ON BINARY MODULAR GROUPS AND THEIR INVARIANTS.

BY PROFESSOR L. E. DICKSON.

A VERY simple determination is here made of all groups G of binary linear transformations with integral coefficients of determinant unity modulo p such that the order of the group is divisible* by the prime p. The corresponding problem for which the coefficients are in any finite field of order a power of p has been treated recently by H. H. Mitchell,† who cites the earlier treatments by Gierster, E. H. Moore, Wiman, and Dickson of the related linear fractional group. To be added to these references is a paper on the present binary homogeneous groups.‡

Any binary modular transformation T multiplies some linear function of x and y by a constant. This constant is unity if T is of period p. Hence after a suitable choice of the variables, we may assume that our group G contains

$$T: \quad x' \equiv x + y, \quad y' \equiv y \pmod{p}.$$

THEOREM. *Either G is the group Γ of all binary transformations with integral coefficients of determinant unity modulo p, or else every transformation of G is of the form*

$$x' \equiv tx + ly, \quad y' \equiv t^{-1}y \pmod{p}. \tag{1}$$

Suppose that G contains a transformation R for which y' involves x, so that $y' = a(x + ky)$, $a \not\equiv 0$. Then G contains§

$$P = R^{-1}T^k: \quad x' \equiv y/a, \quad y' \equiv -ax + by \pmod{p},$$

in which the value of b is immaterial. Next, G contains

$$T^{b/a}P: \quad x'' \equiv y/a, \quad y'' \equiv -ax.$$

* The groups of orders prime to p may be found as in the case of binary collineation groups.

† *Trans. Amer. Math. Soc.*, vol. 12 (1911), p. 207.

‡ Dickson, "Binary modular groups and their invariants," *Amer. Jour. Math.*, vol. 33 (1911), p. 175. Here are found the invariants of any modular group other than one composed only of transformations (1), the case treated in the text.

§ To form the product RP, we note that $x'' = a^{-1}y'$ under P and eliminate y' by means of the equation for R. But $x'' \equiv x + ky$ under T^k.

The latter transforms T into

$$x' \equiv x, \quad y' \equiv y - a^2x.$$

A power of this is $x' \equiv x$, $y' \equiv y + x$. The latter and T are known to generate the group Γ. Hence the theorem is proved.

The group G of transformations (1) is generated by T and

$$x' \equiv \tau x, \quad y' \equiv \tau^{-1}y, \tag{2}$$

where τ belongs to a certain exponent d modulo p. Thus G is of order pd.

Evidently T leaves absolutely unaltered the product

$$\lambda = x(x+y)(x+2y) + \cdots + (x + \overline{p-1}y) \equiv x^p - xy^{p-1} \pmod{p}, \tag{3}$$

the congruence holding in view of Fermat's theorem. Now (2) replaces λ by $\tau\lambda$. Thus G has the relative invariants λ and y.

If (1) leaves the point (x, y) unaltered,

$$tx + ly \equiv \rho x, \quad t^{-1}y \equiv \rho y \pmod{p}. \tag{4}$$

If these congruences hold identically, $l \equiv 0$, $t \equiv \pm 1$, and (1) becomes

$$x' \equiv \pm x, \quad y' \equiv \pm y. \tag{5}$$

First, let d be even and $p > 2$. Then G contains the two transformations (5), which leave every point unaltered. A point is called special if it can not be transformed by G into $pd/2$ distinct points, and hence is unaltered by some transformation (1) not of type (5). For such a transformation, equations (4) are not both identities and determine uniquely x/y as an integer modulo p, and hence a real special point (x, y). But (1, 0) is unaltered by G, while the remaining real points $(k, 1)$ are permuted by the powers of T. Thus any invariant which vanishes at a special point has the factor y or λ. An invariant without a factor y or λ therefore vanishes at imaginary points falling into sets of $pd/2$ points conjugate under G. Now $y^{pd/2}$ and $\lambda^{d/2}$ are unaltered by T and changed in sign by (2), since $\tau^{\pm d/2} \equiv -1 \pmod{p}$. Hence any linear combi-

nation of them is an invariant of G. We can find* a product of such combinations which has integral coefficients and vanishes at any assigned point, not a special point. Thus the invariant is the product of one or more such products.

For d odd, a non-special point is one of pd conjugates under G. We now use the absolute invariants y^{pd}, λ^d.

THEOREM. *As a fundamental system of invariants of a group of transformations* (1), *we may take* y *and* λ.

In particular, this theorem yields the seminvariant leaders of invariants of two pairs of cogredient variables.

UNIVERSITY OF CHICAGO,
February, 1913.

ON SOME SYSTEMS OF COLLINEATION GROUPS.

BY DR. HOWARD H. MITCHELL.

(Read before the American Mathematical Society, April 26, 1913.)

§ 1.

SOME systems of collineation groups which arise in connection with the theory of elliptic functions have been investigated by Klein† and Hurwitz‡. One of them is a system in n variables each group of which contains an invariant subgroup of order n^2. For n a prime the quotient group with respect to this invariant subgroup is (1, 1) isomorphic with the modular group on two indices of order $n(n^2 - 1)$. The group in three variables is the Hessian group of order 216.

For n odd there is also an invariant subgroup of order $2n^2$, and there exist two other groups in $(n - 1)/2$ and $(n + 1)/2$ variables each of which is isomorphic with the quotient group with respect to this subgroup. Thus for $n = 5$ there is both a binary and a ternary G_{60} and for $n = 7$ both a ternary and a quaternary G_{168}.

Similar systems of groups in n^2, $(n^2 - 1)/2$, and $(n^2 + 1)/2$ variables which arise in the theory of hyperelliptic functions

* Dickson, *Trans. Amer. Math. Soc.*, vol. 12 (1911), p. 4.

† *Math. Annalen*, vol. 15 (1879), p. 275; also Klein-Fricke, Modulfunktionen (2) 5.

‡ *Math. Annalen*, vol. 27 (1885), p. 198.