CONJUGACY SEPARABILITY OF GROUPS
OF INTEGER MATRICES

PETER F. STEBE

Abstract. An element $g$ of a group $G$ is conjugacy distinguished if and only if given any element $h$ of $G$ either $g$ is conjugate to $h$ or there is a homomorphism $\xi$ of $G$ onto a finite group such that $\xi(g)$ is not conjugate to $\xi(h)$. Following A. W. Mostowski, a group is conjugacy separable if every one of its elements is conjugacy distinguished. Let $GL(n, Z)$ be the group of $n \times n$ integer matrices with determinant \pm 1. Let $SL(n, Z)$ be the subgroup of $GL(n, Z)$ consisting of matrices with determinant $+1$. It is shown that $GL(n, Z)$ and $SL(n, Z)$ are conjugacy separable if and only if $n=1$ or 2. The groups $SL(n, Z)$ are also called unimodular groups. Let $GL(n, Z_p)$ be the group of invertible $p$-adic integer matrices and $SL(n, Z_p)$ be the group of $p$-adic integer matrices with determinant 1. It is shown that $GL(n, Z_p)$ and $SL(n, Z_p)$ are conjugacy separable for all $n$ and all $p$.

1. Introduction. A. W. Mostowski [4] defined conjugacy separable groups (see the abstract to this paper) and showed that the conjugacy problem is solvable in finitely presented conjugacy separable groups. It has been shown [6] that the free products of conjugacy separable groups are conjugacy separable and the elements of infinite order in a finite extension of a free group are conjugacy distinguished.

According to H. S. M. Coxeter and W. O. J. Moser [2, p. 85], the group $GL(2, Z)$ has the presentation $(x, y, z; x^2=y^2=z^2=1, (xy)^3=(xz)^2, (xz)^4=1)$. Clearly $GL(2, Z)$ is the free product of the groups $G_1=(x, y; x^2=y^2=1, (xy)^3=1)$ and $G_2=(v, z; v^2=z^2=1, (vz)^4=1)$ with amalgamating relations $x=v$ and $(vz)^2=(xy)^3$. Thus an abelian subgroup of order 4 is amalgamated. The group $SL(2, Z)$ is a subgroup of index 2 in $GL(2, Z)$ and has the presentation $(x, y; x^2=y^2, x^4=1)$. These presentations will be used to show that $GL(2, Z)$ and $SL(2, Z)$ are conjugacy separable.

2. Conjugacy separability of $GL(2, Z)$ and $SL(2, Z)$.

Theorem 1. The group $GL(2, Z)$ is conjugacy separable.
Proof. By the remarks in the Introduction, there is a free group $F$ such that $[\text{SL}(2, \mathbb{Z}); F] < \infty$ and $[\text{GL}(2, \mathbb{Z}); \text{SL}(2, \mathbb{Z})] < \infty$. Thus $[\text{GL}(2, \mathbb{Z}); F] < \infty$. According to [6, Theorem 2], every element of infinite order in $\text{GL}(2, \mathbb{Z})$ is conjugacy distinguished in $\text{GL}(2, \mathbb{Z})$. It follows from [3, Corollary 4.9.1] that the elements of finite order in $\text{GL}(2, \mathbb{Z})$ are conjugate to elements of the factors $G_1$ and $G_2$ described in the Introduction. Thus, to show that $\text{GL}(2, \mathbb{Z})$ is conjugacy separable we need only show that the conjugates of elements of $G_1$ and $G_2$ are conjugacy distinguished. Let $g$ be an element of $\text{GL}(2, \mathbb{Z})$ conjugate to an element of $G_1$ or $G_2$. Let $h$ be any element of $\text{GL}(2, \mathbb{Z})$ not conjugate to $g$. If $h$ has infinite order in $\text{GL}(2, \mathbb{Z})$, $h$ is conjugacy distinguished in $\text{GL}(2, \mathbb{Z})$ so there is a homomorphism $\xi$ of $\text{GL}(2, \mathbb{Z})$ onto a finite group such that $\xi(g)$ is not conjugate to $\xi(h)$ in $\xi(\text{GL}(2, \mathbb{Z}))$. Thus we need only consider $h$ of finite order in $\text{GL}(2, \mathbb{Z})$ and hence $h$ conjugate to an element of $G_1$ or $G_2$. Clearly, to show that there is a homomorphism $\xi$ of $\text{GL}(2, \mathbb{Z})$ onto a finite group such that $\xi(g)$ is not conjugate to $\xi(h)$ in $\text{GL}(2, \mathbb{Z})$ we can replace $g$ and $h$ by their conjugates in $G_1$ or $G_2$, and by representatives of their conjugacy classes in these subgroups. The elements 1, $x$, $y$, $xy$, $(xy)^2$ and $(xy)^3$ are a complete set of conjugacy class representatives for the subgroup $G_1$. Note that the defining relation $(xy)^2=(xz)^2$ implies that $yx^2y=xz$. Since $x$, $y$ and $z$ are of order 2, $x$ is conjugate to $y$ in $\text{GL}(2, \mathbb{Z})$. Also, the elements 1, $v$, $z$, $vz$ and $(vz)^2$ are a complete set of conjugacy class representatives for the subgroup $G_2$. Using the identifications $x=v$ and $(vz)^2=(xy)^3$ we conclude that every element of finite order in $\text{GL}(2, \mathbb{Z})$ is conjugate to one of the elements of the set $\{1, x, z, (xz)^2, xy, (xy)^3\}$. The orders of those elements are, respectively $\{1, 2, 2, 4, 2, 6, 3\}$.

If $\eta$ is a finite representation of $\text{GL}(2, \mathbb{Z})$ faithful on the factors $G_1$ and $G_2$ of $\text{GL}(2, \mathbb{Z})$, the images of two elements of different order will not be conjugate in $\eta(\text{GL}(2, \mathbb{Z}))$. According to B. H. Neumann [5, p. 532], such a representation exists. Thus we need only consider $g$ and $h$ conjugate to different elements of the set $(x, z, (xz)^2)$. Let $\xi$ be the representation of $\text{GL}(2, \mathbb{Z})$ induced by imposing the relation $y=x$. The image of $\text{GL}(2, \mathbb{Z})$ is generated by $u=\eta(x)$, $w=\eta(z)$ with relations $u^2=w^2=((uw)^2=1$. Clearly $\eta(x)\not\sim \eta(z)$, $\eta(x)\not\sim \eta((xz)^2)=1$ and $\eta(z)\not\sim \eta((xz)^3)=1$.\n
Theorem 2. The group $\text{SL}(2, \mathbb{Z})$ is conjugacy separable.

Proof. Since $\text{SL}(2, \mathbb{Z})$ has the presentation $(x, y; x^2=y^3, x^4=1)$, it is the free product of a cyclic group of order 4 and a cyclic group of order 6 with amalgamation. Every element of finite order in $\text{SL}(2, \mathbb{Z})$ is conjugate to an element of a factor of $\text{SL}(2, \mathbb{Z})$, so that an element of finite order in $\text{SL}(2, \mathbb{Z})$ is conjugate to a power of $x$ or $y$. Let $\eta$ be the homomorphism of
CONJUGACY SEPARABILITY OF GROUPS

SL(2, Z) onto the cyclic group of order 12 \((u; u^{12} = 1)\) given by \(\eta(x) = u^3, \eta(y) = u^2\). The conjugacy class representatives of the elements of finite order in SL(2, Z) are the elements \((1, x, x^2, x^3, y, y^2, y^3, y^4, y^5)\). Their \(\eta\) images are, respectively, \((1, u^2, u^4, u^6, u^8, u^3, u^5)\). Thus if \(g\) and \(h\) are any two elements of finite order in SL(2, Z), either \(g\) is conjugate to \(h\) or \(\eta(g)\) is not conjugate to \(\eta(h)\). Let \(g\) and \(h\) be any two nonconjugate elements of SL(2, Z). Since SL(2, Z) has a free subgroup of finite index, every element of infinite order in SL(2, Z) is conjugacy distinguished. Hence to prove conjugacy separability, we may assume that \(g\) and \(h\) are of finite order. Then \(\eta(g)\) is not conjugate to \(\eta(h)\), so \(g\) is conjugacy distinguished. Hence SL(2, Z) is conjugacy separable.

3. The groups GL\((n, Z)\) and SL\((n, Z)\). Let \(A\) and \(B\) be the matrices

\[
A = \begin{bmatrix} 17(11) + 1 & 25(11) \\ 11^2 & 16(11) + 1 \end{bmatrix}, \\
B = \begin{bmatrix} 17(11) + 1 & 11 \\ 25(11)^2 & 16(11) + 1 \end{bmatrix}.
\]

Example 1. The matrices \(A\) and \(B\) have the following properties:

(i) determinant \(A = \) determinant \(B = 1\);

(ii) neither \(A\) nor \(B\) has eigenvalue 1;

(iii) if \(n\) is an integer there is an integer matrix \(T_n\) such that \(T_n A \equiv B T_n \mod (n)\) and determinant \(T_n = 1\);

(iv) there is no \(2 \times 2\) integer matrix \(T\) such that \(T A = B T\) and determinant \(T = \pm 1\).

Argument. Properties (i) and (ii) follow from a simple computation. To obtain (iii) we need a lemma.

Lemma 1. Let \(T\) be a \(2 \times 2\) integer matrix. Let \(n\) be an integer. If determinant \(T \equiv 1 \mod n\) there is an integer matrix \(U\) such that determinant \(U = 1\) and \(U \equiv T \mod n\).

Proof. Let \(T = (t_{ij}), i = 1, 2, j = 1, 2\). Let \(d\) be the greatest common divisor of \(t_{11}\) and \(t_{12}\). Let \(t_{11} = t_{11}^* d, t_{12} = t_{12}^* d\), so that \(t_{11}^*\) and \(t_{12}^*\) are relatively prime integers. Thus there are integers \(a\) and \(b\) such that \(at_{12}^* - bt_{11}^* = 1\). Let determinant \(T = 1 + rn\). Let \(U\) be the matrix

\[
\begin{bmatrix}
t_{11} + n(a + ct_{11}) & t_{12} + n(b + ct_{12}) \\
t_{21} + n dt_{11}^* & t_{22} + n dt_{12}^*
\end{bmatrix}
\]

with \(c = bt_{21} - at_{22} - r, d = -cr\). Clearly \(U \equiv T \mod n\) and it follows from evaluation that determinant \(U = 1\).

The matrix \(U\) was suggested by Edward A. Bender.

Lemma 1 implies that (iii) is shown if we can show that for each \(n\) there
is a matrix $T_n$ such that $T_n A \equiv B T_n \mod n$ and determinant $T_n \equiv 1 \mod n$. By the Chinese Remainder Theorem, we can restrict our attention to $n$ a power of a prime $p$.

Let $V(x, y)$ be the polynomial matrix

$$\begin{bmatrix}
x & y \\
11y & 25x - y
\end{bmatrix}.$$

By a computation we obtain $V(x, y)A = BV(x, y)$. Thus, if for each prime power $p^z$ we can obtain integers $x$ and $y$ such that determinant $V(x, y) \equiv 1 \mod p^z$, we have shown (iii). Since determinant $V(x, y) = 25x^2 - xy - 11y^2$ we must solve the congruence $25x^2 - xy - 11y^2 \equiv 1 \mod p^z$. If $p \neq 5$, a solution is $y = 0$, $x$ such that $5x \equiv 1 \mod p^z$. If $p = 5$, $-11$ is a quadratic residue mod $5^z$ for all $z$. Thus for $p = 5$, a solution is $x = 0$, $y$ such that $-11y^2 \equiv 1 \mod 5^z$.

Consider now (iv). Let $T = (t_{ij})$ be an integer matrix such that $TA = BT$. These linear relations imply that $t_{12} = 25t_{11} - t_{22}$ and $t_{21} = 11t_{12}$. The determinant of $T$ is $\pm 1$ if and only if $25t_{11} - t_{12} - 11t_{12} = \pm 1$, which is equivalent to $25t_{11} - t_{12} - 11t_{12} = \pm 1$. Thus to show (iv) we will show that the equations $25x^2 - xy - 11y^2 = \pm 1$ have no integral solution. Now $25x^2 - xy - 11y^2 = -1$ has no integral solution for it is unsolvable modulo 3. Thus we consider only $25x^2 - xy - 11y^2 = 1$. Note that if $x$ and $y$ satisfy the equation, $y$ is relatively prime to 5.

Applying the quadratic formula, $(x, y)$ is an integral solution only if $1101y^2 + 100$ is a perfect square. We will show that all solutions $(u, y)$ of the Pell equation $u^2 = 1101y^2 + 100$ have the property that $y$ is a multiple of 5, and hence $25x^2 - xy - 11y^2 = 1$ has no integral solution.

First we obtain the minimal positive solution of $r^2 = 1101s^2 + 1$. We expand $(1101)^{1/2}$ into a continued fraction of the form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

and obtain $a_0 = 33$, $a_1 = 5$, $a_2 = 1$, $a_3 = 16$, $a_4 = 22$, $a_5 = 16$, $a_6 = 1$, $a_7 = 5$, $a_8 = 66$, $a_{n+10} = a_n$ for $n > 0$. From these values it follows that the convergents $P/Q_i$ to $(1101)^{1/2}$ are given by the table below.

If $(u, y)$ is a solution to the equation $u^2 = 1101y^2 + 1$, $u^2 - 1$ is divisible by 1101 = 3(367). Hence $P_9 = 24313015$ is the least possible candidate for a solution. We have

$$P_9 + 1 = 24313016 = 367(8)(8281) = 367(8)(91)^2,$$
$$P_9 - 1 = 24313014 = 6(4052169) = 6(2013)^2,$$


\[
\begin{array}{cccc}
 i & Q_i = a_iQ_{i-1} + Q_{i-2} & P_i = a_iP_{i-1} + P_{i-2} & P_i \mod 367 & P_i \mod 3 \\
0 & 1 & 33 & 33 & 0 \\
1 & 5 & 166 & 166 & 1 \\
2 & 6 & 199 & 199 & 1 \\
3 & 11 & 365 & -2 & -1 \\
4 & 182 & 6039 & 167 & 0 \\
5 & 4015 & 133223 & 2 & -1 \\
6 & 64422 & 2137607 & 199 & -1 \\
7 & 68437 & 2270830 & 201 & 1 \\
8 & 132859 & 4408437 & 33 & 0 \\
9 & 732732 & 24313015 & -1 & 1 \\
\end{array}
\]

so that

\[
\]

and \((P_9, Q_9)\) is the minimum positive solution to \(u^2 = 1101y^2 + 1\).

Let \(a = P_9 + (1101)^{1/2}Q_9\). If \((u_1, y_1)\) is a particular solution to \(u^2 = 1101y^2 + 100\), every \((x, y)\) satisfying \(x + y(1101)^{1/2} = (u_1 + (1101)^{1/2}y_1)a^n\) is also a solution, and this formula yields a class of solutions containing \((u_1, y_1)\). If we set \(b = a/(a - 1)\), it is well known that there is a representative \((u_1, y_1)\) of each class satisfying

\[
0 \leq u_1 \leq \left(\frac{bP_9 + 100}{2}\right)^{1/2}.
\]

We compute \(0 \leq u_1 \leq 34866\). Since \(0 \leq y_1 < u_1/33\) we have \(0 \leq y_1 \leq 1057\).

Using a computer to test all values of \(y\) in this range, we find only the two solutions \(y_1 = 0, u_1 = 10\) and \(y_1 = 55, u_1 = 1825\). Thus there are just two classes of solutions, and if \(u, y\) is any solution to \(u^2 = 1101y^2 + 100\), then \(5\) divides \(y\). Thus the equation \(25x^2 - xy - 11y^2 = 1\) has no integral solution.

**Example 2.** Let \(k\) be an integer greater than 2. There are two \(k \times k\) integer matrices \(A_k\) and \(B_k\) with determinant \(+1\) such that:

(i) For each integer \(n\) there is an integer matrix \(T_{n,k}\) with determinant \(+1\) such that \(T_{n,k}A_k \equiv B_k T_{n,k} \mod n\).

(ii) There is no integer matrix \(T\) such that \(T A_k = B_k T\) and determinant \(T = \pm 1\).

Let \(I\) be the \((k-2) \times (k-2)\) identity matrix \(0_1\) the \((k-2) \times 2\) zero matrix and \(0_2\) the \(2 \times (k-2)\) zero matrix. Let \(A\) and \(B\) be as in Example 1. For \(k > 2\) let

\[
A_k = \begin{bmatrix} I & 0_1 \\ 0_2 & A \end{bmatrix}, \quad B_k = \begin{bmatrix} I & 0_1 \\ 0_2 & B \end{bmatrix}.
\]
To show (i), let

$$T_{n,k} = \begin{bmatrix} I & 0_1 \\ 0_2 & T_n \end{bmatrix}$$

where $T_n$ is a matrix satisfying Example 1, (iii).

Consider now (ii). If (ii) is false, there is an integer matrix $T$ with determinant $\pm 1$ such that $TA_k = B_kT$. Let $T = \begin{bmatrix} R & S \\ U & V \end{bmatrix}$ where $R$ is $(k-2) \times (k-2)$, $S$ is $(k-2) \times 2$, $U$ is $2 \times (k-2)$ and $V$ is $2 \times 2$. Using block multiplication of matrices, $TA_k = B_kT$ implies

$$\begin{bmatrix} R & SA \\ U & VA \end{bmatrix} = \begin{bmatrix} R & S \\ BU & BV \end{bmatrix}.$$ 

Thus $SA = S$ and $U = BU$. Since neither $A$ nor $B$ has eigenvalue 1, $S = 0_1$ and $U = 0_2$. Then determinant $V$ is a factor of determinant $T$ so determinant $V$ is $\pm 1$ and $VA = BV$. By Example 1, (iv), $V$ and hence $T$ cannot exist.

**Theorem 3.** The group $GL(k, Z)$ and $SL(k, Z)$ are conjugacy separable if and only if $k=1$ or 2.

**Proof.** We have seen in Theorems 1 and 2 that $GL(2, Z)$ and $SL(2, Z)$ are conjugacy separable. The groups $GL(1, Z)$ and $SL(1, Z)$ are finite.

Now suppose $SL(k, Z)$ is conjugacy separable. Since $A_k$ is not conjugate to $B_k$ in $SL(k, Z)$, there is a normal subgroup $N$ of finite index in $SL(k, Z)$ such that $A_k$ is not conjugate to $B_k$ modulo $N$. For $k \geq 2$, it follows from a result of H. Bass, M. Lazard and J.-P. Serre [1], that $N$ contains a congruence subgroup. Thus there is an integer $n$ such that $TA_k \not\equiv B_kT \mod n$ for all integer matrices $T$ with determinant $\pm 1$. But this contradicts Example 2, (ii). Thus $SL(k, Z)$ is not conjugacy separable for $k>2$. Since $SL(k, Z)$ is of index 2 in $GL(k, Z)$, the result quoted from [1] also applies in $GL(k, Z)$. But then the same argument shows that $GL(k, Z)$ is not conjugacy separable for $k>2$.

4. **The groups $GL(n, Z_p)$ and $SL(n, Z_p)$**. Now let $Z_p$ be the ring of $p$-adic integers. For each $m$ there is a naturally defined ring homomorphism $\xi_{p,m}$ from $Z_p$ onto the ring $I_{p,m}$ of integers modulo $p^m$. If $A$ is a $p$-adic integer matrix, let $A_m = \xi_{p,m}(A)$.

Now let $A$ and $B$ be elements of $GL(n, Z_p)$ such that for all $m$, $A_m$ is conjugate to $B_m$ in $I_{p,m}$. Thus for each $m$ we have an integer matrix $T_m$ such that $T_mA_m \equiv B_mT_m \mod p^m$ and det $T_m \equiv 0 \mod p^m$. Thus if $X = (x_{i,j})$ is an $n \times n$ matrix of indeterminates, the equations $XA_m \equiv B_mX$, det $X+y^p - k \equiv 0$, $ke(1, \ldots, p-1)$, are solvable mod $p^m$ for $X$ and $y$. Since a solution mod $p^m$ yields a solution mod $p^{m-1}$ and there are but finitely many values of $k$, it follows that there is a single value of $k$ such that $XA_m \equiv B_mX$, det $X+y^p - k \equiv 0$, fixed $k$, are solvable mod $p^m$ for all $m$. It now follows by
standard methods that there is a $p$-adic integer matrix $T$ such that $TA = BT$ and $\xi_{p,1} \det T = k \neq 0$. But then $T$ is invertible and $A \sim B$ in $\text{GL}(n, \mathbb{Z}_p)$. Thus $\text{GL}(n, \mathbb{Z}_p)$ is conjugacy separable.

If $A$ and $B$ are elements of $\text{SL}(n, \mathbb{Z}_p)$ and we replace $yp + k$ by $-1$ in the above argument, we obtain that $\text{SL}(n, \mathbb{Z}_p)$ is conjugacy separable. We have proved Theorem 4.

**Theorem 4.** The groups $\text{SL}(n, \mathbb{Z}_p)$ and $\text{GL}(n, \mathbb{Z}_p)$ are conjugacy separable for all $n$ and primes $p$.

Note that Theorem 4 does not itself imply that the conjugacy problem is solvable in $\text{SL}(n, \mathbb{Z}_p)$ and $\text{GL}(n, \mathbb{Z}_p)$.

**References**


