ON SUBSEMIGROUPS OF FREE SEMIGROUPS

P. M. COHN

1. In a recent paper [4], Ševrin has given necessary and sufficient conditions for a subsemigroup of the free product of a free group and a free semigroup to be of the same form; in particular he deduces that a subsemigroup T of a free semigroup S is free if and only if[1]

I. *For any* $a \in T$, $s \in S$, *if* $as \in T$ *and* $sa \in T$, *then* $s \in T$.

Now whereas the property of being a free subsemigroup of S is absolute, i.e. it does not depend on the way the subsemigroup is embedded in S, I expresses a condition on T relative to S. Our object here is to note a criterion similar to I, but which does not refer explicitly to S. Namely, a subsemigroup T of a free semigroup S is free if and only if

II. *For any* a, a', b, $b' \in T$, *if* $ab' = ba'$, *then* $a = bx$ *or* $b = ax$ *for some* $x \in T$.

It is not difficult to establish the equivalence of I and II (cf. Theorem 2 below), but since II, with a supplementary condition has been used to characterize free semigroups (cf. Dubreil-Jacotin [3], Clifford [1]), it may be of interest to derive the condition in a somewhat wider context. We shall in fact give a characterization of semigroups which can be expressed as the free product of a group and a free semigroup (Theorem 1); this will include the case considered by Ševrin. From this result it is easy to obtain the above conditions for a subsemigroup of a free semigroup to be again free (Theorem 2). As a second application we determine the structure of the semigroup of homogeneous elements of a free associative algebra (Theorem 3).

2. Throughout we shall only be concerned with cancellation semigroups with a unit-element (even when this is not explicitly stated); the unit-element will always be denoted by 1.

Every semigroup (in the sense just explained) contains a unique maximal subgroup, consisting of all the units, while the remaining elements, the non-units, form the unique maximal proper ideal. For any element a of a semigroup S we define the *height* $h(a)$ of a as the upper bound to the number of non-unit factors in the various decompositions of a. Thus $h(a)$ is a non-negative integer or $+\infty$. Clearly

Received by the editors November 16, 1960.

[1] This condition was given earlier by M. P. Schützenberger: *Sur certains sous-demi-groups qui interviennent dans un probème de mathématiques appliquées*, Publ. Sci. Univ. d'Alger Ser. A **6** (1959), 85–90. I am indebted to the referee for this reference, as well as for correcting some errors in the original version of my paper.

the elements of height zero are precisely the units; the elements of height one are also called the *primes* of S.

THEOREM 1. *Let G be a group and F a free semigroup and denote their free product $G * F$ by S. Then*

(i) *S has no elements of infinite height,*

(ii) *given $a, a', b, b' \in S$, if $ab' = ba'$, then either $a = bx$ or $b = ax$ for some $x \in S$,*

(iii) *given units u and v and a non-unit a such that $ua = av$, then $u = v = 1$.*

Conversely, any cancellation semigroup S satisfying (i)–(iii) *is of the form $G * F$, where G is a group and F is a free semigroup. Here G is uniquely determined while F is determined up to isomorphism.*

PROOF. Let $S = G * F$, then (i) clearly holds. To prove (ii), let $ab' = ba'$, where a, b may be taken to be nonunits without loss of generality. Then the first occurrence of a free generator of F in ab' and ba' must be the same, and must come in a and b. Thus $a = gpa_1$, $b = hpb_1$, where $g, h \in G$, p is a free generator of F and $gpa_1b' = hpb_1a'$. From the representation of elements of S as words in the elements of G and F we see that $g = h$ and $a_1b' = b_1a'$; now (ii) follows by induction on the length of the words a, b. Condition (iii) may be proved similarly.

Conversely, let S be a cancellation semigroup satisfying (i)–(iii). We shall say that two elements a, b of S are *associated*, if $uav = b$ for some units u, v of S. Clearly this relation is reflexive, symmetric and transitive, and associated elements have the same height. Let G be the group of units of S and P a set of primes of S containing just one prime from each class of associated primes. We assert that

(a) *the subsemigroup F of S generated by P is free, with P as free generating set,*

(b) $S = G * F$.

(a) Consider any relation in F:

$$p_1p_2 \cdots p_r = q_1q_2 \cdots q_s \qquad (p_i, q_j \in P). \tag{1}$$

If F is not free on P, then there is a nontrivial relation, i.e., one in which $r \neq s$ or $p_i \neq q_i$ for some i. Let (1) be a nontrivial relation for which $r + s$ has its least value. Then $r, s > 0$ and $p_1 \neq q_1$ (for otherwise we could obtain a shorter nontrivial relation by cancelling p_1). By (ii) $p_1 = q_1x$ or $q_1 = p_1x$ for some $x \in S$, say $p_1 = q_1x$. Since p_1 and q_1 are primes in S, x must be a unit and so p_1 and q_1 are associated; but this contradicts the definition of P. Hence F is free on P.

(b) By (i) every element of S is a product of primes and by the

definition of P every prime can be written as upv, where $p\in P$ and $u, v\in G$. Thus any element s of S has the form

$$s = u_0p_1u_1p_2 \cdots u_{r-1}p_ru_r \qquad (p_i \in P,\ u_i \in G). \tag{2}$$

If for some i, $u_i=1$, then $p_iu_ip_{i+1}=p_ip_{i+1}\in F$, hence (2) may be rewritten as

$$s = x_0a_1x_1a_2 \cdots a_nx_n, \tag{3}$$

where $a_i\in F$, $x_i\in G$, $a_i\neq 1$ $(1\leqq i\leqq n)$, $x_i\neq 1$ $(1\leqq i\leqq n-1)$. If also

$$s = y_0b_1y_1b_2 \cdots b_my_m,$$

where $b_j\in F$, $y_j\in G$, $b_j\neq 1$ $(1\leqq j\leqq m)$, $y_j\neq 1$ $(1\leqq j\leqq m-1)$, and if $a_1=pa_1'$, $b_1=qb_1'$, say $(p, q\in P)$, then by (ii) one of the equations

$$x_0p = y_0qz, \qquad y_0q = x_0pz$$

holds for some $z\in S$, say the first. Comparing heights, we find that $z\in G$, therefore p and q are associated and therefore equal. Thus

$$y_0^{-1}x_0p = pz;$$

by (iii), $z=1$, $x_0=y_0$ and we obtain

$$a_1'x_1a_2 \cdots a_nx_n = b_1'y_1b_2 \cdots b_my_m.$$

By induction on $h(s)$ it follows that these two expressions are identical. Hence the expression (3) for s is unique and (b) follows.

We have shown that $S=G*F$, where G is the unique group of units of S while F has a free generating set of the same cardinal as the set of classes of associated primes in S; this determines F up to isomorphism and the proof is complete.

COROLLARY. *A cancellation semigroup S is free if and only if it has no units other than* 1 *and satisfies* (i), (ii).

This follows immediately, since (iii) is now vacuous. The corollary occurs substantially in [1; 3].

3. If we apply Theorem 1 to subsemigroups of free semigroups, we obtain

THEOREM 2. *A subsemigroup T of a free semigroup S is free if and only if one of the following three equivalent conditions is satisfied:*

I. *Given $a\in T$, $s\in S$, if $as\in T$ and $sa\in T$, then $s\in T$.*

II. *Given $a, a', b, b'\in T$, if $ab'=ba'$, then $a=bx$ or $b=ax$ for some $x\in T$.*

III. *Given $a, b, b'\in T$, if $ab'=ba$, then $a=bx$ or $b=ax$ for some $x\in T$.*

For II the assertion follows from Theorem 1, Corollary if we can show that Theorem 1 (i) holds for any subsemigroup T of S (noting that S, and hence T, has no unit $\neq 1$). Since T and S have the same units, any element of infinite height in T would have infinite height in S; but S has no elements of infinite height, hence neither has T.

Further, III is a special case of II, so assume that III holds and let $ab'=ba'$, then $b'a\cdot b'b=b'b\cdot a'b$; by III we have either $b'a=b'bx$ or $b'b=b'ax$ for some $x\in T$, whence by cancelling b' we obtain the conclusion of II.

We complete the proof by showing that I$\Leftrightarrow$III. If III holds and $au=b$, $ua=b'(a, b, b'\in T)$, then $aua=ba=ab'$, hence by III, $a=bx$ or $b=ax$ for some $x\in T$. If $a=bx$, then $a=aux$ and hence $u=x=1$; if $b=ax$, then $ax=au$ and again $x=u$, therefore in either case $u\in T$, which proves I. Conversely, assume that I holds and let $ab'=ba(a, b, b'\in T)$; without loss of generality we may assume that $b\neq 1$. Let us put $a=b^ru(u\in S)$ with $r(\geqq 0)$ chosen as large as possible. Then $b^rub'=b^{r+1}u$, hence

$$bu = ub'. \tag{4}$$

By III, applied to S, we have $b=uv$ or $u=bv$ for some $v\in S$; here the second alternative conflicts with the definition of r, hence

$$b = uv, \qquad b' = vu. \tag{5}$$

We conclude that $av=b^{r+1}\in T$, $va=b'^{r+1}\in T$; applying I we find that $v\in T$ and hence applying I again to (5) we have $u\in T$. Thus if $r>0$ we have $a=b\cdot b^{r-1}u$, while for $r=0$, $a=u$ and $b=av$. This shows that III holds for T and the proof is complete.

4. There is a characterization of free associative algebras which is analogous to the characterization of free semigroups given in Theorem 1, Corollary (cf. [2]). However this cannot be used as it stands to characterize free subalgebras of free algebras. One difficulty is that whereas in a free semigroup the free generating set is uniquely determined, in a free algebra the free generators are not even determined up to linear transformations; e.g., if A is free on x and y, it is also free on $x+y^2$ and $y-x^2-xy^2-y^2x-y^4$. However we obtain a free semigroup by limiting ourselves to certain homogeneous elements. Let A be a free associative algebra on a free generating set which we suppose totally ordered. Then the monomials may be ordered by increasing degree, while the monomials of the same degree are ordered lexicographically. Using this ordering we can speak of the highest (=last) term of any nonzero element of A.

THEOREM 3. *If A is a free associative algebra over a field F, then the homogeneous elements in which the coefficient of the highest term is* 1 *form a free semigroup.*

PROOF. Clearly the set S of homogeneous elements of A in which the highest term has coefficient 1 form a semigroup. Now in [2] it was shown that for any $a, b, a', b' \in A$, if $ab' = ba' \neq 0$, then

$$a = bq + r \tag{6}$$

for some $q, r \in A$, where r is of lower degree than b. If in particular, $a, b, a', b' \in S$ and the degree of b does not exceed that of a, then by equating the terms of highest degree in (6) we obtain $a = bx$, where x is the homogeneous part of highest degree in q. If the degree of b exceeds that of a, then by reversing the roles of a and b we find that $b = ax$, and in each case x clearly belongs to S. Thus S satisfies (ii) of Theorem 1. S also satisfies (i) since the height of an element of S cannot exceed its degree, and the only unit in S is 1. Now the result follows by Theorem 1, Corollary.

If we do not want to utilize the ordering of the generators, we can state Theorem 3 by saying that the set of all homogeneous elements of A is the direct product of the field F (qua multiplicative semigroup) and a free semigroup S.

REFERENCES

1. A. H. Clifford, Review of [3], Math. Rev. **9** (1948), 174.

2. P. M. Cohn, *On a generalization of the Euclidean algorithm*, Proc. Cambridge Philos. Soc. **57** (1961), 18–30.

3. M.-L. Dubreil-Jacotin, *Sur l'immersion d'un semigroupe dans un groupe*, C. R. Acad. Sci. Paris **225** (1947), 787–788.

4. L. N. Ševrin, *On subsemigroups of free semigroups*, Dokl. Akad. Nauk SSSR **133** (1960), 537–539 (Russian) = Soviet Math. Dokl. **1** (1960), 892–894.

THE UNIVERSITY, MANCHESTER, ENGLAND