we may set $L_{m-1} \neq 0$. Then, by (4) and (5),

$$L_{m-1}^{p^n(p^n-1)} = q_1, \qquad Q_{m-1\,s-1}^{p^n} = q_s \qquad (s = 2, \cdots, m-1).$$

As above, $x_1, \cdots, x_{m-1}$ are linear functions of a set of linearly independent roots $\xi_1, \cdots, \xi_{m-1}$ of

$$\xi^{p^{n(m-1)}} + \sum_{\sigma=2}^{m-1} (-1)^{m-\sigma} q_\sigma^{1/p^n} \xi^{p^{n(\sigma-1)}} + (-1)^{m-1} q_1^{1/p^n} \xi = 0,$$

given by (7) upon replacing s by $\sigma - 1$. Raising this equation to the power p^n we obtain (17) for $\lambda = 0$. Each root of the latter is therefore of multiplicity exactly p^n. In view of $L_m = 0$, there exists (§ 2) a linear relation between $x_1, \cdots, x_m$, with coefficients in the $GF[p^n]$. Since $x_1, \cdots, x_{m-1}$ are linearly independent with respect to this field, x_m is a linear function of $x_1, \cdots, x_{m-1}$ and hence of $\xi_1, \cdots, \xi_{m-1}$, with coefficients in this field. Returning to the initial order of the variables, we conclude that, if $\lambda = 0$, $q_1 \neq 0$, $x_1, \cdots, x_m$ are linear functions of a set $m-1$ linearly independent roots of (17), the matrix of the coefficients being of rank $m-1$.

Next, let $\lambda = q_1 = 0$, $q_2 \neq 0$. Then the minors of the elements of the first row of L_m all vanish. For, if $L_{m-1} \neq 0$, for example, (5_1) would give $Q_{m1} \neq 0$, contrary to $q_1 = 0$. After applying a linear transformation T, we may set $x_m = x_{m-1} = 0$. Then by (7) the quotient L_m / L_{m-1} is zero. Hence by (4) and (5_2),

$$Q^{p^n}_{m-1\, s-1} = q_s \qquad (s = 2, \cdots, m-1).$$

By (7), with m replaced by $m-1$, the quotient L_{m-1}/L_{m-2} vanishes when $x_{m-1} = 0$. Hence by (4) and (5), with m replaced by $m-1$,

$$L^{p^{2n}(p^n-1)}_{m-2} = q_2, \qquad Q^{p^{2n}}_{m-2\, s-2} = q_s \qquad (s = 3, \cdots, m-1).$$

If, for $i \leqq m-2$, we multiply the elements of the i-th column of L_{m-1} by the adjoint minors of the corresponding elements of the last column, we see (compare (7) with m replaced by $m-1$) that $x_1, \cdots, x_{m-2}$ are roots of

$$0 = \xi L^{p^n}_{m-2} + L_{m-2} \sum_{s=1}^{m-3} (-1)^s \xi^{p^{ns}} Q_{m-2\, s} + (-1)^{m-2} \xi^{p^{n(m-2)}} L_{m-2}.$$

Divide by L_{m-2} and raise the resulting equation to the power p^{2n}. We obtain equation (17), since $\lambda = q_1 = 0$. Each root of the latter is now of multiplicity p^{2n}. As above, $x_1, \cdots, x_{m-2}$ are linearly independent linear functions of $m-2$ linearly independent roots $\xi_1, \cdots, \xi_{m-2}$ of (17). Applying the inverse of T, we conclude that the initial values $x_1, \cdots, x_m$ are linear functions of $\xi_1, \cdots, \xi_{m-2}$, the matrix of the coefficients being of rank $m-2$.

Proceeding in a similar manner, we obtain the

Theorem. *If $\lambda = q_1 = \cdots = q_{t-1} = 0$, $q_t \neq 0$, then $x_1, \cdots, x_m$ is a set of solutions of (21) if and only if the x_i are linear functions of $\xi_1, \cdots, \xi_{m-t}$ with coefficients in the $GF[p^n]$ the rank of whose matrix is $m-t$, while $\xi_1, \cdots, \xi_{m-t}$ is any set of roots of (17) linearly independent with respect to the $GF[p^n]$, every root of (17) being a linear function of these $m-t$ roots. If all the invariants are zero, each x_i is zero.*

9. The number of matrices (c_{ij}) of rank $m-t$ with m rows and $m-t$ columns, each c_{ij} being an element of the $GF[p^n]$, is

$$(22) \qquad (p^{nm}-1)(p^{nm}-p^n)\cdots(p^{nm}-p^{n(m-t-1)}).$$

Hence this gives the number of distinct sets of solutions of the form problem when $\lambda = q_1 = \cdots = q_{t-1} = 0$, $q_t \neq 0$.

From the above discussion follows the

Theorem. *The determinant L_m is of rank $m-t$ if and only if*

$$(23) \qquad L_m = 0,\ Q_{m1} = 0,\ \cdots,\ Q_{m\, t-1} = 0,\ Q_{mt} \neq 0.$$

These are necessary and sufficient invariantive conditions that the variables x_i *shall satisfy exactly t linearly independent linear relations in the* $GF[p^n]$.

Solution of the Fundamental Equation.

10. The complete solution of the form problem has been reduced to the solution of the fundamental equation (17). If $\lambda = 0$, the latter equation is the p^n-th power of an equation of like type. Hence it suffices to discuss the solution of equations of type (17) with $\lambda \neq 0$.

We may restrict attention to the case in which the coefficients of (17) belong to the $GF[p^n]$, since in the contrary case the equation is equivalent to one of like form with coefficients in the $GF[p^n]$, but of higher degree. The nature of the proof will be indicated for $m = 2$. Then (17) becomes

$$\xi^{p^{2n}} = q\xi^{p^n} - \lambda\xi. \tag{24}$$

Let q be a root of an equation $Q^2 - aQ + b = 0$, irreducible in the $GF[p^n]$. Its second root is q^{p^n}, so that

$$q^{p^n} + q = a, \qquad q^{p^n+1} = b, \qquad q^{p^{2n}} = q.$$

From the p^n-th power of (24) we eliminate $\xi^{p^{2n}}$ and get

$$\xi^{p^{3n}} = (b - \lambda^{p^n})\xi^{p^n} - q^{p^n}\lambda\xi.$$

From the p^n-th power of the latter we eliminate $q\xi^{p^n}$ by (24) and get

$$\xi^{p^{4n}} = \beta\xi^{p^{2n}} - \lambda^{p^n+1}\xi, \qquad \beta = b - \lambda^{p^{2n}} - \lambda^{p^n}. \tag{25}$$

If λ belongs to the $GF[p^n]$, the required equation is thus

$$\xi^{p^{4n}} - (b - 2\lambda)\xi^{p^{2n}} + \lambda^2\xi = 0. \tag{26}$$

If λ is a root of an equation $L^2 - rL + s = 0$, irreducible in the $GF[p^n]$, the required equation is obviously

$$\xi^{p^{4n}} - (b - r)\xi^{p^{2n}} + s\xi = 0. \tag{27}$$

If λ is a root of an equation $\lambda^3 - c\lambda^2 + d\lambda - e = 0$, irreducible in the $GF[p^n]$, we make repeated use of the relations

$$\lambda + \lambda^{p^n} + \lambda^{p^{2n}} = c, \qquad \lambda^{1+p^n+p^{2n}} = e,$$

raise (25) to the powers $p^{2n}, p^{4n}, \cdots, p^{8n}$, and find that

$$\xi^{p^{12n}} - \{b(b-c)^2 - 2e\}\xi^{p^{6n}} + e^2\xi = 0. \tag{28}$$

11. We therefore consider the fundamental equation (17) with coefficients in the $GF[p^n]$ and $\lambda \neq 0$. There is no multiple root. Let r be a root $\neq 0$.

If $r^{p^n} = xr$, where x belongs to the $GF[p^n]$ then

$$r^{p^{2n}} = xr^{p^n} = x^2 r, \qquad r^{p^{jn}} = x^j r.$$

Hence, by (17), x must satisfy the *characteristic equation*

$$\Delta(x) \equiv x^m + \sum_{s=1}^{m-1} (-1)^{m-s} q_s x^s + (-1)^m \lambda = 0. \tag{29}$$

Thus each root in the $GF[p^n]$ of $\Delta(x) = 0$ furnishes a factor $\xi^{p^n} - x\xi$ of (17). Let this binomial have a factor $f(\xi)$, of degree d, irreducible in the $GF[p^n]$. Its roots are

$$r, \; r^{p^n} = xr, \; r^{p^{2n}} = x^2 r, \; \cdots, \; r^{p^{(d-1)n}} = x^{d-1} r,$$

while x belongs to the exponent d. Since x is in the field, d is a divisor of $p^n - 1$. It follows that

$$f(\xi) = \xi^d - \delta \qquad (\delta = r^d).$$

Theorem. *The irreducible factors of $\xi^{p^n-1} - x$ are all binomial and of equal degree, namely, the exponent to which x belongs.*

Discussion of the Fundamental Equation for $m = 2$.

12. For the present, let $m = 2$. Since $2p^n - 1 < p^{2n}$, equation (24) has an irreducible factor $F(\xi)$, of degree $D > 1$, not of the preceding type $f(\xi)$, and hence has a root r such that r^{p^n}/r is not an element of the $GF[p^n]$. Since, therefore, r and r^{p^n} are linearly independent with respect to that field, we conclude from (18) that every root of (24) is of the form $c_1 r + c_2 r^{p^n}$, where c_1 and c_2 are elements of the $GF[p^n]$. Hence (24) has all its roots in the $GF[p^{nD}]$, but not all in a smaller field.

Theorem. *For $m = 2$, every irreducible factor of the fundamental equation is of degree a divisor of D; each irreducible factor not of the above binomial type is of degree D.*

13. We proceed to determine this integer D which is such that equation (24) is completely solvable in the $GF[p^{nD}]$, but not in the $GF[p^{nl}]$, for $l < D$. By raising (24) to the powers $p^n, p^{2n}, \cdots$, we may express $\xi^{p^{nt}}$ as a linear function l_t of ξ^{p^n} and ξ. We seek the least value D of t for which $l_t \equiv \xi$. Now the coefficients of l_t are the elements of the first line in S^{t-1}, where

$$S = \begin{pmatrix} q & -\lambda \\ 1 & 0 \end{pmatrix}, \qquad \Delta(x) = x^2 - qx + \lambda.$$

The condition for $l_{D+1} = \xi^{p^n}$ is therefore $S^D = 1$. Hence D is the period of the transformation S. According as the characteristic equation $\Delta(x) = 0$ has distinct roots x_1 and x_2 or equal* roots $x = \frac{1}{2}q = \lambda^{\frac{1}{2}}$, the canonical form for S is

$$\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}, \qquad \begin{pmatrix} x & x \\ 0 & x \end{pmatrix}.$$

In the first case, the period of S is the least common multiple of the exponents

* We then employ the new variables $V_1 = v_1$, $V_2 = v_1 - xv_2$.

to which the roots x_1 and x_2 belong. In the second case, the period is p times the exponent to which the double root belongs.

Theorem. *For $m = 2$, the fundamental equation is completely solvable in the $GF[p^{nD}]$, but in no lower field, where D is the least common multiple of the exponents to which belong distinct roots of the characteristic equation, or p times the exponent to which its double root belongs.*

Illustrations of the preceding results are afforded by the following examples in which are given all the irreducible factors other than ξ of (24):

$p^n = 2$. $\xi^3 + 1 \equiv (\xi + 1)(\xi^2 + \xi + 1)$, $\xi^3 - \xi + 1$ irreducible.

$p^n = 3$. $\xi^8 - 1 \equiv (\xi + 1)(\xi - 1)(\xi^2 + 1)(\xi^2 + \xi - 1)(\xi^2 - \xi - 1)$,

$\xi^8 \pm \xi^2 - 1$ irreducible, $\xi^8 + \xi^2 + 1 \equiv (\xi + 1)(\xi - 1)(\xi^3 - \xi + 1)(\xi^3 - \xi - 1)$,

$\xi^8 + 1 \equiv (\xi^4 + \xi^2 - 1)(\xi^4 - \xi^2 - 1)$, $\xi^8 - \xi^2 + 1 \equiv (\xi^2 + 1)(\xi^6 - \xi^4 + \xi^2 + 1)$.

Theory of the General Fundamental Equation.

14. We remove the restriction that $m = 2$ and prove the

Theorem. *If the characteristic function* (29) *reduces in the $GF[p^n]$,*

$$(30) \quad \Delta(x) = \phi(x)\psi(x), \quad \phi(x) = \sum_{i=0}^{a} a_i x^i, \quad \psi(x) = \sum_{j=0}^{m-a} b_j x^j, \quad a_a = b_{m-a} = 1,$$

the fundamental equation (17) *is transformed into*

$$(31) \qquad \Psi(\eta) \equiv \sum_{j=0}^{m-a} b_j \eta^{p^{nj}} = 0$$

by the substitution

$$(32) \qquad \eta = \Phi(\xi) \equiv \sum_{i=0}^{a} a_i \xi^{p^{ni}}.$$

In other words, the fundamental equation factors into*

$$\prod_{k=1}^{p^{n(m-a)}} [\Phi(\xi) - \eta_k] = 0 \qquad [\eta_k \text{ roots of } \Psi(\eta) = 0].$$

For proof, we note that the result of the elimination of η is

$$\sum a_i b_j \xi^{p^{n(i+j)}} \qquad (i = 0, \cdots, a;\ j = 0, \cdots, m - a),$$

which is identical with (17), since by (30) the corresponding sum $\sum a_i b_j x^{i+j}$ is identical with (29).

Since equation (31) has the root $\eta = 0$, we obtain

Corollary I. The fundamental equation has the factor $\Phi(\xi)$ if and only if the characteristic equation has the factor $\phi(x)$ in the $GF[p^n]$.

Corollary II. A root of the fundamental equation satisfies $\Phi(\xi) = 0$, but no similar equation of lower degree, if and only if $\phi(x)$ is a factor of $\Delta(x)$.

* Hence it has the symbolic expression $\psi(\phi)$, as in the theory of the reducibility of linear differential equations.

15. For $k \leqq m$ let D_k denote the number of the non-vanishing roots of the fundamental equation each of which satisfies an equation $\Phi_k(\xi) = 0$, but no equation $\Phi_l(\xi) = 0$, $l < k$. By corollary II, $\phi_k(x)$ must be a factor of $\Delta(x)$. Suppose first that the latter has no multiple factors. Denote by $N_1, N_2, N_3, \cdots$ the number of its irreducible factors of degree $1, 2, 3, \cdots$. Then

$$m = N_1 + 2N_2 + 3N_3 + \cdots.$$

Let $[i] = p^{ni} - 1$. We proceed to show that

$$(33) \qquad D_k = \Sigma \binom{N_1}{n_1}\binom{N_2}{n_2} \cdots \binom{N_k}{n_k} [1]^{n_1}[2]^{n_2} \cdots [k]^{n_k},$$

the sum extending over all sets of positive integers n_i for which

$$k = n_1 + 2n_2 + 3n_3 + \cdots + kn_k, \qquad n_i \leqq N_i.$$

Let a particular factor ϕ_k of $\Delta(x)$ contain $n_1, n_2, n_3, \cdots$ irreducible factors of degree $1, 2, 3, \cdots$. Of the $[k]$ roots of the corresponding equation $\Phi_k(\xi) = 0$, we wish to exclude those which satisfy $\Phi_l(\xi) = 0$, $l < k$. Let ϕ_l have $m_1, m_2, m_3, \cdots$ irreducible factors of degree $1, 2, 3, \cdots$. We assume that (33) holds when k is replaced by a smaller value l. Then the number of roots to be excluded is

$$E = \sum_{l=1}^{k-1} \Sigma \binom{n_1}{m_1}\binom{n_2}{m_2} \cdots \binom{n_l}{m_l} [1]^{m_1}[2]^{m_2} \cdots [l]^{m_l},$$

the inner sum extending over all sets of positive integers m_i for which

$$l = m_1 + 2m_2 + \cdots + lm_l, \qquad m_i \leqq n_i.$$

To prove (33), it remains to show that

$$[k] - E = [1]^{n_1}[2]^{n_2} \cdots [k]^{n_k}.$$

This follows from *

$$1 + E + [1]^{n_1} \cdots [k]^{n_k} = \sum_{l=0}^{k} \Sigma \binom{n_1}{m_1} \cdots \binom{n_l}{m_l} [1]^{m_1} \cdots [l]^{m_l}$$

$$= \left\{ \sum_{m_1=0}^{n_1} \binom{n_1}{m_1} [1]^{m_1} \right\} \cdots \left\{ \sum_{m_k=0}^{n_k} \binom{n_k}{m_k} [k]^{m_k} \right\} = \{1 + [1]\}^{n_1} \cdots \{1 + [k]\}^{n_k} = p^{nk}.$$

Hence if $\Delta(x)$ has no multiple root, the number of the roots of the fundamental equation which satisfy no similar equation of lower degree is

$$D_m = [1]^{N_1}[2]^{N_2} \cdots [m]^{N_m}.$$

If the characteristic equation has multiple roots,

$$\Delta(x) = \prod_i F_{d_i}^{e_i},$$

* Note that, for the added term, $l = k$, whence $m_i = n_i$.

where the F's are distinct irreducible functions, but not necessarily of distinct degrees d_i, the preceding result is to be replaced by

$$(34) \qquad D_m = p^{ne}\prod_i [d_i], \qquad e = \sum_i d_i(e_i - 1).$$

From $D_m > 1$ we infer that the fundamental equation has a root r such that $r^{p^{ni}}$ $(i = 0, 1, \cdots, m-1)$ are linearly independent with respect to the $GF[p^n]$. Hence, by (18), every root is of the form

$$\xi = \sum_{i=0}^{m-1} c_i r^{p^{ni}} \qquad (c\text{'s in } GF[p^n]).$$

Let D be the degree of the equation, irreducible in the $GF[p^n]$, which has the root r and hence also the roots $r^{p^{ni}}$. For $i = D$, the latter equals r. By the linear independence, $D \geqq m$.

Theorem. *Every irreducible factor in the $GF[p^n]$ of the fundamental equation is of degree a divisor of D, where D is not less than m and is the common degree of all the irreducible factors which do not divide a similar equation of lower degree. The fundamental equation is completely solvable in the $GF[p^{nD}]$, but not in a smaller field.*

16. We proceed to determine D. By the powers $p^n, p^{2n}, \cdots$ of (17),

$$\xi^{p^{nt}} = \sum_{i=0}^{m-i} a_i \xi^{p^{ni}} \equiv l_t(\xi) \qquad (t \geqq m).$$

We seek the least value D of t for which $l_t \equiv \xi$. Now, the coefficients of $\xi^{p^{n(m-1)}}, \cdots, \xi^{p^n}, \xi$ in l_t are the elements of the first row of S^{t-m+1}, where

$$S = \begin{vmatrix} q_{m-1} & -q_{m-2} & q_{m-3} & \cdots & (-1)^{m-2}q_1 & (-1)^{m-1}\lambda \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{vmatrix}.$$

If $l_t = \xi$, then $l_{t+1} = \xi^{p^n}, \cdots, l_{t+m-1} = \xi^{p^{n(m-1)}}$, and hence $S^t = 1$. Thus D is the period of the transformation of S. The minor of the element $\pm\lambda$ in the matrix S equals unity. Hence the characteristic determinant $(-1)^m\Delta(x)$ of S is its single invariant-factor. Hence,* if

$$(-1)^m\Delta(x) = F_k^\kappa F_l^\lambda \cdots,$$

where $F_k, F_l, \cdots$ are distinct irreducible functions in the $GF[p^n]$, the first having the roots $K_1, \cdots, K_k$, the second the roots $L_1, \cdots, L_l$, the transformation S has the canonical form

$$\eta'_{i1} = K_i\eta_{i1},\ \eta'_{i2} = K_i(\eta_{i1} + \eta_{i2}),\ \eta'_{i3} = K_i(\eta_{i2} + \eta_{i3}),\ \cdots,\ \eta'_{i\kappa} = K_i(\eta_{i\kappa-1} + \eta_{i\kappa}),$$
$$\zeta'_{i1} = L_i\zeta_{i1},\ \zeta'_{i2} = L_i(\zeta_{i1} + \zeta_{i2}),\ \zeta'_{i3} = L_i(\zeta_{i2} + \zeta_{i3}),\ \cdots,\ \zeta'_{i\lambda} = L_i(\zeta_{i\lambda-1} + \zeta_{i\lambda}),\ \cdots$$

* These Transactions, vol. 3 (1902), p. 291.

where $i=1, \cdots, k$ in the first line, $i=1, \cdots, l$ in the second, $\cdots$. The transformation S therefore has the maximum number of variables in each chain. Let κ be greatest of the exponents $\kappa, \lambda, \cdots$. Then the longest chain contains κ variables. Determine h so that $p^{h-1} < \kappa \leqq p^h$. Let d be the least common multiple of the exponents to which belong the roots $K_1, L_1, \cdots$. Then * $D = dp^h$.

Theorem. *The smallest field in which the fundamental equation is completely solvable is the* $GF[p^{nD}]$, $D = dp^h$, *where d is the least common multiple of the exponents to which belong the roots of the characteristic equation* $\Delta(x) = 0$, *while* p^h *is the least power of p which is equal to or greater than the maximum multiplicity of a root of* $\Delta(x) = 0$.

In the case of the classical equation $\xi^{p^{nm}} - \xi = 0$, we have $\Delta(x) = x^m - 1$, so that $D = m$.

In case $\Delta(x)$ is a primitive irreducible function, we have $D = p^{nm} - 1$. Thus the fundamental equation is the product of ξ and an irreducible equation.

The Interpretation of certain Invariants, § 17–22.

17. Since the determinant $[2m-2, 2m-4, \cdots, 4, 2, 0]$ is the product of the distinct † linear functions of m variables in the $GF[p^{2n}]$, its quotient by L_m is the product J_m of all distinct quadratic forms in the $GF[p^{2n}]$ on m variables which can be transformed into irreducible binary forms. Indeed, each linear factor of J_m is of the form $l_1 + \rho l_2$, where l_1 and l_2 are linear forms in the $GF[p^n]$, $l_2 \neq 0$, and ρ is a root of a quadratic equation irreducible in that field. If ρ' is the second root, $l_1 + \rho' l_2$ is a factor of J_m. The product of the two factors is a quadratic form in the $GF[p^n]$ which $x_1' = l_1$, $x_2' = l_2$ transforms into an irreducible binary form.

For $m = 2$, J_2 is the invariant Q_{21} of the fundamental system.

For $m = 3$, we have the following expression for J_3:

$$J_3 = Q_{31} Q_{32}^{p^n} - L_3^{p^n(p^n-1)}. \tag{35}$$

For proof, we expand the identically vanishing determinant

$$\begin{vmatrix} a_4 & b_4 & c_4 & 0 & 0 & 0 \\ a_3 & b_3 & c_3 & a_3 & b_3 & c_3 \\ a_2 & b_2 & c_2 & a_2 & b_2 & c_2 \\ a_1 & b_1 & c_1 & a_1 & b_1 & c_1 \\ a_0 & b_0 & c_0 & a_0 & b_0 & c_0 \\ 0 & 0 & 0 & a_2 & b_2 & c_2 \end{vmatrix}$$

* JORDAN, *Traité des Substitutions*, p. 127. Jordan's q is the present $h-1$.

† Here and below we shall say that two functions are distinct if their ratio is not a constant.

by Laplace's method according to the minors of the first three columns and get

(36) $$(a_4 b_3 c_2)(a_2 b_1 c_0) - (a_4 b_2 c_1)(a_3 b_2 c_0) + (a_4 b_2 c_0)(a_3 b_2 c_1) \equiv 0 .$$

Taking $a_i = x^{p^{ni}}$, $b_i = y^{p^{ni}}$, $c_i = z^{p^{ni}}$, and dividing by $L_3^{p^n+1}$, we get (35). Since (35) is an irreducible function of its arguments, we conclude that any irreducible binary quadratic form is equivalent to a constant multiple of any other irreducible binary quadratic form within G_3 and hence within G_2.

Invariants relating to Cubic Forms.

18. The product of the distinct linear functions of m variables in the $GF[p^{3n}]$, no one of which is a constant times a linear function in the $GF[p^n]$, equals

$$P_m = [3m-3, 3m-6, \cdots, 6, 3, 0]/L_m .$$

Each linear factor of P_m is of the form

$$\gamma = \sum_{i=1}^{m} \gamma_i x_i , \qquad \gamma_i \equiv c_{i0} + c_{i1}\rho + c_{i2}\rho^2 ,$$

where ρ is a root of a fixed irreducible cubic R in the $GF[p^n]$, and where the ratios of the γ_i do not all belong to the latter field.

If $m = 2$, the factors are $x_1 - \sigma x_2$, where σ is in the $GF[p^{3n}]$, but not in the $GF[p^n]$. Hence P_2 is the product of the distinct irreducible binary cubic forms in the $GF[p^n]$. See (42) below.

If $m \geqq 3$, the rank of the matrix (c_{ij}) is 3 or 2. In the first case $\sum c_{i0} x_i$, $\sum c_{i1} x_i$, $\sum c_{i2} x_i$ are linearly independent, and there exists a transformation of G_m which replaces γ by $x_1 + \rho x_2 + \rho^2 x_3$. The functions obtained from the latter by replacing ρ by either of the remaining roots of the cubic R are factors of P_m. Hence P_m contains as a factor the product K_m of all distinct m-ary cubic forms equivalent to a non-vanishing ternary cubic form.* If the rank is 2, the linear factor is equivalent to $x_1 - \rho x_2$. Hence $P_m = K_m C_m$, where C_m is the product of all distinct m-ary cubic forms equivalent to an irreducible binary form. Now, there are

(37) $$N = (p^{nm} - 1)(p^{nm} - p^n)(p^{nm} - p^{2n})$$

sets of elements c_{ij} in the $GF[p^n]$ such that matrix (c_{ij}) is of rank 3. But two linear functions whose ratio is one of the $p^{3n} - 1$ elements $\neq 0$ of the $GF[p^{3n}]$ give the same factor. Hence the degree of K_m is

(38) $$k_m = N/(p^{3n} - 1) .$$

The degree c_m of C_m is therefore $p_m - k_m$, where

(39) $$p_m = p^{3n(m-1)} - p^{n(m-1)} + p^{3n(m-2)} - p^{n(m-2)} + \cdots + p^{3n} - p^n .$$

* DICKSON, Bulletin of the American Mathematical Society, vol. 14 (1908), p. 161.

19. We proceed to the evaluation of the invariant C_3 of degree

$$c_3 = (p^{3n} - p^n)(p^{2n} + p^n + 1) = p^n(p^{3n} - 1)(p^n + 1).$$

To this end we construct an integral function of the fundamental invariants (2) of G_3 which vanishes identically in y, z for $x = \rho y$, where

$$(40) \qquad \rho^{p^{3n}} = \rho, \qquad \rho^{p^n} \neq \rho.$$

For $x = \rho y$, (1) gives

$$L_2 = (\rho^{p^n} - \rho) y^{p^n+1}, \qquad Q_{21} - k y^{p^{2n}-p^n}, \qquad k \equiv (\rho^{p^{2n}} - \rho)/(\rho^{p^n} - \rho).$$

In view of (40), we have

$$k^{p^n} = (\rho - \rho^{p^n})/(\rho^{p^{2n}} - \rho^{p^n}), \qquad k^{p^n+1} = (\rho - \rho^{p^{2n}})/(\rho^{p^{2n}} - \rho^{p^n}),$$

$$(\rho^{p^n} - \rho)^{p^{2n}-p^n} = (\rho^{p^{3n}} - \rho^{p^{2n}})/(\rho^{p^{2n}} - \rho^{p^n}) = k^{p^n+1},$$

$$(41) \qquad Q_{21}^{p^n+1} = L_2^{p^{2n}-p^n}.$$

Since $p_2 = p^{3n} - p^n$ by (39), we conclude that *

$$(42) \qquad P_2 = Q_{21}^{p^n+1} - L_2^{p^{2n}-p^n}.$$

The desired invariantive relation $C_3 = 0$ is obtained by the elimination of Q_{21} and L_2 from (41), (2_2) and (2_3). We have

$$Q_{31} = Q_{21} Q_{32}, \qquad L_2^{p^{2n}-p^n} = Q_{21}^{p^n+1} = (Q_{31}/Q_{32})^{p^n+1},$$

$$L_3^{p^{2n}-p^n}\left(\frac{Q_{32}}{Q_{31}}\right)^{p^n+1} = \left(\frac{L_3}{L_2}\right)^{p^{2n}-p^n} = (Q_{32} - Q_{21}^{p^n})^{p^n} = Q_{32}^{p^n} - \left(\frac{Q_{31}}{Q_{32}}\right)^{p^{2n}},$$

$$(43) \qquad C_3 = L_3^{p^{2n}-p^n} Q_{32}^{e} - (Q_{31} Q_{32}^{p^n})^{p^n+1} + Q_{31}^{e} \qquad (e = p^{2n} + p^n + 1).$$

We proceed to express the invariant P_3 in terms of the fundamental invariants. With the notation of § 1, we obtain from (36),

$$[623][310] - [631][230] + [630][231] = 0,$$

$$[532][210] - [521][320] + [520][321] = 0,$$

$$[431][120] - [412][310] + [410][312] = 0.$$

We raise the second to the power p^n, the third to the power p^{2n}, and get

$$-[410]^{p^{2n}}[310] + [520]^{p^n}[320] - [630][210]^{p^n} = 0,$$

$$[310]^{p^{3n}}[210]^{p^n} - [410]^{p^{2n}}[320]^{p^n} + [520]^{p^n}[210]^{p^{2n}} = 0,$$

$$-[320]^{p^{3n}}[210]^{p^{2n}} + [310]^{p^{3n}}[310]^{p^{2n}} - [410]^{p^{2n}}[210]^{p^{3n}} = 0.$$

We eliminate $[520]^{p^n}$ and $[410]^{p^{2n}}$ linearly, divide by a power of $[210]$, and get

$$(44) \quad P_3 = [Q_{32}^{p^{3n}+p^{2n}} - Q_{31}^{p^{3n}}][Q_{31}^{p^n+1} - Q_{32} L_3^{p^{2n}-p^n}] - Q_{31} Q_{32}^{p^{3n}} L_3^{p^{3n}-p^{2n}}.$$

*Since Q_{21} is an absolute invariant of G_2 and L_2^r, $r = p^n - 1$, is the least power of L_2 giving an absolute invariant, any invariant factor of (42) must be of degree a multiple of $r(p^n + 1)$ and $p^{2n} - p^n$ and hence a multiple of $rp^n(p^n + 1)$. Thus P_2 is an irreducible invariant. Hence any irreducible binary cubic is equivalent within G_2 to a multiple of any other.

We readily verify the identity

(45) $$Q_{32}^{p^{2n}+p^n} P_3 + Q_{31} C_3^{p^n} - Q_{31}^{p^{3n}} C_3 + Q_{32}^{p^{3n}+p^{2n}} C_3 \equiv 0.$$

Hence the product of all non-vanishing ternary cubics is

(46) $$K_3 = - Q_{32}^{p^{3n}-p^n} + (Q_{31}^{p^{3n}} - Q_{31} C_3^{p^n-1}) / Q_{32}^{p^{2n}+p^n}.$$

The last expression equals an integral function. By (43)

(46′) $$K_3 = - Q_{32}^{p^{3n}-p^n} - \sum_{i=1}^{p^n-1} (Q_{31}^{p^n+1} - Q_{32} L_3^{p^{2n}-p^n})^i Q_{32}^{(p^{2n}+p^n)(i-1)} Q_{31}^{p^{3n}-ei}.$$

Invariants relating to Quadratic Forms.

20. We next determine the invariantive expression for the product Q of all distinct ternary quadratic forms of non-vanishing discriminant* in the $GF[p^n]$. An integral function has the factor $y^2 - xz$ if and only if it vanishes identically in x and t when we set

$$y = tx, \qquad z = t^2 x.$$

For these values,

$$L_2 = x^{p^n+1}(t - t^{p^n}), \qquad Q_{21} = x^{rp^n}(t - t^{p^{2n}})/(t - t^{p^n}), \qquad r \equiv p^n - 1,$$

$$L_3 = x^e (t - t^{p^n})(t - t^{p^{2n}})(t^{p^n} - t^{p^{2n}}), \qquad e \equiv p^{2n} + p^n + 1.$$

By eliminating t, we get the two relations†

(47) $$x^e L_3 = Q_{21} L_2^{p^n+2}, \qquad x^{p^{2n}} - x^{p^n} Q_{21} + x L_2^r = 0.$$

By means of the rth power of the former, we may express $x^{p^{3n}}$ as a multiple of x. Hence (47_2), its p^n-th power, and its p^{2n}-th power yield three linear relations between $x^{p^{2n}}$, x^{p^n}, x, the determinant of whose coefficients is a power of L_2 times

(48) $$A Q_{21}^{p^{2n}-1} L_2^{rp^n} + B L_2^{r(p^{2n}-1)} + Q_{21}^{p^{2n}} L_3^r L_2^{p^{3n}-2p^n+1} - Q_{21}^{p^{2n}+2p^n} L_3^{rp^n} = 0,$$
$$A = L_3^{rp^n} Q_{21}^{p^n} + L_2^{p^{3n}-p^n}, \qquad B = L_3^{p^{2n}-1} + Q_{21}^{p^n} L_3^{rp^n} L_2^r.$$

We eliminate Q_{21} from A by means of (2_3), from B by means of (2_2):

$$A = Q_{31}^{p^n} L_2^{rp^n}, \qquad B = Q_{32} L_3^{rp^n} L_2^r.$$

Similarly, the last two terms of (48) equal

$$Q_{21}^{p^{2n}} \{ (L_3^r / L_2^r - Q_{32})(Q_{31}^{p^n} L_2^{rp^n} - L_2^{p^{3n}-p^n}) + L_3^r L_2^{p^{3n}-2p^n+1} \}$$
$$= Q_{21}^{p^{2n}} \{ L_3^r Q_{31}^{p^n} L_2^{r^2} + L_2^{rp^n} C \}, \qquad C \equiv Q_{32} L_2^{rp^{2n}} - Q_{32} Q_{31}^{p^n}.$$

In view of (2_3) the first term of the latter equals

$$Q_{21}^{p^{2n}-1} (Q_{31}^{p^n+1} L_2^{rp^n} - Q_{31}^{p^n} L_2^{2rp^n}).$$

The last term cancels the first term of (48). By (2_3),

$$C = - Q_{32} Q_{21}^{p^n} L_3^{rp^n} / L_2^{rp^n}.$$

* Semi-discriminant S_3 if $p = 2$, these Transactions, vol. 10 (1909), p. 134.

† The product of the second by L_2 is an identity in x, y, in view of (3).

Hence the new form of (48) is

$$L_2^{rp^{2n}} Q_{32} L_3^{rp^n} + Q_{21}^{p^{2n}-1} Q_{31}^{p^n+1} L_2^{rp^n} - Q_{32} Q_{21}^{p^{2n}+p^n} L_3^{rp^n} = 0.$$

The first and third terms equal $Q_{32} L_3^{rp^n} E^{p^n}$, where

$$E \equiv L_2^{rp^n} - Q_{21}^{p^n+1} = Q_{31} + Q_{32} L_2^{p^{2n}-1}/L_3^r - Q_{31} Q_{32} L_2^r/L_3^r,$$

in view of the product of $Q_{21}^{p^n}$ from (2_2) by Q_{21} from (2_3). Hence

$$(49) \quad Q_{21}^{p^{2n}-1} Q_{31}^{p^n+1} L_2^{rp^n} + L_3^{rp^n} Q_{31}^{p^n} Q_{32} + Q_{32}^{p^n+1} L_2^{p^{3n}-p^n} - Q_{31}^{p^n} Q_{32}^{p^n+1} L_2^{rp^n} = 0.$$

By eliminating Q_{21} between (2_2) and (2_3), we get

$$(50) \qquad L_2^{p^{3n}} - L_2^{p^{2n}} Q_{31}^{p^n} + L_2^r \; L_3^{rp^n} Q_{32} - L_2 L_3^{p^{2n}-1} = 0.$$

Multiply (49) by $L_2^{p^n}$ and eliminate $L_2^{p^{3n}}$ by (50). Then multiply by Q_{21}/L_2^r, replace Q_{21} by its value from (2_3), and $Q_{21}^{p^{2n}}$ by the p^n-th power of the value of $Q_{21}^{p^n}$ from (2_2). We get

$$(51) \quad \begin{aligned} &(Q_{31} - L_2^{rp^n})(Q_{31}^{p^n} Q_{32} L_2^{p^n} L_3^{rp^n} - L_2^{p^n} L_3^{rp^n} Q_{32}^{p^n+2} + L_2 L_3^{p^{2n}-1} Q_{32}^{p^n+1}) \\ &\qquad + L_3^r L_2^{p^{2n}-p^n+1} Q_{31}^{p^n+1} Q_{32}^{p^n} - L_2 L_3^{p^{2n}-1} Q_{31}^{p^n+1} = 0. \end{aligned}$$

Multiply (50) by $Q_{31} Q_{32}^{p^n+1} - Q_{31}^{p^n+1}$, add the result to (51); then divide by $L_2^{rp^n}$. We get

$$(52) \quad \begin{aligned} &L_2^{p^{3n}-p^{2n}+p^n}(Q_{31} Q_{32}^{p^n+1} - Q_{31}^{p^n+1}) + L_2^{p^n}[L_3^{rp^n} Q_{32}^{p^n+2} - L_3^{rp^n} Q_{31}^{p^n} Q_{32} \\ &\qquad - (Q_{31} Q_{32})^{p^n+1} + Q_{31}^{2p^n+1}] + L_2(L_3^r Q_{31}^{p^n+1} Q_{32}^{p^n} - L_3^{p^{2n}-1} Q_{32}^{p^n+1}) = 0. \end{aligned}$$

From the p^n-th power of (51) we eliminate $L_2^{p^{3n}}$ by (50) and obtain an equation involving the same three powers of L_2 as in (52). Eliminating the highest power of L_2 and dividing the resulting relation by $L_3^{rp^n}$, we obtain $FG = 0$, where

$$(53) \qquad F = L_2^{p^n}(Q_{31}^{p^n} - Q_{32}^{p^n+1}) + L_2 L_3^{p^n-1} Q_{32}^{p^n},$$

$$(54) \quad \begin{aligned} G = {} & L_3^{p^{3n}\cdot\, p^n} Q_{32}^e + L_3^{p^{3n}-p^{2n}}(Q_{31}^{p^{2n}+1} Q_{32}^{p^n+1} - Q_{31} Q_{32}^{e+p^n} - Q_{31}^e) \\ & - L_3^{p^{2n}-p^n} Q_{31}^{p^{2n}+p^n} Q_{32}^{p^{2n}+1} + Q_{31}^{e+p^n} Q_{32}^{p^{2n}} \end{aligned}$$

The factor F is extraneous, since it does not vanish for $x \neq 0$, t in the $GF[p^{2n}]$ but not in the $GF[p^n]$. Indeed, we then have

$$L_2 \neq 0, \; Q_{21} = 0, \; L_3 = 0, \; Q_{32} = 0, \; Q_{31} = L_2^{p^{2n}-p^n}, \; F = L_2^{p^{3n}-p^{2n}+p^n}.$$

Hence the desired invariant Q is a factor of G. Now

$$(55) \quad G = J_3(Q_{31}^{p^{2n}+p^n} Q_{32}^{p^{2n}+1} - L_3^{p^{3n}-p^{2n}} Q_{32}^e) + J_3^{p^n}(Q_{31}^e - Q_{31}^{p^{2n}+1} Q_{32}^{p^n+1}),$$

where J_3 is defined by (35). *The invariant Q equals G/J_3.* This follows from the facts that any ternary quadratic form T of non-vanishing discriminant (semi-discriminant, if $p = 2$) is equivalent (*Linear Groups*, p. 158, p. 197) under the total group G_3 to $c(y^2 - xz)$, and that the number of the forms T, no two with a constant ratio, is $N = p^{2n}(p^{3n} - 1)$, while the degree of Q is $2N$.

We may, however, give a direct proof that $Q = G/J_3$ and deduce the preceding facts as corollaries. This proof depends upon the fact that G/J_3 is not the product of two integral invariants of G_3. Since G/J_3 contains a term free of L_3, a factor f must contain such a term and hence be an absolute invariant of G_3. Hence the exponent of L_3 in each term of f is a multiple of $p^n - 1$. But the degrees of Q_{31} and Q_{32} are multiples of p^n. Hence the exponents of L_3 are multiples of $p^n(p^n - 1)$. Thus f is an integral function of J_3. By (35) and (55), we get

$$(55') \quad G/J_3 = Q_{31}^{p^n} Q_{32}^{p^{2n}+1} D^{p^n} + Q_{32}^e J_3^{p^n} + J_3^{p^n-1} Q_{31}^{p^{2n}+1} D, \qquad D \equiv Q_{31}^{p^n} - Q_{32}^{p^n+1}.$$

If this were reducible in J_3, then

$$(56) \qquad \sigma^{p^n} + \sigma Q_{31}^{p^{2n}} / Q_{32}^{p^{2n}+1} + Q_{32}^{p^n}$$

would be reducible in $\sigma = Q_{31} D/J_3$. But values of x, y, z may be found for which Q_{31} and Q_{32} take any assigned values (§ 8). Since the extraction of the p^n-th root is here uniquely possible, the coefficients of (56) may be given any assigned values. By § 13, values may be assigned such that (56) is the product of a linear and an irreducible factor of degree $p^n - 1$. Hence (55′) is either irreducible in its arguments or has a factor f_1 linear in J_3. Suppose the latter to be the case. The coefficient of J_3 is either 1 or Q_{32}^e in view of the part Q_{31}^e of the final term of (55′). If this coefficient is 1, the remaining terms of f_1 are of the same degree as J_3, so that

$$f_1 = J_3 - c Q_{31} Q_{32}^{p^n}.$$

But this is obviously not a factor of (55′). Next, for the factors

$$f_1 = Q_{32}^e J_3 + \lambda, \qquad J_3^{p^n-1} - c Q_{31} Q_{32}^{p^n} J_3^{p^n-2} + \cdots,$$

a comparison of the coefficient of $J_3^{p^n-1}$ of the product with that in (55′) gives

$$\lambda = c Q_{31} Q_{32}^{e+p^n} + Q_{31}^{p^{2n}+1} D.$$

Since λ contains the term Q_{31}^e, while e exceeds the exponent of Q_{31} in each part of the first term of (55′), f_1 is not a factor. Hence G/J_3 is not the product of two integral invariants of G_3 and thus equals Q.

It may happen that Q is the product of integral invariants of the subgroup G_3' of transformations of determinant unity, namely, that Q is a reducible in the arguments L_3, Q_{31}, Q_{32}. Since Q has a term involving only Q_{31} and Q_{32}, whose degrees are $\rho(p^n + 1)$ and ρp^n, where $\rho = p^n(p^n - 1)$, any factor f of Q is of degree a multiple of ρ. Thus the exponent a of L_3 in any term of f is such that ae is a multiple of ρ. The greatest common divisor of $e = p^{2n} + p^n + 1$ and ρ is 3 or 1 according as ρ^n is of the form $3l + 1$ or not. If $p^n \neq 3l + 1$, the exponent a of L_3 is a multiple of ρ, and f is a function of J_3; but Q was shown to be irreducible in J_3. Hence *if* $p^n \neq 3l+1$, *any ternary quadratic form of non-vanishing discriminant is equivalent under* G_3' *to* $c(y^2 - xz)$.

For $p^n = 3l + 1$, Q is the product of three integral functions of $L_3^{\rho/3}$. This is in agreement with the fact that the types are now

$$c(y^2 - kxz) \qquad (k = 1,\ \epsilon,\ \epsilon^2),$$

where ϵ is a fixed not-cube (for example, a primitive root), while no one of the three types is equivalent under G_3' to a constant multiple of another type.

21. **Theorem.** *If* α *is a primitive root of the* $GF[p^n]$, $p^n > 2$, *and* β *is any element, the function*

$$\Sigma = \sigma^{p^n} - \alpha\sigma + \beta$$

is the product of a linear and an irreducible function of degree $p^n - 1$.

Let ξ and η be two distinct roots of $\Sigma = 0$. Let $z = \xi - \eta$. Then

$$z^{p^n} = \alpha z, \qquad z^{p^{2n}} = \alpha z^{p^n} = \alpha^2 z, \ \cdots, \qquad z^{p^{kn}} = \alpha^k z.$$

Since α belongs to the exponent $p^n - 1$, z belongs to the $GF[p^{kn}]$ if $k = p^n - 1$, but not if k is smaller.

Suppose that Σ has a factor f of degree $d\,(d < p^n)$, irreducible in the $GF[p^n]$. The roots of $f = 0$ are ξ, ξ^{p^n}, $\xi^{p^{2n}}$, $\cdots$ and belong to the $GF[p^{dn}]$. The difference z of two of these roots is not zero and belongs to the latter field. Hence by the earlier result, $d = p^n - 1$.

For $p^n > 2$, we have $\alpha \neq 1$. But Σ vanishes if $\sigma = \beta/(\alpha - 1)$, an element of the $GF[p^n]$. Hence there is a linear factor.

For $p^n = 2$, the theorem holds for $\beta = 0$, but fails if $\beta = 1$.

22. We have determined the product Q of the distinct ternary quadratic forms not equivalent to a binary form, and the product J_3 of those equivalent to an irreducible binary form. A quadratic form equivalent to a reducible binary form is the product of two distinct linear forms; hence the product of all such ternary forms is $L_3^{p^{2n}+p^n}$. Finally, the product of the distinct quadratic forms equivalent to a unary form is L_3^2. Since $QJ_3 = G$, we conclude that the product of all distinct ternary quadratic forms is $GL_3^{p^{2n}+p^n+2}$. The degree of the latter product is $2(p^{6n} - 1)/(p^n - 1)$, as should be the case. The invariant G, given by (54), may be expressed as the following determinant:

$$(57) \qquad G = \begin{vmatrix} L_3^{p^{3n}-p^{2n}} & Q_{31} & 1 \\ L_3^{p^{3n}-p^{2n}} Q_{32}^{p^n+1} & L_3^{p^{2n}-p^n} Q_{32} & Q_{31}^{p^n} \\ Q_{31}^{p^{2n}+p^n} Q_{32}^{p^{2n}} & Q_{31}^{p^{2n}+1} & Q_{32}^{p^{2n}+p^n} \end{vmatrix}.$$

THE UNIVERSITY OF CHICAGO,
July, 1910.