ON AUTOMORPHIC GROUPS WHOSE COEFFICIENTS ARE INTEGERS IN A QUADRATIC FIELD*

BY

J. I. HUTCHINSON

In a memoir by X. STOUFF † an interesting method is given for the determination of certain groups of linear transformations of a single variable, the coefficients being of the form $\sum_\sigma \alpha_\sigma(j^\sigma + j^{-\sigma})$ in which σ and α_σ are integers and j is a primitive pth root of unity. This method imposes conditions on the α_σ by reason of which all are linearly expressible in terms of four; these four are connected by a quadratic relation, the condition for determinant 1. The method employed by STOUFF is capable of defining only a very restricted class of groups and the explicit forms of these are deduced only in a few individual cases. The class may be greatly enlarged by including all groups whose coefficients are linear functions of four variable integers subject to a quadratic condition. In the following paper I consider groups of this type whose coefficients are of the form $\alpha + \alpha'\lambda$ in which λ is a root of the equation

$$(1) \qquad \lambda^2 - m\lambda + n = 0,$$

and α, α', m, n are integers. The coefficients of any transformation of the group, $\zeta' = (A\zeta + B)/(C\zeta + D)$, form the determinant

$$(2) \qquad \begin{vmatrix} \alpha + \alpha'\lambda & \beta + \beta'\lambda \\ \gamma + \gamma'\lambda & \delta + \delta'\lambda \end{vmatrix} = \begin{vmatrix} A & B \\ C & D \end{vmatrix}.$$

This determinant is assumed to be unimodular and hence,

$$(3) \qquad \alpha\delta - \beta\gamma - n(\alpha'\delta' - \beta'\gamma') = 1,$$

$$(4) \qquad \alpha\delta' - \alpha'\delta - \beta\gamma' - \beta'\gamma + m(\alpha'\delta' - \beta'\gamma') = 0.$$

I further suppose that the integers $\gamma, \gamma', \delta, \delta'$ are expressible in terms of $\alpha, \alpha', \beta, \beta'$ in the form

* Presented to the Society December 28, 1905. Received for publication May 12, 1906.

† *Sur certains groupes fuchsiens formés avec les racines d'equations binomes*, Annales de Toulouse, vol. 4 (1890), P.

$$
(5) \qquad \begin{aligned}
p\gamma &= a_1\alpha + b_1\alpha' + c_1\beta + d_1\beta', \\
p\gamma' &= a_2\alpha + b_2\alpha' + c_2\beta + d_2\beta', \\
p\delta &= a_3\alpha + b_3\alpha' + c_3\beta + d_3\beta', \\
p\delta' &= a_4\alpha + b_4\alpha' + c_4\beta + d_4\beta',
\end{aligned}
$$

in which p, a_1, $\cdots$ are integers. Let these expressions be substituted in (4) and the coefficients of α^2, $\alpha\alpha'$, α'^2, $\cdots$ be equated to zero. This leads to the following conditions:

$$
(6) \qquad \begin{gathered}
d_1 = mc_1, \quad c_2 = 0, \quad d_2 = -c_1, \quad b_3 = ma_3, \quad c_3 = b_2 - ma_2, \\
d_3 = b_1 + mb_2 - m(a_1 + ma_2), \quad a_4 = 0, \quad b_4 = -a_3, \quad c_4 = a_2, \quad d_4 = a_1 + ma_2.
\end{gathered}
$$

In order that identity may belong to the group the additional conditions $a_1 = a_2 = 0$, $a_3 = p$ must be imposed. The equations (5) now take the simpler form

$$
(7) \qquad \begin{aligned}
p\gamma &= b_1\alpha' + c_1(\beta + m\beta'), \\
p\gamma' &= b_2\alpha' - c_1\beta', \\
p\delta &= p(\alpha + m\alpha') + b_2\beta + (b_1 + mb_2)\beta', \\
\delta' &= -\alpha'.
\end{aligned}
$$

It may readily be verified that the inverse of a given transformation, and the product of any two of the form (7) have coefficients which are also of this form. Hence,

The totality of transformations whose coefficients satisfy conditions (3) *and* (7) *form a group.*

This group will be denoted by g. It remains to show that g is properly discontinuous in the plane of the variable ζ. For this purpose it is sufficient to prove that, if the coefficients A, B, C, D are restricted in numerical value, there are only a finite number of values of α, α', β, β'.* Assuming then the inequalities

$$
|A| < F_1, \qquad |B| < F_2, \qquad |C| < F_3, \qquad |D| < F_4,
$$

in which $F_1, \cdots, F_4$ are any finite positive numbers, let $f_1, \cdots, f_4$ be defined by the equations

$$
f_1 = pc_1(m^2 - m\lambda - 2n) - (b_1^2 + mb_1b_2 + nb_2^2),
$$

$$
f_2 = -\lambda c_1(b_1 + b_2\lambda),
$$

* Cf. STOUFF, loc. cit., p. 5.

$$f_3 = \lambda p\,[b_1 + (m-\lambda)b_2],$$

$$f_4 = \lambda p c_1(2\lambda - m).$$

When these expressions are substituted in the inequality

$$(8)\qquad |f_1 A + f_2 B + f_3 C + f_4 D| < \sum_{i=1}^{4} |f_i| F_i$$

it reduces to

$$|(f_1 + f_4)\alpha| < \Sigma |f_i| F_i.$$

As the right member is a fixed positive number, and α is restricted to integer values, it follows that α can take only a finite number of values provided that the expression

$$(9)\qquad f_1 + f_4 = pc_1(4n - m^2) + b_1^2 + mb_1 b_2 + nb_2^2$$

does not vanish. In like manner by substituting in (8) the expressions

$$-f_1 = f_4 = pc_1(2\lambda - m), \qquad f_2 = -c_1(b_1 + \lambda b_2),$$

$$f_3 = p\,[b_1 + (m-\lambda)b_2],$$

we obtain the inequality

$$|Q\alpha'| < \Sigma |f_i| F_i$$

in which Q denotes the right member of (9). Again, by taking

$$-f_1 = f_4 = p\lambda(b_1 + \lambda b_2), \qquad f_3 = p^2\lambda(2\lambda - m),$$

$$f_2 = pc_1(\lambda - m)(2\lambda - m) - (b_1 + mb_2)(b_1 + \lambda b_2),$$

we deduce

$$|Q\beta| < \Sigma |f_i| F_i;$$

and finally, with the expressions

$$-f_1 = f_4 = p(b_1 + \lambda b_2), \qquad f_3 = p^2(2\lambda - m),$$

$$f_2 = -b_2(b_1 + \lambda b_2) - c_1 p(2\lambda - m),$$

we obtain

$$|Q\beta'| < \Sigma |f_i| F_i.$$

Hence, *if the integer* $Q = pc_1(4n - m^2) + b_1^2 + mb_1 b_2 + nb_2^2$ *does not vanish, there are only a finite number of integer values which* $\alpha, \alpha', \beta, \beta'$ *can take when the numerical values of* A, B, C, D *are restricted, and the group is therefore properly discontinuous in the complex plane.*

The preceding demonstration is necessary only in case λ is real. If λ is imaginary, the group is evidently discontinuous since no complex integer of the form $\beta + \lambda\beta'$ can be infinitesimal.

The group g may be enlarged by including every substitution V whose square belongs to g.* Assuming that the coefficients of V satisfy conditions (6) only, while those of V^2 are of the form (7), we obtain for V a substitution of form (2) whose coefficients are subject to the conditions

$$
\begin{aligned}
p\gamma &= -(mb_1 + 2nb_2)(2\alpha + m\alpha')\Delta^{-1} - c_1(\beta + m\beta'), \\
p\gamma' &= (2b_1 + mb_2)(2\alpha + m\alpha')\Delta^{-1} + c_1\beta', \\
p\delta &= -p(\alpha + m\alpha') - [m(2b_1 + mb_2)\beta + \{m^2 b_1 + m(m^2 - 2n)b_2\}\beta']\Delta^{-1}, \\
p\delta' &= p\alpha' + [(4b_1 + 2mb_2)\beta + \{2mb_1 + 2(m^2 - 2n)b_2\}\beta']\Delta^{-1}, \\
\Delta &= m^2 - 4n.
\end{aligned} \tag{10}
$$

It can be verified that the product of any two substitutions V belongs to g and hence, *the totality of transformations whose coefficients satisfy conditions* (7) *or* (10) *form a group*. This enlarged group will be denoted by G. The transformations of G will be spoken of as of the first or second type and will be denoted by v or V according as they satisfy conditions (7) or (10) respectively.

Since $A + D$ is an integer for substitutions v, it follows that elliptic substitutions v can be of periods 2 and 3 only, and hence elliptic substitutions of the second type cannot have other periods than 2, 4, and 6. But for the substitutions V we have $A + D = (2\lambda - m)I = I\sqrt{\Delta}$ in which I is an integer. Those of period 4 can occur only when $\Delta = 2$, and those of period 6 only when $\Delta = 3$. But if $\Delta = \epsilon(\epsilon = 2, 3)$, we have $m^2 = 4n + \epsilon$ which is impossible since ϵ is not a quadratic residue of 4. Hence, *the substitutions V are either of period* 2, *or hyperbolic.*

In order that the group G may be extended by the reflection $\zeta' = -\bar{\zeta}$ on the imaginary axis it is necessary and sufficient that with every substitution (2) the substitution $\left|\begin{smallmatrix} A & -B \\ -C & D \end{smallmatrix}\right|$ shall also be included in the group (λ being real). This is possible only when $b_1 = b_2 = 0$. Write $c_1 = pq$ and $m - \lambda = \lambda'$. Then, *the most general group G which can be extended by reflection on the imaginary axis consists of the transformations*

$$
\text{(I)} \quad \begin{vmatrix} \alpha + \alpha'\lambda & \beta + \beta'\lambda \\ q(\beta + \beta'\lambda') & \alpha + \alpha'\lambda' \end{vmatrix}, \qquad \text{(II)} \quad \begin{vmatrix} \alpha + \alpha'\lambda & \beta + \beta'\lambda \\ -q(\beta + \beta'\lambda') & -(\alpha + \lambda'\alpha') \end{vmatrix},
$$

the coefficients of which are subject to the condition

$$
\alpha^2 + m\alpha\alpha' + n\alpha'^2 - q(\beta^2 + m\beta\beta' + n\beta'^2) = \pm 1. \tag{11}
$$

* The question naturally arises as to whether it would be possible to extend g by a substitution V whose nth power ($n > 2$) and no lower power is contained in g. That this is not possible in general is shown by proving, as may readily be done, the impossibility of such an extension in case of the particular groups for which $b_1 = b_2 = 0$.

The plus and minus signs correspond to (I) and (II) respectively. This group will be denoted by $G_{\{q,\lambda\}}$ or more briefly by $\{q, \lambda\}$, while the substitutions (I) form a subgroup $g_{\{q,\lambda\}}$.

The determinant for (I) may be written

$$(2\alpha + m\alpha')^2 - \Delta\alpha'^2 - q[(2\beta + m\beta')^2 - \Delta\beta'^2] = 4.$$

Since the sum of the diagonal coefficients is $A + D = 2\alpha + m\alpha'$ it follows that elliptic substitutions are subject to the condition

$$(12) \qquad - \Delta\alpha'^2 - q[(2\beta + m\beta')^2 - \Delta\beta'^2] = \epsilon,$$

in which ϵ is 4 or 3 according as (I) is of period 2 or 3 respectively. If we write $2\beta + m\beta'$ in the form $M\Delta + \mu$, $0 \leqq \mu < \Delta$, it is evident that (assuming $\Delta \neq 3$) relation (12) is impossible unless μ satisfies the congruence $-q\mu^2 \equiv \epsilon \pmod{\Delta}$. Hence, if r denote any quadratic residue of Δ, *the group* $g_{\{q,\lambda\}}$ *has no substitutions of period* 2 *or* 3 *unless the condition* $-qr \equiv 4 \pmod{\Delta}$ *or* $-qr \equiv 3 \pmod{\Delta}$ *can be satisfied by some one of the allowable values of* r.

The condition for a parabolic substitution is

$$\Delta\alpha'^2 + q(2\beta + m\beta')^2 - q\Delta\beta'^2 = 0.$$

Assume $q = cq_1q_2^2$, $\Delta = c\Delta_1\Delta_2^2$ in which q_2^2, Δ_2^2 are the highest quadratic factors in q, Δ, and c is the greatest common divisor of the remaining factors of q and Δ. After multiplying the above relation by $cq_1\Delta_1$ it takes the form

$$q_1(c\Delta_1\Delta_2\alpha')^2 + \Delta_1[cq_1q_2(2\beta + m\beta')]^2 - c(cq_1q_2\Delta_1\Delta_2\beta')^2 = 0.$$

In order that this equation in α', β, β' may have integer solutions it is necessary and sufficient that $c\Delta_1$, cq_1, $-q_1\Delta_1$ be quadratic residues of q_1, Δ_1, c respectively and do not all have the same sign.* Hence, *the group* $G_{\{q,\lambda\}}$ *contains parabolic substitutions when (and only when) integers* z, z', z'' *can be found to satisfy the congruences*

$$z^2 \equiv c\Delta_1 \pmod{q_1},$$
$$z'^2 \equiv cq_1 \pmod{\Delta_1},$$
$$z''^2 \equiv -q_1\Delta_1 \pmod{c},$$

in which q_1, Δ_1, $-c$ *are not all of the same sign.*

The infinity of groups $\{q, \lambda\}$ obtained by giving q different integer values are not all distinct when regarded as abstract groups. For, let $\{q, \lambda\}$ be transformed by means of

$$T = \begin{vmatrix} t + t'\lambda & 0 \\ 0 & 1 \end{vmatrix},$$

* See DIRICHLET, *Zahlentheorie*, p. 432.

in which t, t' are integers. The transformed of the operations (I) are

$$\begin{vmatrix} \alpha + \alpha'\lambda & b + b'\lambda \\ \frac{q}{\tau}(b + b'\lambda') & \alpha + \alpha'\lambda' \end{vmatrix}$$

in which

(13) $b = t\beta - nt'\beta'$, $\quad b' = t\beta' + t'\beta + mt'\beta'$, $\quad \tau = t^2 + mtt' + n$.

On account of (11) we have also the restriction

$$(14) \qquad (\alpha + \alpha'\lambda)(\alpha + \alpha'\lambda') - \frac{q}{\tau}(b + b'\lambda)(b + b'\lambda') = 1.$$

A corresponding result is obtained by transforming (II). Hence, *the transformed of* $\{q, \lambda\}$ *by* T *is the group* $\{q/\tau, \lambda\}$. In particular, whenever m and n are such that -1 can be represented by τ then $\{q, \lambda\}$ is isomorphic with $\{-q, \lambda\}$.

Suppose $q = \tau q'$. To each pair of values of β, β' satisfying (11) corresponds one pair of values of b, b' satisfying (14). But from the equations

$$\beta = \tau^{-1}[(t + mt')b + nt'b'], \qquad \beta' = \tau^{-1}[-t'b + tb'],$$

derived from (13), it is seen that to each pair of integer values of b, b' satisfying (14) do not always correspond integer values of β, β'. Accordingly, *when* $q = \tau q'$ *the group* $\{q, \lambda\}$ *can be transformed into a subgroup of* $\{q', \lambda\}$. In particular, for every number q which can be represented by τ the group $\{q, \lambda\}$ can be transformed into a subgroup of $\{1, \lambda\}$.

This result gives a method of representing an important class of subgroups of the group $\{q, \lambda\}$. Namely, *those values of* β, β' *which satisfy* (11) *and which make the expressions*

$$\tau^{-1}[(t + mt')\beta + nt'\beta'], \qquad \tau^{-1}[-t'\beta + t\beta']$$

integers determine a subgroup of $\{q, \lambda\}$.

The transformed of $\{q, \lambda\}$ by T^{-1} is $\{\tau q, \lambda\}$. If q is not an integer, suppose $q = q_1/q_2$. By choosing t, t' so that τ is divisible by q_2 the number τq reduces to an integer. Hence among the groups $\{q, \lambda\}$ it is sufficient to consider those only in which q is an integer.

We observe further that no new groups are obtained by using $\lambda' = m - \lambda$ in place of λ, since, as may readily be shown, $\{q, \lambda'\} = \{q, \lambda\}$. Moreover it is sufficient to consider only positive values of m. For, if we have $m = -m_1$, $m_1 > 0$, then the substitution (I) may be written

$$\begin{vmatrix} \alpha - \alpha'\lambda_1, & \beta - \lambda_1'\beta' \\ q(\beta - \lambda_1\beta'), & \alpha - \lambda_1\alpha' \end{vmatrix}, \qquad \lambda_1 = \frac{m_1 + \sqrt{m_1^2 - 4n}}{2}.$$

By replacing α', β' by $-\alpha'$, $-\beta'$ this again takes the form (I). Hence we have

$$\{q, \lambda\} = \{q, \lambda_1'\} = \{q, \lambda_1\}.$$

These considerations may readily be extended to the group G defined by (7) and (10) which we will denote for greater explicitness by the symbol $\{b_1, b_2, c_1, \lambda\}$. We obtain as result the relations,

$$\{b_1, b_2, c_1, \lambda'\} = \{-(b_1 + mb_2), b_2, c_1, \lambda\},$$

$$\{b_1, b_2, c_1, \lambda\} = \{-b_1, b_2, c_1, \lambda_1'\} = \{b_1 - mb_2, b_2, c_1, \lambda_1\}.$$

In case λ is real, the groups $\{q, \lambda\}$ are transformed by the substitution $\sqrt{q}\zeta = \eta$ into groups which reproduce the ternary form* $z_1^2 - qz_2^2 - \Delta z_3^2$. If λ be imaginary and q positive,† the substitution

$$\sqrt{q}\zeta = \frac{\eta - i}{\eta + i}$$

transforms (I) and (II) into

$$\left|\begin{matrix} \dfrac{a + b\sqrt{q}}{2}, & \dfrac{c + d\sqrt{q}}{2}\sqrt{-\Delta} \\ \dfrac{-c + d\sqrt{q}}{2}\sqrt{-\Delta}, & \dfrac{a - \sqrt{q}b}{2} \end{matrix}\right|,$$

$$\left|\begin{matrix} \dfrac{c - d\sqrt{q}}{2}\sqrt{-\Delta}, & \dfrac{-a + b\sqrt{q}}{2} \\ \dfrac{a + b\sqrt{q}}{2}, & \dfrac{c + d\sqrt{q}}{2}\sqrt{-\Delta} \end{matrix}\right|,$$

respectively, in which

$$a = -(2\alpha + m\alpha'),\ b = -(2\beta + m\beta'),\ c = \alpha',\ d = -\beta'.$$

These groups evidently coincide with those obtained in the case of a real λ.

In case q and Δ are both negative, the substitutions of type (I) can be reduced to the form

$$\left|\begin{matrix} A & B \\ q\bar{B} & \bar{A} \end{matrix}\right|$$

with the condition

$$A\bar{A} - qB\bar{B} = 1,$$

which can be satisfied only by a finite number of integer values of a, b, c, d since all the terms are positive. Hence the group $\{q, \lambda\}$ is finite when q and Δ are both negative.

CORNELL UNIVERSITY.

*See FRICKE-KLEIN, *Automorphe Functionen*, vol. I, p. 537.

† The orthogonal circle for these groups is $q\zeta\bar{\zeta} = 1$.