THEORY OF LINEAR GROUPS IN AN ARBITRARY FIELD*

BY

LEONARD EUGENE DICKSON

§ 1. *Introduction.*

Various branches of group theory may be correlated by a treatment of groups of transformations in a given field or domain of rationality. In view of the simplicity of their treatment and of their importance as well in applications as in the general theory,† groups of linear transformations offer a natural starting place in the construction of a theory of groups in a given domain of rationality.

The chief result of the present paper is the exhibition of four infinite systems of groups of transformations which are simple groups in every domain of rationality. For the case of the field of all complex numbers these groups are the simple continuous groups of LIE. By the well known investigations of KILLING and CARTAN, the latter groups give the only systems of simple continuous groups of a finite number of parameters.

As in the theories of algebraic and differential equations, so also in the theory of groups of transformations, it is of first importance that the definitions, conceptions and developments shall have reference to a given field or domain of rationality. For example, it is important to have a theory of continuous groups in the field of complex numbers and a theory in the field of real numbers. Two real continuous groups may not be isomorphic, although the corresponding complex groups are isomorphic.‡ If we allow complex transformations to canonical types, there results a complete list of real groups; allowing only reductions by real transformations, the list is often more extensive.

---

* Presented to the Society at the Ithaca Meeting, August 20, 1901. Received for publication June 7, 1901.

† For example, a continuous group G with a finite number of parameters is simply or multiply isomorphic with a linear homogeneous group called the adjoint group of G. If G be simple, it may be exhibited as a linear fractional (projective) group. From the fundamental rôle played by the adjoint group and by the simple groups, the theory of linear groups is of capital importance in LIE's theory of continuous groups.

‡ DICKSON: Bulletin of the American Mathematical Society, (2) vol. 7 (1901), p. 340; SLOCUM: Proceedings of the American Academy of Arts and Sciences, vol. 36 (1900), p. 105.

The chief results in the theory of linear groups in a finite field are presented in the author's treatise on Linear Groups, * to which reference will here be made by the initials L. G.

In certain questions cencerning continuous groups, as that of the structure of a mixed group, the methods here presented often give additional knowledge, not obtained by following LIE's method.

In §§ 9–10 is investigated a group in an arbitrary field which corresponds to the simple continuous group of 14 parameters, an isolated group not in the four systems of LIE. For the case of a finite field of order p^n, we are led to a new simple group of order $p^{6n}(p^{6n}-1)(p^{2n}-1)$.

§ 2. *Definition of fields and groups.*

A set of operators forms a *group* if the following properties hold:

(*a*) The product (compound) of any two operators of the set is itself an operator of the set.

(*b*) The composition of operators is associative: if A, B, C are any operators of the set, then $(AB)C = A(BC)$.

(*c*) To every operator A of the set corresponds an operator A_1 of the set such that $AA_1 = A_1A = I$, where I is the operator identity, which leaves unaltered all possible operands. This A_1 is called the *inverse* of A and is designated A^{-1}.

A set of elements forms a *field* † if they can be combined by addition, subtraction, multiplication and division, the divisor not being the element zero (necessarily in the set), these operations being subject to laws of elementary algebra, and if the resulting sum, difference, product or quotient be uniquely determined as an element of the set.

A field may therefore be characterized by the property that *the rational operations of algebra can be performed within the field.*

As examples of fields may be noted the finite fields, ‡ the field R of all rational numbers, the field $R(i)$ of numbers $a+bi$, where a and b are rational, the field of all real numbers, the field C of all complex numbers, the field $R(\theta)$ of all rational functions of the algebraic number θ, a root of an equation belonging to and irreducible in the field R.

§ 3. *General linear homogeneous and linear fractional groups.*

Let $\xi_1, \xi_2, \cdots, \xi_m$ be arbitrary variables. Consider the linear homogeneous transformation

$$A: \qquad \xi_i' = \sum_{j=1}^{m} a_{ij}\xi_j \qquad (i=1, 2, \cdots, m)$$

* B. G. Teubner, Leipsic, 1901.

† Domain of rationality or Körper. See WEBER'S *Algebra*.

‡ Each is necessarily a Galois field of order a power of a prime (MOORE).

with coefficients a_{ij} in a given field F such that the determinant

$$|A| \equiv |a_{ij}| \neq 0 \qquad (i, j = 1, 2, \cdots, m).$$

Such a transformation A will be said to belong to the field F. Consider a second transformation belonging to F,

$$A': \qquad \xi'_i = \sum_{j=1}^{m} a'_{ij}\xi_j \qquad (i = 1, 2, \cdots, m).$$

By the compound, or product, of A and A' we mean the transformation

$$A'': \qquad \xi'_i = \sum_{j=1}^{m} a''_{ij}\xi_j \qquad (i = 1, 2, \cdots, m),$$

where

$$a''_{ij} \equiv \sum_{k=1}^{m} a'_{ik}a_{kj} \qquad (i, j = 1, 2, \cdots, m).$$

We have here compounded the transformations in the order A, A'; the relation between A, A', A'' is written

$$AA' = A''.$$

By the theorem for the multiplication of determinants,

$$|A''| \equiv |a''_{ij}| = |a'_{ik}| \cdot |a_{kj}| = |A'| \cdot |A| \neq 0.$$

Since a_{ij} and a'_{ij} belong to the field F by hypothesis, the coefficients a''_{ij} also belong to F. Hence the product A'' is a transformation belonging to the field F. The transformation

$$A^{-1}: \qquad \xi'_i = \sum_{j=1}^{m} \frac{A_{ji}}{|A|}\xi_j \qquad (i = 1, 2, \cdots, m),$$

where A_{ji} is the adjoint (first minor with proper sign) of a_{ji} in $|a_{ji}|$, has its coefficients in the field F and has the determinant $|A|^{-1}$. The product AA^{-1} is the identity I; indeed, it replaces ξ_i by the function*

$$\sum_{j,k}^{1,\cdots,m} \frac{A_{ji}a_{jk}}{|A|}\xi_k = \sum_{k=1}^{m} \frac{\delta_{ik}|A|}{|A|}\xi_k = \xi_i.$$

Hence the inverse A^{-1} of A is a transformation in the field F. Moreover, the transformations of the form A are seen to obey the associative law [§ 2, property (b)]. It follows that the totality of transformations A constitutes a group. It will be called *the general linear homogeneous group on m variables with co efficients in the field F* and denoted by the symbol† $GLH(m, F)$.

---

* In KRONECKER's notation, $\delta_{ii} = 1$, $\delta_{ik} = 0\,(k \neq i)$.

† A finite field is uniquely defined by its order, necessarily a power of a prime number, p^n (MOORE). The corresponding group is $GLH(m, p^n)$. [See L. G., §§ 97–98.]

The group $GLH(m, F)$ is generated by the transformations

$$D_{1,\lambda}: \qquad \xi_1' = \lambda\xi_1, \quad \xi_i' = \xi_i \qquad (i = 2, 3, \cdots, m),$$

$$B_{r,s,\lambda}: \qquad \xi_r' = \xi_r + \lambda\xi_s, \quad \xi_i' = \xi_i \quad (i = 1, \cdots, m;\ i \neq r, r \neq s),$$

where λ is an arbitrary quantity $\neq 0$ in the field F.

The proof is identical with that in L. G., § 100. The proof shows that any transformation A of the group can be expressed uniquely as a product $A_1 D_{1,\lambda}$, where $\lambda = |A|$ and where A_1 is derived from the transformations $B_{r,s,k}$, all of which have determinant unity.

The totality of transformations A of determinant unity forms a group Γ called *the special linear homogeneous group $SLH(m, F)$*. It is generated by the transformations $B_{r,s,\lambda}$.

The product $B^{-1}AB$ is called *the transform of A by B*. Since

$$|B^{-1}AB| = |B^{-1}| \cdot |A| \cdot |B| = |B|^{-1} \cdot |A| \cdot |B| = |A|,$$

the transform of A has the same determinant as A.

A subgroup Γ of G is called *invariant (self-conjugate) under G* if the transform of each transformation of Γ by an arbitrary transformation of G belongs to G, i. e., symbolically, if $g^{-1}\gamma g = \gamma'$.

The group $SLH(m, F)$ is an invariant subgroup of $GLH(m, F)$.

By making A_1 correspond to $A \equiv A_1 D_{1,|A|}$, we establish an isomorphism of $SLH(m, F)$ with $GLH(m, F)$. The identity corresponds to the (commutative) group of the transformations $D_{1,\lambda}$. The latter is called the *quotient-group* of the general by the special linear group.

The special linear homogeneous group Γ contains an invariant subgroup H composed of the transformations

$$M_\mu: \qquad \xi_i' = \mu\xi_i \qquad [\mu^m = 1] \qquad (i = 1, \cdots, m).$$

Let J be an invariant subgroup of Γ which contains all the transformations M_μ and still other transformations. By the proof in L. G., § 104, interpreted for an infinite field F, it follows that $J \equiv \Gamma$ if $m > 2$; while, by § 105, it follows, for $m = 2$, that J contains a transformation of the form $B_{2,1,\lambda\rho^2}$, with $\lambda \neq 0$, and ρ an arbitrary quantity in the field F. Having $B_{2,1,\lambda\sigma^2}$, the *group* J contains its inverse $B_{2,1,-\lambda\sigma^2}$. Hence J contains the product, in which ρ and σ are arbitrary in F,

$$B_{2,1,\lambda\rho^2} B_{2,1,-\lambda\sigma^2} \equiv B_{2,1,\lambda(\rho^2-\sigma^2)}.$$

To make $\rho^2 - \sigma^2 = \tau$, an arbitrary quantity in F, we set

$$\rho = \tfrac{1}{2}(\tau + 1), \quad \sigma = \tfrac{1}{2}(\tau - 1),$$

thereby excluding the case in which F has a modulus $p = 2$.

With $B_{2,1,\lambda\tau}$, J contains every $B_{2,1,\kappa}$, κ arbitrary in F. But $B_{2,1,\kappa}$ is transformed into $B_{1,2,-\kappa}$ by $(\xi_1' = \xi_2, \xi_2' = -\xi_1)$, which belongs to Γ. Since $B_{1,2,\kappa}$ and $B_{2,1,\kappa}$ generate Γ, we have $J = \Gamma$. Hence, for any m, H is a maximal invariant subgroup of Γ. The quotient-group Γ/H is therefore *simple.*

The group $SLH(m, F)$ has $(f, 1)$ isomorphism with a simple group, where f is the number of solutions in F of $x^m = 1$, and F is any infinite field or any finite field of order p^n, provided $p^n > 3$ if $m = 2$.*

Introducing the linear fractional transformations

$$x_i' = \frac{a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{im-1}x_{m-1} + a_{im}}{a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mm-1}x_{m-1} + a_{mm}} \qquad (i = 1, \cdots, m-1),$$

we may derive, as in L. G., § 108, the following theorem:

The group $LF(m, F)$ of all linear fractional transformations on $m-1$ variables with coefficients in an infinite field F and of determinant unity is a simple group.

§ 4. *The Abelian linear group.*

A linear homogeneous transformation on $2m$ variables with coefficients in a field F is called *Abelian* if, when operating simultaneously upon two sets of variables ξ_i, η_i; $\bar{\xi}_i, \bar{\eta}_i (i = 1, \cdots, m)$, it leaves formally invariant (up to a factor belonging to F) the function

$$\phi \equiv \sum_{i=1}^{m} (\xi_i \bar{\eta}_i - \eta_i \bar{\xi}_i).$$

The totality of such transformations constitutes the *general Abelian linear group* $GA(2m, F)$. Those transformations which leave ϕ absolutely invariant form a subgroup called the *special Abelian linear group* $SA(2m, F)$.

If F be a continuous field (real or complex), the group $SA(2m, F)$ is simple † (in LIE's sense). If we take for ϕ the function

$$\sum_{i=1}^{m} (\xi_i d\eta_i - \eta_i d\xi_i),$$

we recognize $SA(2m, F)$ to be the homogeneous form of the largest projective group on $2m-1$ variables which leaves invariant a linear complex.‡

---

* In speaking of the index of an invariant subgroup H of a group Γ of infinite order, we mean the number of right-hand multipliers M_i such that the products hM_i, when h runs through the set of operators of H, give once and but once every operator of Γ. If H is of order f, we say that Γ has $(f, 1)$ isomorphism with Γ/H.

† Bulletin of the American Mathematical Society (2), vol. 3 (1897), pp. 267–270. With LIE a simple group is one containing no invariant continuous subgroup.

‡ Ibid., pp. 270, 271.

THEOREM. *In any field F, the group $SA(2m, F)$ is generated by the transformations, all of determinant unity,*

$$M_i: \quad \xi_i' = \eta_i, \quad \eta_i' = -\xi_i;$$
$$L_{i,\lambda}: \quad \xi_i' = \xi_i + \lambda\eta_i;$$
$$N_{i,j,\lambda}: \quad \xi_i' = \xi_i + \lambda\eta_j, \quad \xi_j' = \xi_j + \lambda\eta_i;$$

where λ is an arbitrary quantity in F. The group has a maximal invariant subgroup formed of the identity I and the transformation T which changes the signs of the $2m$ variables.‡ *The case $m = 1$ is exceptional if F be of order 2 or 3.*

The proof proceeds as in L. G., §§ 110, 111, 114, 116, the statements on p. 97, lines 1–3, being replaced by the following argument. Since J contains $L_{2,\lambda\tau^2}$, in which $\lambda \neq 0$ and τ is arbitrary in F, it contains the inverse $L_{2,-\lambda\tau^2}$ and therefore the product

$$L_{2,\lambda\tau_1^2} L_{2,-\lambda\tau_2^2} \equiv L_{2,\lambda(\tau_1^2-\tau_2^2)}.$$

Taking $\tau_1 = \frac{1}{2}(\kappa+1)$, $\tau_2 = \frac{1}{2}(\kappa-1)$, we reach $L_{2,\lambda\kappa}$, where κ is arbitrary in F. Hence J contains $L_{2,\mu}$, μ being arbitrary in F. An analogous change is to be made on p. 97, lines 25–28.

The group obtained as the quotient-group of $SA(2m, F)$ by $\{I, T\}$ will be designated by $A(2m, F)$. It is simple except in the cases $m = 1$, F of order 2 or 3.

THEOREM. *A transformation of period 2 of $SA(2m, F)$ is conjugate within that group with one of the m non-conjugate transformations*

$$T_{1,-1}, \quad T_{1,-1}T_{2,-1}, \quad T_{1,-1}T_{2,-1}T_{3,-1}, \quad \cdots, \quad T \equiv T_{1,-1}T_{2,-1}\cdots T_{m,-1},$$

where $T_{i,-1}$ alters only ξ_i and η_i whose signs it changes.

The proof proceeds as in L. G., §§ 120–121.

The study of the conjugacy of the operators of period 2 in the quotient-group $A(2m, F)$ is not so simple for infinite fields as for finite fields (L. G., §§ 122–123). For the simplest case $m = 1$, a transformation of period 4 in $SA(2, F)$ is conjugate within that group with one of the transformations

$$S_\gamma \equiv \begin{pmatrix} 0 & \gamma \\ -\gamma^{-1} & 0 \end{pmatrix}.$$

The most general transformation of determinant unity which transforms S_γ into S_δ has the form

$$\begin{pmatrix} d\delta\gamma^{-1}, & b\delta \\ -b\gamma^{-1}, & d \end{pmatrix} \qquad (\gamma/\delta = b^2 + d^2).$$

‡ For the second part of the theorem and for the remainder of this section, it is assumed that, *if* there be a modulus p for an infinite field F, $p \neq 2$.

Hence S_γ and S_δ are conjugate within $SA(2, F)$ if, and only if, the ratio γ/δ is expressible as the sum of two squares (including zero) in the field F.

For the field of rational numbers, S_1 is conjugate with S_γ for $\gamma = 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, \cdots, \frac{1}{2}, \frac{1}{4}, \frac{1}{5}, \frac{2}{5}, \frac{4}{5}, \cdots$, a series containing every prime number of the form $4t + 1$, but no prime number of the form $4t + 3$.* It follows readily that there is an infinite number of non-conjugate transformations of period 4, viz., $S_1, S_3, S_7, S_{21}, S_{11}, S_{33}, S_{77}, S_{231}, S_{19}, \cdots$, including every S_τ for which τ is a prime number of the form $4t + 3$, of which there are an infinite number by DIRICHLET's theorem.

In the field C of all complex numbers, every S_γ is conjugate with $S_1 \equiv M_1$ within the group. As in L. G., §§ 122–123, we obtain the theorem:

If $s \equiv m/2$ or $(m-1)/2$ according as m is even or odd, the group $A(2m, C)$ contains exactly $s + 1$ sets of conjugate operators of period 2. As representatives we may take

$$M \equiv M_1 M_2 \cdots M_m, \quad T_{1,-1}, \quad T_{1,-1}T_{2,-1}, \cdots, \quad T_{1,-1}T_{2,-1}\cdots T_{s,-1}.$$

In the field of all real numbers every S_γ is conjugate within the group $SA(2, F)$ either with $S_1 \equiv M_1$ or else with $S_{-1} \equiv M_1 T_{1,-1}$. By a simple modification of the developments in L. G., § 123, we find that, within $SA(2m, F)$, every transformation S, such that $S^2 = T_{1,-1}T_{2,-1}\cdots T_{m,-1}$, is conjugate with one of the transformations M, $MT_{1,-1}$, $MT_{1,-1}T_{2,-1}, \cdots, MT_{1,-1}\cdots T_{m,-1}$. For $m = 1$ these transformations have been shown to be not conjugate. That they are not conjugate when $m = 2$ may be shown as follows. A transformation which transforms M_1M_2 into either $M_1M_2T_{1,-1}$ or $M_1M_2T_{1,-1}T_{2,-1}$ must have the form

$$\left\{\begin{matrix} a_{11} & \gamma_{11} & a_{12} & \gamma_{12} \\ \gamma_{11} & -a_{11} & \gamma_{12} & -a_{12} \\ \cdot & \cdot & \cdot & \cdot \end{matrix}\right\},$$

so that, by one of the Abelian conditions,

$$-a_{11}^2 - \gamma_{11}^2 - a_{12}^2 - \gamma_{12}^2 = 1.$$

The commutative transformation $T_{1,-1}T_{2,-1}$ being introduced, it follows that

$$M_1M_2T_{1,-1}T_{2,-1}$$

is not conjugate with $M_1M_2T_{2,-1}$ or with M_1M_2.

For general m, it follows by a similar proof that neither M nor MT is conjugate with any one of the series $MT_{1,-1}, MT_{1,-1}T_{2,-1}, \cdots, MT_{1,-1}\cdots T_{m-1,-1}$ nor M with MT.

---

*Cf. WEBER, *Algebra*, vol. 1, 1st ed. (1895), p. 585.

For the field F of all real numbers, every operator of period two of the group $A(2m, F)$ is conjugate within the group with one of the following operators

$$T_{1,-1},\ T_{1,-1}T_{2,-1},\ \cdots,\ T_{1,-1}T_{2,-1}\cdots T_{s,-1},\ M \equiv M_1M_2\cdots M_m,$$

$$MT_{1,-1},\ MT_{1,-1}T_{2,-1},\ \cdots,\ MT_{1,-1}T_{s,-1}\cdots T_{3,-1},$$

where $s = m/2$ or $(m-1)/2$ according as m is even or odd.

At least in the cases $m = 1$ and $m = 2$, no two of these $2s+1$ operators are conjugate within the group.

§ 5. *A generalization of the Abelian linear group.*

Those linear homogeneous transformations on mq variables with coefficients in any field F which, if operating simultaneously upon q sets each of mq variables, the jth set being exhibited by the notation

$$x_{i1}^{(j)},\ x_{i2}^{(j)},\ \cdots,\ x_{iq}^{(j)} \qquad (i=1, 2, \cdots, m),$$

leave formally and absolutely invariant the function

$$\phi = \sum_{i=1}^{m} \begin{vmatrix} x_{i1}^{(1)}, & x_{i2}^{(1)}, & \cdots, & x_{iq}^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ x_{i1}^{(q)}, & x_{i2}^{(q)}, & \cdots, & x_{iq}^{(q)} \end{vmatrix},$$

form a group $G(m, q, F)$. For $q = 2$, it is the group $SA(m, F)$ of § 4.

Proceeding as in L. G., §§ 124–128, we obtain the theorems:*

For $q > 2$, the group $G(m, q, F)$ is generated by the substitutions

$$P_{ij} \equiv (x_{i1}x_{j1})(x_{i2}x_{j2})\cdots(x_{iq}x_{jq}) \qquad (i, j=1, 2, \cdots, m),$$

and the totality of transformations in F of determinant unity,

$$x'_{1l} = \sum_{k=1}^{q} a_{lk}x_{1k} \qquad (l=1, 2, \cdots, q).$$

For $q > 2$, $G(m, q, F)$ has an invariant subgroup which is the direct product of m commutative groups each the special linear homogeneous group

* For the case in which F is a continuous field, these theorems were established by the author (using the LIE theory) in the Bulletin of the American Mathematical Society (2), vol. 3, pp. 271–273, May, 1897.

in F on q variables, the quotient-group being generated by the substitutions P_{ij} and thus holoedrically isomorphic with the symmetric group on m letters.*

§ 6. *The compounds of a linear homogeneous group.*

To the transformation (a_{ij}) of § 3 we make correspond the transformation

$$[a]_q: \qquad Y'_{i_1, i_2, \cdots, i_q} = \sum_{l_1, \cdots, l_q} \begin{vmatrix} a_{i_1 l_1} & a_{i_1 l_2} \cdots a_{i_1 l_q} \\ a_{i_2 l_1} & a_{i_2 l_2} \cdots a_{i_2 l_q} \\ \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{i_q l_1} & a_{i_q l_2} \cdots a_{i_q l_q} \end{vmatrix} Y_{l_1, l_2, \cdots, l_q},$$

where the sets $i_1, i_2, \cdots, i_q$ and $l_1, l_2, \cdots, l_q$ take independently all the distinct combinations q at a time of the integers $1, 2, \cdots, m$. Likewise, to the transformation (a'_{ij}) we make correspond the transformation $[a']_q$. Then (L. G., § 153) to the product $(a''_{ij}) \equiv (a_{ij})(a'_{ij})$ corresponds $[a'']_q \equiv [a]_q [a']_q$. Hence, if the transformations (a_{ij}) form a group, the transformations $[a]_q$ form an isomorphic group called the qth *compound* of the former.

By simple modifications of §§ 154–164 of L. G., we obtain the results:

The general linear homogeneous group $GLH(m, F)$ has $(d, 1)$ isomorphism with its qth compound if the equation $x^q = 1$ has exactly d roots in F.

The special linear homogeneous group $SLH(m, F)$ has $(g, 1)$ isomorphism with its qth compound if the equations $x^q = 1$, $x^m = 1$ have in the field F exactly g common solutions.

The second compound of $GLH(m, F)$ leaves invariant the Pfaffian† $[1, 2, \cdots, m]$. For m odd, the transformation $[a]_2$ gives rise to the transformation

$$F'_i = \sum_{j=1}^{m} A_{ij} F_j \qquad (i = 1, 2, \cdots, m)$$

upon the Pfaffians $F_j \equiv [1, 2, \cdots, j-1, j+1, \cdots, m]$, where A_{ij} denotes the first minor of a_{ij} in the determinant $|a_{ij}|$. The transformation $[a]_2$ effects upon the $\frac{1}{2}m(m-1)$ Pfaffians $[i_1, i_2, \cdots, i_{m-2}]$, where each $i = 1, 2, \cdots, m$,

---

* The transformations of the ith group are given by the formula

$$x'_{ij} = \sum_{k=1}^{q} \beta_{ik}^{ij} x_{ik}, \; x'_{sj} = x_{sj} \qquad (s = 1, \cdots, m;\; s \neq i;\; j = 1, \cdots, q),$$

where, for each $i \gtreqless m$, the determinant $|\beta_{ik}^{ij}| = 1 \, (j, k = 1, \cdots, q)$.

† Inversely, in a continuous field F, the largest linear group on $\frac{1}{2}m(m-1)$ variables which leaves the Pfaffian invariant is the second compound of $GLH(m, F)$, Bulletin of the American Mathematical Society, vol. 5 (1898), pp. 338–342.

such that $i_1 < i_2 < \cdots < i_{m-2}$, *a linear homogeneous transformation identical with the transformation* $[a]_{m-2}$ *of the* $(m-2)$*th compound.* *

The q*th and* $(m-q)$*th compounds of* $SLH(m, F)$ *are holoedrically isomorphic.* Indeed, the number of solutions in F of $x^m = 1$, $x^q = 1$ equals the number of solutions in F of $x^m = 1$, $x^{m-q} = 1$.

The general Abelian group $GA(2m, F)$ *is the largest linear homogeneous group in the field* F *on* $2m$ *variables whose second compound has the relative invariant*

$$Z \equiv Y_{12} + Y_{34} + \cdots + Y_{2m-1\,2m}.$$

The second compound of $SA(2m, F)$ *is a simple*† *group with the absolute invariants* Z *and the Pfaffian* $[1, 2 \cdots, 2m]$.

The simple group $A(4, F)$ *is holoedrically isomophic with a subgroup of the quinary linear group in* F *which leaves absolutely invariant*

$$Y^2 + Y_{13}Y_{24} - Y_{14}Y_{23}.$$

According as the field F *does not or does contain a primitive fourth root of unity, the second compound of* $SLH(4, F)$ *is holoedrically isomorphic with the simple group* $LF(4, F)$ *or has a maximal invariant subgroup* $\{I, T\}$, *where* T *changes the signs of the six variables, the quotient-group being holoedrically isomorphic with* $LF(4, F)$.

The second compound of $SLH(4, F)$ *contains the transformation*

$$Y'_{12} = \nu Y_{12}, \quad Y'_{13} = Y_{13}, \quad Y'_{14} = Y_{14}, \quad Y'_{23} = Y_{23}, \quad Y'_{24} = Y_{24}, \quad Y'_{34} = \nu^{-1} Y_{34}$$

if, and only if, ν *be a square in the field* F.

By § 3, the group $SLH(4, F)$ is generated by the transformations $B_{r,s,\lambda}$ $(r, s = 1, 2, 3, 4;\ r \neq s)$, and hence by $B_{1,2,\lambda}$ and

$$A_{12}: (\xi'_1 = \xi_2, \xi'_2 = -\xi_1), \quad A_{13}: (\xi'_1 = \xi_3, \xi'_3 = -\xi_1), \quad A_{34}: (\xi'_3 = \xi_4, \xi'_4 = -\xi_3).$$

The second compounds of these transformations are respectively

$$\begin{aligned}
B'_{1,2,\lambda}: &\quad Y'_{13} = Y_{13} + \lambda Y_{23}, \quad Y'_{14} = Y_{14} + \lambda Y_{24};\\
A'_{12}: &\quad Y'_{13} = Y_{23}, \quad Y'_{14} = Y_{24}, \quad Y'_{23} = -Y_{13}, \quad Y'_{24} = -Y_{14};\\
A'_{13}: &\quad Y'_{12} = -Y'_{23}, \quad Y'_{14} = Y_{34}, \quad Y'_{23} = Y_{12}, \quad Y'_{34} = -Y_{14};\\
A'_{34}: &\quad Y'_{13} = Y_{14}, \quad Y'_{14} = -Y_{13}, \quad Y'_{23} = Y_{24}, \quad Y'_{24} = -Y_{23}.
\end{aligned}$$

The second compound possesses the absolute invariant

$$\theta_6 \equiv Y_{12}Y_{34} - Y_{13}Y_{24} + Y_{14}Y_{23}.$$

---

* For the case of a continuous field F, these theorems were established by the author in the Bulletin of the American Mathematical Society, vol. 5 (1898), pp. 120–135.

† If there be a modulus p, we assume that $p \neq 2$; as also in the rest of the section.

The second compound of $SLH(4, F)$ may be exhibited as that senary linear group G_6, leaving $\xi_1\eta_1 + \xi_2\eta_2 + \xi_3\eta_3$ invariant, which is generated by the transformations $S_{ij} \equiv (\xi_i\eta_i)(\xi_j\eta_j)$ and

$$W_{i,j,\lambda}: \qquad \xi_i' = \xi_i + \lambda\eta_j, \ \xi_j' = \xi_j - \lambda\eta_i.$$

The group G_6 will therefore contain the transformations

$$S_{ij}^{-1} W_{i,j,\lambda} S_{ij} \equiv V_{i,j,\lambda}: \qquad \eta_i' = \eta_i + \lambda\xi_j, \ \eta_j' = \eta_j - \lambda\xi_i;$$

$$S_{jk}^{-1} W_{i,j,\lambda} S_{jk} = Q_{i,j,\lambda}: \qquad \xi_i' = \xi_i + \lambda\xi_j, \ \eta_j' = \eta_j - \lambda\eta_i;$$

$$Q_{j,i,-1} Q_{i,j,1} Q_{j,i,-1} \equiv P_{ij} T_{j,-1};$$

where $P_{ij} \equiv (\xi_i\xi_j)(\eta_i\eta_j)$ and $T_{i,\lambda}$ denotes $\xi_i' = \lambda\xi_i$, $\eta_i' = \lambda^{-1}\eta_i$. Set

$$(1) \qquad Y_{12} \equiv \xi_3, \ Y_{13} \equiv \xi_1, \ Y_{14} \equiv \xi_2, \ Y_{23} \equiv -\eta_2, \ Y_{24} \equiv \eta_1, \ Y_{34} \equiv -\eta_3.$$

Then $B_{1,2,\lambda}'$, A_{12}', A_{13}', A_{34}' become $W_{1,2,-\lambda}$, $S_{12}T_{2,-1}P_{12}$, $S_{23}P_{23}T_{2,-1}$, $P_{12}T_{2,-1}$, respectively. Hence G_6 contains the transformations which correspond to the generators of the second compound. Inversely, from them we derive $W_{1,2,\lambda}$, $P_{12}T_{2,-1}$, S_{12} and therefore the transform S_{13} of S_{12} by $S_{23}P_{23}T_{2,-1}$. We then derive $S_{12}S_{13} \equiv S_{23}$ and $P_{23}T_{2,-1}$. The latter transforms $W_{1,2,\lambda}$ into $W_{1,3,\lambda}$; and $P_{12}T_{2,-1}$ transforms $W_{1,3,-\lambda}$ into $W_{2,3,\lambda}$. We have therefore derived the generators S_{ij}, $W_{i,j,\lambda}$ of G_6.

By § 4 the special Abelian group $SA(4, F)$ is generated by M_1, M_2, $L_{1,\lambda}$, $L_{2,\lambda}$ and $N_{1,2,\lambda}$. Their second compounds are respectively A_{12}', A_{34}', $B_{1,2,\lambda}'$, $B_{3,4,\lambda}'$ and $N_{1,2,\lambda}'$, the first three being exhibited above,* while

$$B_{3,4,\lambda}': \qquad Y_{13}' = Y_{13} + \lambda Y_{14}, \quad Y_{23}' = Y_{23} + \lambda Y_{24};$$

$$N_{1,2,\lambda}': \qquad \begin{cases} Y_{12}' = Y_{12} - \lambda Y_{24}, & Y_{34}' = Y_{34} + \lambda Y_{24}, \\ Y_{13}' = Y_{13} + \lambda Y_{12} - \lambda Y_{34} - \lambda^2 Y_{24}. \end{cases}$$

The last five transformations leave invariant θ_6 and $Z \equiv Y_{12} + Y_{34}$, by the theorem stated above. We introduce the new variables †

$$(2) \qquad \xi_0 = \tfrac{1}{2}(Y_{12} - Y_{34}), \quad \xi_1 = Y_{13}, \quad \eta_1 = Y_{24}, \quad \xi_2 = Y_{14}, \quad \eta_2 = -Y_{23}.$$

Then A_{12}', A_{34}', $B_{1,2,\lambda}'$ and $B_{3,4,\lambda}'$ become $S_{12}T_{2,-1}P_{12}$, $P_{12}T_{2,-1}$, $W_{1,2,-\lambda}$ and $Q_{1,2,\lambda}$ respectively. Finally, $N_{1,2,\lambda}'$ becomes $X_{0,1,\lambda}$, if we use the notation

$$X_{0,j,\lambda}: \qquad \xi_0' = \xi_0 - \lambda\eta_j, \quad \xi_j' = \xi_j + 2\lambda\xi_0 - \lambda^2\eta_j.$$

For later use, we introduce, for the transform of $X_{0,j,\lambda}$ by $S_{jk}(k \neq j)$,

$$Y_{0,j,\lambda}: \qquad \xi_0' = \xi_0 - \lambda\xi_j, \quad \eta_j' = \eta_j + 2\lambda\xi_0 - \lambda^2\xi_j.$$

---

* The present variables ξ_1, η_1, ξ_2, η_2 correspond to the former ξ_1, ξ_2, ξ_3, ξ_4 respectively.

† The last four have the same definition as in the case of the group G_6.

The second compound of $SA(4, F)$ is a simple group which may be exhibited as that quinary linear group G_5 leaving $\xi_0^2 + \xi_1\eta_1 + \xi_2\eta_2$ invariant which is generated by $P_{12}T_{2,-1}$, S_{12}, $W_{1,2,\lambda}$, $Q_{1,2,\lambda}$ and $X_{0,1,\lambda}$.

We obtain an important subgroup of G_5 as follows. The second compound of the special Abelian transformation

$$\begin{Bmatrix} \alpha & 0 & 0 & \beta \\ 0 & \delta & \gamma & 0 \\ 0 & \beta & \alpha & 0 \\ \gamma & 0 & 0 & \delta \end{Bmatrix} \qquad (\alpha\delta - \beta\gamma = 1)$$

affects only four of the six variables Y_{ij} and has the form

$$\begin{array}{r|cccc} & Y_{12} & Y_{13} & Y_{24} & Y_{34} \\ \hline Y'_{12} = & \alpha\delta & \alpha\gamma & -\beta\delta & -\beta\gamma \\ Y'_{13} = & \alpha\beta & \alpha^2 & -\beta^2 & -\alpha\beta \\ Y'_{24} = & -\gamma\delta & -\gamma^2 & \delta^2 & \gamma\delta \\ Y'_{34} = & -\beta\gamma & -\alpha\gamma & \beta\delta & \alpha\delta \end{array}$$

The latter leaves $Y_{12} + Y_{34}$ invariant. Expressed in terms of the variables ξ_0, ξ_1, η_1 defined by (2), it takes the form

$$(3) \qquad \begin{array}{r|ccc} & \xi_0 & \xi_1 & \eta_1 \\ \hline \xi'_0 = & \alpha\delta + \beta\gamma & \alpha\gamma & -\beta\delta \\ \xi'_1 = & 2\alpha\beta & \alpha^2 & -\beta^2 \\ \eta'_1 = & -2\gamma\delta & -\gamma^2 & \delta^2 \end{array} \qquad (\alpha\delta - \beta\gamma = 1),$$

a transformation of determinant unity leaving $\xi_0^2 + \xi_1\eta_1$ absolutely invariant.* *The transformations* (3) *form a simple group isomorphic with $LF(2, F)$.*

To exhibit a subgroup of both G_5 and G_6 which leaves $\xi_1\eta_1 + \xi_2\eta_2$ invariant, we form the second compound of

$$\begin{Bmatrix} \alpha & \beta & 0 & 0 \\ \gamma & \delta & 0 & 0 \\ 0 & 0 & A & B \\ 0 & 0 & C & D \end{Bmatrix} \qquad \left(\begin{matrix} \alpha\delta - \beta\gamma = 1 \\ AD - BC = 1 \end{matrix}\right),$$

* Among them occur $X_{0,1,\lambda}$ and $Y_{0,1,\lambda}$, the latter for $\alpha = \delta = 1$, $\beta = 0$, $\gamma = -\lambda$.

and obtain a transformation affecting only Y_{13}, Y_{14}, Y_{23}, Y_{24}. Introducing ξ_1, ξ_2, $-\eta_2$, η_1, respectively, for the former [as in (1) or (2)], we obtain the transformation

$$(4)\qquad \begin{array}{c|cccc} & \xi_1 & \eta_1 & \xi_2 & \eta_2 \\ \hline \xi_1' = & \alpha A & \beta B & \alpha B & -\beta A \\ \eta_1' = & \gamma C & \delta D & \gamma D & -\delta C \\ \xi_2' = & \alpha C & \beta D & \alpha D & -\beta C \\ \eta_2' = & -\gamma A & -\delta B & -\gamma B & \delta A \end{array}$$

The group of these transformations has, in view of its origin, the factor groups $LF(2, F)$, $LF(2, F)$, and $\{I, T\}$, where T changes the sign of each variable.*

§ 7. *Concerning linear groups with quadratic invariants.*

Consider the group $G(m, F)$ of linear homogeneous transformations

$$S: \quad \begin{cases} \xi_i' = a_{i0}\xi_0 + \sum_{j=1}^{m} (a_{ij}\xi_j + \gamma_{ij}\eta_j) & (i=0, 1, \cdots, m), \\ \eta_i' = \beta_{i0}\xi_0 + \sum_{j=1}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j) & (i=1, \cdots, m), \end{cases}$$

with coefficients in a field† F, which have the absolute invariant

$$g_m \equiv \xi_0^2 + \xi_1\eta_1 + \xi_2\eta_2 + \cdots + \xi_m\eta_m.$$

The conditions for the formal invariance of g_m are

$$(5)\qquad a_{00}^2 + \sum_{i=1}^{m} a_{i0}\beta_{i0} = 1,$$

$$(6)\qquad 2a_{0j}a_{0k} + \sum_{i=1}^{m} (a_{ij}\beta_{ik} + a_{ik}\beta_{ij}) = 0 \qquad (j=0, 1, \cdots, m;\ k=1, \cdots, m),$$

$$(7)\qquad 2\gamma_{0j}\gamma_{0k} + \sum_{i=1}^{m} (\gamma_{ij}\delta_{ik} + \gamma_{ik}\delta_{ij}) = 0 \qquad (j, k=1, \cdots, m),$$

$$(8)\qquad 2a_{0j}\gamma_{0k} + \sum_{i=1}^{m} (a_{ij}\delta_{ik} + \gamma_{ik}\beta_{ij}) = \begin{cases} 1 & (k=j), \\ 0 & (k \neq j), \end{cases} \qquad (j=0, 1, \cdots, m;\ k=1, \cdots, m).$$

* To compare with the earlier proof for finite fields, American Journal of Mathematics, vol. 21 (1899), p. 248, we have only to replace β by $-\gamma$, γ by $-\beta$, B by C, C by B.

† If there be a modulus p, we assume that $p \neq 2$. For a finite field of order 2^n, the structure was given by the writer in the American Journal of Mathematics, vol. 21 (1899), p. 243.

It follows from these relations that the inverse of S is

$$S^{-1}: \quad \begin{cases} \xi_0' = a_{00}\xi_0 + \frac{1}{2}\sum_{j=1}^{m}(\beta_{j0}\xi_j + a_{j0}\eta_j) \\ \xi_i' = 2\gamma_{0i}\xi_0 + \sum_{j=1}^{m}(\delta_{ji}\xi_j + \gamma_{ji}\eta_j) \\ \eta_i' = 2a_{0i}\xi_0 + \sum_{j=1}^{m}(\beta_{ji}\xi_j + a_{ji}\eta_j) \end{cases} \qquad (i=1, \cdots, m).$$

The conditions for the invariance of g_m under S^{-1} are seen to be

$$a_{00}^2 + 4\sum_{i=1}^{m} a_{0i}\gamma_{0i} = 1, \tag{9}$$

$$\tfrac{1}{2}a_{j0}a_{k0} + \sum_{i=1}^{m}(a_{ji}\gamma_{ki} + a_{ki}\gamma_{ji}) = 0 \qquad (j=0, 1, \cdots, m; k=1, \cdots, m), \tag{10}$$

$$\tfrac{1}{2}\beta_{j0}\beta_{k0} + \sum_{i=1}^{m}(\beta_{ji}\delta_{ki} + \beta_{ki}\delta_{ji}) = 0 \qquad (j, k=1, \cdots, m), \tag{11}$$

$$\tfrac{1}{2}a_{j0}\beta_{k0} + \sum_{i=1}^{m}(a_{ji}\delta_{ki} + \beta_{ki}\gamma_{ji}) = \begin{cases} 1 & (k=j) \\ 0 & (k \neq j) \end{cases} \qquad (j=0, 1, \cdots, m; k=1, \cdots, m). \tag{12}$$

S and S^{-1} have equal determinants, so that $|S| = \pm 1$. In fact, we take the variables in the order $\xi_0, \xi_1, \eta_1, \cdots, \xi_m, \eta_m$, and reflect on its main diagonal the determinant of S^{-1}, then interchange the second and third rows, the fourth and fifth rows, $\cdots$, and likewise the corresponding columns. The resulting determinant, aside from the factors 2 and $\frac{1}{2}$ which may be dropped, is identical with the determinant of S.

If in the above formulæ we drop the variable ξ_0 and the coefficients $a_{i0}, a_{0i}, \gamma_{i0}, \cdots$, we obtain results valid for the group $Q(m, F)$ of all linear transformations in F which leave invariant *

$$q_m \equiv \xi_1\eta_1 + \xi_2\eta_2 + \cdots + \xi_m\eta_m.$$

With such modifications, the following investigation of the structure of the group $G(m, F)$ will hold for the group $Q(m, F)$.

Let S be an arbitrary transformation of $G(m, F)$. We proceed to determine a transformation Σ, derived from

$$W_{i,j,\lambda},\ V_{i,j,\lambda},\ Q_{i,j,\lambda},\ X_{0,j,\lambda},\ Y_{0,j,\lambda},\ T_{i,\lambda},\ S_{ij},\ P_{ij}, \tag{13}$$

* For the case in which F is the Galois field of order p^n, this group was studied by the writer in the Proceedings of the London Mathematical Society, vol. 30 (1898), pp 70–98. The calculations of pp. 77–80 are here avoided by the use of the simplicity of the group G_6.

which replaces ξ_1 by the same function that S does, viz.,

$$f_1 \equiv a_{10}\xi_0 + \sum_{j=1}^{m}(a_{1j}\xi_j + \gamma_{1j}\eta_j),$$

where by (10), for $j = k = 1$,

$$\tfrac{1}{4}a_{10}^2 + \sum_{i=1}^{m} a_{1i}\gamma_{1i} = 0. \tag{14}$$

The a_{1i}, $\gamma_{1i}(i = 1, \cdots, m)$ are not all zero, since otherwise $a_{10} = 0$ and $f_1 \equiv 0$.

(a) If $a_{11} \neq 0$, we may take for Σ the product

$$T_{1,\,a_{11}}X_{0,\,1,\,\frac{1}{2}a_{10}}Q_{1,\,2,\,a_{12}}W_{1,\,2,\,\gamma_{12}}\cdots Q_{1,\,m,\,a_{1m}}W_{1,\,m,\,\gamma_{1m}},$$

which replaces ξ_1 by

$$a_{10}\xi_0 + a_{11}\xi_1 - a_{11}^{-1}(\tfrac{1}{4}a_{10}^2 + a_{12}\gamma_{12} + \cdots + a_{1m}\gamma_{1m})\eta_1 + \sum_{j=2}^{m}(a_{1j}\xi_j + \gamma_{1j}\eta_j) \equiv f_1.$$

(b) If $\gamma_{11} \neq 0$, we may choose for Σ the product

$$S_{12}T_{1,\,\gamma_{11}}X_{0,\,1,\,\frac{1}{2}a_{10}}Q_{1,\,2,\,\gamma_{12}}W_{1,\,2,\,a_{12}}\cdot Q_{1,\,3,\,a_{13}}W_{1,\,3,\,\gamma_{13}}\cdots Q_{1,\,m,\,a_{1m}}W_{1,\,m,\,\gamma_{1m}}.$$

(c) Let $a_{1j} = \gamma_{1j} = 0\,(j = 1, \cdots, s-1)$, while a_{1s}, γ_{1s} are not both zero. By case (a) or (b), we obtain a transformation Σ' which replaces ξ_s by f_1. Then will $\Sigma \equiv \Sigma' P_{1s}$ replace ξ_1 by f_1.

We may therefore set $S = S\Sigma'$, where S' is a transformation of $G(m, F)$ which leaves ξ_1 fixed. Let S' replace η_1 by

$$f_1' \equiv \beta_{10}\xi_0 + \sum_{j=1}^{m}(\beta_{1j}\xi_j + \delta_{1j}\eta_j).$$

For S' we have $a_{10} = 0$, $a_{11} = 1$, $a_{1j} = 0\,(j = 2, \cdots, m)$, $\gamma_{1j} = 0\,(j = 1, \cdots, m)$. Then by (12) for $j = k = 1$, we have $\delta_{11} = 1$. By (11) for $j = k = 1$, we have

$$\tfrac{1}{4}\beta_{10}^2 + \sum_{i=1}^{m}\beta_{1i}\delta_{1i} = 0. \tag{15}$$

The transformation

$$\Sigma_1 \equiv Y_{0,\,1,\,\frac{1}{2}\beta_{10}}V_{2,\,1,\,-\beta_{12}}Q_{2,\,1,\,-\delta_{12}}\cdots V_{m,\,1,\,-\beta_{1m}}Q_{m,\,1,\,-\delta_{1m}}$$

leaves ξ_1 fixed and replaces η_1 by f_1'. We may therefore set

$$S' = \Sigma_1 S_1, \quad S \equiv \Sigma\,\Sigma_1 S_1,$$

where S_1 is a transformation of $G(m, F)$ which leaves ξ_1 and η_1 fixed. Hence S_1 is of the form S, written above, with

$$a_{10} = \beta_{10} = 0, \quad a_{11} = \delta_{11} = 1, \quad a_{1j} = \delta_{1j} = 0 \qquad (j = 2, \cdots, m),$$

$$\gamma_{1j} = \beta_{1j} = 0 \qquad (j = 1, \cdots, m).$$

Hence, by (11) and (12), for $j=1$, we get

$$\beta_{k1}=0, \quad \delta_{k1}=0 \qquad (k=2, \cdots, m).$$

By (10) and (12), for $k=1$, we get

$$\gamma_{j1}=0, \quad \alpha_{j1}=0 \qquad (j=0, 2, \cdots, m).$$

Hence S_1 is a transformation of $G(m, F)$ involving only the variables

$$\xi_0, \quad \xi_i, \quad \eta_i \qquad (i=2, \cdots, m).$$

We proceed with S_1 as we did with S. After $m-1$ such steps, we reach a transformation S_{m-1} affecting only ξ_0, ξ_m, η_m. Let it replace ξ_m by

$$f_m \equiv \alpha_{m0}\xi_0 + \alpha_{mm}\xi_m + \gamma_{mm}\eta_m,$$

where, by (10),

$$\tfrac{1}{4}\alpha_{m0}^2 + \alpha_{mm}\gamma_{mm} = 0.$$

If $\alpha_{mm} \neq 0$, the transformation $T_{m, \alpha_{mm}} X_{0, m, \frac{1}{2}\alpha_{m0}}$ replaces ξ_m by f_m. If $\alpha_{mm}=0$, then $\alpha_{m0}=0$ and $\gamma_{mm} \neq 0$, so that we may set

$$S_{m-1} \equiv (\xi_m \eta_m) T_{m, \gamma_{mm}} K,$$

where K leaves also ξ_m fixed.* Let K replace η_m by

$$f'_m \equiv \beta_{m0}\xi_0 + \beta_{mm}\xi_m + \delta_{mm}\eta_m.$$

By (11) and (12) for $i=j=k=m$, we get

$$\delta_{mm}=1, \quad \tfrac{1}{4}\beta_{m0}^2 + \beta_{mm}\delta_{mm} = 0.$$

Hence $K = Y_{0, m, \frac{1}{2}\beta_{m0}} K'$, where K' leaves ξ_m and η_m fixed, and is therefore the identity or C_0, where C_0 alters only ξ_0 whose sign it changes. But

$$C_0 \equiv X_{0i1} Y_{0i1} X_{0i1} T_{i, -1}(\xi_i \eta_i). \tag{16}$$

It follows that an arbitrary transformation of $G(m, F)$ or of $Q(m, F)$ may be given one of the two forms A or $A(\xi_m \eta_m)$, where A is derived from the transformations (13) of determinant unity. Hence these groups contain subgroups of index 2, designated by $G'(m, F)$ and $Q'(m, F)$, generated by the transformations (13).

Consider, for $m \geqq 3$, the following subgroups of $G'(m, F)$ and $Q'(m, F)$:

$$G_1(m, F) \equiv \{S_{ij}, \quad W_{i,j,\lambda}, \quad X_{0,j,\lambda} \ (i, j=1, \cdots, m; i \neq j)\},$$

$$Q_1(m, F) \equiv \{S_{ij}, \quad W_{i,j,\lambda} \qquad (i, j=1, \cdots, m; i \neq j)\},\dagger$$

* For the group $Q(m, F)$, K is necessarily the identity.

† For $m=3$, $Q_1(m, F)$ is the group G_6 of § 6.

where λ is arbitrary in the field F. By the formulæ of § 6, they contain the transformations

$$V_{i,j,\lambda}, \quad Q_{i,j,\lambda}, \quad P_{ij}T_{j,-1} \qquad (i, j=1, \cdots, m; i \neq j),$$

while $G_1(m, F)$ contains also $Y_{0,j,\lambda}$. Hence they contain

$$T_{1,\mu}T_{2,\mu} \equiv S_{12}P_{12}T_{1,-1}V_{1,2,\mu-1}W_{1,2,\mu}V_{1,2,\mu-1}, \tag{17}$$

$$T_{1,\mu^2} \equiv T_{1,\mu}T_{2,\mu} \cdot T_{2,\mu-1}T_{3,\mu-1} \cdot T_{3,\mu}T_{1,\mu}. \tag{18}$$

But $T_{k,\lambda}$ transforms $W_{i,j,\lambda}$, $V_{i,j,\lambda}$, $Q_{i,j,\lambda}$, $X_{0,j,\lambda}$, $Y_{0,j,\lambda}$, $T_{i,\lambda}$ into transformations of the same respective forms. Also

$$T_{i,\lambda}S_{ij} = S_{ij}T_{i,\lambda^{-1}}, \quad T_{i,\lambda}P_{ij} = P_{ij}T_{j,\lambda}. \tag{19}$$

Hence every transformation of the group $G'(m, F)$ or $Q'(m, F)$ may be given one of the forms Σ, $\Sigma T_{m,\nu}$, where Σ belongs to $G_1(m, F)$ or $Q_1(m, F)$, respectively, while ν runs through the series of elements of F which are not-squares and whose ratios are all not-squares.

These results hold true for the group $G_1(2, F) \equiv G_5$ of § 6, viz.,

$$G_1(2, F) \equiv \{P_{12}T_{2,-1}, \ S_{12}, \ W_{1,2,\lambda}, \ Q_{1,2,\lambda}, \ X_{0,1,\lambda}\}.$$

Indeed, the latter group contains $Y_{0,1,\lambda}$, $X_{0,2,\lambda}$, $Y_{0,2,\lambda}$, $V_{1,2,\lambda}$, $Q_{2,1,\lambda}$, $T_{1,\mu}T_{2,\mu}$ and, by (16), $C_0(\xi_1\eta_1)T_{1,-1}$. The latter transforms $T_{1,\mu}T_{2,\mu}$ into $T_{1,\mu-1}T_{2,\mu}$, so that the product T_{2,μ^2} belongs to the group.

The group $G'(m, F)$, for $m \geqq 3$, contains the invariant subgroup $G_1(m, F)$; the group $Q'(m, F)$, for $m \geqq 2$, contains the invariant subgroup $Q_1(m, F)$. The invariant subgroup is extended to the main group by the right-hand extenders $T_{m,\nu}$, where ν runs through the series of those not-squares of F, the ratio of no two of which is a square.

§ 8. *Structure of the groups $G_1(m, F)$ and $Q_1(m, F)$.*

By § 6 we have the results: *

The group $G_1(2, F)$ on five variables is simple. The senary group $Q_1(3, F)$ is simple or has the maximal invariant subgroup composed of the identity I and the transformation $T_{1,-1}T_{2,-1}T_{3,-1}$ according as -1 is a not-square or a square in the field F.

We employ these theorems in dealing with the case of general m. Let J be an invariant subgroup of $G_1(m, F)$ containing a transformation S not the identity I. To treat simultaneously the group $Q_1(m, F)$, let J be an invariant subgroup containing a transformation S neither the identity nor

$$T \equiv T_{1,-1}T_{2,-1}\cdots T_{m,-1},$$

* If there be a modulus p, we assume, in this section, that $p \neq 2$.

in case the latter belongs to $Q_1(m, F)$. The groups $G_1(m, F)$ and $Q_1(m, F)$ will be considered together under the notation G. We assume that $m \geqq 3$.

LEMMA I. *The group J contains a transformation which multiplies ξ_1 by a constant and does not reduce to I or T.*

By hypothesis, J contains a transformation S neither I nor T. Let S replace ξ_1 by

$$f_1 \equiv a_{10}\xi_0 + \sum_{j=1}^{m}(a_{1j}\xi_j + \gamma_{1j}\eta_j) \neq a_{11}\xi_1,$$

the coefficients being subject to the condition (14).

(*a*) If $\gamma_{11} \neq 0$, the group G contains the product

$$P \equiv T_{1,\gamma_{11}^{-1}} T_{2,\gamma_{11}^{-1}} Y_{0,1,\frac{1}{2}a_{10}} V_{2,1,-\gamma_{11}a_{12}} Q_{2,1,-\gamma_{11}^{-1}\gamma_{12}} K,$$

where K denotes the transformation

$$K \equiv V_{3,1,-a_{13}} Q_{3,1,-\gamma_{13}} \cdots V_{m,1,-a_{1m}} Q_{m,1,-\gamma_{1m}}.$$

Employing (14), we find that P replaces ξ_1 by $\gamma_{11}^{-1}\xi_1$ and η_1 by f_1. Hence J contains $S_1 \equiv P^{-1}SP$, which replaces ξ_1 by $\gamma_{11}^{-1}\eta_1$.

If S_1 multiplies ξ_2 by a constant, J contains its transform S_1' by $P_{12}T_{2,-1}$. This S_1' multiplies ξ_1 by a constant and is neither I nor T.

If S_1 does not multiply ξ_2 by a constant, there exists in G a transformation B leaving ξ_1 and η_1 unaltered and not commutative with S_1, so that J contains $S_1^{-1}B^{-1}S_1B$, which leaves ξ_1 fixed and is neither I nor T. In fact, if S_1 be commutative with $V_{2,3,\lambda}$, we find, on equating the expressions by which $S_1V_{2,3,\lambda}$ and $V_{2,3,\lambda}S_1$ replace η_3, that

$$\eta_3' - \lambda\xi_2' = \eta_3' + (\ )\xi_2 + (\ )\xi_3.$$

Similarly, if S_1 be commutative with $Q_{3,2,\lambda}$, we get

$$\xi_3' + \lambda\xi_2' = \xi_3' + (\ )\xi_2 + (\ )\eta_3.$$

Hence would $\xi_2' = (\ )\xi_2$, contrary to hypothesis.

(*b*) If $\gamma_{11} = 0$, we may take* $a_{12} \neq 0$. Then G contains

$$R \equiv T_{2,a_{12}} T_{3,a_{12}} X_{0,2,\frac{1}{2}a_{10}} Q_{2,1,a_{11}} Q_{2,3,a_{12}^{-1}a_{13}} W_{2,3,a_{12}\gamma_{13}} K_1,$$

$$K_1 \equiv Q_{2,4,a_{14}} W_{2,4,\gamma_{14}} \cdots Q_{2,m,a_{1m}} W_{2,m,\gamma_{1m}}.$$

Employing (14), we find that R replaces ξ_2 by f_1 without altering ξ_1. Then J contains $S_2 \equiv R^{-1}SR$ which replaces ξ_1 by ξ_2.

If S_2 multiplies ξ_3 by a constant, J contains its transform S_2' by $P_{13}T_{1,-1}$. But S_2' multiplies ξ_1 by a constant and is neither I nor T.

---

* If $a_{12} = a_{13} = \cdots = a_{1m} = 0$, then $a_{10} = 0$ by (14). Not every γ_{1j} is zero by hypothesis. If $\gamma_{12} \neq 0$, for example, we take in place of S its transform by S_{23}, for which $a_{12}' \neq 0$.

If S_2 does not multiply ξ_3 by a constant, S_2 is not commutative with both $V_{3,1,\lambda}$ and $V_{3,2,\lambda}$, since $S_2 V_{3,k,\lambda}$ and $V_{3,k,\lambda} S_2$ replace η_k by $\eta_k' - \lambda\xi_3'$ and $\eta_k' + (\ )\xi_3 + (\ )\xi_k$, respectively. Hence J contains

$$S_2^{-1} V_{3,k,\lambda}^{-1} S_2 V_{3,k,\lambda} \qquad (k=1, 2)$$

which leave ξ_1 fixed (so that neither is T), and are not both the identity.

LEMMA II. *The group J contains a transformation which leaves ξ_1 and η_1 unaltered and is different from the identity.*

In view of Lemma I, we may suppose that J contains a transformation S, different from I and T, which replaces ξ_1 by $a\xi_1$ and η_1 by

$$\beta_{10}\xi_0 + \sum_{j=1}^{m} (\beta_{1j}\xi_j + \delta_{1j}\eta_j),$$

where by (12), for $j = k = 1$, we have $\delta_{11} = a^{-1}$, and by (11), for $j = k = 1$,

$$\tfrac{1}{4}\beta_{10}^2 + \sum_{i=1}^{m} \beta_{1i}\delta_{1i} = 0. \tag{15}$$

(A) Let $\beta_{11} = 0$, $\beta_{1j} = \delta_{1j} = 0 (j = 2, \cdots, m)$. Then $\beta_{10} = 0$ by (15). Hence $S = T_{1,a} S_1$, where S_1 leaves ξ_1 and η_1 unaltered. Hence,* S_1 involves only the variables ξ_0, ξ_i, $\eta_i (i = 2, \cdots, m)$. If $a = 1$, the Lemma is proved. Let next $a \neq 1$.

If $S_1 = I$, or if, when $G \equiv Q_1(m, F)$, $S = T_{2,-1} T_{3,-1} \cdots T_{m,-1} \equiv \tau$, the group J contains $T_{1,a}$ or $S^2 = T_{1,a^2}$ respectively. In the second case, $a \neq -1$, since $S \neq T$. Transforming by $P_{12} T_{2,-1}$, we obtain in either case a transformation leaving ξ_1 and η_1 fixed and not the identity.

If S_1 be neither I nor τ, there exists in G a transformation Σ_1 affecting the same variables as S_1 and not commutative with S_1.† Hence J contains

$$S^{-1}\Sigma_1^{-1} S \Sigma_1 \equiv S_1^{-1}\Sigma_1^{-1} S_1 \Sigma_1 \neq I,$$

which leaves ξ_1 and η_1 unaltered.

(B) Let $\beta_{11} = 0$, and β_{1j}, $\delta_{1j} (j = 2, \cdots, m)$ be not all zero. Then, by § 7, G contains a transformation L which leaves ξ_1 and η_1 fixed and replaces ξ_2 by

$$\beta_{10}\xi_0 + \sum_{j=2}^{m} (\beta_{1j}\xi_j + \delta_{1j}\eta_j) \qquad \left[\tfrac{1}{4}\beta_{10}^2 + \sum_{j=2}^{m} \beta_{1j}\delta_{1j} = 0\right].$$

Hence J contains $S_1 = L^{-1} S L$, which replaces ξ_1 by $a\xi_1$ and η_1 by $\xi_2 + a^{-1}\eta_1$. The latter function is invariant under the transformations $Q_{3,2,\lambda}$, $V_{2,3,\lambda}$, T_{3,μ^2} and $T_{1,\lambda} T_{2,\lambda^{-1}}$ belonging to G. If any one of these, say Σ, is not commuta-

* See § 7, case (c).

† For $G \equiv G_1(m, F)$, the transformation changing the signs of $\xi_0, \xi_2, \eta_2, \cdots, \xi_m, \eta_m$ is of determinant -1 and hence does not belong to G.

tive with S_1, then J contains $S_1^{-1}\Sigma^{-1}S_1\Sigma \neq I$, which leaves ξ_1 and η_1 fixed. Suppose next that they are all commutative with S_1. Equating the two expressions by which $S_1 V_{2,3,\lambda}$ and $V_{2,3,\lambda}S_1$ replace η_2, and the two by which they replace η_3, we get

$$\xi_3' = \delta_{22}\xi_3 - \delta_{23}\xi_2, \quad \xi_2' = -\delta_{32}\xi_3 + \delta_{33}\xi_2.$$

Equating the expressions by which $S_1 Q_{3,2,\lambda}$ and $Q_{3,2,\lambda}S_1$ replace ξ_3, and those by which they replace η_2, we find that

$$\xi_2' = a_{33}\xi_2 - \gamma_{32}\eta_3, \quad \eta_3' = -\beta_{23}\xi_2 + \delta_{22}\eta_3.$$

The field F contains an element λ different from 0 and 1. If we equate the expressions by which $T_{1,\lambda}T_{2,\lambda^{-1}}S_1$ and $S_1 T_{1,\lambda}T_{2,\lambda^{-1}}$ replace η_2, we find that $\beta_{23} = \delta_{23} = 0$. Hence S_1 merely multiplies ξ_3 and η_3 by the same constant δ_{22}. Transforming S_1 by $P_{13}T_{1,-1}$, we obtain a transformation of the kind treated in case (A).

(C) Let $\beta_{11} \neq 0$, β_{1j}, δ_{1j} $(j = 2, \cdots, m)$ be not all zero. By a simple transformation, we may take $\delta_{12} \neq 0$. Transforming S by $T_{2,\delta_{12}}T_{3,\delta_{12}}$, we reach a transformation S' with $\beta_{11} \neq 0$, $\delta_{12} = 1$. Then

$$\omega \equiv Y_{0,2,\frac{1}{2}\beta_{10}} Q_{3,2,-\delta_{13}} V_{2,3,\beta_{13}} \cdots Q_{m,2,-\delta_{1m}} V_{2,m,\beta_{1m}}$$

leaves ξ_1, η_1, and ξ_2 unaltered and replaces η_2 by

$$\beta_{10}\xi_0 + (\beta_{11}\delta_{11} + \beta_{12})\xi_2 + \eta_2 + \sum_{j=3}^{m}(\beta_{1j}\xi_j + \delta_{1j}\eta_j).$$

Then J contains $S_1 \equiv \omega^{-1}S'\omega$, which replaces ξ_1 by $a\xi_1$, and η_1 by

$$\beta_{11}\xi_1 + a^{-1}\eta_1 - a^{-1}\beta_{11}\xi_2 + \eta_2.$$

Let $\mu \equiv -\beta_{11}a^{-1} \neq 0$. If among the transformations $Q_{3,2,\mu}W_{2,3,1} \equiv \sigma$, $T_{3,\mu}T_{2,\mu}S_{23}$, etc., of G, which leave ξ_1, η_1, and $\mu\xi_2 + \eta_2$ invariant, there exists one, say R, which is not commutative with S_1, then J contains $S_1^{-1}R^{-1}S_1R$ which leaves ξ_1 and η_1 fixed and differs from the identity. In the contrary case, we find, on equating the functions by which $S_1\sigma$ and σS_1 replace ξ_2, that

$$\eta_3' = (\ )\eta_3 - a_{23}\eta_2 + \mu a_{23}\xi_2.$$

Then, by (11) for $j = k = 3$, we have $a_{23} = 0$. Finally, if S_1 be commutative with $T_{3,\mu}T_{2,\mu}S_{23}$, it must multiply ξ_3 and η_3 by the same constant.

(D) Let $\beta_{11} \neq 0$, $\beta_{1j} = \delta_{1j} = 0$ $(j = 2, \cdots, m)$. Then, by (15),

$$\tfrac{1}{4}\beta_{10}^2 + \beta_{11}\delta_{11} = 0, \quad \delta_{11} = a^{-1}.$$

Hence S replaces ξ_1 by $a\xi_1$ and replaces η_1 by

$$\beta_{10}\xi_0 + \beta_{11}\xi_1 + a^{-1}\eta_1 = a^{-1}(\eta_1 + 2\lambda\xi_0 - \lambda^2\xi_1),$$

if we set $2\lambda \equiv a\beta_{10}$. Hence $S = Y_{0,1,\lambda}T_{1,a}S_1$, where S_1 leaves ξ_1 and η_1 unaltered and so involves only $\xi_0, \xi_i, \eta_i (i = 2, \cdots, m)$. Then

$$T_{1,\rho}^{-1} S T_{1,\rho} \cdot S^{-1} \equiv Y_{0,1,\lambda\rho^{-1}-\lambda}$$

belongs to J and is not the identity if $\rho \neq 1$. Transforming it by $P_{12}T_{2,-1}$, we obtain in J a transformation $\neq I$, which leaves ξ_1 and η_1 unaltered.

In the proofs of lemmas I and II, we assumed the existence of the variables $\xi_0, \xi_1, \eta_1, \xi_2, \eta_2, \xi_3, \eta_3$ only. If $m \geqq 4$, we may therefore conclude that J contains a transformation different from I and T which leaves $\xi_1, \eta_1, \xi_2, \eta_2$ unaltered. After $m - 2$ applications of the lemmas, we reach in J a transformation, neither I nor T, which affects only $\xi_0, \xi_{m-1}, \eta_{m-1}, \xi_m, \eta_m$. Transforming it by $P_{1\,m-1}P_{2m}$, which belongs to G, we obtain a transformation, neither I nor T, which affects only $\xi_0, \xi_1, \eta_1, \xi_2, \eta_2$. From the simplicity of $G_1(2, F)$, it follows, when $G \equiv G_1(m, F)$, that J contains all the transformations of $G_1(2, F)$. Transforming them by the $P_{ij}T_{j,-1}$, we reach in J all the generators of $G_1(m, F)$. Since $Q_1(3, F)$ is simple or has the maximal invariant subgroup $\{I, T\}$, it follows, when $G \equiv Q_1(m, F)$, that J contains the generators of $Q_1(3, F)$ and, therefore, by transformation by the $P_{ij}T_{j,-1}$, the generators of $Q_1(m, F)$.

If $m \geqq 2$, the group $G_1(m, F)$ is simple. If $m \geqq 3$, the group $Q_1(m, F)$ is simple or has the maximal invariant subgroup $\{I, T\}$, according as -1 is a not-square or a square in the field F.

§ 9. *Definition and generators of a subgroup of $G_1(3, F)$.*

We next define and investigate the septenary group in an arbitrary* field F which becomes, for the case of a continuous field, the continuous group of fourteen parameters studied by KILLING, ENGEL,† and CARTAN.‡

The totality of linear homogeneous transformations S on seven variables with coefficients in F which leave absolutely invariant

$$g_3 \equiv \xi_0^2 + \xi_1\eta_1 + \xi_2\eta_2 + \xi_3\eta_3$$

form a group $G(3, F)$. Taking $m = 3$, and giving S the notation of § 7, we may take as the conditions upon S the relations (9), (10), (11), (12). We study the group H of transformations S, belonging to $G(3, F)$, which, when operating cogrediently upon the two sets of variables

$$(20) \qquad \xi_0, \xi_1, \eta_1, \xi_2, \eta_2, \xi_3, \eta_3; \quad \bar{\xi}_0, \bar{\xi}_1, \bar{\eta}_1, \bar{\xi}_2, \bar{\eta}_2, \bar{\xi}_3, \bar{\eta}_3,$$

* As in §§ 7–8, we assume that $p \neq 2$, if F has a modulus p.

† LIE-ENGEL, *Transformationsgruppen*, vol. 3, pp. 763–765, 777.

‡ CARTAN, *Thèses*, Paris, 1894, pp. 146, 149–151.

leave invariant the system of equations

$$(21)\qquad \begin{cases} X_1 + Y_{23} = 0, & X_2 + Y_{31} = 0, & X_3 + Y_{12} = 0, \\ Y_1 + X_{23} = 0, & Y_2 + X_{31} = 0, & Y_3 + X_{12} = 0. \end{cases}$$

We have here employed the notations

$$X_i \equiv \begin{vmatrix} \xi_0 & \xi_i \\ \bar{\xi}_0 & \bar{\xi}_i \end{vmatrix}, \quad Y_i \equiv \begin{vmatrix} \xi_0 & \eta_i \\ \bar{\xi}_0 & \bar{\eta}_i \end{vmatrix}, \quad X_{ij} \equiv \begin{vmatrix} \xi_i & \xi_j \\ \bar{\xi}_i & \bar{\xi}_j \end{vmatrix}, \quad Y_{ij} \equiv \begin{vmatrix} \eta_i & \eta_j \\ \bar{\eta}_i & \bar{\eta}_j \end{vmatrix}, \quad Z_{ij} \equiv \begin{vmatrix} \xi_i & \eta_j \\ \bar{\xi}_i & \bar{\eta}_j \end{vmatrix}.$$

Multiplying the equations in the first row of (21) by η_1, η_2, η_3, respectively, and adding the results, we get $X_1\eta_1 + X_2\eta_2 + X_3\eta_3 = 0$, since

$$Y_{23}\eta_1 + Y_{31}\eta_2 + Y_{13}\eta_3 \equiv \begin{vmatrix} \eta_1 & \eta_2 & \eta_3 \\ \eta_1 & \eta_2 & \eta_3 \\ \bar{\eta}_1 & \bar{\eta}_2 & \bar{\eta}_3 \end{vmatrix} \equiv 0.$$

Similarly from the equations in the second row of (21), we get

$$Y_1\xi_1 + Y_2\xi_2 + Y_3\xi_3 = 0.$$

In view of the identity

$$Y_i\xi_i - X_i\eta_i \equiv \xi_0(\xi_i\bar{\eta}_i - \bar{\xi}_i\eta_i) \equiv \xi_0 Z_{ii},$$

we derive the equation* [a consequence of equations (21)]

$$(22)\qquad Z_{11} + Z_{22} + Z_{33} = 0.$$

An inspection of equations (21) and (22) leads to a proof of the following

LEMMA: *A linear equation involving X_i, Y_i, X_{ij}, Y_{ij}, Z_{ij} will be a consequence of equations* (21) *if, and only if, the coefficient of X_i equals that of Y_{jk}, the coefficient of Y_i equals that of X_{jk}, the coefficients of Z_{11}, Z_{22}, Z_{33} are all equal, and the coefficient of each $Z_{r,s}$ $(r, s = 1, 2, 3;\ r \neq s)$ is zero; where i, j, k is any cyclic permutation of* 1, 2, 3.

When operating cogrediently upon the variables (20), the transformation

$$S: \begin{cases} \xi_i' = a_{i0}\xi_0 + a_{i1}\xi_1 + a_{i2}\xi_2 + a_{i3}\xi_3 + \gamma_{i1}\eta_1 + \gamma_{i2}\eta_2 + \gamma_{i3}\eta_3 & (i = 0, 1, 2, 3) \\ \eta_i' = \beta_{i0}\xi_0 + \beta_{i1}\xi_1 + \beta_{i2}\xi_2 + \beta_{i3}\xi_3 + \delta_{i1}\eta_1 + \delta_{i2}\eta_2 + \delta_{i3}\eta_3 & (i = 1, 2, 3) \end{cases}$$

---

* Other equations may be derived from (21); for example,

$$Y_{12}X_{12} + Y_{23}X_{23} + Y_{31}X_{31} = 0, \quad Y_{12}^2 + Z_{32}X_{32} + Z_{31}X_{31} = 0.$$

Since they are quadratic in each set of variables ξ, η; $\bar{\xi}$, $\bar{\eta}$, they do not enter into the discussion of the invariance of equations (21).

replaces the function X_l by the expression

$$\sum_{i=1}^{3}\begin{vmatrix} a_{00} & a_{0i} \\ a_{l0} & a_{li}\end{vmatrix} X_i + \sum_{i=1}^{3}\begin{vmatrix} a_{00} & \gamma_{0i} \\ a_{l0} & \gamma_{li}\end{vmatrix} Y_i + \sum_{i,j}^{1,2,3}\begin{vmatrix} a_{0i} & \gamma_{0j} \\ a_{li} & \gamma_{lj}\end{vmatrix} Z_{ij}$$
$$+ \sum_{\substack{i,j=1,2,3\\ i<j}}\left\{\begin{vmatrix} a_{0i} & a_{0j} \\ a_{li} & a_{lj}\end{vmatrix} X_{ij} + \begin{vmatrix} \gamma_{0i} & \gamma_{0j} \\ \gamma_{li} & \gamma_{lj}\end{vmatrix} Y_{ij}\right\}.$$

Let l, m, n be any cyclic permutation of $1, 2, 3$. Then S replaces Y_{mn} by

$$\sum_{i=1}^{3}\begin{vmatrix} \beta_{m0} & \beta_{mi} \\ \beta_{n0} & \beta_{ni}\end{vmatrix} X_i + \sum_{i=1}^{3}\begin{vmatrix} \beta_{m0} & \delta_{mi} \\ \beta_{n0} & \delta_{ni}\end{vmatrix} Y_i + \sum_{i,j}\begin{vmatrix} \beta_{mi} & \delta_{mj} \\ \beta_{ni} & \delta_{nj}\end{vmatrix} Z_{ij}$$
$$+ \sum_{i,j}\left\{\begin{vmatrix} \beta_{mi} & \beta_{mj} \\ \beta_{ni} & \beta_{nj}\end{vmatrix} X_{ij} + \begin{vmatrix} \delta_{mi} & \delta_{mj} \\ \delta_{ni} & \delta_{nj}\end{vmatrix} Y_{ij}\right\}.$$

Hence S replaces the equation $X_l + Y_{mn} = 0$ by an equation which is linear in $X_i, Y_i, X_{ij}, Y_{ij}, Z_{ij}$. Applying the above lemma, we see that the resulting equation will be a consequence of equations (21) if, and only if, the conditions (23), (24), (25) below are satisfied. Similarly, S replaces the equation $Y_l + X_{mn} = 0$ by an equation which is linear in $X_i, Y_i, X_{ij}, Y_{ij}, Z_{ij}$ with coefficients obtained from the corresponding coefficients in the earlier equation by interchanging a_{r0} with β_{r0}, a_{ri} with β_{ri}, γ_{ri} with δ_{ri}, for $r = 1, 2, 3$; $i = 1, 2, 3$. In view of the lemma, the resulting equation will be a consequence of equations (21), if, and only if, the conditions (26), (27), (28) are satisfied.

$$(23)\qquad \begin{vmatrix} a_{00} & a_{0i} \\ a_{l0} & a_{li}\end{vmatrix} + \begin{vmatrix} \beta_{m0} & \beta_{mi} \\ \beta_{n0} & \beta_{ni}\end{vmatrix} = \begin{vmatrix} \gamma_{0j} & \gamma_{0k} \\ \gamma_{lj} & \gamma_{lk}\end{vmatrix} + \begin{vmatrix} \delta_{mj} & \delta_{mk} \\ \delta_{nj} & \delta_{nk}\end{vmatrix}.$$

$$(24)\qquad \begin{vmatrix} a_{00} & \gamma_{0i} \\ a_{l0} & \gamma_{li}\end{vmatrix} + \begin{vmatrix} \beta_{m0} & \delta_{mi} \\ \beta_{n0} & \delta_{ni}\end{vmatrix} = \begin{vmatrix} a_{0j} & a_{0k} \\ a_{lj} & a_{lk}\end{vmatrix} + \begin{vmatrix} \beta_{mj} & \beta_{mk} \\ \beta_{nj} & \beta_{nk}\end{vmatrix}.$$

$$(25)\qquad \begin{vmatrix} a_{0i} & \gamma_{0j} \\ a_{li} & \gamma_{lj}\end{vmatrix} + \begin{vmatrix} \beta_{mi} & \delta_{mj} \\ \beta_{ni} & \delta_{nj}\end{vmatrix} \equiv C_{ij}, \quad \begin{cases} C_{11} = C_{22} = C_{33}. \\ C_{ij} = 0 \end{cases} \qquad (i, j = 1, 2, 3;\ i \neq j).$$

$$(26)\qquad \begin{vmatrix} a_{00} & a_{0i} \\ \beta_{l0} & \beta_{li}\end{vmatrix} + \begin{vmatrix} a_{m0} & a_{mi} \\ a_{n0} & a_{ni}\end{vmatrix} = \begin{vmatrix} \gamma_{0j} & \gamma_{0k} \\ \delta_{lj} & \delta_{lk}\end{vmatrix} + \begin{vmatrix} \gamma_{mj} & \gamma_{mk} \\ \gamma_{nj} & \gamma_{nk}\end{vmatrix}.$$

$$(27)\qquad \begin{vmatrix} a_{00} & \gamma_{0i} \\ \beta_{l0} & \delta_{li}\end{vmatrix} + \begin{vmatrix} a_{m0} & \gamma_{mi} \\ a_{n0} & \gamma_{ni}\end{vmatrix} = \begin{vmatrix} a_{0j} & a_{0k} \\ \beta_{lj} & \beta_{lk}\end{vmatrix} + \begin{vmatrix} a_{mj} & a_{mk} \\ a_{nj} & a_{nk}\end{vmatrix}.$$

$$(28)\qquad \begin{vmatrix} a_{0i} & \gamma_{0j} \\ \beta_{li} & \delta_{lj}\end{vmatrix} + \begin{vmatrix} a_{mi} & \gamma_{mj} \\ a_{ni} & \gamma_{nj}\end{vmatrix} = d_{ij}, \quad \begin{cases} d_{11} = d_{22} = d_{33}, \\ d_{ij} = 0 \end{cases} \qquad (i, j = 1, 2, 3;\ i \neq j).$$

The formulæ hold for any cyclic permutations i, j, k; l, m, n of $1, 2, 3$.

The transformations S of the group H may be defined by the conditions (9), (10), (11), (12) *and* (23)–(28).

Among the transformations of H occur the simple types: *

$$(29)\qquad Q_{i,j,\tau},\ T_{i,\tau^{-2}}T_{j,\tau}T_{k,\tau},\ X_{0,i,\tau}V_{j,k,\tau},\ Y_{0,i,\tau}W_{j,k,\tau},$$

where τ is arbitrary in the field F, and i, j, k form any cyclic permutation of $1, 2, 3$. From them we obtain, as in § 6,

$$T_{i,-1}P_{ij} \equiv P_{ij}T_{j,-1} = Q_{j,i,-1}Q_{i,j,1}Q_{j,i,-1};$$

$$\begin{aligned} X_{0,1,1}V_{2,3,1}\cdot Y_{0,1,1}W_{2,3,1}\cdot X_{0,1,1}V_{2,3,1} &= X_{0,1,1}Y_{0,1,1}X_{0,1,1}\cdot V_{2,3,1}W_{2,3,1}V_{2,3,1} \\ &= C_0(\xi_1\eta_1)T_{1,-1}\cdot T_{2,-1}P_{23}S_{23} = (\xi_1\eta_1)(\xi_2\eta_2)(\xi_3\eta_3)C_0T_{1,-1}T_{2,-1}P_{23}, \end{aligned}$$

upon applying formulæ (16), (17), the latter with $\mu = 1$, and with $2, 3$ in place of $1, 2$. Since $T_{2,-1}P_{23}$ belongs to H, it follows that H contains

$$(30)\qquad \Sigma \equiv (\xi_1\eta_1)(\xi_2\eta_2)(\xi_3\eta_3)C_0T_{1,-1}.$$

The transformations $T_{i,\tau}T_{j,\tau^{-1}}$ leave invariant g_3 and the equations (21), and therefore belong to the group H. From the transformations (29) we readily derive $T_{i,\tau}T_{j,\tau^{-1}}$, for the case in which τ is a cube in the field.

THEOREM: *The transformations of H of determinant $+1$ form a subgroup H' of index 2 which is generated by the transformations*

$$(31)\qquad Q_{i,j,\tau},\quad T_{i,\tau}T_{j,\tau^{-1}},\quad X_{0,i,\tau}V_{j,k,\tau},\quad Y_{0,i,\tau}W_{j,k,\tau}.$$

Let S be an arbitrary transformation of H and let it be exhibited in the above form. We are to prove that there exists a transformation K derived from the types (31) such that $KS = I$, the identity, or $C_0T_{3,-1}$, the latter of determinant -1.

We may assume that $a_{11} \neq 0$ in S. For, if $a_{1i} \neq 0$, the product $T_{i,-1}P_{i1}S$ has $a_{11} \neq 0$; if $\gamma_{1i} \neq 0$, the product ΣS has $a_{1i} \neq 0$; while the case $a_{1i} = \gamma_{1i} = 0$ $(i = 1, 2, 3)$ is excluded, since then $a_{10} = 0$ by (14). The product $S_1 \equiv T_{1,a_{11}^{-1}}T_{2,a_{11}}S$ replaces ξ_1 by a function of the form

$$f \equiv a_{10}\xi_0 + \xi_1 + a_{12}\xi_2 + a_{13}\xi_3 + \gamma_{11}\eta_1 + \gamma_{12}\eta_2 + \gamma_{13}\eta_3.$$

Then $Y_{0,2,\gamma_{13}}W_{3,1,\gamma_{13}}S_1 \equiv S_2$ replaces ξ_1 by a function of the form f with $\gamma_{13} = 0$. Then $Q_{1,3,-a_{13}}S_2 \equiv S_3$ replaces ξ_1 by a function f with $\gamma_{13} = a_{13} = 0$. Next, $Q_{1,2,-a_{12}}S_3 \equiv S_4$ replaces ξ_1 by a function

$$f' \equiv a_{10}\xi_0 + \xi_1 + \gamma_{11}\eta_1 + \gamma_{12}\eta_2.$$

Then, by (14), we have $\frac{1}{4}a_{10}^2 + \gamma_{11} = 0$. If $\gamma_{11} \neq 0$, $Q_{2,1,\kappa}S_4 \equiv S_5$ replaces ξ_1

* They correspond respectively to the generators X_{ij}, X_{ii}, X_{i0}, $-X_{0i}$ of CARTAN, p. 146.

by a function of the form f' with $\gamma_{12}-\kappa\gamma_{11}$ in place of γ_{12}. By a proper choice of κ, we make the new γ_{12} equal to zero. Hence S_5 replaces ξ_1 by

$$\xi_1 + a_{10}\xi_0 - \tfrac{1}{4}a_{10}^2\eta_1,$$

so that $(X_{0,1,\frac{1}{2}a_{10}}V_{2,3,\frac{1}{2}a_{10}})^{-1}S_5$ leaves ξ_1 unaltered. But, if $\gamma_{11}=0$, then $f'\equiv\xi_1+\gamma_{12}\eta_2$, so that $Y_{0,3,-\gamma_{12}}W_{1,2,-\gamma_{12}}S_4$ leaves ξ_1 unaltered.

Consider a transformation S' which replaces ξ_1 by ξ_1, and η_1 by

$$f_1 \equiv \beta_{10}\xi_0+\beta_{11}\xi_1+\eta_1+\beta_{12}\xi_2+\beta_{13}\xi_3+\delta_{12}\eta_2+\delta_{13}\eta_3.$$

Then, by applying in succession as left-hand multipliers $Q_{3,1,\delta_{13}}$, $X_{0,2,\beta_{13}}V_{3,1,\beta_{13}}$, $Q_{2,1,\delta_{12}}$, we obtain a transformation S'' which replaces ξ_1 by ξ_1, and η_1 by $\beta_{10}\xi_0+\beta_{11}\xi_1+\eta_1+\beta_{12}\xi_2$. By (15), $\beta_{11}=-\frac{1}{4}\beta_{10}^2$. If $\beta_{11}=0$, S'' replaces η_1 by $\eta_1+\beta_{12}\xi_2$, so that

$$X_{0,3,-\beta_{12}}V_{1,2,-\beta_{12}}S''$$

leaves ξ_1 and η_1 unaltered. If $\beta_{11}\neq 0$,

$$(Y_{0,1,\frac{1}{2}\beta_{10}}W_{2,3,\frac{1}{2}\beta_{10}})^{-1}S''\equiv S'''$$

replaces ξ_1 by ξ_1, and η_1 by $\eta_1+\beta_{12}\xi_2-\frac{1}{2}\beta_{10}\eta_3$. Then $Q_{3,1,-\frac{1}{2}\beta_{10}}S'''$ replaces ξ_1 by ξ_1, and η_1 by $\eta_1+\beta_{12}\xi_2$, a case just considered.

It remains to discuss those substitutions S of H which do not alter ξ_1 and η_1 and therefore have (compare § 7)

$$a_{11}=\delta_{11}=1,\quad a_{12}=a_{13}=a_{21}=a_{31}=0,\quad \delta_{12}=\delta_{13}=\delta_{21}=\delta_{31}=0,$$

$$a_{01}=a_{10}=\beta_{10}=\gamma_{01}=0,\quad \beta_{1i}=\beta_{i1}=\gamma_{1i}=\gamma_{i1}=0\quad (i=1,2,3).$$

By (25), for $(l,i,j)=(1,1,2),(1,1,3),(2,2,1),(2,3,1),(3,2,1),(3,3,1)$, we get respectively

$$\gamma_{02}=0,\quad \gamma_{03}=0,\quad \beta_{32}=0,\quad \beta_{33}=0,\quad \beta_{22}=0,\quad \beta_{23}=0.$$

By (28), for $(l,i,j)=(1,2,1),(1,3,1),(2,1,2),(2,1,3),(3,1,2),(3,1,3)$, we get respectively

$$a_{02}=0,\quad a_{03}=0,\quad \gamma_{32}=0,\quad \gamma_{33}=0,\quad \gamma_{22}=0,\quad \gamma_{23}=0.$$

By (24), for $(l,i)=(3,1)$, $\beta_{20}=0$; for $(l,i)=(2,1)$, $\beta_{30}=0$. By (26), for $(l,i)=(3,1)$, $a_{20}=0$; for $(l,i)=(2,1)$, $a_{30}=0$. By (27), for $(l,i)=(3,2),(2,3),(3,3),(2,2)$, we get respectively

$$-a_{23}=a_{00}\delta_{32},\quad -a_{32}=a_{00}\delta_{23},\quad a_{22}=a_{00}\delta_{33},\quad a_{33}=a_{00}\delta_{22}.$$

Finally, by (23), for $(l,i)=(1,1)$, and by (9), we get respectively

$$\begin{vmatrix}\delta_{22} & \delta_{23}\\ \delta_{32} & \delta_{33}\end{vmatrix}=a_{00},\quad a_{00}^2=1. \tag{32}$$

Hence S has the following form:

$$\xi_0' = a_{00}\xi_0, \quad \eta_2' = \delta_{22}\eta_2 + \delta_{23}\eta_3, \quad \xi_2' = a_{00}\delta_{33}\xi_2 - a_{00}\delta_{32}\xi_3,$$
$$\eta_3' = \delta_{32}\eta_2 + \delta_{33}\eta_3, \quad \xi_3' = -a_{00}\delta_{23}\xi_2 + a_{00}\delta_{22}\xi_3,$$

subject to relations (32). Its determinant equals

$$a_{00}^3 \begin{vmatrix} \delta_{22} & \delta_{23} \\ \delta_{32} & \delta_{33} \end{vmatrix}^2 = a_{00} = \pm 1.$$

Denote by S_1 the preceding substitution S for the case $a_{00} = +1$. For $a_{00} = -1$, $S = S' C_0 T_{3,-1}$, where S' is of the form S_1, of determinant $+1$.

The general substitution S_1 has the form

$$\eta_2' = \kappa\eta_2 + \lambda\eta_3, \quad \eta_3' = \mu\eta_2 + \nu\eta_3, \quad \xi_2' = \nu\xi_2 - \mu\xi_3, \quad \xi_3' = -\lambda\xi_2 + \kappa\xi_3, \tag{33}$$
$$\kappa\nu - \lambda\mu = 1.$$

If $\kappa = \nu = 0$, then $S_1 = T_{2,\mu^{-1}} T_{3,\mu} T_{3,-1} P_{23}$. If κ, ν are not both zero, we may take $\nu \neq 0$; for, if $\nu = 0$, $\kappa \neq 0$, the transform of S_1 by $T_{3,-1}P_{23}$ has $\nu \neq 0$. Then $Q_{2,3,\mu\nu^{-1}} S_1$ may be expressed as the product

$$Q_{3,2,-\lambda\nu^{-1}} T_{2,\nu} T_{3,\nu^{-1}}.$$

THEOREM.—*The group H' in the $GF[p^n]$ has the order* *

$$\Omega \equiv p^{6n}(p^{6n}-1)(p^{2n}-1). \tag{34}$$

It has been shown that H' contains a transformation which replaces ξ_1 by

$$\sum_{j=0}^{3} a_{1j}\xi_j + \sum_{j=1}^{3} \gamma_{1j}\eta_j,$$

in which $a_{10}, \cdots, \gamma_{13}$ are arbitrary marks, not all zero, such that

$$\tfrac{1}{4}a_{10}^2 + a_{11}\gamma_{11} + a_{12}\gamma_{12} + a_{13}\gamma_{13} = 0. \tag{35}$$

By various methods, this equation is seen to have p^{6n} sets of solutions in the $GF[p^n]$. Hence $\Omega = p^{6n}\Omega_1$, where Ω_1 denotes the number of transformations of H' which leave ξ_1 fixed. As shown above, H' contains a transformation which leaves ξ_1 fixed and replaces η_1 by f_1, in which $\beta_{10}, \cdots, \delta_{13}$ are any marks which satisfy (15), viz.;

$$\tfrac{1}{4}\beta_{10}^2 + \beta_{11} + \beta_{12}\delta_{12} + \beta_{13}\delta_{13} = 0. \tag{36}$$

Hence $\beta_{10}, \beta_{12}, \delta_{12}, \beta_{13}, \delta_{13}$ may be chosen arbitrarily, the value of β_{11} being then determined uniquely. Hence $\Omega_1 = p^{5n}\Omega_2$, where Ω_2 denotes the number of transformations S_1 of H' which leaves ξ_1 and η_1 unaltered. As shown above,

* As a check, we note that p^n, the order of the field, enters to the power 14, which is the number of parameters in the continuous group.

S_1 must be of the form (33). Inversely, all the $p^n(p^{2n}-1)$ transformations (33) belong to H'. Hence the order of H' is given by (34).

We observe the special values:

$$p^n = 3, \quad \Omega = 2^6 \cdot 3^6 \cdot 7 \cdot 13 \equiv 4{,}245{,}696;$$
$$p^n = 5, \quad \Omega = 2^6 \cdot 3^3 \cdot 5^6 \cdot 7 \cdot 31 \equiv 5{,}859{,}000{,}000.$$

These simple groups are not in the writer's list of known simple groups.*

§ 10. *Simplicity of the group H'.*

Suppose that H' contains an invariant subgroup J which possesses a transformation S not the identity I. Let S replace ξ_1 by

$$f_1 \equiv a_{10}\xi_0 + \sum_{j=1}^{3}(a_{1j}\xi_j + \gamma_{1j}\eta_j) \qquad \text{[subject to (35)]}.$$

LEMMA: *J contains a transformation $\neq I$ which multiplies ξ_1 by a constant.*

(*a*) Let first $\gamma_{11} \neq 0$. It was shown in § 9 that H' contains a transformation R which replaces ξ_1 by ξ_1 and η_1 by

$$\beta_{10}\xi_0 + \beta_{11}\xi_1 + \eta_1 + \beta_{12}\xi_2 + \delta_{12}\eta_2 + \beta_{13}\xi_3 + \delta_{13}\eta_3,$$

in which β_{1i}, δ_{1i} are any quantities of the field F satisfying (36). By suitable choice of these quantities, the product

$$P \equiv T_{1,\gamma_{11}^{-1}} T_{2,\gamma_{11}} R$$

replaces ξ_1 by $\gamma_{11}^{-1}\xi_1$ and η_1 by f_1. Hence J contains

$$S_1 \equiv P^{-1}SP$$

which replaces ξ_1 by $\gamma_{11}^{-1}\eta_1$. If H' contains a transformation B leaving ξ_1 and η_1 unaltered and not commutative with S_1, then J contains $S_1^{-1}B^{-1}S_1B$, which leaves ξ_1 fixed and is not the identity. In the contrary case S_1 is commutative with $Q_{3,2,\lambda}$, $T_{2,-1}P_{23}$. Equating the functions by which $S_1Q_{3,2,\lambda}$ and $Q_{3,2,\lambda}S_1$ replace η_2 and the functions by which they replace ξ_3, we see that S_1 must replace ξ_2 and η_3 by respectively

$$\xi_2' = a\xi_2 + b\eta_3, \quad \eta_3' = c\eta_3 - d\xi_2.$$

Since S_1 is to be commutative with $T_{2,-1}P_{23}$, it replaces η_2 and ξ_3 by

$$\eta_2' = c\eta_2 + d\xi_3, \quad \xi_3' = a\xi_3 - b\eta_2.$$

Then (23), for $l = 1$, $i = 1$, gives $c = 0$. Then J contains

$$S_1^{-1}(T_{1,\mu}T_{2,\mu-1})^{-1}S_1(T_{1,\mu}T_{2,\mu-1})$$

* Bulletin of the American Mathematical Society, ser. 2, vol. 5 (1899), p. 470–475.

which replaces η_2 by $\mu\eta_2$. Its transform by $T_{1,-1}P_{12}\Sigma$ replaces ξ_1 by $\mu\xi_1$ and is not the identity if $\mu \neq 0, 1$, where Σ is defined by (30).

(*b*) Let $\gamma_{11} = 0$, but a_{12} and a_{13} not both zero. By an evident transformation within H', we may make $a_{12} = 1$. Transforming S by

$$Y_{0,1,\gamma_{13}} W_{2,3,\gamma_{13}} \cdot Q_{2,3,a_{13}},$$

we reach in J a transformation S' which replaces ξ_1 by

$$a_{10}\xi_0 + a_{11}\xi_1 + \xi_2 + \gamma_{12}\eta_2 \qquad (\tfrac{1}{4}a_{10}^2 + \gamma_{12} = 0).$$

Then the transform of S' by $Q_{2,1,a_{11}}$ replaces ξ_1 by $\xi_2 + a_{10}\xi_0 - \frac{1}{4}a_{10}^2\eta_2$. Transforming by $X_{0,2,\frac{1}{2}a_{10}} V_{3,1,\frac{1}{2}a_{10}}$, we reach in J a transformation S_2 which replaces ξ_1 by ξ_2. Then J contains

$$S_2^{-1} \cdot T_{2,-1}T_{3,-1}S_2T_{2,-1}T_{3,-1}, \tag{37}$$

which replaces ξ_1 by $-\xi_1$.

(*c*) Let $\gamma_{11} = a_{12} = a_{13} = 0$. Then $a_{10} = 0$ by (35). If $\gamma_{12} = \gamma_{13} = 0$, S replaces ξ_1 by $a_{11}\xi_1$. In the contrary case, S is conjugate with a transformation S' with $\gamma_{12} = 1$; it replaces ξ_1 by $a_{11}\xi_1 + \eta_2 + \gamma_{13}\eta_3$. The transform of S' by $Q_{3,2,-\gamma_{13}}$ replaces ξ_1 by $a_{11}\xi_1 + \eta_2$. Transforming it by $X_{0,3,-a_{11}} V_{1,2,-a_{11}}$, we obtain a transformation S_2 which replaces ξ_1 by η_2. Then J contains (37), which replaces ξ_1 by $-\xi_1$.

LEMMA. *The group J contains a transformation, not the identity, which does not alter ξ_1 or η_1.*

In view of the preceding lemma, J contains a transformation $S \neq I$ which replaces ξ_1 by $a\xi_1$ and η_1 by

$$\beta_{10}\xi_0 + \sum_{j=1}^{3}(\beta_{1j}\xi_j + \delta_{1j}\eta_j) \qquad [\text{subject to (15)};\ \delta_{11} = a^{-1}].$$

According as δ_{12}, δ_{13} are both zero or not both zero, β_{12}, β_{13} both zero or not both zero, we distinguish four cases. Transforming by one or more of the transformations $T_{2,-1}P_{23}$, $Q_{2,3,\lambda}$, $Q_{3,2,\lambda}$, $T_{2,\lambda}T_{3,\lambda^{-1}}$, we obtain a transformation in J which replaces ξ_1 by $a\xi_1$ and η_1 by one of the four functions

$$f \equiv \beta_{10}\xi_0 + \beta_{11}\xi_1 + a^{-1}\eta_1, \quad f + \xi_2, \quad f + \beta_{12}\xi_2 + \eta_2, \quad f + \beta_{13}\xi_3 + \eta_2.$$

Let first S replace ξ_1 by f. By (15), $a^{-1}\beta_{11} + \frac{1}{4}\beta_{10}^2 = 0$. Hence

$$S = T_{1,a}T_{2,a^{-1}}Y_{0,1,\beta}W_{2,3,\beta}S_1 \qquad (\beta \equiv \tfrac{1}{2}\beta_{10}),$$

where S_1 leaves ξ_1 and η_1 fixed, belongs to H', and hence has the form (33). If $\beta = 0$, the lemma is proved when $a = 1$. For $\beta = 0$, $a \neq 1$, S_1 does not reduce to the identity I or to $T_{2,-1}T_{3,-1}$ and hence is not commutative with every (33). If S_1 be not commutative with Σ_1 of the form (33), then J contains

$$S^{-1}\Sigma_1^{-1}S\Sigma_1 \equiv S_1^{-1}\Sigma_1^{-1}S_1\Sigma_1 \neq I$$

which leaves ξ_1 and η_1 unaltered. Let next $\beta \neq 0$. Then S is transformed by $T_{2,-1}P_{23}$ into $S_2 \equiv T_{1,\alpha}T_{3,\alpha^{-1}}Y_{0,1,\beta}W_{2,3,\beta}S'$, where

$$S' \equiv P_{23}T_{2,-1}S_1T_{2,-1}P_{23}.$$

Hence J contains the transformation

$$S_2' \equiv T_{2,\alpha}T_{3,\alpha^{-1}}S^{-1}T_{2,\alpha^{-1}}T_{3,\alpha}S_2 \equiv T_{2,\alpha}T_{3,\alpha^{-1}}S_1^{-1}S',$$

which leaves ξ_1 and η_1 unaltered. If S_2' be the identity, $\nu = a\kappa$, $\mu = -a\lambda$ in (33). Again, $T_{1,\alpha^{-1}}T_{2,\alpha}$ transforms S into $S_3 \equiv Y_{0,1,\beta}W_{2,3,\beta}S_1T_{1,\alpha^{-1}}T_{2,\alpha}$. Then J contains the product

$$S_4 \equiv S_3^{-1}Q_{2,3,1}^{-1}S_3Q_{2,3,1} \equiv T_{2,\alpha^{-1}}S_1^{-1}Q_{2,3,1}^{-1}S_1T_{2,\alpha}Q_{2,3,1},$$

since $Q_{2,3,\tau}$ and $W_{2,3,\beta}$ are commutative. Now S_4 leaves ξ_1 and η_1 fixed. If S_4 reduce to the identity, we find that $\lambda = 0$, $\kappa = a\nu$ in (33). Hence if S_2' and S_4 are both the identity, (33) becomes $T_{2,\kappa^{-1}}T_{3,\kappa}$. In this case J contains

$$T_{1,-1}T_{2,-1}S^{-1}T_{1,-1}T_{2,-1}S \equiv T_{2,\kappa}T_{3,\kappa^{-1}}Y_{0,1,2\beta}W_{2,3,2\beta}T_{2,\kappa^{-1}}T_{3,\kappa},$$

and therefore its transform by $T_{2,\kappa}T_{3,\kappa^{-1}}$, giving $Y_{0,1,2\beta}W_{2,3,2\beta}$. Hence J contains every $Y_{0,1,\tau}W_{2,3,\tau}$ and $X_{0,1,\tau}V_{2,3,\tau}$. As in § 9, we derive $\Sigma' = \Sigma T_{2,-1}P_{23}$, where Σ is given by (30). Transforming Σ' by $P_{23}T_{2,-1}$, we reach $T_{2,-1}P_{23}\Sigma$. The product of the two gives $T_{2,-1}T_{3,-1}$, which leaves ξ_1 and η_1 unaltered and is not the identity.

The remaining three cases may be treated in a similar manner.

In view of the two lemmas, the group J contains a transformation, not the identity, which does not alter ξ_1 or η_1 and hence (§ 9) has the form (33). If it be $T_{2,-1}T_{3,-1}$, it is transformed into $Q_{1,2,2\lambda}T_{2,-1}T_{3,-1}$ by $Q_{1,2,-\lambda}$. Hence would J contain $Q_{1,2,2\lambda}$ and therefore $Q_{2,3,2\lambda}$. It follows that J contains a transformation (33) neither I nor $T_{2,-1}T_{3,-1}$. But the transformations (33) form a group holoedrically isomorphic with the binary group $SLH(2, F)$. It follows that J contains all the transformations (33) and hence every $Q_{i,j,\tau}$, $T_{i,-1}P_{i,j}$, $T_{i,\mu}T_{j,\mu^{-1}}$. But $X_{0,3,\tau}V_{1,2,\tau}$ transforms $T_{2,-1}T_{3,-1}$ into $X_{0,3,-2\tau}V_{1,2,-2\tau}T_{2,-1}T_{3,-1}$. Hence J contains every $X_{0,3,\lambda}V_{1,2,\lambda}$. Transforming it by suitable $T_{i,-1}P_{i,j}$ and by Σ, we reach every $X_{0,i,\tau}V_{j,k,\tau}$, $Y_{0,i,\tau}W_{j,k,\tau}$. Hence $J \equiv H'$, so that H' is simple in any field F not having the modulus $p = 2$.

§ 11. *Linear groups with invariants of degree $d > 2$.*

Consider the group $G(q, r, F)$ of linear transformations S on rq variables with coefficients in an arbitrary field F which leave formally and absolutely invariant the function

$$\sum_{i=1}^{r} \xi_{i1}\xi_{i2}\cdots\xi_{iq}.$$

For $q > 2$, we may express every S as a product, $S = AB$, where A merely multiplies each variable ξ_{ij} by a constant a_{ij}, while B is a substitution on the letters ξ_{ij} having the imprimitive systems*

$$\xi_{11}, \xi_{12}, \cdots, \xi_{1q}; \quad \xi_{21}, \xi_{22}, \cdots, \xi_{2q}; \quad \cdots; \quad \xi_{r1}, \xi_{r2}, \cdots, \xi_{rq}.$$

The transformations A form a commutative group invariant under $G(q, r, F)$. The quotient-group $\{B\}$ has an invariant subgroup R, the direct product of r symmetric groups, the general one being the symmetric group on the q letters $\xi_{i1}, \xi_{i2}, \cdots, \xi_{iq}$. The quotient-group $\{B\}/R$ is the symmetric group on r letters, the above imprimitive systems.

Consider the group $H(m, r, F)$ of linear transformations S on m variables with coefficients in a field F, not possessing a modulus, which leave formally and absolutely invariant the function

$$\lambda_1 \xi_1^r + \lambda_2 \xi_2^r + \cdots + \lambda_m \xi_m^r \qquad (\text{each } \lambda_i \neq 0 \text{ in } F).$$

If $r > 2$, we may set $S = AL$, where A is a transformation of the form

$$\xi_i' = a_i \xi_i \quad [a_i^r = 1] \qquad (i = 1 \cdots, m),$$

and L is a literal substitution on the letters $\xi_1, \xi_2, \cdots, \xi_m$.†

On the other hand, there exist linear groups in an arbitrary field F which possess invariants of degree $d > 2$ and which lead to simple groups. Examples of such groups are furnished by the second compounds of the groups $GLH(m, F)$ and $GA(2m, F)$, each possessing an invariant Pfaffian (see § 6).

§ 12. *Canonical forms of linear homogeneous transformations.*

Consider a transformation with coefficients in a field F,

$$S: \qquad \xi_i' = a_{i1}\xi_1 + a_{i2}\xi_2 + \cdots + a_{im}\xi_m \qquad (i = 1, 2, \cdots, m).$$

The determination of a linear function which S multiplies by a constant K depends upon the *characteristic equation*

$$\Delta(K) \equiv \begin{vmatrix} a_{11} - K & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} - K & \cdots & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mm} - K \end{vmatrix} = 0.$$

If we introduce new variables defined by the transformation

$$T: \qquad \eta_i \equiv \beta_{i1}\xi_1 + \beta_{i2}\xi_2 + \cdots + \beta_{im}\xi_m \qquad (i = 1, 2, \cdots, m),$$

*Proceedings of the London Mathematical Society, vol. 30 (1899), pp. 200–208. The factor C should be $t_1!\, t_2! \cdots t_r!$ For an elementary treatment of the case $q = 3$, see L. G., §§ 211–212.

†Mathematische Annalen, vol. 52, p. 563; L. G., §§ 139–141.

the transformation S becomes the transformation $S_1 \equiv T^{-1}ST$ on the variables η_i and the characteristic determinant $\Delta(K)$ of S_1 is equal to the characteristic determinant of S (L. G., §§ 101, 102). *The characteristic equation is unaltered under linear transformation.*

Let $\Delta(K)$ be decomposed in the field F into irreducible factors,

$$\Delta(K) \equiv [F_k(K)]^\alpha [F_l(K)]^\beta \cdots \qquad (k\alpha + l\beta + \cdots = m).$$

Let $F_k(K) = 0$ have the roots $K_1, K_2, \cdots, K_k$; $F_l(K) = 0$ the roots $L_1, L_2, \cdots, L_l$; etc. To exhibit compactly the general type of canonical form of transformations S, let $\alpha, \beta, \cdots$ be partitioned into positive integers,

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_{r+1}, \quad \beta = b_1 + b_2 + \cdots + b_{s+1}, \quad \cdots$$

Let $a, b, \cdots$, denote an arbitrary one of the respective sets of integers

$$(a) \qquad 1, \quad \alpha_1 + 1, \quad \alpha_1 + \alpha_2 + 1, \quad \cdots, \quad \alpha_1 + \alpha_2 + \cdots + \alpha_r + 1;$$

$$(b) \qquad 1, \quad b_1 + 1, \quad b_1 + b_2 + 1, \quad \cdots, \quad b_1 + b_2 + \cdots + b_s + 1;$$

etc. Let A denote an arbitrary positive integer $\overline{\overline{<}}\, \alpha$ and not an a; let B denote an arbitrary positive integer $\overline{\overline{<}}\, \beta$ and not a b; etc.

Proceeding as in L. G., §§ 214–218, we obtain the theorems:

By a suitable linear homogeneous transformation of variables (not belonging to F in general), S can be reduced to a canonical form

$$\eta'_{ia} = K_i \eta_{ia}, \quad \eta'_{iA} = K_i \eta_{iA} + K_i \eta_{iA-1} \qquad (i = 1, 2, \cdots, k)$$

$$\zeta'_{ib} = L_i \zeta_{ib}, \quad \zeta'_{iB} = L_i \zeta_{iB} + L_i \zeta_{iB-1} \qquad (i = 1, 2, \cdots, l)$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

in which the new variables $\eta_{ij}, \zeta_{ij}, \cdots$ have the properties:

(1) *The variables $\eta_{1j} (j = 1, 2, \cdots, \alpha)$ are linear homogeneous functions of the ξ_i whose coefficients are polynomials in K_1 with coefficients in F;*

(2) *The variables η_{ij} are obtained from the η_{1j} by replacing K_1 by K_i;*

(3) *The variables $\zeta_{1j} (j = 1, 2, \cdots, \beta)$ are linear functions of the ξ_i whose coefficients are polynomials in L_1 with coefficients in F;*

(4) *The variables ζ_{ij} are obtained from the ζ_{1j} by replacing L_1 by L_i;*

(5) *The $k\alpha$ variables $\eta_{ij} (i = 1, \cdots, k; j = 1, \cdots, \alpha)$ may be replaced by $k\alpha$ linear homogeneous functions y_{ij} of the ξ_i with coefficients in F, such that S replaces each y_{ij} by a linear function of the y_{ij} with coefficients in F; similarly for the $l\beta$ variables ζ_{ij}; etc.*

Two linear homogeneous transformations S_1 and S_2 belonging to a field F have the same canonical form if, and only if, S_1 is the transform of S_2 by a linear homogeneous transformation T in the field F and on the same variables.

To determine all linear homogeneous transformations T commutative with a given one S, each in the field F and affecting m variables ξ_i, we apply the transformation of indices which reduces S to its canonical form S',

$$S' \equiv Y_1 Y_2 \cdots Y_k Z_1 Z_2 \cdots Z_l \cdots,$$

where each transformation Y_i, $Z_i, \cdots$, is defined thus:

$$Y_i: \qquad \eta'_{ia} = K_i \eta_{ia}, \quad \eta'_{iA} = K_i \eta_{iA} + K_i \eta_{iA-1} \qquad \text{(for every } a, A\text{)};$$

$$Z_i: \qquad \zeta'_{ib} = L_i \zeta_{ib}, \quad \zeta'_{iB} = L_i \zeta_{iB} + L_i \zeta_{iB-1} \qquad \text{(for every } b, B\text{)}.$$

If T' be commutative with S', then

$$T' \equiv Y'_1 Y'_2 \cdots Y'_k Z'_1 Z'_2 \cdots Z'_l \cdots,$$

where Y'_i, Z'_i, $\cdots$, are of the form

$$Y'_i: \qquad \eta'_{ij} = \sum_{u=1}^{\alpha} \rho_{ju}(K_i) \eta_{iu} \qquad (j = 1, \cdots, \alpha);$$

$$Z'_i: \qquad \zeta'_{ij} = \sum_{v=1}^{\beta} \sigma_{jv}(L_i) \zeta_{iv} \qquad (j = 1, \cdots, \beta),$$

the coefficients of the polynomials $\rho_{ju}(K_i)$, $\cdots$, belonging to F.

Inversely, if T' have the above form and if Y'_1 be commutative with Y_1, Z'_1 commutative with Z_1, $\cdots$, then the transformation T (T' expressed in the in itial variables ξ_i) will be commutative with S and will have its coefficients in the field F.

Y'_1 and Y_1 are commutative if, and only if, for every a, A, A',

$$\rho_{aA} = 0, \quad \rho_{A-1\,a-1} = 0, \quad \rho_{A-1\,a} = 0, \quad \rho_{A-1\,A'-1} = \rho_{AA'}.$$

THE UNIVERSITY OF CHICAGO,
June 1, 1901.