New proof of a basic theorem about the modular group

By DAREL HARDY (Fort Collins, Colo.)
and ROBERT J. WISNER (Las Cruces, N.M.)

1. *Introduction.* Denote by Γ, as usual, the classical modular group of all linear fractional transformations

$$z \to \frac{az+b}{cz+d}$$

of the complex plane, where a, b, c, d are integers, and $ad-bc = 1$. Then Γ can also be described as the multiplicative group of all 2×2 unimodular matrices over the ring Z of integers in which

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{1}$$

and $-A$ are identified. It is well-known that Γ is the free product of a group of order 2 with a group of order 3, with perhaps the shortest and most beatiful published proof of this fact being given by KUROSH [1] (Appendix B). The proof given there does not fully use the powerful but elementary idea of dominance in matrices, however, which in the unimodular 2×2 case is natural.

It is the purpose of this note to give a very short proof of the aforementioned structure theorem about Γ, a proof based on an idea from a paper about a matrix semigroup [2].

In § 2, the main theorem of [2] is proved again as a Lemma, and in a much shorter way than was presented in [2]. Then in § 3, the new proof of the basic structure theorem of Γ is given.

2. *A lemma.* Using the notation of [2], let U_2^0 be the semigroup of Γ consisting of all elements of Γ having non-negative entries. It was proved in [2] that U_2^0 is a free semigroup on the two generators

$$L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

For completeness (and, indeed, for a new proof of this fact), we prove this fact again.

Recall that the matrix A of (1) is said to have a dominating first row if $a \geqq c$ and $b \geqq d$. A has a dominating second row if $c \geqq a$ and $d \geqq b$.

Lemma. *U_2^0 is a free semigroup on the two generators L and R.*

PROOF. To show that L and R generate U_2^0, let

$$I \neq A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_2^0$$

where I is the identity matrix. Then either $a \leqq c$ or $a > c$. If $a \leqq c$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c-a & d-b \end{pmatrix} = LX$$

for some $X \in U_2^0$. If $a > c$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a-c & b-d \\ c & d \end{pmatrix} = RX$$

for some $X \in U_2^0$. If $X = I$ in either case, we are through. Otherwise, write $X = LY$ or $X = RY$ for some $Y \in U_2^0$. Since the sum of the entries in $A, X, Y, \ldots$ decreases, this process must end, so L and R generate U_2^0. At the same time, this shows that factorization of A is unique, because at each state the factorization is determined by which row dominates.

3. *The theorem.*

Theorem. *Γ is the free product of a group of order 2 and a group of order 3.*

PROOF. Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

so that $S^2 = T^3 = I$. Let G be the subgroup of Γ generated by S and T. Then $U_2^0 \subset G$ since $ST = R$ and $ST^2 = L$. As in (1), take $A \in \Gamma$. If $a, d \geqq 0$ and $b, c \leqq 0$, then $A \in G$ since $A^{-1} \in U_2^0$. If $a, b \leqq 0$ and $c, d \geqq 0$, then $A \in G$ since $A = SB$ where

$$B = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix} \in U_2^0$$

If $a, c \geqq 0$ and $b, d \leqq 0$, then $A \in G$ since $A = CS$ where

$$C = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix} \in U_2^0$$

Thus, $G = \Gamma$.

And now Γ must be free, because the above paragraph shows that any non-unique factorization in Γ would lead to a non-unique factorization in U_2^0.

References

[1] A. G. KUROSH, The Theory of Groups, vol. 1, *New York*, 1955.
[2] B. JACOBSON and ROBERT J. WISNER, Matrix number theory, I: Factorization of 2×2 unimodular matrices, *Publ. Math. Debrecen*, **13** (1966), 67—72.

(Received July 22, 1969.)