ON THE SINGULAR TRANSFORMATIONS OF GROUPS GENERATED BY INFINITESIMAL TRANSFORMATIONS.

BY PROFESSOR HENRY TABER.

(Read before the American Mathematical Society, December 28, 1899.)

By means of r independent infinitesimal transformations

$$X_j = \sum_1^n{}_i\xi_{ji}(x_1, x_2, \cdots, x_n)\frac{\partial}{\partial x_i} \qquad (j = 1, 2, \cdots, r)$$

we may construct a family of transformations

$$(1) \qquad x_i' = x_i + \sum_1^r{}_j a_j X_j x_i + \tfrac{1}{2}\sum_1^r{}_j\sum_1^r{}_k a_j a_k X_j X_k x_i + \cdots$$
$$\equiv f_i(x_1, \cdots, x_n, a_1, \cdots, a_r) \qquad (i = 1, 2, \cdots, n)$$

with r essential parameters $a_1, a_2, \cdots, a_r$. The transformations defined by these equations, for assigned values of the a's, may be denoted by T_a. Each transformation of this family is paired with its inverse.

For finite values of the parameters a, the transformation T_a (provided it is not illusory) belongs to a one parameter group generated by the infinitesimal transformation

$$a_1X_1 + \cdots + a_rX_r.$$

As the a's approach certain limiting values, one or more of which is infinite, T_a may have a definite finite transformation T as a limit. The transformation T may be regarded as a transformation of the family, and, if equivalent to a transformation T_b with finite parameters, can be generated by an infinitesimal transformation of the family (namely, $b_1X_1 + \cdots + b_rX_r$), but not otherwise.*

Let it be assumed that

$$X_jX_k - X_kX_j = \sum_1^r{}_s c_{jks}X_s \qquad (j,k = 1, 2, \cdots, r),$$

*Thus, if the transformation T_a, for one or more of the a's infinite, is finite and definite, but is not equivalent to a transformation of the family with finite parameters, the transformation T_a cannot be generated by an infinitesimal transformation of the family. To this extent Lie's theorem on p. 65 of the Transformationsgruppen, vol. 1, requires modification.

the c's being constants. Then, by the chief theorem of Lie's theory, the family of transformations (1) forms a group G with continuous parameters; and each transformation of G is, in general, generated by an infinitesimal transformation of the group. Thus from

$$(1) \qquad x_i' = f_i(x_1, \cdots, x_n, \; a_1, \cdots, a_r) \qquad (i = 1, 2, \cdots, n)$$

and

$$(2) \qquad x_i'' = f_i(x_1', \cdots, x'_n, \; b_1, \cdots, b_r) \quad (i = 1, 2, \cdots, n)$$

we derive

$$(3) \qquad x_i'' = f_i(x_1, \cdots, x_n, \; c_1, \cdots, c_r) \qquad (i = 1, 2, \cdots, n)$$

where

$$(4) \qquad c_j = \varphi_j(a_1, \cdots, a_r, \; b_1, \cdots, b_r) \; (j = 1, 2, \cdots, r).$$

For finite values of the a's and b's it may happen that every branch of one or more of the functions φ is infinite. In this case, while each of the transformations T_a and T_b is generated by an infinitesimal transformation of the group, the transformation T_bT_a, resulting from their composition, cannot be generated thus, and the group cannot properly be said to be continuous. A transformation of G which cannot be generated by an infinitesimal transformation of G may be termed *essentially singular.*

In what follows I shall signify by T_a, T_b, etc., transformations of the groups with finite parameters generated, respectively, by the infinitesimal transformations

$$a_1X_1 + a_2X_2 + \cdots + a_rX_r, \quad b_1X_1 + b_2X_2 + \cdots + b_rX_r, \quad \text{etc.}$$

Group G may contain a transformation T_a (generated by an infinitesimal transformation) which, in composition with every transformation of some one (or more) subgroups of G with one parameter, in particular with the infinitesimal transformation of such subgroup, results in an essentially singular transformation. Such a transformation T_a I term *non-essentially singular.* The values of the a's for which T_a is non-essentially singular may be termed *critical* values of the parameters. The critical values of the parameters are included among those for which one or more of the roots of the equation in ρ

$$\begin{vmatrix} \sum_1^r {}_j a_j c_{j11} - \rho, & \sum_1^r {}_j a_j c_{j21} \quad , & \cdots \\ \sum_1^r {}_j a_j c_{j12} \quad , & \sum_1^r {}_j a_j c_{j22} - \rho, & \cdots \\ \cdots\cdots & \cdots\cdots & \cdots \end{vmatrix} = 0,$$

is equal to an even multiple, not zero, of $\pi\sqrt{-1}$. This condition is necessary but not sufficient. That is to say, for values of the a's for which one or more of the roots of this equation is an even multiple, not zero, of $\pi\sqrt{-1}$, T_a is not necessarily singular.

I find that every transformation of G, in particular every essentially or non-essentially singular transformation, can be obtained by the composition of two non-singular transformations. Also that, corresponding to every essentially singular transformation T of G, a non-singular transformation T_a, whose parameters are functions of a variable λ, can be found which can be made to approach as nearly as we please to T by taking λ sufficiently small, and such that $\lim_{\lambda=0} T_a = T$.*

In every group G containing essentially singular transformations which I have examined, non-essentially singular transformations also exist, and any non-singular transformation T_a whatever combined with some one, or more, non-singular or non-essentially singular transformations T_b results in an essentially singular transformation. These relations undoubtedly hold invariably.

Let $\mathfrak{F}_a$ denote the bilinear form

$$\sum_1^r {}_\mu \sum_1^r {}_\nu \left(\sum_1^r {}_j a_j c_{j\nu\mu}\right) u_\mu v_\nu,$$

and let I denote the bilinear form $\sum_1^r {}_\mu u_\mu v_\mu$. The coefficient of $u_\mu v_\nu$ in the bilinear form

$$\frac{e^{\mathfrak{F}_a} - I}{\mathfrak{F}_a} = I + \tfrac{1}{2}\mathfrak{F}_a + \tfrac{1}{3!}\mathfrak{F}_a^{\,2} + \cdots$$

is a power series in the a's, which may be denoted by $P_{\mu\nu}(a)$, and which is convergent for all finite values of the a's. Let now $\triangle_a$ denote the determinant

* These theorems were given for subgroups of the projective group by the author in a paper read at the February Meeting of the Society, 1899.

$$\left|\begin{array}{l} P_{11}(a),\ P_{12}(a),\ \cdots \\ P_{21}(a),\ P_{22}(a),\ \cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \end{array}\right|$$

and let $A_{\mu\nu}$ denote the first minor of $\triangle_a$ relative to $P_{\nu\mu}(a)$. Then, if we put

$$a_j = \varphi_j(\bar{a}_1, \cdots, \bar{a}_r,\ tb_1, \cdots, tb_r) \quad (j = 1, 2, \cdots, r),$$

regarding $\bar{a}_1, \cdots, \bar{a}_r,\ b_1, \cdots, b_r$ as fixed and the a's as functions of t, the latter satisfy the differential equations

$$\triangle_a \frac{da_j}{dt} = A_{j1}b_1 + A_{j2}b_2 + \cdots + A_{jr}b_r \qquad (j = 1, 2, \cdots, r).$$

The A's are integral functions (transcendental or rational) of the a's, and $\triangle_a$ vanishes only if one or more of the roots of the characteristic equation of $\mathfrak{F}_a$ is an even multiple, not zero, of $\pi\sqrt{-1}$.*

The functions φ are multivalued. Returning to the original notation, let

$$c_j = \varphi(a_1, \cdots, a_r\,;\ b_1, \cdots, b_r) \quad (j = 1, 2, \cdots, r).$$

For assigned values of the a's and b's the difference between any two branches of $\varphi_j(a, b)$ is equal to

$$2\pi\sqrt{-1}\sum_{1}^{r}{}_k\, m_k\, \psi_{kj}(a, b),$$

where the m's are integers, and the ψ's are rational functions of the coefficients of the bilinear form $e^{\mathfrak{F}_a}e^{\mathfrak{F}_b}$.

The equations defining the transformations of one group may restrict the functions φ_j to fewer branches than in the case of another group of the same structure (*Zusammensetzung.*) Consequently, of two groups of the same structure, one may be continuous and the other may be discontinuous, that is, may possèss essentially singular transformations.†

* If we denote by T_{tb} the transformation of G whose parameters are $tb_1, tb_2, \cdots, tb_r$, which is generated by the infinitesimal transformation $b_1X_1 + \cdots + b_rX_r$, the transformation $T_{tb}T_{\bar{a}}$ is essential singular only for those values of t for which the determinant is zero of the bilinear form $\dfrac{e^{\mathfrak{F}}{}_b e^{\mathfrak{F}_{\bar{a}}} - \mathrm{I}}{\mathfrak{F}_{tb}\mathfrak{F}_{\bar{a}}}$.

† My attention was first drawn to this fact by my pupil, Mr. S. E. Slocum.

If, however, the adjoined of any group G is discontinuous, G itself, and, of course, every group of the same structure is discontinuous. The bilinear form $\mathfrak{F}_a$ is closely related to the adjoined group. In fact, if ϕ_a denotes the matrix of $\mathfrak{F}_a$, the infinitesimal equations of the adjoined are

$$(a_1', a_2', \cdots, a_r) = (1 + \partial t\phi_a)(a_1, a_2, \cdots, a_r);$$

and we have
$$e^{\mathfrak{F}\beta}e^{\mathfrak{F}a} = e^{\mathfrak{F}\gamma}$$

where
$$\gamma_j = \varphi_j(a_1, \cdots, a_r, \beta_1, \cdots, \beta_r) \qquad (j = 1, 2, \cdots, r).$$

Clark University,
December, 1899.

PROOF OF THE EXISTENCE OF THE GALOIS FIELD OF ORDER p^r FOR EVERY INTEGER r AND PRIME NUMBER p.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, December 28, 1899.)

Existence proofs have been given by Serret* and by Jordan.† The developments used by Serret are lengthy but quite in the spirit of Kronecker's ideas. The short proof by Jordan, however, assumes with Galois the existence of imaginary roots of an irreducible congruence modulo p.

The proof sketched in this note proceeds by induction. Assuming the existence of the $GF[p^n]$, we derive that of the $GF[p^{nq}]$, q being an arbitrary prime number. Since the $GF[p]$ exists, being the field of integers taken modulo p, it will follow that the $GF[p^q]$ exists, and by a simple induction that the $GF[p^r]$ exists for r arbitrary.

We employ the lemma: *A factor of $x^{p^{nm}} - x$, belonging to and irreducible in the $GF[p^n]$, can be of degree m' if and only if m' divides m.* In particular, the irreducible factors of $x^{p^{nq}} - x$ are of degree q or 1. But the product of the distinct ‡ linear factors $x - \nu_i$ belonging to the $GF[p^n]$ is $x^{p^n} - x$.

*Algèbre supérieure, 2, pp. 122–142.

† Traité des substitutions, pp. 16, 17.

‡ Two functions belonging to the $GF[p^n]$ are called distinct if one is not the product of the other by a constant, a mark of the field.