DETECTING PRODUCTS OF ELEMENTARY MATRICES IN $GL_2(\mathbf{Z}[\sqrt{d}])$

RANDY TULER

ABSTRACT. An elementary $n \times n$ matrix over a ring R has 1 in each diagonal position and at most one additional nonzero element. Let $R = \mathbf{Z}[\sqrt{d}]$ where d is an integer less than -4 . We give an algorithm for determining whether or not a 2×2 invertible matrix over R is generated by elementary matrices. This is connected with the theory of integral binary quadratic forms.

1. Introduction. Let R be a commutative ring with identity. Denote the group of invertible $n \times n$ matrices over R by $GL_n R$. An elementary matrix in $GL_n R$ is one with 1 everywhere on the main diagonal and at most one nonzero entry off the main diagonal. Let $GE_n R$ be the subgroup of $GL_n R$ generated by the elementary matrices and the invertible diagonal matrices.

Now specialize to $R = \mathbf{Z}[\sqrt{d}]$ and $n = 2$ with $d \in \mathbf{Z}$ and $d < -4$. See [3 and 4] for the available literature on this type of group. In this case, since the units of R are ± 1 , it is easy to verify that $GE_2 R$ is generated by matrices of the forms

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \quad \begin{pmatrix} r & 1 \\ -1 & 0 \end{pmatrix}$$

where $\alpha, \beta = \pm 1$ and $r \in R$. One of the main results of [1] is

THEOREM 1. *The groups $GL_2 R$ and $GE_2 R$ are distinct.*

The purpose of this short note is to give a simple algorithm for determining whether or not a given matrix in $GL_2 R$ is actually in $GE_2 R$. As an application of this, we get a result concerning the integral equivalence of positive definite binary quadratic forms (see [2]). See [5] for related results.

2. Preliminaries. Set

$$E(r) = \begin{pmatrix} r & 1 \\ -1 & 0 \end{pmatrix}.$$

Let $|c|$ denote the length of $c \in R$.

LEMMA 1. *Any matrix*

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GE_2(R)$$

Received by the editors April 13, 1981 and, in revised form, October 19, 1982.
1980 *Mathematics Subject Classification.* Primary 20H05, 10D07, 10C02.

may be written

$$(2.1) \quad \begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix} E(a_1) \cdots E(a_k),$$

where $\gamma, \delta = \pm 1$ and $a_i \neq 0, \pm 1$ if $1 < i < k$.

PROOF. By definition, M is a product of matrices $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ and $E(r)^{\pm 1}$. The relations

$$E(r) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} E(-r) \quad \text{and} \quad E(r)^{-1} = E(0)E(-r)E(0)$$

imply that M may be written in the form

$$(2.2) \quad \begin{pmatrix} \varepsilon & 0 \\ 0 & \rho \end{pmatrix} E(b_1) \cdots E(b_l).$$

If $b_i = 0$ for some i with $1 < i < l$, use the relation

$$E(b_{i-1})E(0)E(b_{i+1}) = -E(b_{i-1} + b_{i+1})$$

to shorten (2.2). If $b_i = \pm 1$ for some i with $1 < i < l$, use the relation

$$E(b_{i-1})E(\pm 1)E(b_{i+1}) = \pm E(b_{i-1} \mp 1)E(b_{i+1} \mp 1)$$

to shorten (2.2). Continue shortening until the form (2.1) is reached. This proves the lemma.

Referring to the standard form (2.1), we have

LEMMA 2. If $a_k \neq 0, \pm 1$ and at least one of A, B is not a rational integer, then $|A| > |B|$.

PROOF. Denote the matrix product

$$\begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix} E(a_1) \cdots E(a_i), \quad 1 \leq i \leq k,$$

by

$$\begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix}.$$

By assumption, $a_i \neq 0, \pm 1$ for $i > 1$. Since $d < -4$, this implies $|a_i| \geq 2$ for $i > 1$ with strict inequality if $a_i \notin \mathbf{Z}$. We have

$$A_{i+1} = a_{i+1}A_i - B_i \quad \text{and} \quad B_{i+1} = A_i$$

for $1 \leq i \leq k-1$. If $|A_i| \geq |B_i|$ for some i , then

$$|A_{i+1}| = |a_{i+1}A_i - B_i| \geq |a_{i+1}| ||A_i| - |B_i|| \geq 2|A_i| - |B_i| \geq |A_i| = |B_{i+1}|.$$

Furthermore, if $|A_i| > |B_i|$, then $|A_{i+1}| > |B_{i+1}|$. Checking that $|A_1| \geq |B_1|$ if $a_1 \neq 0$, and $|A_2| > |B_2|$ if $a_1 = 0$, we have $|A_i| \geq |B_i|$ for each $i \geq 1$ or $i \geq 2$, respectively. Since at least one of A and B is not a rational integer, there is some i with $a_i \notin \mathbf{Z}$ and, consequently, $|a_i| > 2$. For this i , $|A_i| > |B_i|$ and, therefore, $|A| = |A_{ik}| > |B_k| = |B|$.

We are now in a position to show

THEOREM 2. Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{GE}_2(R)$. Then there are $t, s \in R$ so that either

$$(1) \quad A = tb + s \quad \text{with} \quad |s| < |B|$$

or

$$(2) \quad A = tB + s \quad \text{with } B, s \in \mathbf{Z}.$$

PROOF. Write M in the standard form (2.1) and consider

$$\begin{aligned} ME(a_k)^{-1} &= \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & a_k \end{pmatrix} \\ &= \begin{pmatrix} B & a_k B - A \\ * & * \end{pmatrix} = \begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix} E(a_1) \cdots E(a_{k-1}). \end{aligned}$$

By Lemma 2, either $|B| > |a_k B - A|$ or both B and $a_k B - A$ are rational integers. Take $t = a_k$ and $s = A - tB$. This proves the theorem.

It is now clear that $\text{GL}_2 R = \text{GE}_2 R$ if and only if R is a Euclidean ring with the standard norm. Since this is not the case for $R = \mathbf{Z}[\sqrt{d}]$, $d < -4$, we have Theorem 1.

3. The algorithm. We wish to determine whether or not

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{GL}_2(R)$$

is in $\text{GE}_2(R)$. If $A, B \in \mathbf{Z}$, then $M \in \text{GE}_2(R)$. Otherwise, apply Theorem 2 to the pair (A, B) . If s does not exist, then $M \notin \text{GE}_2(R)$. If s does exist, then we first observe that (B, s) is the first row of an element of $\text{GE}_2(R)$ if and only if $M \in \text{GE}_2(R)$. Consequently, if $B, s \in \mathbf{Z}$, then $M \in \text{GE}_2(R)$. Otherwise we may reapply Theorem 2 to the pair (B, s) . Continuing in this way, we find that the matrix M is in $\text{GE}_2(R)$ if and only if a pair with rational integer entries is obtained after a finite iteration of this procedure. Furthermore, it is clear that the number of iterations required is no larger than $|B|$.

A specific choice for s , if s exists, is the element $s_0 \in R$ of minimal norm which satisfies $A = tB + s_0$ for some $t \in R$. We find s_0 as follows: Write $A\bar{B} = K + L\sqrt{d}$. Let $M \equiv K \pmod{B\bar{B}}$ and $N \equiv L \pmod{B\bar{B}}$ with $|M| \leq \frac{1}{2}B\bar{B}$, $|N| \leq \frac{1}{2}B\bar{B}$. Then

$$s_0 = (M + N\sqrt{d})/\bar{B}.$$

EXAMPLE 1. Is

$$M = \begin{pmatrix} 29 & 7 - \sqrt{-37} \\ 7 + \sqrt{-37} & 3 \end{pmatrix}$$

in $\text{GE}_2(\mathbf{Z}[\sqrt{-37}])$? Taking $A = 29$ and $B = 7 - \sqrt{-37}$, we find $s_0 = 15 + 2\sqrt{-37}$. Since $|s_0| > |B|$, $M \notin \text{GE}_2(\mathbf{Z}[\sqrt{-37}])$.

4. Binary quadratic forms. Let $\begin{pmatrix} \alpha & \gamma \\ \gamma & \beta \end{pmatrix}$ be an integral binary quadratic form of determinant $d = \det \begin{pmatrix} \alpha & \gamma \\ \gamma & \beta \end{pmatrix} > 5$. We say $\begin{pmatrix} \alpha & \gamma \\ \gamma & \beta \end{pmatrix}$ is equivalent to the principal form $\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$ if there is $U \in \text{GL}_2 \mathbf{Z}$ with

$$\begin{pmatrix} \alpha & \gamma \\ \gamma & \beta \end{pmatrix} = U \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} U^T.$$

The classical problem of determining whether or not $(\begin{smallmatrix} \alpha & \gamma \\ \gamma & \beta \end{smallmatrix})$ is equivalent to the principal form is related to the preceding material by

THEOREM 3. *If $(\begin{smallmatrix} \alpha & \gamma \\ \gamma & \beta \end{smallmatrix})$ is equivalent to $(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix})$, then the matrix*

$$\begin{pmatrix} \alpha & \gamma - \sqrt{1-d} \\ \gamma + \sqrt{1-d} & \beta \end{pmatrix} \in \text{GL}_2(\mathbf{Z}[\sqrt{1-d}])$$

is in $\text{GE}_2(\mathbf{Z}[\sqrt{1-d}])$.

PROOF. If there is equivalence, then the following matrix equation holds over $\text{GL}_2(\mathbf{Z}[\sqrt{1-d}])$:

$$\begin{pmatrix} \alpha & \gamma - \sqrt{1-d} \\ \gamma + \sqrt{1-d} & \beta \end{pmatrix} = U \begin{pmatrix} d & -\sqrt{1-d} \\ \sqrt{1-d} & 1 \end{pmatrix} U^T.$$

Since U , U^T , and

$$\begin{pmatrix} d & -\sqrt{1-d} \\ \sqrt{1-d} & 1 \end{pmatrix}$$

are in $\text{GE}_2(\mathbf{Z}[\sqrt{1-d}])$, the theorem follows.

EXAMPLE 2. The example in the preceding section, along with Theorem 2, shows that the forms $(\begin{smallmatrix} 29 & 7 \\ 7 & 3 \end{smallmatrix})$ and $(\begin{smallmatrix} 38 & 0 \\ 0 & 1 \end{smallmatrix})$ are inequivalent.

As an immediate consequence of Theorems 2 and 3 we have

THEOREM 4. *Let ρ be the absolute least remainder of $\gamma \pmod{\alpha}$. Then if $|\alpha| > 1$ and $\alpha^2 \leq \rho^2 + d - 1$, the form $(\begin{smallmatrix} \alpha & \gamma \\ \gamma & \beta \end{smallmatrix})$ is not equivalent to the principal form.*

PROOF. Apply the algorithm to the pair $(\alpha, \gamma - \sqrt{1-d})$.

This result should also follow from the reduction theory for positive definite integral binary quadratic forms. We also remark that, using Theorem 2, it is not hard to prove the converse of Theorem 3.

REFERENCES

1. P. M. Cohn, *On the structure of GL_2 of a ring*, Inst. Hautes Études Sci. Publ. Math. **30** (1966), 5–53.
2. B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Math. Mono. no. 10, 1950.
3. R. Riley, *Applications of a computer implementation of Poincaré's theorem on fundamental polyhedra*, Math. Comp. (to appear).
4. R. G. Swan, *Generators and relations for certain special linear groups*, Adv. in Math. **6** (1971), 1–77.
5. R. Tuler, *Subgroups of $\text{SL}_2\mathbf{Z}$ generated by elementary matrices*, Proc. Roy. Soc. Edinburgh Sect. A **88A** (1981).

DEPARTMENT OF MATHEMATICAL SCIENCES, STATE UNIVERSITY OF NEW YORK, BINGHAMTON, NEW YORK 13901

Current address: Department of Statistics and Computer Science, University of Georgia, Athens, Georgia 30602