EXPRESSING UNIPOTENT MATRICES OVER RINGS AS PRODUCTS OF INVOLUTIONS

Thomas J. Laffey

Let R be a ring with 1 and let $M_n(R)$ be the ring of $n \times n$ matrices with entries in R. An element $A \in M_n(R)$ is called *unipotent* if it is of the form $I_n + N$ where I_n is the identity $n \times n$ matrix and N is either strictly upper triangular or strictly lower triangular. An element $J \in M_n(R)$ is called an *involution* if $J^2 = I_n$. In this note we prove:

Theorem 1 *Let R be a ring and n a positive integer. Then every unipotent element A in $M_n(R)$ is the product of ten involutions.*

Proof: We can assume A is upper triangular, say

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & 1 & a_{23} & \cdots & a_{2n} \\ \vdots & \ddots & & & \\ 0 & \cdots & 0 & 1 & a_{n-1\,n} \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

Write $A = HK$ where

$$H = \begin{pmatrix} 1 & a_{12} & a_{12}a_{23} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & a_{23} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & a_{34} & a_{34}a_{45} & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & a_{45} & 0 & \cdots & 0 \\ \vdots & & & & \ddots & & & \\ \vdots & & & & & \ddots & & \\ 0 & & & & & & 1 & a_{n-1\,n} \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

For j odd, row j of H is of the form

$$(0, 0, \ldots, 0, 1, a_{j\,j+1}, a_{j+1\,j+2}, \ldots, 0)$$

while for j even, it has the form

$$(0, 0, \ldots, 1, a_{j\,j+1}, 0, \ldots, 0).$$

Note that $K = H^{-1}A$ has the form

$$K = \begin{pmatrix} 1 & 0 & k_{13} & \cdots & \cdots & k_{1n} \\ 0 & 1 & 0 & k_{24} & \cdots & k_{2n} \\ & & \ddots & & & \vdots \\ & & & \ddots & & k_{n-2\,n} \\ & & & & \ddots & 0 \\ 0 & 0 & & & 0 & 1 \end{pmatrix}$$

Note that H is expressible as product $H = H_1 H_2$, where

$$H_1 = \begin{pmatrix} 1 & a_{12} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & a_{34} & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & a_{56} & \cdots & 0 \\ \vdots & & & & & \ddots & & \vdots \\ \vdots & & & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix},$$

and

$$H_2 = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & a_{34} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & a_{45} & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & & \ddots & & \vdots \\ \vdots & & & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

Using the factorization

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\alpha \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

where the two matrices on the right are involutions, we see that H is the product of four involutions.

Note that

$$K = JL$$

where J is the full Jordan block

$$\begin{pmatrix} 1 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & \cdots & 0 \\ & & \ddots & \ddots & & & \vdots \\ & & & \ddots & \ddots & & \vdots \\ & & & & \ddots & \ddots & 0 \\ & & & & & 1 & 1 \\ 0 & 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

and L is of the form

$$\begin{pmatrix} 1 & -1 & l_{13} & \cdots & \cdots & \cdots & l_{1n} \\ 0 & 1 & -1 & l_{24} & \cdots & \cdots & l_{2n} \\ & & \ddots & \ddots & & & \vdots \\ & & & \ddots & \ddots & & \vdots \\ & & & & \ddots & \ddots & 0 \\ & & & & & 1 & -1 \\ 0 & 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

If D is the diagonal matrix $\operatorname{diag}\left(1, -1, 1, -1, \ldots, (-1)^{n-1}\right)$ then we define the matrix L_0 by

$$L_0 = D^{-1}LD = \begin{pmatrix} 1 & 1 & l_{13} & -l_{14} & \cdots & \cdots \\ 0 & 1 & 1 & l_{24} & \cdots & \vdots \\ \vdots & & \ddots & & & \vdots \\ \vdots & & & \ddots & & l_{n-2\,n} \\ 0 & & & 0 & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

By a result of Dennis and Vaserstein, L_0 is similar to J via an element T of $GL(n,R)$. In fact, just take T to be a unipotent upper-triangular matrix and observe that the linear system

$$TL_0 = JT$$

is solvable inductively over every ring. (See [2], proof of Lemma 13.)

The desired result then follows from our next result.

Proposition *The full unipotent Jordan block J is the product of three involutions.*

Proof: Let C be the companion matrix of $(x-1)^n$, so

$$C = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & \cdots & 0 \\ & & & \ddots & & & \vdots \\ & & & & \ddots & & \vdots \\ & & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \\ (-1)^{n-1} & \cdots & \cdots & \cdots & \binom{n}{3} & -\binom{n}{2} & n \end{pmatrix}$$

Put

$$\begin{aligned} v_1 &= (0,0,\ldots,0,1)^T, \\ v_2 &= Cv_1 - v_1 = (0,0,\ldots,0,1,n-1)^T, \\ v_3 &= Cv_2 - v_2 = (0,0,\ldots,0,1,n-2,\binom{n-1}{2})^T, \\ v_4 &= Cv_3 - v_3 = (0,0,\ldots,0,1,n-3,\binom{n-2}{2},\binom{n-1}{3})^T, \\ \vdots \quad & \quad \vdots \\ v_n &= Cv_{n-1} - v_{n-1} = (1,1,\ldots,1)^T, \end{aligned}$$

and let $Q = (v_1\, v_2\, \cdots\, v_n)$. Then $\det Q = (-1)^{\binom{n}{2}}$ and $CQ = QJ$.

So J is similar to C over R.

But C is expressible as the product $C = C_1C_2$, where

$$C_1 = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ \vdots & & & \ddots & & & \vdots \\ \vdots & & & & \ddots & & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 1 & 0 \\ & \cdots & \cdots & \binom{n}{3} & -\binom{n}{2} & n & -1 \end{pmatrix}$$

and

$$C_2 = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & & & 0 \\ \vdots & & & & \ddots & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \\ (-1)^n & 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix}.$$

Now C_1 is an involution and C_2 is the product of two involutions (when n is even, this follows from the fact that every permutation is the product of two involutions and for n odd, we use a slight modification of this argument). See [3] for this factorization of a companion matrix.

Hence C and therefore J is the product of three involutions. ∎

A well-known result of Gustafson, Halmos and Radjavi, [3], states that if F is a field and $A \in M_n(F)$ is such that $\det A = \pm 1$, then A is the product of four involutions in $GL(n, F)$, but in general not the product of fewer than four. A number of results on matrices A which are the product of three involutions is presented by Liu, [5].

Ishibashi [4] has obtained a version of the Gustafson-Halmos-Radjavi result for integer matrices. He proves that if $n > 2$ and $A \in GL(n, \mathbf{Z})$, then A is the product of $3n + 9$ involutions in $GL(n, \mathbf{Z})$.

It can be deduced from Bass, [1], that if $n \geq 3$ and $A \in GL(n, \mathbf{Z})$, then

$$A = U_1 L_1 U_2 L_2 \begin{pmatrix} S & 0 \\ 0 & I_{n-2} \end{pmatrix}$$

where U_1, U_2 are unipotent upper-triangular and L_1, L_2 are unipotent lower-triangular integer matrices and $S \in GL(2, \mathbf{Z})$ (see also [2], Lemma 9). Since

$$U_1 L_1 U_2 L_2 = (U_1 L_1 U_1^{-1})(U_1 U_2) L_2$$

and $U_1 U_2$ is unipotent upper-triangular, we deduce from the theorem that $U_1 L_1 U_2 L_2$ is the product of 30 involutions and applying Ishibashi's result in the case $n = 3$, we deduce that A is the product of 48 involutions. Using Bass's result, Dennis and Vaserstein, [2], show that for n sufficiently large (one can check that $n \geq 82$ will do), every $A \in SL(n, \mathbf{Z})$ can be written as a product $U_1 L_1 U_2 L_2 U_3 L_3$ where U_1, U_2, U_3 are unipotent upper-triangular and L_1, L_2, L_3 unipotent lower-triangular integer matrices. Note that

$$U_1 L_1\, U_2 L_2\, U_3 L_3 = (U_1 L_1 U_1^{-1})((U_1 U_2) L_2 (U_1 U_2)^{-1})(U_1 U_2 U_3) L_3$$

Using this and the fact that if $\det A = -1$ and

$$D := \mathrm{diag}(-1, 1, 1, \ldots, 1)$$

then D is an involution and $AD \in SL(n, \mathbf{Z})$, Theorem 1 yields:

Theorem 2 *Every $A \in GL(n, \mathbf{Z})$ ($n \geq 3$) can be written as a product of 48 (or fewer) involutions in $GL(n, \mathbf{Z})$. For $n \geq 82$, this number can be reduced to 41.*

Remark (i) It would be interesting to get best possible bounds. (ii) Ishibashi, [4], shows that for elements in $GL(2, \mathbf{Z})$, no such bound is possible.

References

[1] H. Bass, *K-theory and stable algebra*, Publ. Math. IHES. **22** (1964), 5-60.

[2] R. K. Dennis and L. N. Vaserstein, *On a question of M. Newman on the number of commutators*, J. Algebra **118** (1988), 150-161.

[3] W. H. Gustafson, P. R. Halmos and H. Radjavi, *Products of involutions*, Collection of articles dedicated to Olga Taussky Todd. Linear Algebra Appl. **13** (1976), 157-162.

[4] H. Ishibashi, *Involutory expressions of elements in $GL_n(Z)$ and $SL_n(Z)$*, Linear Algebra Appl. **219** (1995), 165-177.

[5] Kang-Man Liu, *Decomposition of matrices into three involutions*, Linear Algebra Appl. **111** (1988), 1-24.

Thomas J. Laffey
Department of Mathematics,
University College Dublin,
Belfield,
Dublin 4,
Ireland.