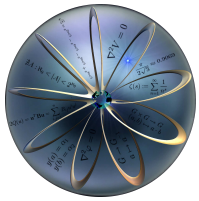

planetmath.org

Math for the people, by the people.

subsemigroup of a cyclic semigroup

Canonical name	SubsemigroupOfACyclicSemigroup
Date of creation	2013-03-22 19:01:48
Last modified on	2013-03-22 19:01:48
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	6
Author	CWoo (3771)
Entry type	Result
Classification	msc 20M99

It is a well-known fact that the subgroup of a cyclic group is cyclic. Is this true for semigroups? The answer is clearly no. For example, take the cyclic semigroup of positive integers under addition, and the subsemigroup generated by, say, 7 and 17. If it were cyclic, generated by some positive integer n, then n must divide both 7 and 17, which implies that $n = 1$. But there are no positive integers p and q such that $1 = 7p + 17q$, and the result follows. However, the following does hold:

Proposition 1. *Every subsemigroup of a cyclic semigroup is finitely generated.*

Proof. Let S be a cyclic semigroup. The result is obvious if S is finite. So assume that S is infinite. Since every infinite cyclic semigroup is isomorphic to the semigroup of positive integers under addition, we may as well assume that $S = \{1, 2, \ldots\}$. Let T be a subsemigroup of S. Since S is well-ordered, so is T. Take the least element p_1 of T. If $\langle p_1 \rangle = T$, then we are done. Otherwise, $T - \langle p_1 \rangle$ is non-empty, and thus has a least element p_2. So by the Euclidean algorithm, $p_2 = q_1 p_1 + r_1$, where $0 < r_1 < p_1$. If $\langle p_1, p_2 \rangle = T$, then we are done. Otherwise, continue this process. Along the way, we collect the quotients $\{q_1, q_2, \ldots\}$, as well as the remainders $\{r_1, r_2, \ldots\}$. We make the following observations:

1. Since $p_1 < p_2 < \cdots$, the quotients are non-decreasing: $q_1 \leq q_2 \leq \cdots$. For if $q_{j+1} < q_j$, then

   $$p_{j+2} = q_{j+1}p_1 + r_{j+1} < q_{j+1}p_1 + p_1 = (1 + q_{j+1})p_1 \leq q_j p_1 < q_j p_1 + r_j = p_{j+1},$$

   which is a contradiction.

2. Elements of $\{r_1, r_2, \ldots\}$ are pairwise distinct, for if $r_i = r_j$ for $i < j$, then

   $$p_{j+1} = q_j p_1 + r_j = q_j p_1 + r_i = (q_i p_1 + r_i) + (q_j - q_i)p_1 = p_{i+1} + (q_j - q_i)p_1.$$

   Since $q_i \leq q_j$ by the first observation, p_{j+1} lies in the subsemigroup generated by p_{i+1} and p_1, contradicting the construction of p_{j+1}.

Since the remainders are integers between 0 and p_1, the set $\{r_1, r_2, \ldots\}$ of remainders can not be infinite. Suppose the set has k elements. Then we must have $\langle p_1, p_2, \ldots, p_{k+1} \rangle = T$. Otherwise, we may continue the process and find p_{k+2}, q_{k+1}, and r_{k+1}. This means that r_{k+1} is among one of $r_1, \ldots, r_k$. But by the second observation, this means that $p_{k+2} \in \langle p_1, p_2, \ldots, p_{k+1} \rangle$ after all. $\square$

In fact, the above proof shows that there is an algorithm for finding a finite set of generators for the subsemigroup T.

The following result is immediate:

Corollary 1. *Any submonoid of a cyclic monoid is finitely generated.*

As an application to formal language theory, we have the following:

Corollary 2. *The Kleene star of any language over a singleton alphabet is* `http://planetmath.org/RegularLanguage`*regular.*

Proof. The Kleene star of a language L over $\{a\}$ is just a submonoid of the cyclic monoid $\langle a \rangle = \{a\}^*$, and hence is generated by some finite set F by the proposition above. Since every finite set is regular, so is $F^* = L^*$. □

References

[1] A. Salomaa, *Formal Languages*, Academic Press, New York (1973).