

GENERATORS AND RELATIONS FOR CERTAIN SPECIAL LINEAR GROUPS

BY RICHARD G. SWAN

Communicated by Saunders Mac Lane, January 23, 1968

Several years ago I calculated presentations for several of the groups $SL(2, R)$ where R is the ring of integers of a quadratic imaginary number field $K = \mathbb{Q}((-m)^{1/2})$. The method used was extremely tedious and was never published. Recently, while checking these calculations, I discovered a much simpler approach to the problem which I will outline here. The interest in these calculations is considerably increased by recent results of Serre [6]. He considers the congruence subgroup problem for the groups $SL(2, R)$ where R is the ring of integers \mathcal{O} of an algebraic number field (and, more generally for $R = \mathcal{O}[a^{-1}]$ where $a \in \mathcal{O}$). He obtains the expected results [1], [5] whenever R has a unit of infinite order. Thus the only exceptions are $R = \mathbb{Z}$ and the case which I will consider here. Serre has also shown that all of these cases are true exceptions. The case $R = \mathbb{Z}$ is, of course, well known. Hopefully, the calculations outlined here will throw some light on the remaining cases. At present, I have only carried out the calculations for fields K with discriminants D between -1 and -24 . The length of the calculation increases rapidly with $|D|$ but the calculation could easily be extended to arbitrarily large values of $|D|$ by machine computation. This has not been done at the present time. Full details of the calculations will be published elsewhere. I would like to thank H. Bass for communicating Serre's results to me.

1. Transformation groups. The original calculation depended on a theorem of Macbeath [4]. However, this leads to an excessively large number of generators and relations and so to the long and tedious process of simplifying the presentation. The main simplification results from a generalization of Macbeath's theorem to non-simply-connected spaces.

Let X be a pathwise connected topological space. Let G be a group acting on X by homeomorphisms and let V be a pathwise connected open subset of X whose transforms cover $X = GV$. Let E be the set of elements $\sigma \in G$ such that $V \cap \sigma V \neq \emptyset$. Let Γ be a group with one generator $[\sigma]$ for each $\sigma \in E$ and with the relations $[\sigma\tau] = [\sigma][\tau]$ whenever $V \cap \sigma V \cap \sigma\tau V \neq \emptyset$. Let $\epsilon: \Gamma \rightarrow G$ by $\epsilon([\sigma]) = \sigma$. Macbeath's theorem asserts that ϵ is an isomorphism if $\pi_1(X) = 0$. In the general case, the following result holds.

THEOREM 1. *There is an exact sequence*

$$1 \rightarrow N \rightarrow \pi_1(X) \xrightarrow{\theta} \Gamma \xrightarrow{\epsilon} G \rightarrow 1$$

where N is the subgroup of $\pi_1(X)$ generated by all elements which can be represented by a loop in at least one of the sets $V \cup \sigma V, \sigma \in E$.

The map θ is defined by subdividing a loop λ into small paths contained successively in sets $\rho_0 V, \rho_1 V, \dots, \rho_n V, \rho_n = \rho_0$ and setting $\theta(\lambda) = [\rho_0^{-1}\rho_1][\rho_1^{-1}\rho_2] \dots [\rho_{n-1}^{-1}\rho_n]$.

2. Hermitian forms. We consider binary hermitian forms $Q(x, y) = A [|x + zy|^2 + \zeta^2 |y|^2]$ where $z \in \mathbb{C}, \zeta > 0, A > 0$. We ignore A and consider the space $H = \{(z, \zeta)\} = \mathbb{C} \times \mathbb{R}^+$. The group $GL(2, \mathbb{C})$ acts on H by changing the variables x, y in the usual way. Bianchi and Humbert [2], [3] have given a reduction theory for such forms under the action of $G = SL(2, R) \subset GL(2, \mathbb{C})$, R being the ring of integers of a quadratic imaginary number field $K \subset \mathbb{C}$. Consider all $\xi, \eta \in R$ with $R\xi + R\eta = R$. At these points, consider the value $Q(\xi, \eta)$ and suppose that the minimum of these values occurs at (ξ_0, η_0) . By an element of $SL(2, R)$ we can change variables so that $(\xi_0, \eta_0) \mapsto (1, 0)$. Let B be the subset of H for which the minimum occurs at $(\xi_0, \eta_0) = (1, 0)$. Then $H = GB$. It is easy to see that B consists of all points of H lying above all the spheres $S(\lambda/\mu): |\mu z - \lambda|^2 + \zeta^2 |\mu|^2 \geq 1$ for all $\lambda, \mu \in R$ with $R\lambda + R\mu = R$. It is important that locally a finite number of $S(\lambda/\mu)$ suffice to bound B . In fact every point of the boundary $\mathbb{C} \times \{0\}$ of $H = \mathbb{C} \times \mathbb{R}^+$ lies strictly below one of the $S(\lambda/\mu)$ except for a discrete set (the "singular" points). This was partially shown by Humbert [3] but he considered only points with coordinates in K . The remaining points may be disposed of by using the following theorem of diophantine approximation.

THEOREM 2. *Let $K \subset \mathbb{C}$ be a quadratic imaginary number field with ring of integers R . Then there is a constant A depending only on K such that for any $z \in \mathbb{C}$ with $z \notin K$, there are an infinite number of solutions $\lambda, \mu \in R$ of the inequality*

$$|z - \lambda/\mu| \leq A/|\mu|^2$$

which satisfy the condition $R\lambda + R\mu = R$.

In spite of its classical appearance, I have not been able to find this theorem in the literature except in the simple case where the class number h of K is 1. In this case we can easily obtain solutions with $R\lambda + R\mu = R$ by factoring out the greatest common divisor of λ and μ . The general case requires a more complicated argument.

3. **A presentation for $SL(2, R)$.** Using the notations of §2, it is easy to see that the boundary of B has a regular cell decomposition with 2-cells of the form $B \cap S(\lambda/\mu)$ for certain $\lambda, \mu \in R$ with $R\lambda + R\mu = R$. I will refer to this cell decomposition as the Bianchi diagram of K . Let E_0 be the 1-skeleton of the Bianchi diagram and let E be the union of all σE_0 for $\sigma \in G = SL(2, R)$. Then E is a regular 1-complex stable under G and E_0 is a subcomplex of E . We now apply Theorem 1 to G and the space $X = H - E$ and $V = B - E = B - E_0$, compensating in the usual way for the fact that V is closed rather than open. The necessity for the generalized form of Theorem 1 now becomes clear. Most intersections $B \cap \sigma B$ will have dimension ≤ 1 . By excising E we eliminate all such intersections and so eliminate all the excess generators and relations.

We must now determine the group Γ . Note that B and the Bianchi diagram are stable under the group H of upper triangular matrices in $G = SL(2, R)$. Let $S(\lambda_i/\mu_i) \cap B, i = 1, \dots, r$ represent all 2-cells of the Bianchi diagram modulo the action of H . Choose matrices

$$A_i = (\lambda_i^* \mu_i^*) \in G.$$

Then Γ is generated by H and the $[A_i]$ with easily determined relations. To find G , we factor out the image of $\pi_1(X)$ in Γ . It will suffice to look at small loops about the edges of the Bianchi diagram, and to take a set of representatives for the edges modulo H .

If $x \in G$ lies in one of the double cosets HA_iH , we choose a representation $x = h_1 A_i h_2$ and define $[x] = h_1 A_i h_2$ as a formal word. If e is an edge of the Bianchi diagram, consider all spheres $S(\lambda/\mu)$ with $R\lambda + R\mu = R$ such that e lies on $S(\lambda/\mu)$. There are a finite number of these and the values $\alpha = \lambda/\mu$ all lie on a straight line in \mathbb{C} . Let $\alpha_1, \dots, \alpha_n$ be the values so obtained in order along the line. Choose matrices

$$\rho_j = (\lambda_j^* \mu_j^*) \in SL(2, R)$$

with $\alpha_j = \lambda_j/\mu_j$. Then $[\rho_j \rho_{j+1}^{-1}]$ is defined for all j . The "edge relation" corresponding to e is defined to be the relation

$$R_e = [\rho_1^{-1}] [\rho_1 \rho_2^{-1}] \cdots [\rho_{n-1} \rho_n^{-1}] [\rho_n] = 1.$$

This relation obviously holds in G and G is obtained from Γ by adding all these relations.

If we ignore the cases $K = Q((-1)^{1/2})$ and $K = Q((-3)^{1/2})$, we can choose as generators for H the matrices

$$J = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

and

$$U = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$$

where $1, \omega$ is an integral base for R .

THEOREM 3. *If $K \neq Q((-1)^{1/2})$ or $Q((-3)^{1/2})$, $SL(2, R)$ is generated by J, T, U, A_1, \dots, A_r with the relations*

(1) J is central, $TU = UT, J^2 = 1$.

(2) $A_i^{-1} = [A_i^{-1}], i = 1, \dots, r$.

(3) *The edge relations $R_e = 1$ for a set of representatives of the edges of the Bianchi diagram mod H .*

The relation (2), of course, stands for a relation of the form $A_i^{-1} = hA_jh'$ for some $h, h' \in H, 1 \leq j \leq r$. The right hand side of this is uniquely determined modulo the relations (1).

4. Explicit calculations. I will now give a few examples of representations obtained by the above method, beginning with the two cases omitted in Theorem 3. The letters J, T, U will always have the same meaning as in Theorem 3. In addition, A will stand for

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

For $K = Q((-1)^{1/2})$ we choose $\omega = i = (-1)^{1/2}$ in U and let

$$L = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

THEOREM 4. *The group $SL(2, \mathbf{Z}[i])$ is generated by J, T, U, L, A with the relations $TU = UT, J^2 = 1, J$ central, $L^2 = J, (TL)^2 = J, (UL)^2 = J, (AL)^2 = J, A^2 = J, (TA)^3 = J, (UAL)^3 = J$.*

For $K = Q((-3)^{1/2})$ we choose $\omega = \frac{1}{2}(-1 + (-3)^{1/2})$ in U and let

$$L = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix}.$$

THEOREM 5. *The group $SL(2, \mathbf{Z}[\omega])$ for $K = Q((-3)^{1/2})$ is generated by J, T, U, L, A with the relations $TU = UT, J^2 = 1, J$ central, $L^3 = 1, L^{-1}TL = T^{-1}U^{-1}, L^{-1}UL = T, A^2 = J, (AL)^2 = J, (TA)^3 = J, (UAL)^3 = J$.*

In each of these theorems I have slightly altered the edge relations to make the presentation a bit simpler.

For $K = \mathcal{Q}((-5)^{1/2})$, we choose $\omega = (-5)^{1/2}$ and let

$$B = \begin{pmatrix} -\omega & 2 \\ 2 & \omega \end{pmatrix}, \quad C = \begin{pmatrix} -\omega - 4 & -2\omega \\ 2\omega & \omega - 4 \end{pmatrix}.$$

THEOREM 6. *The group $SL(2, \mathbf{Z}[(-5)^{1/2}])$ is generated by J, T, U, A, B, C with the relations $J^2=1, J$ central, $TU=UT, A^2=J, B^2=J, (TA)^3=J, (AB)^2=J, (AUBU^{-1})^2=J, ACA=JTCT^{-1}, UBU^{-1}CB=JTCT^{-1}$.*

It follows from this that the abelianized group $G/[G, G]$ for $G=SL(2, \mathbf{Z}[(-5)^{1/2}])$ has rank 2. The elementary subgroup (generated by T and U) has rank 1. Serre has shown by other methods that this sort of behavior is to be expected of quadratic imaginary fields. In the few examples I have computed, the rank of $G/[G, G]$ turns out to be equal to the class number. I do not know whether this is true in general. It also turns out that $G/[G, G]$ is finite for $G=GL(2, R)$ rather than $SL(2, R)$. Again I do not know if this is always the case.

5. Extending the calculations. The main difficulty in extending the calculations is to determine the Bianchi diagram. For the calculations above, this was taken from Bianchi's paper [2]. In the general case it is necessary to calculate the diagram directly. The first step is to determine all singular points. This is easily done by elaborating the methods of Humbert [3].

The singular points of K form a finite number of cosets of R in K . There are none outside of K . We assume m is squarefree.

THEOREM 7. *The singular points of $K = \mathcal{Q}((-m)^{1/2})$ modulo R are given by the formula $p(r + (-m)^{1/2})/s$ where $r, s \in \mathbf{Z}, s > 0, -s/2 < r \leq s/2, s^2 \leq r^2 + m$ and*

(1) *If $m \not\equiv 3 \pmod{4}$, then $s \mid r^2 + m, s \neq 1, (p, s) = 1$, and p is taken mod s .*

(2) *If $m \equiv 3 \pmod{4}$, then $2 \mid s, s \neq 2, 2s \mid r^2 + m, (p, s/2) = 1$, and p is taken mod $s/2$.*

It is also worth noting that if we ignore p and omit the conditions $s \neq 1$ and $s \neq 2$, the ideals $(s, r + (-m)^{1/2})$ form a complete set of representatives for the ideal classes of R .

We can now find the diagram by a trial and error procedure. To check whether the diagram we obtain is the true Bianchi diagram we have only to check whether some nonsingular vertex of the diagram lies strictly below one of the spheres $S(\lambda/\mu)$ with $(\lambda, \mu) = R$.

If it does, we throw in that $S(\lambda/\mu)$ and its translates by R and begin again. It is not hard to give an upper bound for the number of steps needed.

REFERENCES

1. H. Bass, J. Milnor and J.-P. Serre, *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and SP_{2n} ($n \geq 2$)*, Inst. Hautes Études Sci. Publ. Math. (to appear).
2. L. Bianchi, *Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari*, Math. Ann. **40** (1892), 332–412.
3. G. Humbert, *Sur la réduction des formes d'Hermite dans un corps quadratique imaginaire*, C. R. Acad. Sci. Paris **161** (1915), 189–196.
4. A. M. Macbeath, *Groups of homeomorphisms of a simply connected space*, Ann. of Math. **79** (1964), 473–488.
5. C. C. Moore, *Group extensions of p -adic and adelic linear groups*, (to appear).
6. J.-P. Serre, *Le problème des groupes de congruence pour SL_2* , (to appear).

THE UNIVERSITY OF CHICAGO