INVARIANTS OF THE LINEAR GROUP MODULO $\pi = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$*

BY

CORNELIUS GOUWENS

1. Introduction

The object of this paper is to obtain a fundamental system of polynomial invariants with integral coefficients of the linear group in q variables with respect to an arbitrary modulus π.

For the case in which π is a prime p_i Dickson† proved that a fundamental system is given by

$$L_{i,q}, \qquad Q_{i,q,s} \qquad (s = 1, \cdots, q-1)$$

where

$$L_{i,q} = \begin{vmatrix} x_1^{p_i^{q-1}} & \cdots & x_q^{p_i^{q-1}} \\ x_1^{p_i^{q-2}} & \cdots & x_q^{p_i^{q-2}} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ x_1^{p_i} & \cdots & x_q^{p_i} \\ x_1 & \cdots & x_q \end{vmatrix}, \qquad Q_{i,q,s} = \begin{vmatrix} x_1^{p_i^{q}} & \cdots & x_q^{p_i^{q}} \\ \cdot & \cdot & \cdot \\ x_1^{p_i^{s+1}} & \cdots & x_q^{p_i^{s+1}} \\ x_1^{p_i^{s-1}} & \cdots & x_q^{p_i^{s-1}} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ x_1 & \cdots & x_q \end{vmatrix} \div L_{i,q}.$$

Mrs. Ballantine‡ proved that for $\pi = p_1 p_2 \cdots p_n$, $q = 2$, every invariant is of the form

$$\sum_{i=1}^{n} k_i \frac{\pi}{p_i} \varphi_i(L_{i,q}, Q_{i,q,s})$$

where k_i is an integer and φ_i is a polynomial with integral coefficients.

Feldstein§ proved that for $\pi = p_i^{\lambda_i}$ a fundamental system is given by

$$L_{i,q}^{p_i^{\lambda_i-1}}, \quad Q_{i,q,s}^{p_i^{\lambda_i-1}} (s = 1, \cdots, q-1), \quad R_{i,q,a,b,j} = p_i^j L_{i,q}^{a p_i^{\lambda_i-j-1}} \prod_{s=1}^{q-1} Q_{i,q,s}^{b_s p_i^{\lambda_i-j-1}}$$
$$(j = 1, \cdots, \lambda_i - 1),$$

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

* Presented to the Society, April 19, 1924.

† *Madison Colloquium Lectures*, p. 39.

‡ American Journal of Mathematics, vol. 45 (1923), pp. 286 ff.

§ These Transactions, vol. 25 (1923), pp. 223 ff. The notation $R_{i,q,a,b,j}$ was introduced by the present writer.

In the present paper it is shown that the method of Mrs. Ballantine can be extended from 2 to q variables. After a simplification of that method which enables us to avoid the use of the actual coefficients of the transformation employed the conclusion reached is the theorem

Every invariant of the group Γ of classes of transformations with determinant congruent to unity, modulo $\pi = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, is a sum of invariants of Γ, modulo π, each of which is expressible as a product of $m_i = \pi/p_i^{\lambda_i}$ by an invariant of the group H_i of classes of transformations congruent to unity, modulo $p_i^{\lambda_i}$, and conversely, every such product is an invariant of Γ.

2. The groups Γ, G_i, H_i

We call two linear transformations congruent modulo π if their corresponding coefficients are congruent. All transformations congruent to a chosen one T, modulo π, are said to form a class $[T]_\pi$. The classes $[T]_\pi$ with determinant $|T| \equiv 1 \pmod{\pi}$ are the elements of a group Γ.

Let p_i be a prime factor of π and let $P = p_i^{\lambda_i}$ be the highest power of p_i which divides π. Write $\pi = m_i P$. Let G_i denote the subgroup formed of those classes of transformations of Γ which are congruent modulo m_i to the identity transformation I. Hence G_i is composed of the classes

$$(1) \qquad [T]_\pi, \qquad T \equiv I \pmod{m_i}, \qquad |T| \equiv 1 \pmod{P},$$

the final congruence being a necessary and sufficient condition that $|T| \equiv 1 \pmod{\pi}$, when $|T| \equiv |I| = 1 \pmod{m_i}$.

Our investigation is based on the theorem that G_i is simply isomorphic with the group H_i of all classes $[S]_P \pmod{P}$ of transformations S whose determinants are congruent to unity modulo P. First, all transformations in a class (1) are congruent modulo π and hence modulo P, and therefore in a class $[S]_P$. Second, two transformations T and T_1 in different classes (1) are in different classes $[S]_P$. For if $T \equiv T_1 \pmod{P}$, then $T \equiv I \equiv T_1 \pmod{m_i}$ implies $T \equiv T_1 \pmod{\pi = m_i P}$. Third, there is a class (1) which corresponds to any given class $[S]_P$. For we can find T (unique modulo π) such that $T \equiv S \pmod{P}$, $T \equiv I \pmod{m_i}$ since we can find an integer (unique modulo π) which is congruent to two assigned integers with respect to the relatively prime moduli P and m_i. Hence the classes (1) are in (1,1) correspondence with the classes $[S]_P$. Finally, if $T_1 \equiv T_1'$, $T_2 \equiv T_2' \pmod{\pi}$ where all four T's satisfy the congruences (1), then $T_3 = T_1 T_2 \equiv T_1' T_2' = T_3' \pmod{\pi}$ and T_3 and T_3' satisfy the congruences (1). Hence the product $[T_1]_\pi [T_2]_\pi$ of the two classes (1) is uniquely defined as a class $[T_3]_\pi$. Since the foregoing congruences hold also modulo P, we have $[T_1]_P[T_2]_P = [T_3]_P$. Since $p_i^{\lambda_i}$ was the highest power of p_i, any one of the n distinct prime factors p_i of π, we have

THEOREM I. *In the group Γ of all classes of transformations with determinant congruent to unity, modulo π, the subgroup G_i of all classes of transformations congruent to the identity transformation modulo $m_i = \pi/p_i^{\lambda_i}$ is simply isomorphic with the group H_i of all classes of transformations molulo $p_i^{\lambda_i}$ with determinant congruent to unity modulo $p_i^{\lambda_i}$.*

3. THE GROUPS $G_1, G_2, \cdots, G_n$ GENERATE Γ

We shall now prove the following

LEMMA. *The products $T_1 T_2 \cdots T_i$ are all distinct when $T_1, T_2, \cdots, T_i$ range over the classes of transformations of $G_1, G_2, \cdots, G_i$ respectively, and (for $i < n$) these products form the subgroup J_i of classes $[U_i]_\pi$ of transformations U_i of Γ which are congruent to the identity transformation modulo $l_i = \pi/(p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_i^{\lambda_i})$.* This is true by definition where $i = 1$, that is $l_i = m_1$. Suppose it true when the above i is replaced by $i-1$. Then first, the groups J_{i-1} and G_i have no class in common save that of transformations congruent to the identity transformation modulo π. For, suppose

$$[U_{i-1}]_\pi = [T_i]_\pi, \text{ viz., } U_{i-1} \equiv T_i \qquad (\text{mod } \pi).$$

But

$$T_i \equiv I \qquad (\text{mod } m_i)$$

and

$$U_{i-1} \equiv I \qquad (\text{mod } l_{i-1})$$

and hence, since $p_i^{\lambda_i}$ is a divisior of both l_{i-1} and π, we have

$$T_i \equiv U_{i-1} \equiv I \qquad (\text{mod } p_i^{\lambda_i}).$$

Since m_i is prime to $p_i^{\lambda_i}$ and their product is π we get

$$T_i \equiv I \qquad (\text{mod } \pi).$$

Further, the classes $[U_{i-1} T_i]_\pi$ are all distinct where U_{i-1}, T_i range over representatives of the classes of transformations of J_{i-1}, G_i respectively. For, if

$$[U_{i-1} T_i]_\pi = [U_{i-1}^* T_i^*]_\pi,$$

then

$$U_{i-1} T_i \equiv U_{i-1}^* T_i^* \qquad (\text{mod } \pi)$$

and

$$U_{i-1}^{*-1} U_{i-1} \equiv T_i^* \quad T_i^{-1} \qquad (\text{mod}\, \pi).$$

By the preceding result we have

$$T_i^* \quad T_i^{-1} \equiv I \qquad (\text{mod}\, \pi)$$

and

$$U_{i-1}^{*-1} U_{i-1} \equiv I \qquad (\text{mod}\, \pi),$$

therefore

$$U_{i-1}^* \equiv U_{i-1}, \qquad T_i \equiv T_i^* \qquad (\text{mod}\, \pi)$$

imply

$$[U_{i-1}^*]_\pi = [U_{i-1}]_\pi, \qquad [T_i^*]_\pi = [T_i]_\pi.$$

The product of two transformations U_{i-1}, T_i belonging to J_{i-1} and G_i respectively is a transformation U_i of the class $[U_i]_\pi$, $U_i \equiv I \ (\text{mod}\, l_i)$, $|U| \equiv 1 \ (\text{mod}\, \pi)$. For

$$U_{i-1} \equiv I \qquad (\text{mod}\, l_{i-1}),$$

$$T_i \equiv I \qquad (\text{mod}\, m_i)$$

imply $U_{i-1} T_i \equiv I \ (\text{mod}\, l_i)$, since l_i is a divisor of both l_{i-1} and m_i.

Conversely, given a transformation U_i of the class $[U_i]_\pi$, $U_i \equiv I \ (\text{mod}\, l_i)$, $|U_i| \equiv 1 \ (\text{mod}\, \pi)$, we can find U_{i-1} and T_i (unique modulo π) such that $U_{i-1} T_i \equiv U_i \ (\text{mod}\, \pi)$. Now $U_i = I + K l_i$ where I is the identity matrix and K is a known matrix. Take

$$U_{i-1} = I + sKl_{i-1}, \qquad T_i = I + rKm_i,$$

where the integers s, r are solutions of

$$(1) \qquad s l_{i-1} + r m_i = l_i.$$

This last equation is solvable since l_i is the greatest common divisor of l_{i-1} and m_i. Then

$$\begin{aligned} U_{i-1} T_i &= I + sKl_{i-1} + rKm_i + rsK^2 l_{i-1} m_i \\ &= I + Kl_i + rsK^2 l_{i-1} m_i \\ &\equiv U_i \qquad (\text{mod}\, \pi), \end{aligned}$$

since $l_{i-1} m_i$ is divisible by π. Also $|U_{i-1}|$ and $|T_i|$ are of the form $1 + ysl_{i-1}$ and $1 + xrm_i$, respectively. Then, since $|U_i| \equiv 1 \ (\text{mod}\, \pi)$, we have

$$(1 + ysl_{i-1})(1 + xrm_i) \equiv 1 \qquad (\text{mod}\, \pi).$$

that is

$$y s l_{i-1} + x r m_i \equiv 0 \qquad (\operatorname{mod} \pi).$$

By (1)

$$r m_i = l_i - s l_{i-1},$$

hence

$$x l_i + (y - x) s l_{i-1} \equiv 0 \qquad (\operatorname{mod} \pi).$$

But l_{i-1} is divisible by $p_i^{\lambda_i}$, therefore $x l_i$ is divisible by $p_i^{\lambda_i}$. Since l_i is prime to $p_i^{\lambda_i}$, it follows that x is divisible by $p_i^{\lambda_i}$ and is of the form $z p_i^{\lambda_i}$. The determinant $|T_i|$ is therefore of the form $l + z r p_i^{\lambda_i} m_i$, hence congruent to unity, modulo π. Therefore also $|U_{i-1}| \equiv 1 (\operatorname{mod} \pi)$. This completes the induction.

When $i = n$ the first half of the lemma still holds; thus all the products $T_1\, T_2 \cdots T_n$ are distinct, where $T_1, T_2, \cdots, T_n$ range over representatives of all the classes of $G_1, G_2, \cdots, G_n$ respectively. The order of Γ is thus the product of the orders of the subgroups $G_1, G_2, \cdots, G_n$. Hence

THEOREM II. *The total group Γ of classes of transformations with determinant congruent to unity, modulo π, is obtainable by composition of the n subgroups G_i each composed of those classes of Γ whose transformations are congruent to the identity transformation, modulo $m_i = \pi / p_i^{\lambda_i}$.*

4. DETERMINATION OF THE INVARIANTS OF Γ

Let $I(x_1, \cdots, x_q)$ be any homogeneous rational integral function with integral coefficients which is an invariant of Γ modulo π, that is

$$I(x_1', \cdots, x_q') \equiv I(x_1, \cdots, x_q) \qquad (\operatorname{mod} \pi),$$

where

$$x_j' = \sum_{k=1}^{q} a_{jk} x_k \qquad (j = 1, \cdots, q) \qquad \text{and} \qquad |a_{jk}| \equiv 1 \qquad (\operatorname{mod} \pi).$$

In particular, $I(x_1, \cdots, x_q)$ is invariant under every class of transformations $[T]_\pi$, $T \equiv I (\operatorname{mod} m_i)$, $|T| \equiv 1 (\operatorname{mod} \pi)$, that is under the coincident class of transformations $[S]_P$, $S \equiv I (\operatorname{mod} m_i)$, $|S| \equiv 1 (\operatorname{mod} P)$. By the isomorphism proved in Theorem I, when T_i ranges over representatives of all the classes of G_i, S_i ranges over representatives of all the classes of H_i and thus $I(x_1, \cdots, x_q)$ is invariant under all the transformations of $H_i (\operatorname{mod} p_i^{\lambda_i})$ $(i = 1, \cdots, n)$. Conversely, if $I(x_1, \cdots, x_q)$ is a rational integral invariant under the group H_i of all transformations S of classes $[S]_P$, $S \equiv I (\operatorname{mod} m_i)$, $|S| \equiv 1 (\operatorname{mod} P)$, we see again by the isomorphism in Theorem I that $I(x_1, \cdots, x_q)$ is invariant under the corresponding G_i of the classes $[T_i]_\pi$, $T_i \equiv I(\mathrm{mod}\, m_i)$, $|T_i| \equiv 1(\mathrm{mod}\, \pi)$. For it is invariant modulo $p_i^{\lambda_i}$ and unchanged modulo m_i, therefore invariant modulo π.

Since by Theorem II the subgroups $G_i (i = 1, \cdots, n)$ generate the total group Γ, modulo π, if any rational function with integral coefficients is invariant under every H_i, modulo $p_i^{\lambda_i}$ $(i = 1, \cdots, n)$ it is an invariant of Γ modulo π. Hence we have

THEOREM III. *A necessary and sufficient condition for the invariance of a rational integral function $I(x_1, \cdots, x_q)$ with integral coefficients under the group Γ of classes of transformations with determinant congruent to unity, modulo $\pi = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, is that $I(x_1, \cdots, x_q)$ be invariant under every group H_i of classes of transformations with determinant congruent to unity, modulo $p_i^{\lambda_i}$ $(i = 1, \cdots, n)$.*

Thus

$$(1) \quad I(x_1, \cdots, x_q) = \varphi\left(L_{i,q}^{p_i^{\lambda_i - 1}}, Q_{i,q,s}^{p_i^{\lambda_i - 1}}, R_{i,q,a,b,j}\right) + p_i^{\lambda_i} f_i(x_1, \cdots, x_q) \qquad (i = 1, \cdots, n),$$

where φ_i is a rational integral function with integral coefficients. Since the greatest common divisor of the $m_i (i = 1, \cdots, n)$ is unity there exist integers k_i such that

$$\sum_{i=1}^{n} m_i k_i = 1$$

and each k_i is prime to the corresponding $p_i^{\lambda_i}$, as otherwise the left hand member would be divisible by $p_i^{\lambda_i}$.

Multiplying each of the equations (1) by the corresponding $k_i m_i$ and adding we have

$$(2) \quad I(x_1, \cdots, x_q) = \sum_{i=1}^{n} k_i m_i \varphi_i\left(L_{i,q}^{p_i^{\lambda_i - 1}}, Q_{i,q,s}^{p_i^{\lambda_i - 1}}, R_{i,q,a,b,j}\right) + \pi \sum_{i=1}^{n} k_i f_i(x_1, \cdots, x_q).$$

As $k_i \varphi_i$ is an invariant of $H_i\, (\mathrm{mod}\, p_i^{\lambda_i})$ and does not vanish modulo p_i^{λ} unless φ_i vanishes modulo $p_i^{\lambda_i}$ we have finally the theorem stated in the introduction.

IOWA STATE COLLEGE,
AMES, IOWA.