ACTA ARITHMETICA
V (1959)

An arithmetic property of groups of linear transformations

by

K. MAHLER (Manchester)

The connection between the geometrical theory of the *modular group* and that of the minima of *binary quadratic forms* is classical and well known. In the present note, I study the analogous problem for groups of linear transformations

$$z \to \frac{\alpha_k z+\beta_k}{\gamma_k z+\delta_k} \qquad (\alpha_k, \beta_k, \gamma_k, \delta_k \text{ real};\ \alpha_k\delta_k-\beta_k\gamma_k = 1;\ k = 1, 2, 3, \ldots)$$

the fundamental region of which is *compact in the hyperbolic plane*. By means of a theorem due to G. A. Hedlund, it will be proved that if $f(u, v)$ is any positive definite quadratic form, then the values

$$f(\alpha_k, \gamma_k) \qquad (k = 1, 2, 3, \ldots)$$

lie *dense on the positive real axis*. In the cases where the arithmetic structure of the coefficients $\alpha_k, \beta_k, \gamma_k, \delta_k$ is known, one is thus led to new arithmetic properties of quadratic forms.

1. Let Ψ be the open complex upper half-plane

$$y > 0, \quad \text{where} \quad z = x+yi,$$

and let U be its frontier consisting of

(i) the line $y = 0$,

(ii) the point $z = \infty$.

We interpret Ψ in the usual way as the non-Euclidean *hyperbolic plane*, and U as the *line at infinity* of this geometry.

The *hyperbolic lines* consist of (i) all semi-circles in Ψ with their centres on U, and (ii) all semi-lines in Ψ perpendicular to U. These lines are permuted under the *rigid motions of hyperbolic geometry* which, in explicit form, are defined by the linear transformations

$$S: z \to \frac{\alpha z+\beta}{\gamma z+\delta}$$

of Ψ into itself; here the coefficients $\alpha, \beta, \gamma, \delta$ are real numbers which may be assumed of determinant

$$\alpha\delta-\beta\gamma = 1.$$

The rigid motions leave the *hyperbolic distance* $d(z_1, z_2)$ of any two points $z_1 = x_1+y_1 i$ and $z_2 = x_2+y_2 i$ in Ψ invariant. If suitably normed, this distance is given by the equation

$$\sinh\frac{d(z_1, z_2)}{2} = \sqrt{\frac{(z_1-x_2)^2+(y_1-y_2)^2}{4y_1y_2}}.$$

In hyperbolic geometry there are three distinct types of *circles*, depending on their numbers of points of intersection with the line U. We are mainly interested in the *horocycles* which are those hyperbolic circles that meet U in just *one* point. There are two distinct types of horocycles, viz. (i) those of the form

$$(x-a)^2+(y-b)^2 = b^2, \quad \text{where} \quad b>0,$$

which are tangent to U at a finite point $z = a$, and (*ii*) those of the form

$$y = b, \quad \text{where} \quad b>0,$$

which may be considered as being tangent to U at $z = \infty$. The rigid motions of the hyperbolic plane change horocycles again into horocycles. In particular, the horocycles of the second form are invariant under the special motions

$$W\colon z \to z+\beta \quad (\beta \text{ real}).$$

2. Let F be any Fuchsian group of linear transformations S fo Ψ into itself. A horocycle C is said to be *transitive with respect to* F if its images $S(C)$ under all the elements S of F lie everywhere dense in Ψ. In explicit form, if z_0 is any point in Ψ, and

$$V\colon d(z, z_0) < \varepsilon, \quad \text{where } \varepsilon > 0,$$

is an arbitrary neighbourhood of z_0, then at least one image $S(C)$ of C with $S \in F$ passes through this neighbourhood.

The theory of transitive horocycles has been studied in detail by G. A. Hedlund [1], and one of his results forms the basis for this paper.

Let us, for shortness, say that the Fuchsian group F is *admissible* if it possesses a *compact fundamental region*; i. e. F has a fundamental region, R_0 say, which lies entirely in Ψ and does not meet the line U.

By way of example, every Schwarzian triangle group in Ψ which is generated by a triangle with *positive* angles is admissible. The modular

group, however, is *not* admissible, because its fundamental regions either contain the point $z = \infty$ or an equivalent point on U.

Theorem 2.5 of Hedlund's paper implies the following important result.

THEOREM 1. *If the Fuchsian group F is admissible, then every horocycle C in Ψ is transitive with respect to F.*

In the example of the modular group this theorem does, of course, not hold, and it is, in fact, obvious that no horocycle $y = b$ can be transitive.

3. We need a result which is slightly stronger than Theorem 1 for the application to quadratic forms.

THEOREM 2. *Let F be an admissible Fuchsian group, and let b_1 and b_2 be real numbers such that $0 < b_1 < b_2$. For every point z_0 in Ψ there exists an element S of F such that $S(z_0) = z_1 = x_1+y_1 i$ satisfies the inequality*

$$b_1 < y_1 < b_2.$$

Proof. Choose an arbitrary real number b^* such that $b_1 < b^* < b_2$. There is then a positive constant ε such that every circular disc

$$d(z, z^*) < \varepsilon$$

of radius ε and with its centre z^* on the horocycle $y = b^*$ lies entirely in the horizontal strip

$$b_1 < y < b_2$$

between the two horocycles $y = b_1$ and $y = b_2$. By Theorem 1, the horocycle C^*: $y = b^*$ is transitive. There is then a transformation $S_1 \in F$ such that the image $C^{**} = S_1(C^*)$ of C^* passes through the disc

$$d(z, z_0) < \varepsilon.$$

Choose an arbitrary z^{**} in C^{**} satisfying

$$d(z^{**}, z_0) < \varepsilon,$$

and put

$$S = S_1^{-1}, \quad z^* = Sz^{**}, \quad z_0^* = Sz_0,$$

so that also $S \in F$. By the invariance and the symmetry of the hyperbolic distance, also

$$d(z^*, z_0^*) = d(z_0^*, z^*) < \varepsilon.$$

Since z^{**} lies on C^{**}, z^* lies on the original horocycle C^*. It follows that $S(z_0)$ is situated in some disc of radius ε with its centre z^* on $y = b^*$; hence this point $S(z_0)$ satisfies the assertion.

4. As before, let F be an admissible Fuchsian group, and let

$$S_k\colon\ z \to \frac{\alpha_k z+\beta_k}{\gamma_k z+\delta_k} \qquad (k=1,2,3,\ldots)$$

be all its elements; here $\alpha_k, \beta_k, \gamma_k, \delta_k$ are real numbers such that

$$\alpha_k\delta_k-\beta_k\gamma_k=1.$$

We associate with S_k the *homogeneous linear transformation*

$$S_k^*\colon\ u \to \alpha_k u+\beta_k v, \qquad v \to \gamma_k u+\delta_k v.$$

Next let

$$f(u,v)=au^2+2buv+cv^2$$

be any binary positive definite quadratic form; hence

$$a>0, \qquad c>0, \qquad d=ac-b^2>0.$$

The transformation S_k^* changes $f(u,v)$ into a new positive definite form

$$f_k(u,v)=f(\alpha_k u+\beta_k v,\ \gamma_k u+\delta_k v)=a_k u^2+2b_k uv+c_k v^2$$

with coefficients

$$a_k=f(\alpha_k,\gamma_k), \qquad b_k=a\alpha_k\beta_k+b(\alpha_k\delta_k+\beta_k\gamma_k)+c\gamma_k\delta_k, \qquad c_k=f(\beta_k,\delta_k).$$

Again

$$a_k>0, \qquad c_k>0, \qquad a_kc_k-b_k^2=ac-b^2>0,$$

with the third relation following from the identity

$$a_kc_k-b_k^2=(ac-b^2)(\alpha_k\delta_k-\beta_k\gamma_k)^2.$$

Put

$$\omega=\frac{-b+i\sqrt{ac-b^2}}{a}, \qquad \omega_k=\frac{-b_k+i\sqrt{ac-b^2}}{a_k},$$

where the square root is taken with the positive sign; thus both ω and ω_k lie in Ψ. These two numbers may also be defined as the roots in Ψ of the two quadratic equations

$$f(z,1)=0 \quad \text{and} \quad f_k(z,1)=0,$$

respectively. Therefore

$$0=f_k(\omega_k,1)=f(\alpha_k\omega_k+\beta_k,\ \gamma_k\omega_k+\delta_k)=(\gamma_k\omega_k+\delta_k)^2 f\left(\frac{\alpha_k\omega_k+\beta_k}{\gamma_k\omega_k+\delta_k},1\right),$$

where evidently

$$\gamma_k\omega_k+\delta_k\neq 0, \qquad \text{hence} \qquad f\left(\frac{\alpha_k\omega_k+\beta_k}{\gamma_k\omega_k+\delta_k},1\right)=0.$$

Thus

$$\omega=\frac{\alpha_k\omega_k+\beta_k}{\gamma_k\omega_k+\delta_k}=S_k(\omega_k),$$

and conversely,

$$\omega_k=\frac{\delta_k\omega-\beta_k}{-\gamma_k\omega+\alpha_k}=S_k^{-1}(\omega);$$

S_k^{-1} denotes the inverse of S_k. As S_k runs over all elements of F, its inverse S_k^{-1} does the same since F is a group.

5. Write

$$\omega=\xi+\eta i \quad \text{and} \quad \omega_k=\xi_k+\eta_k i,$$

so that

$$\xi=-\frac{b}{a}, \quad \eta=\frac{\sqrt{ac-b^2}}{a} \quad \text{and} \quad \xi_k=-\frac{b_k}{a_k}, \quad \eta_k=\frac{\sqrt{ac-b^2}}{a_k}.$$

On applying Theorem 2, we obtain the following result. If again

$$0<b_1<b_2,$$

then there exists a transformation $S=S_k^{-1}$ in F such that the imaginary part η_k of $\omega_k=S_k^{-1}(\omega)$ satisfies the inequality

$$b_1<\eta_k<b_2.$$

This means that

$$a_k=f(\alpha_k,\gamma_k)$$

satisfies the inequality

$$\frac{\sqrt{ac-b^2}}{b_2}<a_k<\frac{\sqrt{ac-b^2}}{b_1}.$$

Since the constants b_1 and b_2 are still at our disposal, the result so proved may be expressed as follows.

THEOREM 3. *Let F be an admissible Fuchsian group consisting of the linear transformations*

$$s_k\colon\ z \to \frac{\alpha_k z+\beta_k}{\gamma_k z+\delta_k} \qquad (k=1,2,3,\ldots)$$

where $\alpha_k, \beta_k, \gamma_k, \delta_k$ *are real numbers satisfying*

$$\alpha_k \delta_k - \beta_k \gamma_k = 1.$$

Let further

$$f(u, v) = au^2 + 2buv + cv^2$$

be an arbitrary positive definite quadratic form. The values

$$f(\alpha_k, \gamma_k) \quad (k = 1, 2, 3, \ldots)$$

of this form lie everywhere dense in the positive real axis.

This theorem may, of course, not be applied to the modular group for which, in fact, the values $f(\alpha_k, \gamma_k)$ have *no* finite limit point.

I conjecture that if the form $f(u, v)$ is *indefinite* and F is again admissible, then the values $f(\alpha_k, \gamma_k)$ lie everywhere dense on *both the positive and the negative real axis.*

6. Theorem may be applied to many known Fuchsian groups. As an example we consider a group which is related to the theory of indefinite ternary quadratic forms (see Fricke-Klein [2], p. 533 ff).

Let p, q, r be three squarefree positive integers which are relatively prime in pairs and are such that the ternary form

$$f(z_1, z_2, z_3) = pz_1^2 - qz_2^2 - rz_3^2$$

is distinct from zero for all integers z_1, z_2, z_3 except $z_1 = z_2 = z_3 = 0$. We denote (a, b, c, d) all integral solutions of the quaternary Pellian equation

$$a^2 - b^2 pr + c^2 qr - d^2 pq = 4.$$

It is then proved that the unimodular transformations

$$s: z \to \frac{\alpha z - \beta}{\gamma z - \delta} \qquad (\alpha\delta - \beta\gamma = 1),$$

where

$$\alpha = \frac{a + b\sqrt{pr}}{2}, \qquad \beta = \frac{c\sqrt{r} + d\sqrt{p}}{2}\sqrt{q},$$

$$\gamma = \frac{-c\sqrt{r} + d\sqrt{p}}{2}\sqrt{q}, \qquad \delta = \frac{a - b\sqrt{pr}}{2}$$

form an admissible Fuchsian group. We deduce therefore at once from Theorem 3 that if again $f(u, v)$ is any positive definite quadratic form,

then the values

$$f\left(\frac{a + b\sqrt{pr}}{2}, \frac{-c\sqrt{r} + d\sqrt{p}}{2}\sqrt{q}\right)$$

lie dense on the positive real axis.

It seems probable that Theorem 3 has an analogue for Kleinian polyhedron groups and positive definite Hermitean form.

References

[1] G. A. Hedlund, *Fuchsian groups and transitive horocycles*, Duke Math. J. 2 (1936), p. 530-542.

[2] R. Fricke und F. Klein, *Automorphe Funktionen*, Band 1, Leipzig 1897.

MATHEMATICS DEPARTMENT, MANCHESTER UNIVERSITY
28 August, 1958

Reçu par la Rédaction le 12. 9. 1958