INVARIANTS OF THE LINEAR GROUP MODULO p^k*

BY

M. M. FELDSTEIN

INTRODUCTION

Professor L. E. Dickson in his paper *A fundamental system of invariants of the general modular linear group with a solution of the form problem*† gave a fundamental system of invariants for the group of all linear homogeneous transformations in n variables with coefficients in the Galois field of order p^n, denoted by $GF[p^n]$.

Dr. J. S. Turner extended the results for the binary group in $GF[p]$ to the binary group H with coefficients ranging over integers modulo p^2 and the determinant of transformation congruent to unity modulo p^2.

This thesis deals with the invariants of the linear homogeneous group in n variables with the coefficients ranging over integers modulo p^k, and the determinant of transformation congruent to unity modulo p.

The writer avails himself of this occasion to express his gratitude to Professor Dickson for the conduct of this research and for suggesting both the problem and the group-theoretic principles applied in the following pages.

1. PRELIMINARY

We shall consider linear homogeneous transformations (T) in indeterminates $x_1, x_2, \ldots, x_n$ with integral coefficients and having determinant of transformation $\equiv 1 \pmod{p}$.

The above transformations will be applied to forms in $x_1, x_2, \ldots, x_n$ with integral coefficients.

Two forms F_1 and F_2 will be considered identically congruent modulo p^k if and only if

$$F_1(x_1, x_2, \ldots, x_n) \equiv F_2(x_1, x_2, \ldots, x_n) + p^k F_3(x_1, x_2, \ldots, x_n)$$

---

* Presented to the Society, April 13, 1923.

† These Transactions, vol. 12 (1911), pp. 75–98. Professor E. H. Moore constructed the invariant called L_n in the sequel.

algebraically, where F_3 is a form. The identity will be denoted by

$$F_1(x_1, x_2, \ldots, x_n) \equiv F_2(x_1, x_2, \ldots, x_n) \pmod{p^k}.$$

A formal invariant $F(x_1, x_2, \ldots, x_n)$ is a form which under all transformations

$$T: x_i = a_{i1}x_1' + a_{i2}x_2' + \cdots + a_{in}x_n' \qquad (i = 1, \ldots, n)$$

gives

$$F(x_1, x_2, \ldots, x_n) \equiv F(x_1', x_2', \ldots, x_n') \pmod{p^k},$$

after the new variables x_i' are replaced by their values in terms of the old variables obtained by solving the above n equations.

Two substitutions whose corresponding coefficients are congruent modulo p^k replace any form by two forms which are identically congruent, and which therefore play equivalent rôles in the theory of modular invariants. Accordingly, we shall say that two such substitutions belong to the same class.

In the sequel, for purposes of enumeration, we shall frequently represent a class by a "residual matrix" whose elements are least positive residues modulo p^k.

The classes of transformations can be put into one-to-one correspondence with the system of residual matrices, since to the compound of two classes corresponds the compound modulo p^k of the respective residual matrices.

The classes of substitutions T form a finite group; therefore the system of residual matrices forms a finite group of the same order under composition modulo p^k.

2. Group-theoretic introduction

Let $G(n, p^k)$ be the total linear homogeneous group in n indeterminates with coefficients modulo p^k. Then the system of residual matrices may be represented by

$$\| a_{ij} + \alpha_{ij}^{(1)}p + \alpha_{ij}^{(2)}p^2 + \cdots + \alpha_{ij}^{(k-1)}p^{k-1} \| \qquad (i, j = 1, \ldots, n)$$

where the determinant of $\|a_{ij}\|$ is $\equiv 1 \pmod{p}$ and the elements $a_{ij}, \alpha_{ij}^{(1)}, \ldots, \alpha_{ij}^{(k-1)}$ range independently over the integers $0, 1, 2, \ldots, p-1$.

There are* $d = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})(p^n-p^{n-1})/(p-1)(p-1)$ sets of solutions of the determinantal congruence $|a_{ij}| \equiv 1 \pmod{p}$,

* L. E. Dickson, *Linear Groups*, p. 82.

and with every set we can associate $P = p^{n^2(k-1)}$ sets $\alpha_{ij}^{(1)}, \alpha_{ij}^{(2)}, \ldots, \alpha_{ij}^{(k-1)}$. Therefore the order of the group $G(n, p^k)$ is dP.

In the sequel we shall consider two ways of decomposing $G(n, p^k)$ into a factor-group.

(1) Dividing every element in the matrices of the residual system by p, we obtain them in the form

$$\| b_{ij} + \beta_{ij} p \| \quad (i, j = 1, \ldots, n), \qquad |b_{ij}| \equiv 1 \pmod{p},$$

where b_{ij} ranges over the integers $0, 1, 2, \ldots, p-1$, and β_{ij} ranges over the integers $0, 1, 2, \ldots, p^{k-1}-1$.

The set of matrices $\| b_{ij} \|$ we shall denote by

$$H_1 \equiv (h_1, h_2, \ldots, h_m, \ldots, h_d).$$

The invariant subgroup of matrices $\| \beta_{ij} p \|$, with 1 added to the elements of the diagonal, we shall denote by

$$A_1 \equiv (a_1, a_2, \ldots, a_m, \ldots, a_P).$$

The group $G(n, p^k)$ may be decomposed into a factor-group of order d:

$$A_1 h_1, A_1 h_2, \ldots, A_1 h_m, \ldots, A_1 h_d.$$

The decomposition is exhaustive since no matrix of the subgroup A_1 is present in H_1, with the exception of the unit matrix, and the order of the subgroup A_1 multiplied by the number of matrices in H_1 gives the order of the group $G(n, p^k)$.

(2) Dividing every element in the matrices of the residual system by p^{k-1}, we obtain them in the form

$$\| c_{ij} + \gamma_{ij} p^{k-1} \| \quad (i, j = 1, \ldots, n), \qquad |c_{ij}| \equiv 1 \pmod{p},$$

where c_{ij} ranges over the integers $0, 1, 2, \ldots, p^{k-1}-1$, and γ_{ij} ranges over the integers $0, 1, 2, \ldots, p-1$.

The set of matrices $\| c_{ij} \|$ we shall denote by

$$H_{k-1} \equiv (h_1', h_2', \ldots, h_m', \ldots, h_\varkappa'), \qquad \varkappa = dp^{n^2(k-2)}.$$

The invariant abelian subgroup of matrices, $\|\gamma_{ij}p^{k-1}\|$, with 1 added to the elements of the diagonal, we shall denote by

$$A_{k-1} \equiv (a'_1, a'_2, \ldots, a'_m, \ldots, a'_{p^{n^2}}).$$

The group $G(n, p^k)$ may be decomposed into the factor-group

$$A_{k-1}h'_1, A_{k-1}h'_2, \ldots, A_{k-1}h'_m, \ldots, A_{k-1}h'_\varkappa, \qquad \varkappa = dp^{n^2(k-2)},$$

the exhaustiveness of the decomposition being proved as in (1), mutatis mutandis.

3. The invariants of the group $G(n, p^2)$

In this case the groups A_1 and A_{k-1}, and the sets H_1 and H_{k-1} coincide.

A comparison of the set H with the matrices of the group $G(n, p)$ shows that H has representatives of all the classes comprised by $G(n, p)$. Therefore the invariants of $G(n, p^2)$ may be put into the form

$$F(x_1, x_2, \ldots, x_n) + pF_1(x_1, x_2, \ldots, x_n), \tag{1}$$

where $F(x_1, x_2, \ldots, x_n)$ is an invariant of $G(n, p)$ and $F_1(x_1, x_2, \ldots, x_n)$ is some form.

As a preliminary step we shall inquire as to the conditions under which expressions of the type (1) are invariant under the sets of the factor-group

$$Ah_1, Ah_2, \ldots, Ah_m, \ldots, Ah_d.$$

Evidently (1) has to be invariant under the subgroup A.

Consider a general substitution of the subgroup A,

$$x'_i = x_i + p(\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n) \qquad (i = 1, \ldots, n).$$

On applying it to (1) we observe that $pF_1(x_1, x_2, \ldots, x_n)$ remains invariant under the transformation, because of the factor p. Therefore $F(x_1, x_2, \ldots, x_n)$ should be invariant under the subgroup A.

Applying the substitution to F by means of Taylor's expansion, we obtain

$$F(x_1', x_2', \ldots, x_n') \equiv F(x_1, x_2, \ldots, x_n) + p\sum_{i=1}^{n}(\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n)\frac{\partial F}{\partial x_i} \equiv 0 \pmod{p^2}.$$

($G(n, 2^2)$ is treated in Section 5.) This shows that F will be an invariant if the following congruence holds:

$$\sum_{i=1}^{n}(\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in})\frac{\partial F}{\partial x_i} \equiv 0 \pmod{p}.$$

By taking $\alpha_{ii} = 1$ and the remaining $\alpha_{ij} = 0$, we get

$$x_i\frac{\partial F}{\partial x_i} \equiv 0 \pmod{p} \qquad (i = 1, \ldots, n),$$

whence we obtain the differential congruences, giving the necessary and sufficient conditions for invariance under A:

$$\frac{\partial F}{\partial x_1} \equiv \frac{\partial F}{\partial x_2} \equiv \cdots \equiv \frac{\partial F}{\partial x_n} \equiv 0 \pmod{p}. \tag{2}$$

Before proceeding with the application of conditions (2), we shall have need of more detailed information* as to the structure of the invariants of $G(n, p)$.

If we define

$$[e_1, e_2, \ldots, e_n] = \begin{vmatrix} x_1^{p^{e_1}} & x_2^{p^{e_1}} & \cdots & x_n^{p^{e_1}} \\ x_1^{p^{e_2}} & x_2^{p^{e_2}} & \cdots & x_n^{p^{e_2}} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ x_1^{p^{e_n}} & x_2^{p^{e_n}} & \cdots & x_n^{p^{e_n}} \end{vmatrix}$$

* L. E. Dickson, *A fundamental system of invariants*, these Transactions, vol. 12 (1911), p. 76.

then a fundamental system of invariants of $G(n,p)$ is given by the following set:

$$L_n = [n-1, n-2, \ldots, 1, 0],$$
$$Q_{ns} = \frac{[n, n-1, \ldots, s+1, s-1, \ldots, 1, 0]}{L_n} \qquad (s = 1, \ldots, n-1).$$

These invariants in terms of the invariants of $G(n-1,p)$ and L_n may be written

$$Q_{n1} = Q_{n-11}\left(\frac{L_n}{L_{n-1}}\right)^{p-1} + L_{n-1}^{p^2-p},$$
$$Q_{ns} = Q_{n-1s}\left(\frac{L_n}{L_{n-1}}\right)^{p-1} + Q_{n-1s-1}^{p} \qquad (s = 2, \ldots, n-2),$$
(3)
$$Q_{nn-1} = \left(\frac{L_n}{L_{n-1}}\right)^{p-1} + Q_{n-1n-2}^{p},$$
$$L_n = x_n L_{n-1}^{p} + L_{n-1}\sum_{s=1}^{n-2}(-1)^s x_n^{p^s} Q_{n-1s} + (-1)^{n-1} x_n^{p^{n-1}} L_{n-1}.$$

LEMMA. *No syzygy subsists among the invariants of $G(2,p)$, either algebraically or in the sense of a congruence.*

Assume the contrary, and arrange the polynomial in L_2 and Q_2 according to descending powers of Q_2; then we have

$$c_1 Q_2^{i_1} L_2^{j_1} + c_2 Q_2^{i_2} L^{j_2} + \cdots + c_m Q_2^{i_m} L_2^{j_m} = 0.$$

Here $c_1 Q_2^{i_1} L_2^{j_1}$ contains the highest power of x_1, for Q_2 contains a power of x_1 as a term, whereas L_2 contains only terms of the form $x_1^a x_2^b$. Therefore either the coefficients $c_1 = c_2 = \cdots = c_m = 0$, if we speak of an algebraic syzygy, or $c_1 \equiv c_2 \equiv \cdots \equiv c_m \equiv 0 \pmod{p^k}$, if we speak of it in the sense of a congruence.

THEOREM I.* *The invariants of $G(n,p)$ are not connected by a syzygy modulo p^k.*

Let the syzygy connecting the invariants be arranged according to powers of L_n:

$$\sum_m L_n^m \sum_{q_m} c_{q_m} \prod_{s=1}^{n-1} Q_{ns}^{a_{sq_m}} \equiv 0, \qquad c_{q_m} \not\equiv 0 \pmod{p^k}. \tag{4}$$

* Compare loc. cit., p. 83.

If m_0 is the lowest power of L_n in the above polynomial, we divide (4) by $L_n^{m_0}$ and obtain a sum of products not containing L_n as a factor:

$$\sum_{q_m} c_{q_m} \prod_{s=1}^{n-1} Q_{ns}^{a_{sq_m}} \text{ for } m = m_0. \tag{5}$$

All those terms which have L_n as a factor contain x_n, but (5) contains terms free of x_n whose sum therefore must be congruent to zero modulo p^k.

A reference to the preceding page shows that we obtain these terms by performing the substitution

$$S = \begin{pmatrix} Q_{n1} & Q_{n2} & \cdots & Q_{ns} & \cdots & Q_{nn-1} \\ L_{n-1}^{p^2-p} & Q_{n-11}^{p} & \cdots & Q_{n-1s-1}^{p} & \cdots & Q_{n-1n-2}^{p} \end{pmatrix}, \tag{6}$$

where distinct elements are replaced by distinct elements.

We obtain, therefore,

$$\sum_{q_m} c_{q_m} L_{n-1}^{(p^2-p)a_{1q_m}} \prod_{s=2}^{n-1} Q_{n-1s-1}^{pa_{sq_m}} \equiv 0 \pmod{p^k} \text{ for } m = m_0. \tag{7}$$

Since the products under the summation are formally distinct, (7) is a syzygy among the invariants of $G(n-1, p)$; this completes the induction, since by the lemma there is no syzygy connecting the invariants of $G(2, p)$.

THEOREM II. *Any form written as a polynomial in L_n and Q_{ns} $(s = 1, 2, \ldots, n-1)$, satisfying the differential congruences (3), and not containing coefficients congruent to zero modulo p, involves L_n and Q_{ns} to powers whose exponents are multiples of p.*

Let

$$F(x_1, x_2, \ldots, x_n) \equiv \sum_m L_n^m \sum_{q_m} c_{q_m} \prod_{s=1}^{n-1} Q_{ns}^{a_{sq_m}},\ c_{q_m} = 0 \pmod{p}. \tag{8}$$

We shall first prove that $m \equiv 0 \pmod{p}$. By Euler's formula, we have

$$x_1 \frac{\partial F}{\partial x_1} + x_2 \frac{\partial F}{\partial x_2} + \cdots + x_n \frac{\partial F}{\partial x_n} \equiv dF(x_1, x_2, \ldots, x_n) \pmod{p},$$

where d is the degree of the form F. Now since the left member is congruent to zero modulo p by (3), d must be divisible by p.

But

$$d \equiv m(p^{n-1}+\cdots+p+1)+\sum_{s=1}^{n-1} a_{sq_m}(p^n-p^s) \equiv 0 \pmod{p},$$

and since $\sum_{s=1}^{n-1} a_{sq_m}(p^n-p^s) \equiv 0 \pmod{p}$, m is divisible by p, whence $\frac{\partial F}{\partial L_n} \equiv 0 \pmod{p}$. Thus shall

$$\frac{\partial F}{\partial x_n} \equiv \frac{\partial F}{\partial L_n}\frac{\partial L_n}{\partial x_n}+\sum_{s=1}^{n-1}\frac{\partial F}{\partial Q_{ns}}\frac{\partial Q_{ns}}{\partial x_n} \equiv 0 \pmod{p}.$$

By the preceding, $\frac{\partial F}{\partial L_n} \equiv 0 \pmod{p}$, therefore it remains to consider

$$\sum_{s=1}^{n-1}\frac{\partial F}{\partial Q_{ns}}\frac{\partial Q_{ns}}{\partial x_n} \equiv 0 \pmod{p}. \tag{9}$$

Arranging it according to powers of L_n, we obtain

$$\frac{\partial F}{\partial x_n} \equiv \sum_m L_n^m \sum_{q_m} c_{q_m}\frac{\partial}{\partial x_n}\prod_{s=1}^{n-1} Q_{ns}^{a_{sq_m}} \equiv \Big(\sum_m L_n^m B_m\Big) C \equiv 0 \pmod{p},$$

where, for brevity,

$$B_m \equiv \sum_{q_m} c_{q_m}\left(\sum_{i=1}^{n-2} a_{iq_m} Q_{n-1\,i}\, Q_{ni}^{a_{iq_m}-1}\prod_{\substack{s=1\\ s\neq i}}^{n-1} Q_{ns}^{a_{sq_m}} + a_{n-1\,q_m} Q_{n\,n-1}^{a_{n-1\,q_m}-1}\prod_{s=1}^{n-2} Q_{ns}^{a_{sq_m}}\right)$$

$$C \equiv \frac{\partial\left(\frac{L_n}{L_{n-1}}\right)^{p-1}}{\partial x_n},$$

as follows by the use of (3).

Since by computation $C \not\equiv 0 \pmod{p}$, $\sum_m L_n^m B_m$ must be zero modulo p. Dividing it by the lowest power of L_n occurring there, i. e., with exponent $m = m_0$, we obtain a sum of products not containing L_n as a factor, i.e., B_{m_0}. B_{m_0} is the only part of $\dfrac{\sum_m L_n^m B_m}{L_n^{m_0}}$ free of the factor L_n. Now L_n itself contains x_n as a factor, therefore the only terms free of x_n are obtainable from B_{m_0}, and their sum should be congruent to zero modulo p.

We obtain this sum by performing substitution S (formula (6)) on B_{m_0}:

$$\sum_{q_m} c_{q_m} \left(\sum_{i=1}^{n-2} a_{iq_m} Q_{n-1\,i} Q_{n-1\,i-1}^{p(a_{iq_m}-1)} L_{n-1}^{(p^2-p)a_{iq_m}} \prod_{\substack{s=2 \\ s \neq i}}^{n-1} Q_{n-1\,s-1}^{pa_{sq_m}} \right.$$

$$\left. + a_{n-1\,q_m} Q_{n-1\,n-2}^{p(a_{n-1\,q_m}-1)} L_{n-1}^{(p^2-p)a_{1q_m}} \prod_{s=2}^{n-2} Q_{n-1\,s-1}^{pa_{sq_m}} \right) \equiv 0$$

$$(m = m_0) \pmod{p}.$$

Examining the products under the inner summation, we observe that they are distinct. In the ith product all the factors have as exponents multiples of p with the exception of $Q_{n-1\,i}$ which occurs raised to the $(pa_{sq_m}+1)$th power. The last product is the only product for a given q_m having all exponents of the factors multiples of p.

We thus see that the products arising from the differentiation of a certain $c_{q_m} \prod_{s=1}^{n-1} Q_{ns}^{a_{sq_m}} (m = m_0)$ in (8) are all distinct.

Two distinct products, as

$$c_{q_{1m}} \prod_{s=1}^{n-1} Q_{ns}^{a_{sq_{1m}}} \text{ and } c_{q_{2m}} \prod_{s=1}^{n-1} Q_{ns}^{a_{sq_{2m}}} \qquad (m = m_0),$$

could not give identical products on differentiation. An examination of the exponents would indicate that both were differentiated with respect to the same Q_{ns}, from the argument above. A substitution inverse to S (formula (6)) would lead to the same derivatives, and then we should arrive at the same primitives. The process is uniquely reversible.

All the products in the above are distinct and have as factors invariants of $G(n-1,p)$. But since no syzygy exists by the preceding theorem, the exponents appearing as coefficients $a_{sq_m}(m = m_0;\ s = 1, \ldots, n-1;$ for all $q_{m_0})$, are separately congruent to zero modulo p.

We can therefore divide by the next highest power of L_n, say $L_n^{m_1}$, and repeat the argument verbatim.

Therefore the a_{sq_m} are multiples of p for all s and q_m.

We thus see that $F(x_1, x_2, \ldots, x_n)$ must be a polynomial in L_n^p and Q_{ns}^p $(s = 1, \ldots, n-1)$ in order to be invariant under A. But this is also a sufficient condition for invariance under $G(n,p^2)$. Taking for example L_n^p and applying to it any substitutions of $G(n,p^2)$, we get

$$L_n^p(x_1', x_2', \ldots, x_n') \equiv (L_n(x_1, x_2, \ldots, x_n) + pf(x_1, x_2, \ldots, x_n))^p$$

$$\equiv L_n^p(x_1, x_2, \ldots, x_n) \pmod{p^2},$$

where $f(x_1, x_2, \ldots, x_n)$ is some form.

Since $F(x_1, x_2, \ldots, x_n)$ is an invariant of $G(n,p^2)$, $pF_1(x_1, x_2, \ldots, x_n)$ must also be invariant under the group. However, operation upon a form pf with $G(n,p^2)$ is equivalent to operation upon f with $G(n,p)$, therefore $F_1(x_1, x_2, \ldots, x_n)$ must be a polynomial in L_n and $Q_{ns}(s = 1, \ldots, n-1)$.

We thus arrive at a fundamental system of invariants of the group $G(n,p^2)$, viz.,

$$L_n^p, \qquad Q_{ns}^p \quad (s = 1, \ldots, n-1), \qquad pL_n^a \prod_{s=1}^{n-1} Q_{ns}^{b_s},$$

where a and b_s may assume values from 0 to $p-1$, but may not all be zero.

4. Invariants of the group $G(n,p^k)$

A comparison of the matrices of the set H_{k-1} with those of the group $G(n,p^{k-1})$, shows that H_{k-1} has representatives of all the classes contained in $G(n,p^{k-1})$. Therefore the invariants of $G(n,p^k)$ may be put into form

$$P(x_1, x_2, \ldots, x_n) + p^{k-1}f(x_1, x_2, \ldots, x_n) \tag{1}$$

where $P(x_1, x_2, \ldots, x_n)$ is an invariant of $G(n, p^{k-1})$ and $f(x_1, x_2, \ldots, x_n)$ is some form.

We shall next investigate the form of expressions (1) which remain invariant under the sets of the factor-group

$$A_1 h_1,\ A_1 h_2,\ \ldots,\ A_1 h_m,\ \ldots,\ A_1 h_d,$$

d having the value indicated in Section 2.

Evidently they have to be invariant under the transformations of the invariant subgroup A_1.

A general substitution T_a of A_1 may be written

$$x_i' = x_i + p(\alpha_{i1} x_1 + \alpha_{i2} x_2 + \cdots + \alpha_{in} x_n) \qquad (i = 1, \ldots, n).$$

We have to apply the substitution only to $P(x_1, x_2, \ldots, x_n)$, since $p^{k-1} f(x_1, x_2, \ldots, x_n)$ is invariant under the subgroup A_1.

Since $P(x_1, x_2, \ldots, x_n)$ is an invariant of $G(n, p^{k-1})$, we shall assume, for purposes of induction, that it may be written in the form

$$(2) \qquad P(x_1, x_2, \ldots, x_n) \equiv F_0 + pF_1 + p^2 F_2 + \cdots + p^{k-2} F_{k-2}$$

where

$$(3) \qquad F_j \text{ is a polynomial in } Q_{ns}^{p^{k-j-2}},\ L^{p^{k-j-2}} \qquad \begin{matrix}(s = 1, \ldots, n-1)\\ (j = 0, \ldots, k-2)\end{matrix}$$

not involving coefficients congruent to zero modulo p.

From (3) it is clear that

$$(4) \qquad \frac{\partial F_j}{\partial x_i} \equiv \frac{\partial F_j}{\partial L_n}\frac{\partial L_n}{\partial x_i} + \sum_{s=1}^{n-1} \frac{\partial F_j}{\partial Q_{ns}}\frac{\partial Q_{ns}}{\partial x_i} \equiv 0 \pmod{p^{k-j-2}}$$
$$(j = 0, \ldots, k-2).$$

Also it is obvious that for the case of polynomials with integral exponents

$$\frac{\partial F_j}{\partial x_i} \equiv 0 \pmod{p^{k-j-2}} \text{ implies } \frac{\partial^r F_j}{\partial x_i^r} \equiv 0 \pmod{p^{k-j-2}}.$$

The application of T_a to $P(x_1, x_2, \ldots, x_n)$ gives by Taylor's expansion

$$(5)\quad P(x_1', x_2', \ldots, x_n') \equiv P(x_1, x_2, \ldots, x_n) + \frac{1}{r!}\sum_{r=1}^{m}\sum_{j=0}^{k-2} p^{j+r}\left[\sum_{i=1}^{n}(\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n)\frac{\partial F_j}{\partial x_i}\right]^r,$$

r having the usual symbolical significance as a power, and m being the highest degree in any one variable of the polynomial of the highest order.

Since $F_j (j = 0, \ldots, k-2)$ are polynomials, the coefficients of the expansions are integers.

Now by (4), since $\frac{\partial F_j}{\partial x_i} \equiv 0 \pmod{p^{k-j-2}}$, we see that

$$(6)\quad \frac{1}{r!}\sum_{r=2}^{m}\sum_{j=0}^{k-2} p^{j+r}\left(\sum_{i=1}^{n}(\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n)\frac{\partial F_j}{\partial x_i}\right)^r \equiv 0 \pmod{p^k}$$

for all odd primes. The case $p = 2$ will be considered separately.

From (5) and (6) it follows that $P(x_1, x_2, \ldots, x_n)$ will be an invariant of subgroup A_1 if

$$\sum_{j=0}^{k-2}\sum_{i=1}^{n} p^{j+1}(\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n)\frac{\partial F_j}{\partial x_i} \equiv 0 \pmod{p^k}.$$

By taking $\alpha_{ii} = 1$ and the remaining $\alpha_{ij} = 0$, we obtain the equivalent set of n differential congruences

$$(7)\quad \sum_{j=0}^{k-2} p^{j+1}\frac{\partial F_j}{\partial x_i} \equiv 0 \pmod{p^k} \qquad (i = 1, \ldots, n).$$

We shall obtain now additional information about $P(x_1, x_2, \ldots, x_n)$ from the consideration of its homogeneity in $x_1, x_2, \ldots, x_n$.

If the power of L_n and Q_{ns} in any one term of F_j be $a_j p^{k-j-2}$ and $b_{js} p^{k-j-2}$, by recalling that the degree of L_n is $(p^{n-1} + \cdots + p + 1)$ and that of Q_{ns} is $(p^n - p^s)$, we obtain the following set of equations:

$$a_0 p^{k-2}(p^{n-1}+\cdots+p+1)+\sum_{s=1}^{n-1} b_{0s} p^{k-2}(p^n-p^s)$$

$$= a_1 p^{k-3}(p^{n-1}+\cdots+p+1)+\sum_{s=1}^{n-1} b_{1s} p^{k-3}(p^n-p^s)$$

$$= \cdots\cdots$$

$$= a_{k-2}(p^{n-1}+\cdots+p+1)+\sum_{s=1}^{n-1} b_{k-2s}(p^n-p^s),$$

from which it follows that

$$a_1 \equiv a_2 \equiv \cdots \equiv a_{k-2} \equiv 0 \pmod{p}.$$

LEMMA 1. *In this way we see that L_n occurs in F_j $(j=1, \ldots, k-2)$ raised to powers which are multiples of p^{k-j-1}, and therefore*

$$\sum_{j=1}^{k-2} p^{j+1} \frac{\partial F_j}{\partial L_n} \equiv 0 \pmod{p^k}.$$

This considerably simplifies the differential congruences (7), which we shall write as follows:

$$(8)\quad p\frac{\partial F_0}{\partial L_n}\frac{\partial L_n}{\partial x_i}+\sum_{j=0}^{k-2}\sum_{s=1}^{n-1} p^{j+1}\frac{\partial F_j}{\partial Q_{ns}}\frac{\partial Q_{ns}}{\partial x_i} \equiv 0 \pmod{p^k} \quad (i=1,\ldots,n).$$

Multiplying the ith congruence by x_i, adding, and applying Euler's formula for homogeneous functions, we obtain from (8)

$$p\frac{\partial F_0}{\partial L_n} L_n \equiv 0 \pmod{p^k},$$

since the degree of Q_{ns} is divisible by p.

LEMMA 2. *By the proof of Theorem* I, *this shows that L_n occurs in F_0 raised to powers which are multiples of p^{k-1}.*

From the preceding result, we obtain (8) in the following simplified form:

$$(9) \qquad \sum_{j=0}^{k-2} \sum_{s=1}^{n-1} p^{j+1} \frac{\partial F_j}{\partial Q_{ns}} \frac{\partial Q_{ns}}{\partial x_i} \equiv 0 \pmod{p^k} \qquad (i = 1, \ldots, n).$$

We shall confine our attention to the nth congruence and prove that Q_{ns} $(s = 1, \ldots, n-1)$ must appear in F_j with an exponent which is congruent to zero modulo p^{k-j-1}.

The proof of Theorem II from the point where the differential congruence is simplified to the form (9) allows us to state the following theorem without proof:

THEOREM III. *The polynomial* $\sum_{j=0}^{k-2} F_j$, *defined by* (3), *Section* 4, *satisfying the congruence*

$$\sum_{j=0}^{k-2} \sum_{s=1}^{n-1} p^{j+1} \frac{\partial F_j}{\partial Q_{ns}} \frac{\partial Q_{ns}}{\partial x_n} \equiv 0 \pmod{p_k}$$

involves Q_{ns} $(s = 1, \ldots, n-1)$ *raised to powers which are multiples of* p.

But this will give $\sum_{s=1}^{n-1} p^{k-1} \frac{\partial F_{k-2}}{\partial Q_{ns}} \equiv 0 \pmod{p^k}$, and enable us to restate Theorem III in the following way:

The polynomial $\sum_{j=0}^{k-3} F_j$, *defined by* (3), *Section* 4, *satisfying the congruence*

$$\sum_{j=0}^{k-3} \sum_{s=1}^{n-1} p^{j+1} \frac{\partial F_j}{\partial Q_{ns}} \frac{\partial Q_{ns}}{\partial x_n} \equiv 0 \pmod{p_k}$$

involves Q_{ns} $(s = 1, \ldots, n-1)$ *raised to powers which are multiples of* p^2.

This theorem in its turn will yield the result

$$\sum_{s=1}^{n-1} p^{k-2} \frac{\partial F_{k-3}}{\partial Q_{ns}} \equiv 0 \pmod{p^k}.$$

Proceeding in this way we arrive at the result that F_j involves Q_{ns} $(s = 1, \ldots, n-1)$ raised to powers which are congruent to zero modulo p^{k-j-1}.

Collecting results, we obtain from Lemmas 1, 2, Theorem III and sequel, that F_j is a polynomial in $L_n^{p^{k-j-1}}$ and $Q_{ns}^{p^{k-j-1}}$

Conversely, exactly as at the conclusion of Section 3, we can prove that $p^j L_n^{p^{k-j-1}}$ and $p^j Q_{ns}^{p^{k-j-1}}$ $(s = 1, \ldots, n-1)$, for $j = 0, \ldots, k-1$, are invariants of the group $G(n, p^k)$.

Thus a fundamental system of invariants of group $G(n, p^k)$ is given by the following set:

$$L_n^{p^{k-1}},\ Q_{ns}^{p^{k-1}}\ (s = 1, \ldots, n-1),\ p^j L_n^{ap^{k-j-1}} \prod_{s=1}^{n-1} Q_{ns}^{b_s p^{k-j-1}} \quad (j = 1, \ldots, k-1),$$

where a and b_s range over $0, 1, \ldots, p-1$, but may not all be zero.

5. Invariants of the group $G(n, 2^k)$

In this case, which was not considered in Section 4, but was alluded to in connection with congruence (6), the condition for invariance under the subgroup A_1 takes the form

$$\sum_{j=0}^{k-2} 2^{j+1} \sum_{i=1}^{n} (\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n) \frac{\partial F_j}{\partial x_i} + \sum_{j=0}^{k-2} 2^{j+1} \left[\sum_{i=1}^{n} (\alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{in}x_n) \frac{\partial F_j}{\partial x_i} \right]^2 \equiv 0 \pmod{2^k}.$$

By taking $\alpha_{ii} = 1$ and the remaining $\alpha_{ij} = 0$, the above simplifies into n congruences,

$$(1) \qquad \sum_{j=0}^{k-2} 2^{j+1} \frac{\partial F_j}{\partial x_i} + \sum_{j=0}^{k-2} 2^{j+1} x_i \frac{\partial^2 F_j}{\partial x_i^2} \equiv 0 \pmod{2^k} \qquad (i = 1, \ldots, n),$$

by dividing each congruence by x_i.

If we employ the following sets of values for α_{ij}, $\alpha_{kk+1} = 1$ and the remaining $\alpha_{ij} = 0$ (the subscripts being taken modulo n), we obtain, by dividing through respectively by $x_2, x_3, \ldots, x_n, x_1$, the n congruences

$$(2) \qquad \sum_{j=0}^{k-2} 2^{j+1} \frac{\partial F_j}{\partial x_i} + \sum_{j=0}^{k-2} 2^{j+1} x_{i+1} \frac{\partial^2 F_j}{\partial x_i^2} \equiv 0 \pmod{2^k} \qquad (i = 1, \ldots, n),$$

where the subscript of x_{i+1} in the second term is taken modulo n.

By subtracting the ith congruence of (2) from the ith congruence of (1), we obtain the n relations

$$(x_i - x_{i+1}) \sum_{j=0}^{k-2} 2^{j+1} \frac{\partial^2 F_j}{\partial x_i^2} \equiv 0 \pmod{2^k} \qquad (i = 1, \ldots, n).$$

Since $x_i - x_{i+1} \not\equiv 0 \pmod{2^k}$, we must have

$$\sum_{j=0}^{k-2} 2^{j+1} \frac{\partial^2 F_j}{\partial x_i^2} \equiv 0 \pmod{2^k} \qquad (i = 1, \ldots, n). \tag{3}$$

The congruential identities (3) when substituted in (1) give

$$\sum_{j=0}^{k-2} 2^{j+1} \frac{\partial F_j}{\partial x_i} \equiv 0 \pmod{2^k} \qquad (i = 1, \ldots, n).$$

i. e., exactly the results (7) Section 4 for modulus 2^k.

Therefore all the conclusions arrived at in Section 4 for powers of odd prime moduli hold for 2^k.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.