Canad. Math. Bull. Vol. 17 (1), 1974.

ORBITAL LATTICES OF $SL^+(2, \mathbf{Z})$

BY
S. A. RANKIN[1]

The results described in this paper were obtained in the study of analytic maps between flat two-tori. It is felt that analogous results will be obtained from a similar study of the analytic maps between higher-dimensional flat tori.

It is well-known that the multiplicative group $GL^+(2, \mathbf{Q})$ acts on the upper half-plane $\mathfrak{H}=\{z \in \mathbf{C} \mid \Im(z)>0\}$ as a group of linear fractional transformations, i.e. for each element $T=\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ of $GL^+(2, \mathbf{Q})$, $T(z)=(\alpha z+\beta)/(\gamma z+\delta)$ for all $z \in \mathfrak{H}$. Similarly, the subgroup $SL^+(2, \mathbf{Z})$ of $GL^+(2, \mathbf{Q})$ also acts on $\mathfrak{H}$ as a group of linear fractional transformations. The orbits of $\mathfrak{H}$ under $SL^+(2, \mathbf{Z})$ and $GL^+(2, \mathbf{Q})$ will be called S-orbits and G-orbits respectively. Moreover, we shall abbreviate $SL^+(2, \mathbf{Z})$ to SL^+ and $GL^+(2, \mathbf{Q})$ to GL^+.

To each S-orbit ρ of $\mathfrak{H}$ one can assign a unique lattice $\mathfrak{L}(\rho)$ in $\mathbf{C}$. This lattice could be called the lattice of complex multiplications of ρ since the elements of ρ determine isomorphic elliptic curves each having $\mathfrak{L}(\rho)$ as its set of complex multiplications [1]. As well, $\mathfrak{L}(\rho)$ could be called the lattice of complex distortions of ρ [2]. It is the purpose of this paper to investigate the relationship between the lattices assigned to the S-orbits which are contained in a common G-orbit. We shall consider only ample orbits, i.e., those orbits which contain an ample complex number [2], since $\mathfrak{L}(\rho)=\mathbf{Z}$ for all non-ample S-orbits ρ. An element $h \in \mathbf{C}$ is said to be ample if $\Re(h)$ and $|h|^2$ are rational. The set of all ample elements of $\mathfrak{H}$ will be denoted by $\mathfrak{H}^*$.

DEFINITION 1. Two S-orbits ρ and σ are said to be immersion-equivalent if there exists a G-orbit Λ such that $\rho \cup \sigma \subset \Lambda$.

H. G. Helfenstein [2] has shown that for immersion-equivalent S-orbits ρ and σ, there exist $h \in \sigma$ and $a \in \mathbf{Z}^+$ such that $ah \in \rho$, where $\mathbf{Z}^+$ denotes the positive integers.

DEFINITION 2. For immersion-equivalent S-orbits ρ and σ, let $\mathrm{Rep}(\rho, \sigma)=\{(a, h) \in \mathbf{Z}^+ \times \sigma \mid ah \in \rho\}$.

For any $m \in \mathbf{Z}^+$, let $SL^+(m)$ be the subgroup of SL^+ consisting of those matrices $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL^+$ for which $\gamma \equiv 0 \pmod m$. It is clear that if $(a, h) \in \mathrm{Rep}(\rho, \sigma)$ and

(1) The author gratefully acknowledges support of this research by the National Research Council.

https://doi.org/10.4153/CMB-1974-015-6 Published online by Cambridge University Press

$T \in SL^+(a)$, then $(a, T(h)) \in \mathrm{Rep}(\rho, \sigma)$. Now for each $m \in \mathbf{Z}^+$, define the functions I^m, η^m, μ^m, ν^m from $\mathfrak{H}^*$ into $\mathbf{Z}$ as follows: for each $h \in \mathfrak{H}^*$, $\mathfrak{R}(h)$ and $|h|^2$ are elements of $\mathbf{Q}$. Let $2\mathfrak{R}(h)=p/q$ and $|h|^2=r/s$ for integers p, q, r, and s such that $(p, q)=(r, s)=1$ and $q>0$, $s>0$. Let $k=(m(q, s), qs)$, and define $I^m(h)=k/(q, s)$, $\eta^m(h)=qs/k$, $\mu^m(h)=qr/k$, and $\nu^m(h)=mps/k$. It is a matter of computation to verify the following useful equations: for all $m \in \mathbf{Z}^+$ and $h \in \mathfrak{H}^*$,

$$\eta^1(h) = I^m(h)\eta^m(h), \quad \text{and} \tag{1}$$

$$\mu^1(mh)\eta^1(h) = m^2\eta^1(mh)\mu^1(h). \tag{2}$$

LEMMA 1. *Let $m \in \mathbf{Z}^+$. Then for every $h \in \mathfrak{H}^*$ and $T \in SL^+(m)$, $\eta^m(h)\mathfrak{I}(h)=\eta^m(T(h))\mathfrak{I}(T(h))$.*

Proof. Let $g=T(h)$. It can be shown that the positive definite quadratic forms

$$F(x, y) = mx^2+\nu^m(h)xy+\eta^m(h)\mu^m(h)y^2$$

and

$$G(x, y) = mx^2+\nu^m(g)xy+\eta^m(g)\mu^m(g)y^2$$

represent the same set of integers, whence the discriminants of F and G are equal. Thus $(\nu^m(h))^2-4m\eta^m(h)\mu^m(h)=(\nu^m(g))^2-4m\eta^m(g)\mu^m(g)$. But it is readily seen that

$$(\nu^m(h))^2-4m\eta^m(h)\mu^m(h) = -(m\eta^m(h)\mathfrak{I}(h))^2$$

and

$$(\nu^m(g))^2-4m\eta^m(g)\mu^m(g) = -(m\eta^m(g)\mathfrak{I}(g))^2.$$

Suppose now that ρ and σ are ample immersion-equivalent S-orbits.

DEFINITION 3. To each $(a, h) \in \mathrm{Rep}(\rho, \sigma)$, let $\mathfrak{L}(a, h)$ be the lattice generated by 1 and $\eta^a(h)h$ in $\mathbf{C}$.

THEOREM 1. *Let $(a, h) \in \mathrm{Rep}(\rho, \sigma)$. Then for each $T \in SL^+(a)$, $\mathfrak{L}(a, h)=\mathfrak{L}(a, T(h))$.*

Proof. Let $g=T(h)$. Since $\eta^a(h)\mathfrak{I}(h)=\eta^a(g)\mathfrak{I}(g)$ by Lemma 1, it is sufficient to show that

$$\eta^a(h)\mathfrak{R}(h)-\eta^a(g)\mathfrak{R}(g)$$

is an integer. Since σ is ample, every element of σ is ample. Thus there exists a square-free positive integer m and integers x, y, v, and w such that $(x, y)=(v, w)=1$ and $h=x/y+v\sqrt{m}i/w$. Furthermore, since $T \in SL^+(a)$, there exist integers α, β, γ, and δ such that $T=\begin{bmatrix} \alpha & \beta \\ a\gamma & \delta \end{bmatrix}$. Let $u_1=(\alpha x+\beta y)w$, $u_2=(a\gamma x+\delta y)w$ and $u_3=a\alpha\gamma(vy)^2m$. Then define $j=2(u_1u_2+u_3)$, $k=(u_2)^2+u_3$ and $l=(u_1)^2+(\alpha vy)^2m$. Then one has $g=(j+2y^2wv\sqrt{m}i)/2k$ and so $\eta^1(g)(j, k, l)=k$. If $t=(xw)^2+(vy)^2m$, then it is easily seen that $\eta^1(h)(t, (yw)^2, 2yw^2)=(yw)^2$, whence both $\eta^1(g)\mathfrak{I}(g)(j, k, l)$ and $\eta^1(h)\mathfrak{I}(h)(t, (yw)^2, 2yw^2)$ are equal to $y^2vw\sqrt{m}$. By Lemma 1, this implies that

https://doi.org/10.4153/CMB-1974-015-6 Published online by Cambridge University Press

$(j, k, l)=(t, (yw)^2, 2yw^2)$. Further computation yields $I^a(g)\eta^a(g)\mathfrak{R}(g)=j/2(j,k,l)$ and $I^a(h)\eta^a(h)\mathfrak{R}(h)=xyw^2/(t, (yw)^2, 2yw^2)$. Furthermore, $I^a(h)=\eta^1(h)\mathfrak{I}(h)/\eta^a(h)\mathfrak{I}(h)=\eta^1(g)\mathfrak{I}(g)/\eta^a(g)\mathfrak{I}(g)=I^a(g)$ and so $[\eta^a(g)\mathfrak{R}(g)-\eta^a(h)\mathfrak{R}(h)]\mathfrak{I}^a(h)$ is equal to

$$a\alpha\gamma\frac{t}{(j, k, l)}+\beta\delta\frac{(yw)^2}{(j, k, l)}+a\beta\gamma\frac{2xyw^2}{(j, k, l)}.$$

It is clearly sufficient to show that $I^a(h)(j, k, l)$ divides $(yw)^2$. But by (1), $\eta^a(h)I^a(h)(j, k, l)=\eta^1(h)(j, k, l)$ and it is readily seen that $\eta^1(h)(j, k, l)=(yw)^2$.

In particular, for any ample S-orbit ρ, we have $(1, h)\in \operatorname{Rep}(\rho, \rho)$ for all $h\in\rho$. Since $SL^+(1)=SL^+$, we have the following

Corollary 1. *Let $h\in\rho$. Then for each $T\in SL^+$, $\mathfrak{L}(1, h)=\mathfrak{L}(1, T(h))$.*

Definition 4. For each ample S-orbit ρ, let $\mathfrak{L}(\rho)$ denote the lattice $\mathfrak{L}(1, h)$ for $h\in\rho$. By Corollary 1, $\mathfrak{L}(\rho)$ is well-defined. Furthermore, let $C(\rho)=\eta^1(h)\mathfrak{L}(h)$ for any $h\in\rho$. By Lemma 1, $C(\rho)$ is a well-defined real number assigned to ρ.

We are now able to determine the condition under which $\mathfrak{L}(\rho)\subset\mathfrak{L}(\sigma)$ for ample immersion-equivalent S-orbits ρ and σ. It is interesting to observe that this information can be obtained from local parameters of the orbit pair and yet, as one might expect, the condition can by phrased in terms of orbital invariants. By local parameter of the orbit pair, we mean a function κ from $\operatorname{Rep}(\rho, \sigma)$ into $\mathbf{Z}^+$ defined as follows: for each (a, h) in $\operatorname{Rep}(\rho, \sigma)$, let $\kappa(a, h)=\mu^1(ah)/\mu^1(h)$. It can readily be shown that if one sets $2\mathfrak{R}(h)=p/q$ and $|h|^2=r/s$ as before, then $\kappa(a, h)=a^2(q, s)/(a^2q, as, qs)$, from which it follows that $\kappa(a, h)\in\mathbf{Z}^+$.

Theorem 2. *$\mathfrak{L}(\rho)\subset\mathfrak{L}(\sigma)$ iff $a \mid \kappa(a, h)$ for any $(a, h)\in \operatorname{Rep}(\rho, \sigma)$. Moreover, $\mathfrak{L}(\sigma)\subset\mathfrak{L}(\rho)$ iff $\kappa(a, h)\mid a$.*

Proof. Suppose firstly that $\kappa(a, h)\mid a$. Since by (2), $\mu^1(ah)/\mu^1(h)=a^2\eta^1(ah)/\eta^1(h)$, it follows that $a^2\eta^1(ah)=\kappa(a, h)\eta^1(h)$, whence $a\eta^1(ah)ah/\kappa(a, h)=\eta^1(h)h$. But $\mathfrak{L}(\sigma)$ is generated by 1 and $\eta^1(h)h$ and $\mathfrak{L}(\rho)$ is generated by 1 and $\eta^1(ah)ah$, whence $\mathfrak{L}(\sigma)\subset\mathfrak{L}(\rho)$. Conversely, suppose that $\mathfrak{L}(\sigma)\subset\mathfrak{L}(\rho)$. Then for any element (a, h) of $\operatorname{Rep}(\rho, \sigma)$, $\mathfrak{L}(1. h)\subset\mathfrak{L}(1, ah)$. There exist integers m and n such that $\eta^1(h)h=m+n\eta^1(ah)ah$, whence $\eta^1(h)\mathfrak{I}(h)=n\eta^1(ah)\mathfrak{I}(ah)$. This implies that $a=n\kappa(a, h)$, and thus $\kappa(a, h)\mid a$.

Finally, observe that if $(a, h)\in\operatorname{Rep}(\rho, \sigma)$, and $J=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$, then $(a, J(ah))\in\operatorname{Rep}(\sigma, \rho)$. Again, it is a matter of computation to show that $\kappa(a, h)\kappa(a, J(ah))=a^2$. But now by the above argument, we have

$$\mathfrak{L}(\rho)=\mathfrak{L}(1, J(ah))\subset\mathfrak{L}(1, aJ(ah))=\mathfrak{L}(\sigma)$$

iff $\kappa(a, J(ah))\mid a$, i.e. iff $a\mid\kappa(a, h)$.

Corollary 2. *$\mathfrak{L}(\rho)\subset\mathfrak{L}(\sigma)$ iff $C(\sigma)\mid C(\rho)$.*

https://doi.org/10.4153/CMB-1974-015-6 Published online by Cambridge University Press

Proof. It is immediate that if $(a, h) \in \mathrm{Rep}(\rho, \sigma)$, then $aC(\rho)=\kappa(a, h)C(\sigma)$, for by definition, $C(\rho)=\eta^1(ah)\mathfrak{I}(ah)$ and $C(\sigma)=\eta^1(h)\mathfrak{I}(h)$. Thus $C(\rho)/C(\sigma)= a\eta^1(ah)/\eta^1(h)=\kappa(a, h)/a$.

References

1. A. Boerl, S. Chowla, C. S. Herz, K. Iwasawa, and J-P. Serre, Seminar on Complex Multiplication, Lecture Notes in Math., no. 92, Springer-Verlag, Berlin and New York, 1966.

2. H. G. Helfenstein, *Analytic maps between tori*, Comm. Math. Helv. **45** (1970), 530–540.

University of Ottawa
Ottawa, Ontario

https://doi.org/10.4153/CMB-1974-015-6 Published online by Cambridge University Press