A dominance semigroup of the modular group[1])

By DAREL HARDY[2]) (Fort Collins, Colo.)
and ROBERT J. WISNER (Las Cruces, N.M.)

1. *Introduction.* We denote by Γ the multiplicative group of all 2×2 unimodular matrices with entries from Z, the ring of integers. The set U_2^0 of all elements of Γ with nonnegative entries forms a semigroup under matrix multiplication, and it was studied in [2], the main result being that U_2^0 is free on the two generators

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

which we denote by L and R, respectively. In number-theoretic language, U_2^0 has but two primes, L and R, and factorization into primes is unique. This is in sharp contrast to the result (also in [2]) that the semigroup U_2^1 of 2×2 unimodular matrices with positive integral entries has infinitely many primes and factorization is not unique.

In this paper, we study another semigroup contained in Γ, and this semigroup, very much unlike U_2^0 and U_2^1, has unique factorization and infinitely many primes. The semigroup under consideration is suggested by the array of Farey fractions written, somewhat unusually, in decreasing order. This array is

$$\begin{array}{c} \frac{1}{1}\ \frac{0}{1} \\ \frac{1}{1}\ \frac{1}{2}\ \frac{0}{1} \\ \frac{1}{1}\ \frac{2}{3}\ \frac{1}{2}\ \frac{1}{3}\ \frac{0}{1} \\ \frac{1}{1}\ \frac{3}{4}\ \frac{2}{3}\ \frac{1}{2}\ \frac{1}{3}\ \frac{1}{4}\ \frac{0}{1} \end{array} \tag{1}$$

and so forth, each row consisting of the proper reduced fractions with denominator limited by the number of the row. It is well known that if

$$\frac{a}{b} \quad \text{and} \quad \frac{c}{d}$$

[1]) Presented to the American Mathematical Society April 9, 1966.

[2]) Supported in part by NSF Grant GP377.

are adjacent fractions in the Farey array, then $ad-bc=1$, and so the associated matrix

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

is an element of Γ.

Now let $\mathbf{F}$ be the set of all such matrices, along with the identity matrix I. Another description of $\mathbf{F}$ is: $A \in \mathbf{F}$ if and only if $A=I$ or $A \in U_2^0$ and the second row of A dominates the first. It is easy to check that $\mathbf{F}$ is a multiplicative semigroup within Γ.

In § 2, a characterization of $\mathbf{F}$ in terms of L and R is given, and this is basic to most of the remaining ideas: a description of the primes in $\mathbf{F}$ (also in § 2), a discussion of factorization (§ 2), a prime number theorem which naturally involves an ordering in $\mathbf{F}$ (§ 3), and § 4 is concerned with further results on the order itself as applied to U_2^0 and in a hereditary manner to $\mathbf{F}$.

Further results on semigroups that are related to $\mathbf{F}$ and on many other semigroups within Γ have been obtained and will be presented in a later study.

2. *Primes in* $\mathbf{F}$. Let

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathbf{F}$$

where $A \neq I$, and since $\mathbf{F} \subset U_2^0$, consider the complete factorization of A in U_2^0. Since $b \geqq a$ and $d > c$, we may write

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

as an equation in U_2^0; thus, every element in $\mathbf{F}$ has L as a left factor within U_2^0 Conversely, if $C \in U_2^0$, then LC is unimodular with the second row dominating the first, so $LC \in \mathbf{F}$. We have, then, a characterization of $\mathbf{F}$ which we state as

Lemma 1. *$A \in \mathbf{F}$ if and only if $A=I$ or A has L as a left factor in U_2^0.*

Thus, $\mathbf{F} = \{LX \mid X \in U_2^0\}$. Now suppose again that A is an arbitrary element of $\mathbf{F}$ with $A \neq I$. If $A=L$, it is surely prime since L is prime in U_2^0 (prime of course means that only trivial factorizations are possible within the semigroup in question). If $A \neq L$, then $A=LB$ for $B \in U_2^0$. Factoring A completely in U_2^0, we have

$$A = L^{n_1} R^{m_1} L^{n_2} R^{m_2} \ldots \tag{2}$$

where all exponents are uniquely determined [2]. By Lemma 1, A will fail to factor in $\mathbf{F}$ if and only if $n_1=1$ and $n_2=m_2=\cdots=0$. Thus, we have

Proposition 1. P is a prime in $\mathbf{F}$ if and only if $P=LR^m$. This means that the primes in $\mathbf{F}$ are computed as follows:

$$P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m \\ 1 & m+1 \end{pmatrix}.$$

Thus, the primes are just those matrices which are obtained by running "down the left edge" in the Farey display (1).

Proposition 2. If $A \in \mathbf{F}$, then $A = I$, A is a prime, or A factors uniquely as a product of primes. (In other words, $\mathbf{F}$ is a free semigroup on the generators $L, LR, LR^2, \dots$.)

Proof. We write in U_2^0, as in (2),

$$A = L^{n_1} R^{m_1} L^{n_2} R^{m_2} \dots \tag{3}$$

where the exponents are uniquely determined. By Proposition 1, if A is neither I nor a prime, we may factor A in $\mathbf{F}$ into primes as follows (where the product sign indicates the indicated number of prime factors):

$$A = \left(\prod_{i=1}^{n_1-1} L\right)(LR^{m_1})\left(\prod_{i=1}^{n_2-1} L\right)(LR^{m_2})\dots$$

If this factorization into primes were not unique, then the representation (3) would not be unique in U_2^0, in contradiction to the results of [2].

A question which arises in parallel with [2] is: if we look only at that subsemigroup of F where the matrix entries are positive, do we still have unique factorization? The answer is negative by a simple example. We may look at $LRLLR$. In this subsemigroup, LR, LRL, and LLR are all irreducible, and

$$\begin{aligned} LRLLR &= (LR)(LLR) \\ &= (LRL)(LR) \end{aligned}$$

gives two factorizations into irreducible factors.

Another question has to do with factorization in the semigroup $\mathbf{F} - \{P \mid P$ is prime in $F\}$. That is, what happens in the semigroup obtained by leaving off the fractions $\frac{1}{1}$ in the Farey scheme? It is easy to check that

$$\begin{aligned} LRLLLL &= (LRL)(L^3) \\ &= (LRL^2)(L^2) \end{aligned}$$

and that, in this semigroup, the elements LRL, L^3, LRL^2, L^2 are all irreducible.

3. *A prime number theorem.* Let $A = X_1 X_2 \dots X_n$ and $B = Y_1 Y_2 \dots Y_m$, where the X_i, Y_j are prime in U_2^0. We put an ordering on U_2^0 by defining $A < B$ if and only if either (i) $n < m$, or (ii) $n = m$ and for some j, $X_i = Y_i$ for $i < j$, $X_j = L$, $Y_j = R$.

Suppose $A \neq B$. Then $n < m$, $n > m$, or $n = m$ and $X_k \neq Y_k$ for some k. In any case, $A < B$ or $A > B$, so U_2^0 is fully ordered.

Let U be a nonempty subset of U_2^0 and take p to be the least integer such that $X_1 X_2 \dots X_p \in U$, where X_i is prime in U_2^0. Let $U_p = \{A \in U\colon A$ has p prime factors$\}$. Since there are only two primes, L and R, in U_2^0, U_p is a finite set, is fully ordered, hence has a least element B. Clearly, B is a least element for U, so U_2^0 is well ordered.

We now look at $\mathbf{F}$ with an ordering inherited as a subset of U_2^0. With this ordering, $\mathbf{F}$ is well ordered, with the first few elements being I, L, L^2, LR, L^3, L^2R, LRL, LR^2, L^4, etc. Let $N(A)$ be the number of elements of $\mathbf{F}$ which precede or equal A, $\pi(A)$ the number of primes which precede or equal A. We can now prove the following prime number theorem for $\mathbf{F}$.

Proposition 3. Let $A\in\mathbf{F}$ and write $N(A)=2^n+m$, where $0\leqq m<2^n$. Then $\pi(A)=n$.

PROOF. In the sequence $I, L, L^2, LR, L^3, L^2R, \ldots$, there are 2^{n-1} elements which factor in U_2^0 into exactly n prime factors, where $n=1$. Thus there are

$$1+1+2+2^2+\cdots+2^{n-1}=\frac{2^n-1}{2-1}+1=2^n$$

elements preceding the first element in the sequence having exactly $n+1$ primes in its factorization in U_2^0. Hence, if A has $n+1$ prime factors in U_2^0, then $N(A)=$ $=2^n+m$, where $0\leqq m<2^m$. For each $k=1$, there is exactly one prime with k factors in U_2^0, namely,

$$LR^{k-1}=\begin{pmatrix}1 & k-1\\ 1 & k\end{pmatrix}.$$

Thus $\pi(A)=n$.

Let P denote the set of primes of $\mathbf{F}$. The following proposition is in contrast to a well-known theorem in prime number theory.

Proposition 4. $\sum_{p\in P}\frac{1}{N(p)}<\infty$.

PROOF. $\sum_{p\in P}\frac{1}{N(p)}=\sum_{n=1}^{\infty}\frac{1}{2^n}=1.$

4. *U_2^0 and* $\mathbf{F}$ *as ordered semigroups.* The terminology in this section is as in [1]. The ordering introduced in § 3 turns out to have some nice properties which are studied here.

Proposition 5. U_2^0 and $\mathbf{F}$ admit orderings under which they are fully ordered, positively ordered, archimedian, cancellative, and well-ordered semigroups.

PROOF. Let $A=X_1X_2\ldots X_n$, $B=Y_1Y_2\ldots Y_m$, and $C=Z_1Z_2\ldots Z_p$ be elements of U_2^0 written in their prime factorizations, and suppose $A<B$.

Case 1. Suppose $n<m$. Then $n+p<m+p$ implies $AC<BC$ and $CA<CB$.

Case 2. Suppose $n=m$, and let j be the least integer such that $X_j\neq Y_j$. Then $n+p=m+p$ and $X_1\ldots X_nZ_1\ldots Z_p<Y_1\ldots Y_mZ_1\ldots Z_p$ since $X_i=Y_i$ for $i<j$ and $X_j=L$, $Y_j=R$. Also, $Z_1\ldots Z_pX_1\ldots X_n<Z_1\ldots Z_pY_1\ldots Y_m$ since $Z_i=Z_i$, $X_i=Y_i$ for $i<j$ and $X_j=L$, $Y_j=R$. Hence $A<B$ implies $AC<BC$ and $CA<CB$, as U_2^0 is a partially ordered semigroup.

Since I is the least element, $I\neq A$ implies $I<A$, which in turn implies $B<AB$ and $B<BA$; hence, $\mathbf{F}$ is positively ordered.

Suppose $A^n<B$ for all positive integers n. Assume A has p prime factors and B has q prime factors. Then if $A^{q+1}<B$, $p(q+1)\leqq q$, which means that $pq<q$. Thus $p<1$, making $p=0$; i.e., $A=I$. Hence U_2^0 is archimedian.

U_2^0 is cancellative since factorization is unique.

U_2^0 is fully ordered and well ordered from statements in § 3.

It is immediate that **F** with the ordering inherited as a subset of U_2^0 is a fully ordered, positively ordered, archimedian, well ordered semigroup. **F** is cancellative since factorization in **F** is unique.

Anomalous pairs are easy to classify in U_2^0.

Proposition 6. $A \neq I$ and $B \neq I$ form an anomalous pair if and only if A and B have the same number of prime factors.

PROOF. Suppose A and B each have $n \geqq 1$ prime factors. Then A^m has nm prime factors, B^{m+1} has $n(m+1)$ prime factors, so $A^m < B^{m+1}$. Similarly, $A^{m+1} > B^m$, so A and B form an anomalous pair.

Conversely, if A and B form an anomalous pair and A has p prime factors and B has q prime factors, then $A^m < B^{m+1}$ for all m implies $pm \leqq q(m+1)$ for all m. Thus,

$$p \leqq \lim_{m \to \infty} q \left(\frac{m+1}{m} \right) = q.$$

Similarly, $p \geqq q$, so $p = q$.

References

[1] L. FUCHS, Partially ordered algebraic systems, *Oxford, New York*, 1963.

[2] B. JACOBSON, and R. J. WISNER, Matrix number theory I: Factorization of 2×2 unimodular matrices, *Publ. Math. (Debrecen)*, (1967), 67—72.

(Received June 18, 1969.)