A PAIR OF GENERATORS FOR THE UNIMODULAR GROUP

Stanton M. Trott

(received June 4, 1962)

It is well known that $\mathfrak{M}_n$, the multiplicative group consisting of n-rowed square matrices with integer entries and determinant equal to ± 1 can be generated by:

$$U_1 = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix} \qquad U_2 = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 1 & 0 & \ldots & 0 & 0 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

$$U_3 = \begin{pmatrix} -1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix} \qquad U_4 = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

It is also known that U_4 can be generated by U_1, U_2, and U_3 (cf. [2] p. 85).

However, by a construction which is much simpler than the one just mentioned for U_4, it is possible to generate U_3 by just U_2 and U_4. Since U_2 and U_4 affect only the first

Canad. Math. Bull. vol. 5, no. 3, September 1962.

https://doi.org/10.4153/CMB-1962-024-x Published online by Cambridge University Press

two rows and columns of any matrix which they multiply, we need discuss only the case $n = 2$. U_3 can be obtained from U_2 by taking the following steps in sequence:

1. subtract column 1 from column 2
2. add column 2 to column 1
3. interchange columns 1 and 2.

Steps 2 and 3 can be effected by right multiplication by U_2 and U_4 respectively. Step 1 can be effected by right multiplication by $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$; this matrix is obtainable from U_2^{-1} by interchanging its rows and its columns, i. e. by right and left multiplication by U_4. Combining these observations, we conclude:

THEOREM 1.

$$(1) \qquad U_3 = U_2 U_4 U_2^{-1} U_4 U_2 U_4 .$$

The correctness of this equation can be verified by direct computation.

Hence $\mathfrak{M}_n$ can be generated by U_1, U_2, and U_4.

When $n = 2$, U_1 is the same as U_4, and in this case the group is generated by just two elements, U_1 and U_2. It has been shown by D. Beldin [1] that $\mathfrak{M}_n$ is a 2-generator group even when $n > 2$, but can $\mathfrak{M}_n$ be generated by just two of U_1, U_2, U_3, and U_4? If it can be, U_1 and U_2 will certainly be required, for any product of U_2, U_3, and U_4 affects only the first two rows and the first two columns, while any product of U_1, U_3, and U_4 has exactly n non-zero entries. However, when n is odd, both U_1 and U_2 have determinant equal to $+1$, and if we are to generate the whole group, at least one of our generators must have determinant equal to -1. Hence $\mathfrak{M}_n$ cannot always be generated by just U_1 and U_2.

https://doi.org/10.4153/CMB-1962-024-x Published online by Cambridge University Press

It will be shown that when n is even, $\mathfrak{M}_n$ is generated by U_1 and U_2, and that when n is odd U_1 and U_2 generate $\mathfrak{M}_n^+$, the Modular Group of n-rowed square matrices with integer entries and determinant equal to + 1 . In any case U_1 and U_2 generate the B_{ij} defined below, and these generate $\mathfrak{M}_n^+$. The principal result of this paper is that $\mathfrak{M}_n$ is generated by U_2 and

$$U = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ & & & \dots & & \\ 0 & 0 & 0 & \dots & 0 & 1 \\ (-1)^n & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

The results stated in the preceding paragraph are consequences of:

THEOREM 2. *For $i \neq j$, let B_{ij} be the unit matrix with the zero at the intersection of the i^{th} row and j^{th} column replaced by 1. Then any B_{ij} can be generated by just U and $B_{21} = U_2$.*

To prove this we need three lemmas.

Lemma 1. *If $i = 2, 3, \dots, n-1$, then* $B_{i+1\,i} = U^{-(i-1)} B_{21} U^{i-1}$; *and* $B_{1n} = U\, B_{21}^{(-1)^n} U^{-1}$.

Proof: Left multiplying any matrix by U^{i-1} cyclically permutes rows, placing the i^{th} row at the top, and (if n is odd) reversing the signs of the bottom i-1 rows of the new matrix. But since $i \leq n-1$, the top 2 rows have signs unchanged. B_{21} then adds the first row of this new matrix to the second. Finally $U^{-(i-1)}$, by cyclically permuting the

https://doi.org/10.4153/CMB-1962-024-x Published online by Cambridge University Press

rows, returns them to their original positions, changing the signs of just those rows affected by sign changes in the first step. The net effect on the unit matrix I is to add the i^{th} row of I to the $(i+1)^{th}$, and this is how $B_{i+1\,i}$ is produced. A slight modification of this argument produces the formula for B_{1n}.

Lemma 2. Let $C = B_{n\,n-1} B_{n-1\,n-2} \ldots B_{54} B_{43}$. Then $B_{12} = C B_{32}^{-1} C^{-1} B_{1n} C B_{32} C^{-1} B_{1n}^{-1}$.

Proof: Left multiplication of I by $C^{-1} B_{1n}^{-1}$ subtracts in turn the n^{th} row from the first, the $(n-1)^{th}$ row from the n^{th}, etc., stopping with subtraction of the 3^{rd} row from the 4^{th}.

$$C^{-1}B_{1n}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 & -1 \\ 0 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & -1 & 1 & \ldots & 0 & 0 \\ & & & & \ldots & & \\ 0 & 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & 0 & \ldots & -1 & 1 \end{pmatrix}$$

Left multiplication of $C^{-1} B_{1n}^{-1}$ by $B_{1n} C B_{32}$ produces by row additions the matrix

https://doi.org/10.4153/CMB-1962-024-x Published online by Cambridge University Press

$$B_{1n} C B_{32} C^{-1} B_{1n}^{-1} = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 0 \\ & & & & \dots & & \\ 0 & 1 & 0 & 0 & \dots & 1 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

The row subtractions effected by left multiplication by $B_{32}^{-1} C^{-1}$ produce the matrix

$$B_{32}^{-1} C^{-1} B_{1n} C B_{32} C^{-1} B_{1n}^{-1} = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & -1 & 1 & \dots & 0 & 0 \\ & & & & \dots & & \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & -1 & 1 \end{pmatrix}$$

Finally, the row additions effected by left multiplication by C remove the -1 entries from this matrix producing B_{12}.

We note that only $B_{i+1,i}$ $(i = 2, 3, \dots, n-1)$ and B_{1n} appear in this formula. Hence, using lemma 1 and the fact that U^n commutes with every matrix of $\mathcal{M}_n$, we obtain:

$$(2)\quad B_{12} = U(UU_2)^{n-3} U(UU_2)^{-(n-2)} U_2^{(-1)^n} (UU_2)^{n-2} U^{-1} (UU_2)^{-(n-3)} U_2^{-(-1)^n} U^{-1}.$$

https://doi.org/10.4153/CMB-1962-024-x Published online by Cambridge University Press

Lemma 3. If $i = 2, 3, \ldots, n-1$, then $B_{i\ i+1} = U^{-(i-1)} B_{12} U^{i-1}$, and $B_{n1} = U B_{12}^{(-1)^n} U^{-1}$.

The proof is similar to the proof of lemma 1.

We are now ready to prove the theorem. In the following, read the indices modulo n. By lemma 1, we know that $B_{j+1,j}$ can be generated. Let $2 \leq k \leq n-1$ and suppose that $B_{j+k-1,j}$ can be generated. It is not difficult to see that

$$B_{j+k,j} = B^{-1}_{j+k-1,j+k} B_{j+k,j+k-1} B_{j+k-1,j} B^{-1}_{j+k,j+k-1} B_{j+k-1,j+k}.$$

For the left multipliers of $B_{j+k-1,j}$ add the 1 required at $(j+k, j)$ and remove the unwanted 1 from $(j+k-1, j)$. The right multipliers then correct the unwanted changes produced by the row operations.

This induction shows that any B_{ij} can be generated by just U and U_2, as we asserted in the statement of theorem 2.

It is not hard to show that the B_{ij} generate $\mathfrak{M}^+_n$. Hence U and U_2 generate $\mathfrak{M}^+_n$, which is a subgroup of index 2 in $\mathfrak{M}_n$. U has determinant equal to -1 and hence is not in $\mathfrak{M}^+_n$. It follows that U and U_2 generate $\mathfrak{M}_n$.

Since, when n is even, $U = U_1$, we see that, in that case, $\mathfrak{M}_n$ is generated by U_1 and U_2. It can in fact be shown that U_1 and U_2 always generate the B_{ij}. To do this it is only necessary to modify slightly the statements and proofs of lemmas 1 and 3 of theorem 1. The modifications required are obvious, and the proofs are actually somewhat simpler. Thus $\mathfrak{M}^+_n$ is generated by U_1 and U_2.

It is of some interest to express U_1, U_3, and U_4 in terms of U and U_2, and to state U in terms of the others.

https://doi.org/10.4153/CMB-1962-024-x Published online by Cambridge University Press

Right multiplication by U_3 changes the sign of the first column, and $U_3{}^2 = I$. Hence $U_1 = UU_3^n$ and $U = U_1 U_3^n$.

We already have U_3 in terms of U_2 and U_4 (cf. formula (1)), so that the only remaining task is to obtain an expression for U_4 in terms of U and U_2. It is not difficult to verify that

$$U_4 = \left(\prod_{i=3}^{n} (B_{i\ i-1} B_{i-1\ i}^{-1} B_{i\ i-1}) \right) U .$$

The B_{ij} in this expression are of the forms treated in lemmas 1 and 3. Hence U_4 can be expressed in terms of B_{12}, B_{21}, and U:

$$U_4 = (U^{-1} B_{21} B_{12}^{-1} B_{21})^{n-2} U^{n-1} .$$

B_{21} is U_2, and B_{12} is given by formula (2).

What generating relations are suitable to define $\mathfrak{M}_n$ in terms of U and U_2? Coxeter and Moser, ([2] p. 85) show that the group defined by

$$R_1{}^2 = R_2{}^2 = R_3{}^2 = E, \ (R_1 R_2)^3 = (R_1 R_3)^2 = Z, \ Z^2 = E,$$

where E denotes the identity and

$$R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \quad R_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

is $\mathfrak{M}_2$.

Since

$$R_1 = U, \ R_2 = UU_2^{-1} UU_2 U, \ R_3 = U_2 UU_2^{-1} UU_2 U$$

and

https://doi.org/10.4153/CMB-1962-024-x Published online by Cambridge University Press

$$U = R_1, \quad U_2 = R_3 R_2,$$

$\mathcal{M}_2$ has the equivalent abstract definition

$$(3) \qquad U^2 = (U_2^{-1} U U_2 U)^6 = E, \quad U_2^{-1} U U_2 U U_2^{-1} = U U_2 U U_2^{-1} U U_2 U.$$

Letting $U U_2 U = W^{-1}$, (3) is more attractively written:

$$U^2 = (W U_2)^6 = U U_2 U W = E, \quad U_2 W U_2 = W U_2 W.$$

The question which naturally suggests itself is: what group is defined by the relations:

$$(4) \qquad U^{2n} = (W U_2)^6 = E, \quad U_2 W U_2 = W U_2 W,$$

where $W^{-1} = B_{12}$ and is given by formula (2)?

If U and U_2 are the n-rowed square matrices defined earlier, the period of U is n or $2n$ according as n is even or odd, so that $U^{2n} = E$. Words in U_2 and its transpose, W^{-1}, affect only the first two rows and columns of any matrix in $\mathcal{M}_n$. Hence the other relations are also valid in $\mathcal{M}_n$. It follows that $\mathcal{M}_n$ is a factor group of the group in question, but whether the relations (4) suffice to define $\mathcal{M}_n$ is unknown.

REFERENCES

1. Beldin, D. - Thesis, Reed College, 1957.

2. Coxeter, H. S. M. and Moser, W. O. J. - Generators and Relations for Discrete Groups, Springer-Verlag, 1957.

University of Toronto
and
University of Tasmania