LARGE EXCLUSIVE FAMILIES

BY

S. K. STEIN

ABSTRACT

Three examples of an infinite family of semigroups are constructed such that there is no homomorphism from one member of the family to another member. The third example is intimately related to a number-theoretic theorem of C. L. Siegel.

A family $\mathscr{F}$ of semigroups is *exclusive* if there is no homomorphism from any member of $\mathscr{F}$ to any other member of $\mathscr{F}$. Some finite exclusive families were constructed by Tamura [4] where the concept was introduced. The present note exhibits various infinite exclusive families of semigroups. The first example consists of c (continuum) subsemigroups of the additive group of lattice points in the plane; the second example consists of 2^c subsemigroups of the additive group of real numbers; the third example consists of c subsemigroups of the multiplicative group of positive rational numbers.

Let m be a negative irrational number and $S_m = \{(i,j) \mid j > im,\ i \text{ and } j \text{ integers}\}$. Make S_m into a semigroup by defining $(i,j) + (i',j')$ to be $(i + i', j + j')$. Observe that if u and v are elements of S_m then precisely one of the equations, $u + x = v$ and $v + x = u$, has a solution x in S_m. If we have $u + x = v$ let us write $v > u$.

Consider now two negative irrational numbers m and m' and their corresponding semigroups S_m and $S_{m'}$. If $f: S_m \to S_{m'}$ is a homorphism and $u, v \in S_m$, $u > v$, then $u = v + x$, $f(u) = f(v) + f(x)$ and $f(u) > f(v)$. Thus f is one-to-one.

Let $f(1,0) = a$ and $f(0,1) = b$. Then for positive nonnegative integers x_1 and x_2, $(x_1, x_2) \in S_m$, we have

$$f(x_1, x_2) = x_1 a + x_2 b.$$

From this it follows easily that for any point $(x_1, x_2) \in S_m$ we have

$$f(x_1, x_2) = x_1 a + x_2 b.$$

Thus f is the restriction to S_m of a linear transformation $T: R_2 \to R_2$ of the whole Euclidean plane. The line $y = mx$ partitions the lattice points (other than 0,0) into two sets S_m and S_m^*. It is not hard to show that $T(S_m) \cap S_{m'}^* = \emptyset$. From

Received March 31, 1967, and in revised form November 19, 1967.

this it follows that T carries the line $y = mx$ into the line $y = m'x$. Hence $T(1, m)$ is on the line $y = m'x$, that is, $a + mb$ is on the line $y = m'x$. Letting $a = (a_1, a_2)$ and $b = (b_1, b_2)$ we have

$$a_2 + mb_2 = m'(a_1 + mb_1)$$

or

$$m' = \frac{a_2 + mb_2}{a_1 + mb_1}.$$

This proves

THEOREM 1. *There is a homomorphism from S_m to $S_{m'}$ if and only if there are integers a_1, b_1, a_2, b_2 such that*

$$m' = \frac{a_2 + mb_2}{a_1 + mb_1}.$$

From this theorem we deduce the existence of a continuum of semigroups such that there is no homomorphism from any one of them to any other. To do this, we introduce a relation among the negative irrational numbers, setting $m' \sim m$ if and only if there are integers a_1, a_2, b_1, b_2 such that $m' = (a_2 + mb_2)/(a_1 + mb_1)$. This equivalence relation partitions the set of negative irrational numbers into sets, each of which is denumerable. Hence there are a continuum of sets in the partition. Choose a representative, m, from each class; the family of corresponding semigroups S_m has the property that there is no homomorphism from one of them to another.

Our next example of an exclusive family of semigroups will be constructed within the additive structure of real numbers. It depends basically on the well-known Lemma 2 below, which may be proved with the aid of Lemma 1.

LEMMA 1. *Let R^+ be the set of positive real numbers and $f: R^+ \to R^+$ satisfy the functional equation $f(x + y) = f(x) + f(y)$. Then there is a number $k \in R^+$ such that $f(x) = kx$ for all x in R^+.*

LEMMA 2. *Let $A \subset R^+$ be dense in R^+, closed under addition, and satisfy the condition: if $a_1, a_2 \in A$, $a_1 < a_2$, then there is an element $a \in A$ such that $a_1 + a = a_2$. Let $B \subset R^+$ and $f: A \to B$ satisfy the functional equation $f(x + y) = f(x) + f(y)$. Then there is a number $k \in R^+$ such that $f(a) = ka$ for all $a \in A$.*

LEMMA 3. *If F_1 and F_2 are two subfields of the real numbers, then there is a function $f: F_1 \cap R^+ \to F_2 \cap R^+$ that satisfies the equation $f(x + y) = f(x) + f(y)$ if and only if F_1 is a subfield of F_2.*

Proof. Observe that F_1 and F_2 are dense in R since both contain the set of rational numbers. By Lemma 2, there is an element $k \in R^+$ such that $f(x) = kx$

for all $x \in F_1 \cap R^+$. In particular $f(1) = k \cdot 1 = k$; thus $k \in F_2$. If $a \in F_1 \cap R^+$, $f(a) = ka \in F_2 \cap R^+$; thus $a \in F_2 \cap R^+$ and $F_1 \cap R^+ \subseteq F_2$ It follows that $F_1 \subseteq F_2$ and the proof is done.

THEOREM 2. *There is an exclusive family $\mathscr{F}$, consisting of 2^c subsemigroups of the positive real numbers under addition.*

Proof. Let C be a maximal set of algebraically independent real numbers. The cardinality of C is c. Construct a family $G = \{X_\alpha\}$ of pairwise incomparable subsets of C such that the cardinality of G is 2^c. (For instance partition C into c denumerable sets $Y_1, Y_2 \cdots$ and let G be the images of the set of functions, $Y_1 \times Y_2 \times \cdots$). Each X_α generates a field $F(X_\alpha)$. For $\alpha \neq \beta$, X_α is incomparable with X_β and $X_\alpha \cup X_\beta$ consists of algebraically independent elements. Thus any element in $X_\alpha - X_\beta$ is not in $F(X_\beta)$. Thus $F(X_\alpha) \nsubseteq F(X_\beta)$; similarly $F(X_\beta) \nsubseteq F(X_\alpha)$. By Lemma 3, $\{F(X_\alpha) \cap R^+\}$ is an exclusive family of subsemigroups of R^+ under addition. This ends the proof.

Since R^+ under addition is isomorphic to the set of real numbers greater than 1 under multiplication, we have the following result, equivalent to Lemma 2, which will be of use in considering semigroups of rational numbers under multiplication.

LEMMA 4. *Let $A \subseteq (1, \infty) = \{x \mid x > 1\}$ be dense in $(1, \infty)$, closed under multiplication, and satisfy the condition: if $a_1, a_2 \in A$, $a_1 < a_2$, then there is an element $a \in A$ such that $a_1 a = a_2$. Let $B \subseteq (1, \infty)$ and $f: A \to B$ satisfy the condition $f(xy) = f(x)f(y)$. Then there is a number $k \in (1, \infty)$ such that $f(a) = a^k$ for all $a \in A$.*

The final construction depends on the following result of C. L. Siegel, quoted in [1] page 455: If p_1, p_2, and p_3 are distinct primes, and p_1^r, p_2^r, and p_3^r are rational then r is an integer. (See [2], page 9, or [3] page 189 for material relating to this result.)

If P is a set of primes let $S(P)$ denote the multiplicative semigroup of rational numbers greater than 1 that are expressible as the quotient of integers whose prime factorization involves only primes in P.

THEOREM 3. *Let P and Q be sets of primes such that P has at least three elements. Then there is a multiplicative homomorphism from $S(P)$ to $S(Q)$ if and only if $P \subseteq Q$.*

Proof. Assume that $f: S(P) \to S(Q)$ is such a homomorphism. $S(P)$ is dense in $(1, \infty)$. By Lemma 4, there is a real number r such that $f(x) = x^r$ for all $x \in S(P)$. By Siegel's theorem r is an integer. Thus $P \subseteq Q$.

Theorem 3 can be used to construct an exclusive family of semigroups of cardinality c within the multiplicative rational numbers. Whether "three" can be replaced by "two" in Theorem 3 is not known. In [1], p. 449 we have the related question concerning distinct primes, p and q: "$\cdots$is it true that p^x and q^x are both rationals only if x is an integer?"

The constructions used in Theorems 1 and 3 are related. Let $P = \{p_1, p_2\}$ and $Q = \{q_1, q_2\}$. Then $p_1^{n_1} p_2^{n_2} > 1$ if and only if $n_1 \ln p_1 + n_2 \ln p_2 > 0$; that is, if and only if $(n_1, n_2) \in S_m$ where $m = -\ln p_1/\ln p_2$. Similarly $S(Q)$ corresponds to $S_{m'}$, where $m' = -\ln q_1/\ln q_2$. (By the fundamental theorem of arithmetic, m and m' are irrational.) If we knew that for these m and m', $m \nsim m'$, then Theorem 1 would imply that there is no homomorphism from $S(P)$ to $S(Q)$.

Note also that S_m can be imbedded in the multiplicative semigroup $(1, \infty)$ by mapping (i,j) into e^{j-im}. Thus Theorem 1 could be phrased in terms of the real numbers under multiplication.

I am indebted to Ernst Straus for calling my attention to Siegel's theorem, and to Dov Tamari for several improvements in the exposition.

References

1. L. Alaoglu and P. Erdös, *On highly composite and similar numbers*, Trans. Amer. Math. Soc., **56** (1944), 448–469.

2. S. Lang, *Introduction to Transcendental Numbers*, Addison-Wesley, New York, 1967.

3. W. J. LeVeque, *Topics in Number Theory*, vol. 2, Addison-Wesley, New York, 1956.

4. T. Tamura, *Examples of completely exclusive direct product*, Port. Math., **25** (1964), 41–54.

University of California at Davis