PRIMARY SEMIGROUPS

Pierre Antoine Grillet

1. A commutative semigroup S is *primary*, relative to a commutative ring R with identity, in case the semigroup algebra R [S] contains a primary ideal that separates S, in other words, contains no nontrivial difference of two elements of S. Our main results give various properties of primary semigroups in general, and a characterization of finite primary semigroups when R is a suitable field such as $\mathbb{C}$.

Our interest in primary semigroups stems from the fact that each finitely generated commutative semigroup is a subdirect product of finitely many primary semigroups (when R is Noetherian); this is an easy consequence of primary decompositions and the Hilbert basis theorem. It presents primary semigroups as basic building blocks for an important class of semigroups, and it makes their determination of some interest, particularly in the finitely generated case. The choice of R is of secondary importance in this, so long as R yields a wide class of primary semigroups, and there are indications that $\mathbb{C}$ is as good a choice as any. The author is primarily interested in the structure of semigroups, rather than in the interplay between semigroups and rings; maximum generality has not been sought as far as R is concerned.

2. Our main results on primary semigroups are as follows. First, there are three kinds of primary semigroups: relative to each R, a primary semigroup is either a cancellative semigroup, or a nilsemigroup, or what we call a *subelementary* semigroup, that is, the union $S = N \cup C$ of a nilsemigroup N and a cancellative semigroup C, in which N is an ideal and every element of C is cancellative in the whole semigroup. In the last case, C is also primary if S is primary.

All nilsemigroups are primary (relative to each R). For a cancellative semigroup S to be primary, the torsion part of its group of quotients must be locally cyclic (cyclic, if S is finitely generated); the converse holds if S is finitely generated and R is a field K of characteristic 0 that contains all roots of unity (for example $K = \mathbb{C}$). The case where S is subelementary is more difficult. A subelementary semigroup is easily completed into an elementary one (one whose cancellative part is a group), and this does not affect primariness. When $R = K$ as above, and the primary semigroup $S = N \cup G$ is elementary (with G a group), then the torsion part of G is locally cyclic; this is completed by the following necessary condition on the action of G on S (G acts on S by multiplication in S): under the action of any cyclic subgroup of G, all the finite nonzero orbits in S must have the same number of elements. We could not prove the converse holds except when G is cyclic (finite or infinite). However, this suffices to clean the problem in the finite case.

3. These results require a certain amount of preliminary material. The easier basic properties of subelementary semigroups and primary semigroups will be found in Section 1. Section 2 studies prime semigroups, which are defined like primary semigroups but in terms of prime ideals; this is useful for the main results, because when $R = K$ as above, a primary cancellative semigroup is necessarily prime (and conversely). The main results can then be obtained in Section 3.

Received February 25, 1975.

4. The notation is generally as in [1], and the reader is referred to [1] and, say, [7] for all basic concepts. We depart from the notation in [1] by denoting the identity and zero element of S (if any) by e and z, respectively. This is pretty much a must, since $z \neq 0 \in R[S]$ and $e \neq 1 \in R$. The letter K generally denotes a field of characteristic 0 containing all roots of unity. The letter R denotes a commutative ring with identity. *All* semigroups and rings under consideration are commutative; this should be kept in mind by the reader, since it is usually not recalled in the text.

The results of this paper have been announced in [4].

1. SUBELEMENTARY SEMIGROUPS

1. A commutative semigroup S is *subelementary* in case S is a disjoint union $S = N \cup C$, where N is a nilsemigroup and an ideal of S, while C is a cancellative semigroup, and every element of C is cancellative in S; we say that S is *elementary* if furthermore C is a group. In the latter case, the terminology is due to I. S. Ponizovskiĭ [9]. The zero element z of N is also a zero element of S (if $c \in C$, then $zc \in N$, and the relation $x(zc) = zc$ for all $x \in N$ shows that zc is a zero element of N, so that $zc = z$). If C has an identity element e (for example, if S is elementary), then e is also the identity element of S (because $e(ex) = ex$, $x \in N$, $ex \in N$ implies $ex = x$, for all $x \in N$). In fact, if $C = G$ is a group, the condition that e is an identity element of S is equivalent to the cancellativity in S of every element of G: for the relation $gx = gy$ implies $x = y$ trivially if $x, y \in G$; it cannot happen if $x \in N$ and $y \in G$; and it implies

$$x = ex = g^{-1}gx = g^{-1}gy = ey = y$$

if $x, y \in N$. For instance, it is readily seen that a finite commutative semigroup S is elementary if and only if it has an identity, a zero, and no other idempotent.

A basic property of subelementary semigroups is that they can always be completed to elementary semigroups. In general, let S be commutative semigroup, and let C be a subsemigroup of S, every element of which is cancellative in S. We can then form a semigroup of fractions $C^{-1}S$, whose elements are all fractions s/a ($s \in S$, $a \in C$), with $s/a = t/b \Leftrightarrow bs = at$, multiplied according to the rule $(s/a)(t/b) = st/ab$; when $c \in C$ and $s \in S$, then $\alpha s = sc/c \in C^{-1}S$ does not depend on the choice of c, and $\alpha\colon S \to C^{-1}S$ is easily seen to be an injective homomorphism. In the sequel, it is convenient to identify s and αs, which makes $S \subseteq C^{-1}S$ and α an inclusion map. For instance, if $S = C$ is cancellative, then $C^{-1}S = S^{-1}S$ is the group of fractions (or group of quotients, or universal group) of S, which we also denote by G(S). This construction is well known, and it is a particular case of much more general constructions (see [8], for example).

PROPOSITION 1.1. *If* $S = N \cup C$ *is subelementary, then* $C^{-1}S$ *is elementary, with* $C^{-1}S = C^{-1}N \cup G(C)$ *and* $C^{-1}N = \{x/c \in C^{-1}S;\ x \in N\}$.

Proof. We see that z/c is a zero element of $C^{-1}S$ (in particular, it does not depend on c) and that $C^{-1}N$ is a nilsemigroup and an ideal of $C^{-1}S$. Also, $S = N \cup C$ implies $C^{-1}S = C^{-1}N \cup C^{-1}C$; the right-hand member is a disjoint union, since the equation $x/c = y/d$ has no solutions when $x \in N$ and $y, c, d \in C$. Finally, for each $c \in C$, we see that c/c is an identity element of $C^{-1}S$; in particular, it does not depend on c, and thus the identity element of $C^{-1}C = G(C)$ is the same as that of $C^{-1}S$. ■

Before we go on with the study of subelementary semigroups, we make one more observation on the general semigroup $C^{-1}S$ (with S commutative and every element of the subsemigroup C cancellative in S):

PROPOSITION 1.2. *For each commutative ring* R *with identity,* $R[C^{-1}S] \cong C^{-1}R[S]$.

Proof. First, C is a multiplicative subsemigroup of the commutative ring $R[S]$, so that we can construct the localization $C^{-1}R[S]$. Now take $c, d \in C$, $a = \sum_{s\in S} r_s s$, $b = \sum_{t\in S} r'_t t$ in $R[S]$, and assume $da = cb$. Then

$$\sum_{s\in S} r_s(ds) = \sum_{t\in S} r'_t(ct);$$

since c and d are cancellative in S, a one-to-one correspondence between the finite sets $\{s \in S;\ r_s \neq 0\}$ and $\{t \in S;\ r'_t \neq 0\}$ is obtained from $ds = ct$; when s and t correspond to each other in this way, then $r_s = r'_t$ and $s/c = t/d$ in $C^{-1}S$; therefore

$$\sum_{s\in S} r_s(s/c) = \sum_{t\in S} r'_t(t/d) \quad \text{in } R[C^{-1}S].$$

It follows that a mapping $\theta\colon C^{-1}R[S] \to R[C^{-1}S]$ is well-defined by the condition

$$\theta(a/c) = \sum_{s\in S} r_s(s/c) \quad \text{whenever } c \in C,\ a = \sum_{s\in S} r_s s \in R[S].$$

The mapping θ is readily seen to be a homomorphism (being R-linear and preserving multiplication of generators s/c). Furthermore, $\theta(a/c) = 0$ clearly implies $a = 0$ (since all s/c $(s \in S)$ are distinct), so that θ is injective. Finally, let

$$b = \sum_{i\in I} r_i(s_i/c_i) \in R[C^{-1}S];$$

there we may assume that I is finite, $r_i \neq 0$, and the elements s_i/c_i are pairwise distinct. Let $c \in C$ be the product of all [finitely many] c_i; then $b = \sum_{i\in I} r_i(t_i/c)$, where the elements $t_i \in S$ are pairwise distinct (since the t_i/c are pairwise distinct); therefore $b = \theta(a/c)$, with $a = \sum_{i\in I} r_i t_i \in R[S]$. ∎

2. If $S = N \cup G$ is an elementary semigroup, the group G acts on the set S by multiplication. If $x \in S$ and $g \in G$, then the equality $g^{-1}(gx) = x$ shows that $x \mathcal{H} gx$. Conversely, if $x \mathcal{H} y$, so that $y = ux$ and $x = vy$ for some $u, v \in S$ $[= S^1]$, then $x = uvx$ implies $x = (uv)^n x$ for all n, so that, if $x \neq z$, then $(uv)^n \neq z$ for all n, that is, $uv \notin N$, $uv \in G$, $u \in G$, and $y \in Gx$; if $x = z$, then again $y = z = ez \in Gx$. Thus the $\mathcal{H}$-classes of S are precisely the orbits under the action of G on S; for this reason, they will also be called *orbits* in what follows. The quotient semigroup $S/\mathcal{H}$ is the *semigroup of orbits* of S. We see that G is a single orbit and the remaining orbits are nilpotent in $S/\mathcal{H}$; thus the semigroup of orbits of S is a nilsemigroup with adjoined identity, and for this reason we shall denote it by Ω^1 in what follows (with Ω a nilsemigroup).

These definitions can be generalized to any subelementary semigroup $S = N \cup C$ as follows. The binary relation $Cx \cap Cy \neq \emptyset$ on S is readily seen to be transitive, and hence it is an equivalence relation on S; the equivalence classes are again called *orbits*. Since $Cx \cap Cy \neq \emptyset$ implies $Cxs \cap Cys \neq \emptyset$ for all $s \in S$, our equivalence relation is in fact a congruence; the quotient-semigroup is the *semigroup of orbits* of S. These definitions reduce to the above if S is elementary; but in general, we cannot interpret orbits as $\mathcal{H}$-classes, if only because $\mathcal{H}$ is trivial when S lacks an identity element, whereas C itself is an orbit, by commutativity. Again the semigroup of orbits is a nilsemigroup with adjoined identity, and we denote it by Ω^1.

The following result gives an alternate description of the orbits of S.

PROPOSITION 1.3. *When* $S = N \cup C$ *is subelementary, all the orbits of* $C^{-1}S$ *intersect* S, *and these intersections are precisely the orbits of* S. *Thus,* S *and* $C^{-1}S$ *have isomorphic semigroups of orbits.*

Proof. When $s/c \in C^{-1}S$, we see that $s = sc/c = (s/c)(c^2/c)$, and hence the orbit of s/c contains $s \in S$. This also shows that s and s/c always lie in the same orbit of $C^{-1}S$. If now s and t lie in the same orbit of S, then $ds = ct$ for some $c, d \in C$; since $s/c = t/d$, it follows that s and t lie in the same orbit of $C^{-1}S$. Conversely, if $s, t \in S$ lie in the same orbit of $C^{-1}S$, then $s = (c/d)t = ct/d$ for some $c, d \in C$ such that $ds = ct$, and s and t lie in the same orbit of S. The various parts of the statement then follow immediately. ■

PROPOSITION 1.4. *If* $S = N \cup C$ *is a finitely generated subelementary semigroup, then* C *is finitely generated and the orbit semigroup is finite.*

Proof. Since N is an ideal, C is generated by the generators of S that lie in C. Furthermore, the semigroup of orbits of S is a finitely generated nilsemigroup with adjoined identity, and therefore it is finite. ■

Recall that the nilsemigroup N can always be partially ordered by the rule $a \leq b \Leftrightarrow a \in N^1 b$. We see that $a < b$ if and only if $a \in Nb$ and $b \neq z$; hence $a < b$ implies that the orbits Ω_a and Ω_b of a and b satisfy the condition $\Omega_a < \Omega_b$ in Ω^1. It follows from Proposition 1.4 that if S is finitely generated, then N has finite height (a maximal chain of N cannot be longer than the longest maximal chain of Ω).

3. We conclude this section with the definition of primary semigroups and some basic properties.

Let R be a commutative ring with identity. An ideal $\mathfrak{a}$ of the semigroup algebra $R[S]$ is said to *separate* S in case the conditions $s, t \in S$, $s - t \in \mathfrak{a}$ imply $s = t$. Note that $\mathfrak{a}$ can then contain at most one element of S; if $\mathfrak{a}$ does contain one element z of S, then $z - zs \in \mathfrak{a}$ for all $s \in S$, and it follows that z is a zero element of S. The semigroup S is called R-*primary* in case it is separated by a primary ideal of $R[S]$.

PROPOSITION 1.5. *A commutative semigroup* S *is* R-*primary if and only if there exists a primary commutative* R-*algebra that contains a multiplicative semigroup isomorphic to* S.

Proof. If the primary ideal $\mathfrak{q}$ of $R[S]$ separates S, then the R-algebra $R[S]/\mathfrak{q}$ contains a multiplicative subsemigroup isomorphic to S, and its zero ideal is clearly primary. Conversely, if the primary R-algebra A contains a subsemigroup $T \cong S$, then the isomorphism $S \to T$ extends to a homomorphism $\phi: R[S] \to A$ whose kernel $\mathfrak{q}$ separates S, since ϕ is injective on S, and is primary by the condition on A. ■

Our interest in primary semigroups stems from the following result.

PROPOSITION 1.6. *Let* S *be a finitely generated commutative semigroup. Then* S *is a subdirect product of finitely many* R-*primary semigroups, whenever* R *is a commutative Noetherian ring with identity.*

Proof. If S is generated by $x_1, \cdots, x_n$, say, it is a homomorphic image of the free commutative semigroup F on $x_1, \cdots, x_n$. Hence R[S] is a homomorphic image of $R[F] \cong R[X_1, \cdots, X_n]$; if R is Noetherian, the Hilbert basis theorem then implies that R[S] is Noetherian. [This elementary fact will be used again.] The zero ideal of R[S] is then the intersection of finitely many primary ideals $\mathfrak{q}_1, \cdots, \mathfrak{q}_r$. Each $\mathfrak{q}_j$ induces on S a congruence $\mathscr{C}_j$ defined by the rule $x \mathscr{C}_j y \Leftrightarrow x - y \in \mathfrak{q}_j$; since $\bigcap \mathfrak{q}_j = 0$, we see that $\bigcap \mathscr{C}_j$ is the equality on S and hence S is a subdirect product of the semigroups $S/\mathscr{C}_1, \cdots, S/\mathscr{C}_r$. Now the R-algebra $R[S]/\mathfrak{q}_j$ is primary, and we see that it contains an isomorphic copy of $S/\mathscr{C}_j$; therefore Proposition 1.5 implies that every $S/\mathscr{C}_j$ is R-primary. ■

PROPOSITION 1.7. *An* R-*primary semigroup is either cancellative or nil or subelementary.*

Proof. Let $\mathfrak{q}$ be a primary ideal of R[S] that separates S, and let $\mathfrak{p}$ be its radical (a prime ideal of R[S]). Because $R[S] \setminus \mathfrak{p}$ is multiplicatively closed, we see that $C = S \setminus \mathfrak{p}$ is a subsemigroup (possibly empty) of S. Because $\mathfrak{p}$ is an ideal of R[S], we see that $N = S \cap \mathfrak{p}$ is an ideal (possibly empty) of S. If $x, y \in S$, $c \in C$, and $cx = cy$, then $c(x - y) \in \mathfrak{q}$; since $\mathfrak{q}$ is primary and $c \notin \mathfrak{p}$, this implies that $x - y \in \mathfrak{q}$ and hence $x = y$; thus every element of C is cancellative in S. Assume $x \in N$ (in particular, $N \neq \emptyset$). Then $x \in \mathfrak{p}$, so that $x^n \in \mathfrak{q}$ for some n; in particular, $S \cap \mathfrak{q} \neq \emptyset$, and since $\mathfrak{q}$ separates S, the intersection $S \cap \mathfrak{q}$ consists of just a zero element z of S. Also, in the considerations above, $x^n = z$ (since $x^n \in S \cap \mathfrak{q}$), and thus N is a nilsemigroup. The different cases for S in the statement then arise according to whether $N = \emptyset$, $C = \emptyset$, or $N, C \neq \emptyset$. ■

COROLLARY 1.8. *Every finitely generated commutative semigroup is a subdirect product of finitely many cancellative, nil, and subelementary semigroups.* ■

In the finite case, this result was obtained by Ponizovskiĭ [9], who also showed that explicit decompositions of this type are readily available. For finitely generated commutative semigroups, it is the basis of a further investigation of subdirect decompositions (announced in [5]) and for the completion theorem in [6].

2. PRIME SEMIGROUPS

1. Let R be a commutative ring with identity. A commutative semigroup S is R-*prime* in case it is separated by a prime ideal of R[S].

It is natural to wonder whether the prime ideal in this definition can be assumed to be zero (a similar question applies to the definition of primary semigroups). Evidently, this requires that R is an integral domain; but even then the following result (together with later results) shows that the answer is no.

PROPOSITION 2.1. *Let* R *be an integral domain of characteristic* 0. *For a commutative semigroup* S, *these are equivalent:*

(a) R[S] *is an integral domain;*

(b) *every zero divisor in* $R[S]$ *is nilpotent;*

(c) S *is cancellative and power-cancellative* (*that is,* $x^n = y^n$ *implies* $x = y$).

Proof. Assume (b) holds. If the equation $ac = bc$ holds in S, then $(a - b)c = 0$ in $R[S]$; since $c^n \neq 0$ in $R[S]$ for all n, it follows that $a = b$, so that S is cancellative. Now assume $a^n = b^n$ holds in S. We may assume $n > 1$. Then $a^n - b^n = (a - b)u = 0$ holds in $R[S]$, where

$$u = a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \qquad (u = a + b \text{ if } n = 2).$$

The coefficient of $a^{(n-1)k}$ in u^k is a positive integer in R (it is the number of times a product of k elements $a^{n-p}b^{p-1}$ equals $a^{(n-1)k}$ in S); since R has characteristic 0, it follows that $u^k \neq 0$ for all k, and again $a = b$. Thus (b) implies (c).

Conversely, assume that (c) holds. If $R[S]$ has zero divisors, these will be linear combinations of finitely many elements of S, and therefore some subalgebra $R[T]$ of $R[S]$, where T is a finitely generated subsemigroup of S, will also have zero divisors. Therefore we may assume from the start that S is finitely generated. Then $G(S)$ is also finitely generated; since S is power-cancellative, $G(S)$ is also torsion-free, and hence it is a finitely generated free abelian group, say on $X_1, \cdots, X_n$; if F is the free semigroup on $X_1, \cdots, X_n$, then also $G(S) = F^{-1}F$. It follows from Proposition 1.2 that the group algebra $R[G(S)]$ arises from the polynomial algebra $R[F]$ by localization, and therefore it is also an integral domain. Therefore, the same is true of $R[S] \subseteq R[G(S)]$. Thus (c) implies (a); trivially, (a) implies (b). ■

For group algebras, results much more general than the above are available for the equivalence of (a) and (c) (see [2] for example). Proposition 2.1 is sufficient to imply that the algebra of a finite cyclic group (with R any integral domain) has zero divisors, whereas we shall see that such groups are prime semigroups, relative to $\mathbb{C}$, for example.

In general, we see that (as for primary semigroups) S is R-prime if and only if there exists a (commutative) R-algebra A without zero divisors that contains a multiplicative subsemigroup isomorphic to S (see Proposition 1.5). In particular, primeness is inherited by subsemigroups. The following is another easy result of general interest (similar to Proposition 1.7).

PROPOSITION 2.2. *A prime semigroup is either cancellative or cancellative with a zero adjoined.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $R[S]$ that separates S. First assume that $\mathfrak{p}$ contains no element of S. Then $ac = bc$ in S implies $(a - b)c = 0 \in \mathfrak{p}$, whence $a - b \in \mathfrak{p}$ (since $c \notin \mathfrak{p}$) and $a = b$: then S is cancellative. Now assume that $\mathfrak{p}$ does contain an element of S; we have seen that S then has a zero and that $\mathfrak{p} \cap S = \{z\}$. If $ab = z$ in S, then $ab \in \mathfrak{p}$, whence $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, that is, $a = z$ or $b = z$: thus S is obtained by the adjunction of a zero element to $S \setminus z$. Furthermore, the semigroup $S \setminus z$ is cancellative, for $ac = bc$ with $a, b, c \in S \setminus z$ (in particular, $c \notin \mathfrak{p}$) implies, as above, that $a = b$. ■

PROPOSITION 2.3. *If* S *does not have a zero, then* S^0 *is prime if and only if* S *is prime.*

Proof. If S^0 is prime, then so is $S \subseteq S^0$. Conversely, if S is prime, then there is a prime ideal of the contracted semigroup algebra $R_0[S^0] \cong R[S]$ that separates

S, hence also separates S^0, since S has no zero element. Since

$$R_0[S^0] \cong R[S^0]/Rz,$$

this immediately yields a prime ideal of $R[S^0]$ that separates S^0. ■

By Proposition 2.3, we need only consider the case where S is cancellative. The following result shows that the determination of prime semigroups in this case is essentially a group problem:

PROPOSITION 2.4. *When* S *is cancellative, then* S *is prime if and only if* G(S) *is prime.*

Proof. If G(S) is prime, then so is $S \subseteq G(S)$. Conversely, let $\mathfrak{p}$ be a prime ideal of $R[S]$ that separates S. We know that $G(S) = S^{-1}S$, and it follows from Proposition 1.2 that then $R[G(S)] \cong S^{-1}R[S]$. Let

$$S^{-1}\mathfrak{p} = \{u/s \in S^{-1}R[S];\ u \in \mathfrak{p}\};$$

it follows immediately that $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}R[S]$. Assume $a/b - c/d \in S^{-1}\mathfrak{p}$, where $a, b, c, d \in S$, so that $da - bc/bd = u/s$ for some $u \in \mathfrak{p}$ and $s \in S$. Then $s(da - bc) = bdu \in \mathfrak{p}$ and $s \notin \mathfrak{p}$ (since $S \neq S^0$), and hence $da - bc \in \mathfrak{p}$; since $\mathfrak{p}$ separates S, it follows that $da = bc$; that is, $a/b = c/d$, so that $S^{-1}\mathfrak{p}$ separates G(S). ■

2. We now prove somewhat deeper results, which will lead to a characterization of prime semigroups in the finitely generated case, provided R has sufficiently many units.

THEOREM 2.5. *If* S *is a cancellative prime semigroup, the torsion part of* G(S) *is locally cyclic.*

Proof. If S is prime and cancellative, then G(S) is prime, by Proposition 2.4, and hence so is every finitely generated subgroup of the torsion part of G(S); therefore it suffices to show that a finite abelian group that is not cyclic cannot be a prime semigroup. By the fundamental theorem on finitely generated abelian groups, a finite abelian group that is not cyclic necessarily contains a subgroup of the form $\mathbb{Z}(p) \oplus \mathbb{Z}(p)$, where p is prime, and it suffices to show that such a group G cannot be prime. We achieve this by producing finitely many elements $a_i \neq e$ such that $\prod(e - a_i) = 0$ in $R[G]$: for then each prime ideal $\mathfrak{p}$ of $R[G]$ contains $\prod(e - a_i)$, and hence some $e - a_i$, and thus it fails to separate G.

If $p = 2$, then $G = \mathbb{Z}(2) \oplus \mathbb{Z}(2)$ has the multiplication table

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

and we see that $(e - a)(e - b)(e - c) = e - a - b - c + bc + ca + ab - abc = 0$ in $R[G]$; therefore G is not prime.

Now assume $p \neq 2$; let $C = \mathbb{Z}(p)$, so that $G = C \oplus C$, let e be the identity element, and let a be a generator of C. Let $u = \prod_{t=0}^{p-1} ((e, e) - (a^t, a))$; we shall prove that $(e, e)u = (a, e)u$, so that the product $((e, e) - (a, e))u$ is 0 in $R[G]$ and therefore G is not prime.

For this we calculate u. Expansion of the product yields 2^p terms of the form $(-1)^k (a^v, a^k)$ (where k is the number of times we have used the second term $-(a^t, a)$ in the differences $(e, e) - (a^t, a)$). There is only one term with $k = 0$, namely (e, e), and one term with $k = p$, namely $(-1)^p (a^{p(p-1)/2}, a^p)$; these cancel each other, since p is odd. Hence

$$u = \sum_{k=1}^{p-1} \left(\sum_{a^v \in C} A_{a^v,k} (a^v, a^k) \right),$$

where $A_{a^v,k}$ is an integer in R.

We now observe that u is also equal to

$$\prod_{t=0}^{p-1} ((e, e) - (a^{t+1}, a)) = \prod_{t=0}^{p-1} ((e, e) - (a^t a, a)).$$

Expanding this product exactly as above, we find that

$$u = \sum_{k=1}^{p-1} \left(\sum_{a^v \in C} A_{a^v,k} (a^v a^k, a^k) \right)$$

(with the same coefficients). Comparison shows that $A_{a^v,k} = A_{a^v a^k,k}$ for all $a^v \in C$ and all k $(0 < k < p)$. Since p is prime, a^k also generates C, and repeated applications of this equality yield the relation $A_{a^v,k} = A_{a^w,k}$ for all $a^v, a^w \in C$; in other words, $A_{a^v,k}$ depends solely on k, that is,

$$u = \sum_{k=1}^{p-1} \left(\sum_{a^v \in C} A_k (a^v, a^k) \right).$$

[It is then clear that $A_k = (-1)^k \frac{1}{p} \binom{p}{k}$.] From this we see that $(e, e)u = (a, e)u$, because each sum $\sum_{a^v \in C} A_k(a^v, a^k)$ has this property. ■

The difficulty in proving converses lies with the construction of prime ideals that the proof requires. A similar difficulty will be encountered in the next section. For later results we need only a simple converse where this difficulty is bypassed. The hypothesis in the next result, that R contains the algebraic closure of $\mathbb{Q}$ (for example, that R is an algebraically closed field of characteristic 0) can be weakened, because R only needs to contain the subfield of $\overline{\mathbb{Q}}$ generated by the roots of unity.

COROLLARY 2.6. *Assume that* R *is an integral domain containing the algebraic closure of* $\mathbb{Q}$, *and that* S *is finitely generated. The following are then equivalent:*

(a) S *is* R-*prime;*

(b) S *is isomorphic to a multiplicative subsemigroup of* $\mathbb{C}$;

(c) S *is isomorphic to either* C *or* C^0, *where* C *is a cancellative semigroup such that the torsion part of* G(C) *is cyclic.*

Proof. It follows from Propositions 2.3 and 2.4 that the validity of (a) is not affected by the adjunction or removal of a zero element of S, nor (in the case without zero) by the replacement of S by G(S); the same is true of (b) and (c). Hence we may assume from the start that S is a finitely generated abelian group. In this case, Theorem 2.5 shows that (a) implies (c). Similarly, (b) implies (c), since the torsion part of G(S) = S is finite and $\mathbb{C}$ is a field. Now assume that (c) holds. Then $S = F \oplus G$, where F is a finitely generated free abelian group and G is cyclic; F is isomorphic to a multiplicative group of positive rationals, and G to a group of roots of unity; therefore S is isomorphic to a multiplicative subgroup of the group of units of R. Since we can here use $\mathbb{C}$ instead of R, we see that (c) implies (b). Furthermore, R is an R-algebra without zero divisors; since it contains a copy of S, it follows that S is R-prime. ■

Although this converse of Theorem 2.5 is quite simple, it does show (together with the theorem) that if a finitely generated semigroup is R-prime for some ring R, then it is also $\mathbb{C}$-prime. Thus the choice $R = \mathbb{C}$ gives us the greatest family of prime semigroups (so would the choice of any algebraically closed field of characteristic 0).

3. We now complete these results with various technical remarks to be used in the next section.

First, let R be as in Corollary 2.6, and let G be a finitely generated abelian group. If G is not R-prime, then by Corollary 2.6 the torsion part T(G) of G is not cyclic; looking back at the proof of Theorem 2.5, we see that each prime ideal of R[G] contains a difference $e - a_i \neq 0$, where a_i can be chosen in a subgroup $\mathbb{Z}(p) \oplus \mathbb{Z}(p)$ of G. Thus we have the following result.

COROLLARY 2.7. *Let* R *be as in Corollary* 2.6, *and let* G *be a finitely generated abelian group. If* G *is not* R-*prime, then every prime ideal of* R[G] *contains a difference* e - a, *where* e *is the identity element of* G *and* a *has prime order.* ■

In the rest of this section, we let G be cyclic of order n, with identity element e and generator a, and we let R = K be a field of characteristic 0 that contains all nth roots of unity; ω denotes a primitive nth root of unity. (We need a field, in what follows, for considerations of dimension.). The proof of Corollary 2.6 shows that G is K-prime, and what follows will in particular illustrate the separation of G by prime ideals. We note that $K \cong Ke \subseteq K[G]$ and hence the ideals of the ring K[G] are the same as the ideals of the algebra K[G]. Although K[G] is semisimple (hence isomorphic to K^n), it is easier to manipulate it through the homomorphism $K[X] \to K[G]$ that sends X to a.

First we find all the prime ideals of K[G]. Since $a^n = e$ and K[G] has dimension n, the kernel of $K[X] \to K[G]$ is the ideal $(X^n - 1)$ generated by $X^n - 1$. We have the relation $(X^n - 1) = \bigcap_{k=0}^{n-1} (X - \omega^k)$ in K[X], and hence $0 = \bigcap_{k=0}^{n-1} (a - \omega^k e)$ in K[G]; furthermore, each $(X - \omega^k)$ has codimension 1 in K[X], so that each $(a - \omega^k e)$ has dimension n - 1 in K[G] and (by maximality, or from K[X]) is a prime ideal of K[G]. Furthermore, a prime ideal of K[G] must contain the product of these ideals (which is 0), and hence it contains one of them; it follows that the ideals $(a - \omega^k e)$ are all the prime ideals of $K[G]$.

An alternate description of $(a - \omega^k e)$ can be given in terms of the algebra homomorphism ϕ_k: $K[G] \to K$ induced by the homomorphism $G \to K$ that sends a to ω^k. For each $u \in K[G]$, Euclidean division in $K[X]$ shows that

$$u = (a - \omega^k e)v + \phi_k(u)e$$

for some $v \in K[G]$; therefore $(a - \omega^k e) = \operatorname{Ker} \phi_k$. [This is also clear since $(a - \omega^k e) \subseteq \operatorname{Ker} \phi_k$ and both have dimension $n - 1$.]

We see that ϕ_k is injective on G if and only if ω^k is a primitive nth root of 1; this implies the following result.

LEMMA 2.8. *The prime ideal* $(a - \omega^k e)$ *of* $K[G]$ *separates* G *if and only if* ω^k *is a primitive* n*th root of* 1; *and these ideals are all the prime ideals of* $K[G]$ *that separate* G. ■

For later use, we need a further lemma.

LEMMA 2.9. *For every* $m > 0$, *there exists* $u \in K[G]$ *such that* $e - a = (e - a)^m u$.

Proof. We see that $\phi_k((e - a)^m) = (1 - \omega^k)^m = 0$ if and only if $k = 0$; since 0 is the intersection of all $\operatorname{Ker} \phi_k$, it follows that $(e - a)^m v = 0$ if and only if v lies in the intersection V of all $\operatorname{Ker} \phi_k$ with $0 < k < n$. Since all $\operatorname{Ker} \phi_k$ have dimension $n - 1$ and trivial intersection, we see that V has dimension 1; now the element $v_0 = e + a + \cdots + a^{n-1} \neq 0$ satisfies the equation $(e - a)^m v_0 = 0$; therefore $v = \sum \lambda_i a^i$ is in V (that is, it satisfies the equation $(e - a)^m v = 0$) if and only if it is proportional to v_0, in other words, if and only if $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1}$.

It follows from this that the elements $(e - a)^m a, (e - a)^m a^2, \cdots, (e - a)^m a^{n-1}$ are linearly independent in $K[G]$. Since they all lie in $\operatorname{Ker} \phi_0$, they constitute a basis of $\operatorname{Ker} \phi_0$; therefore $e - a \in \operatorname{Ker} \phi_0$ is a linear combination of $(e - a)^m a, (e - a)^m a^2, \cdots, (e - a)^m a^{n-1}$. ■

3. PRIMARY SEMIGROUPS

1. We saw (Proposition 1.7) that a primary semigroup is either nil or cancellative or subelementary. The criterion in Proposition 1.5 also implies that every subsemigroup of a primary semigroup is primary. We need one more result of general interest:

PROPOSITION 3.1. *Suppose that* $S = C$ *or* $S = N \cup C$ *is cancellative or subelementary. Then* S *is primary if and only if* $C^{-1}S$ *is primary.*

Proof. If $C^{-1}S$ is primary, then so is $S \subseteq C^{-1}S$. Conversely, let $\mathfrak{q}$ be a primary ideal of $R[S]$ that separates S. Let

$$C^{-1}\mathfrak{q} = \{u/c \in C^{-1}R[S]; u \in \mathfrak{q}\};$$

we see that $C^{-1}\mathfrak{q}$ is an ideal of $C^{-1}R[S] \cong R[C^{-1}S]$. Note that $u/c = v/d$ and $u \in \mathfrak{q}$ implies $v \in \mathfrak{q}$; for $cv = du \in \mathfrak{q}$, whereas $c^n \in C$ never lies in $\mathfrak{q}$, since otherwise C, which is separated by $\mathfrak{q}$, would have a zero element. It then follows immediately that $C^{-1}\mathfrak{q}$ is primary. If now $s/c - t/d \in C^{-1}\mathfrak{q}$, where $s, t \in S$, then as above $ds - tc \in \mathfrak{q}$, whence $ds = tc$ and $s/c = t/d$; thus $C^{-1}\mathfrak{q}$ separates $C^{-1}S$. ■ [This is quite similar to Proposition 2.4 and its proof.]

2. We now study separately the three possible kinds of primary semigroups. First:

PROPOSITION 3.2. *A nilsemigroup is primary (relative to each* R).

Proof. If S is a nilsemigroup, with zero element z, consider the ideal Rz of R[S], which evidently separates S. Every $u \in R[S]$ has a power in Rz: if $u = \sum_{i\in I} \lambda_i s_i$, where I is finite, then $s_i^{k_i} = z$ for some k_i, and we see that $u^k \in Rz$ whenever $k \geq \sum k_i$. Hence Rz is (trivially) primary. ■

For the cancellative case, our main result below uses the lemmas at the end of Section 2. and thus we must let R be a field. More precisely:

THEOREM 3.3. *Let* K *be a field of characteristic* 0 *containing all roots of unity. A finitely generated cancellative semigroup* S *is* K*-primary if and only if it is* K*-prime.*

Proof. It follows from Propositions 2.4 and 3.1 that we may assume from the start that S is a finitely generated abelian group G. If G is prime, it is evidently primary; therefore, we assume that G is K-primary but not K-prime, we let $\mathfrak{q}$ be a primary ideal of K[G] that separates G, and we let $\mathfrak{p}$ be its prime radical. Since G is not prime, it follows from Corollary 2.7 (and the remarks preceding Corollary 2.6) that $\mathfrak{p}$ contains a difference $e - a$, where e is the identity element of G and $a \in G$ has finite order. Therefore $(e - a)^m \in \mathfrak{q}$ for some $m > 0$. Applying Lemma 2.9 to the subgroup H of G generated by a, we obtain the relation $e - a = (e - a)^m u$ for some $u \in K[H] \subseteq K[G]$. This implies $e - a \in \mathfrak{q}$, and thus contradicts the hypothesis that $\mathfrak{q}$ separates G. ■

COROLLARY 3.4. *Let* K *be as in Theorem* 3.3, *and let* S *be cancellative. If* S *is* K*-primary, then the torsion part of* G(S) *is locally cyclic.*

Proof. By Proposition 3.1, G(S) is also K-primary. So is every finitely generated subgroup of the torsion part of G(S), which by Proposition 3.3 must then be K-prime and therefore cyclic. ■

3. We now turn to the last case, where S is subelementary. In view of Propositions 3.1 and 1.1, we may in fact let $S = N \cup G$ be elementary (with G a group). If K is as in Theorem 3.3 and S is finitely generated, then G is finitely generated (by Proposition 1.4), and it follows from Corollary 3.4 that the torsion part of G must be cyclic if S is K-primary. The following result gives another condition on S.

LEMMA 3.5. *Let* K *be as in Theorem* 3.3, *and let* $S = N \cup G$ *be an elementary* K*-primary semigroup. Assume* $c \in G$ *satisfies* $cx = x$ *for some* $x \in N \setminus z$. *Then either* $c = e$ *or* c *has infinite order; furthermore, if* $c^n y = y \neq z$ *and* $y \in N$, *then* $cy = y$.

Proof. Let $\mathfrak{q}$ be a primary ideal of K[S] that separates S. Then $cx = x \neq z$ implies $(c - e)x \in \mathfrak{q}$; since $x \neq z$ is not in $\mathfrak{q}$, we see that $(c - e)^m \in \mathfrak{q}$ for some $m > 0$. If c has finite order $(c \neq e)$, then we can apply Lemma 2.9 (to the subgroup of G generated by c) to conclude that $c - e \in \mathfrak{q}$, a contradiction; hence either $c = e$ or c has infinite order. [We shall see that the latter may happen.]

Further, assume $c^n y = y$, where $n > 0$ and $y \in N \setminus z$. We may also assume that $c \neq e$ and that n is the least positive integer such that $c^n y = y$. If H is the subgroup of G generated by c, then $Hy = \{y, cy, \cdots, c^{n-1} y\}$, and these elements are all distinct. Let V be the subspace of K[S] generated by Hy. We turn V into a $K[\mathbb{Z}(n)]$-module, as follows. Let ε and α denote the identity element and a generator of $\mathbb{Z}(n)$. Multiplication by c (in K[S]) induces an automorphism of V, of order n; hence there exists a homomorphism $\phi: \mathbb{Z}(n) \to \mathrm{End}_K(V)$ such that $\phi(\alpha)v = cv$ for all $v \in V$. This in turn extends to an algebra homomorphism $K[\mathbb{Z}(n)] \to \mathrm{End}_K(V)$, which makes V a $K[\mathbb{Z}(n)]$-module; clearly, the module action is given by $\alpha \cdot v = cv$, hence

$$\left(\sum_{i=0}^{n-1} \lambda_i \alpha^i \right) \cdot v = \sum_{i=0}^{n-1} \lambda_i c^i v \qquad \text{for all } v \in V .$$

[It is easy to see that V is free on $\{y\}$, as a $K[\mathbb{Z}(n)]$-module.]

We remember that $(c - e)^m \in \mathfrak{q}$ for some $m > 0$. By Lemma 2.9, we also have the relation $\alpha - \varepsilon = (\alpha - \varepsilon)^m \upsilon$ for some $\upsilon \in K[\mathbb{Z}(n)]$. It follows that

$$cy - y = (\alpha - \varepsilon) \cdot y = \upsilon(\alpha - \varepsilon)^m \cdot y = \upsilon \cdot (c - e)^m y .$$

However, the left action of υ amounts to multiplication by a linear combination of powers of c; because $\mathfrak{q}$ is an ideal, it follows that $cy - y \in \mathfrak{q}$. Therefore $cy = y$. ■

This completes the condition on G given by Proposition 3.4 with a condition on the action of G on N (note that Proposition 3.2 yields no condition on N itself). This condition is simplest to express when G is cyclic. Let a be a generator of G. If G is finite, then $ax = x \neq z$ never happens; similarly, $a^n x = x \neq z$ never happens unless $a^n = e$; it follows that for each $x \neq z$ the orbit of x consists of $x, ax, \cdots, a^{n-1} x$ and these are all distinct; hence every orbit of S (other than $\{z\}$) has n elements. An elementary semigroup with this property was called equisected in [4], but we now prefer to call it *homogeneous*. If G is infinite ($G \cong \mathbb{Z}$), and if $x \neq z$ has finite orbit, then the order of its orbit is the least $n > 0$ with $a^n x = x$; if $y \neq z$ also has a finite orbit of order m, then $(a^n)^m y = y \neq z$, and the second part of the lemma implies (if we take $c = a^n$) that $a^n y = y$ and therefore $m \leq n$. By symmetry, $n \leq m$. Thus, all the finite nonzero orbits of S have the same order. This does not make S homogeneous, since S also contains at least one infinite orbit (namely, G); we say that S is *quasi-homogeneous* if all its finite nonzero orbits have the same order. If G is finite, there is no infinite orbit, and hence quasi-homogeneity is then equivalent to homogeneity.

These homogeneity conditions are interesting because they yield the only sufficient condition we know for primariness:

THEOREM 3.6. *Let* K *be a field of characteristic* 0, *containing all roots of unity, and let* $S = N \cup G$ *be an elementary semigroup in which the group* G *is cyclic. Then* S *is* K*-primary if and only if it is quasi-homogeneous.*

Proof. That this condition is necessary has just been shown (and essentially it follows from Lemma 3.5). The difficult part is the converse. We prove it by distinguishing several cases.

The most trivial case is when G is trivial. Here, Kz is an ideal of K[S], and it clearly separates S. The proof of Proposition 3.2 shows that the radical of Kz is

$K[N] \subseteq K[S]$; clearly, $K[N]$ is a maximal ideal of $K[S]$, and this implies that Kz is primary (a proof of this elementary fact can be found in [3], for example).

In the next cases, a denotes a generator of G. We now consider the case when $G \cong \mathbb{Z}$ is infinite and there is no finite orbit except z. Then the elements $a^n x$ $(n \in \mathbb{Z})$ are all distinct if $x \neq z$. Again we consider the ideal Kz of $K[S]$, which separates S, and whose radical $K[N]$ is a prime ideal of $K[S]$ (but not maximal). To show that Kz is primary, assume that $u, v \in K[S]$ are such that $uv \in Kz$, $u \notin K[N]$, $v \notin Kz$. Then $v \in K[N]$ and

$$u = \lambda z + \sum_{i \in I} \lambda_i x_i + \sum_{j \in \mathbb{Z}} \lambda_j a^j, \qquad v = \mu z + \sum_{k \in L} \mu_k x_k,$$

where all x_i, $x_k \in N \setminus z$, I, L are finite, and the set $\{j: \lambda_j \neq 0\}$ is finite. Since $v \notin Kz$ and $u \notin K[N]$, we see that $L \neq \emptyset$ and $\lambda_j \neq 0$ for some j. Next we select a maximal element x_0 of $\{x_k; k \in L\}$ (under the partial order $x \leq y \iff x \in N^1 y$ on N). Finally, we may assume that the elements x_k are all distinct and that $\mu_k \neq 0$ for all $k \in L$.

It cannot happen that $a^n x_0 = u x_k$ with $u \in N$ (otherwise, $x_0 = (a^{-n}u)x_k < x_k$). Therefore, in the expansion of uv the only terms with $a^n x_0$ come from the terms in a^j of u and the terms in x_k of v. Furthermore, $a^n x_0 = a^j x_k$ implies $x_k = a^m x_0$ for some m ($= n - j$). For each $m \in \mathbb{Z}$, let ν_m denote the coefficient of $a^m x_0$ in v; we see that $\nu_0 \neq 0$ and the set $\{m; \nu_m \neq 0\}$ is finite. Since by hypothesis the elements $a^m x_0$ $(m \in \mathbb{Z})$ are all distinct, it follows from this argument that the coefficient of $a^n x_0$ in uv is $\sum_{j+m=n} \lambda_j \nu_m$. However, $uv \in Kz$, which then implies $\sum_{j+m=n} \lambda_j \nu_m = 0$ for all n. At the same time, there exist a greatest j_0 with $\lambda_{j_0} \neq 0$ and a greatest m_0 with $\nu_{m_0} \neq 0$, and when $n = j_0 + m_0$, we find $\sum_{j+m=n} \lambda_j \nu_m = \lambda_{j_0} \nu_{m_0} \neq 0$. This contradiction shows that Kz is primary, and the theorem is proved in this case.

In the remaining cases, the difficulty is in showing not that the ideal we pick is primary, but that it separates S. We interrupt the proof of the theorem to prove a lemma to be used in all those cases.

LEMMA 3.7. *Let* $\mathfrak{q}$ *be the ideal of* $K[S]$ *generated by* $q_0 \in K[G]$ *and* z. *Then* $\mathfrak{q}$ *separates* S *if and only if*

(i) *the principal ideal* (q_0) *of* $K[G]$ *separates* G;

(ii) *if* $x \in N \setminus z$, $x' \in Gx$, *and* $x' - x = \sum_{y \in Gx} \lambda_y q_0 y$, *then* $x = x'$;

(iii) *when* $x \in N \setminus z$, $x = \sum_{y \in Gx} \lambda_y q_0 y$ *never happens.*

Proof. All three conditions are clearly necessary. For the converse, we note that $K[S] = K[N] \oplus K[G]$ (as K-modules) and for every $u \in K[S]$ we write $u = u' + u''$, where $u' \in K[N]$ and $u'' \in K[G]$. Assume $s - t \in \mathfrak{q}$, where $s, t \in S$, so that $s - t = \lambda z + q_0 u$ for some $\lambda \in K$ and $u \in K[S]$.

If $s, t \in G$, then $s - t = (s - t)'' = q_0 u''$, and it follows from (i) that $s = t$.

If $s \in G$ and $t \in N$, then as above we see that $s = (s - t)'' = q_0 u''$; by (i), this implies that s is a zero element of G, so that G is trivial; but this case has been eliminated; thus it cannot happen that $s \in G$ and $t \in N$.

This leaves the case where $s, t \in N$. Here $s - t = \lambda z + q_0 u'$, so that we may assume that $u = u' \in K[N]$, in which case $u = \sum_{i \in I} \lambda_i x_i$, where $x_i \in N$ and I is finite. Let V be the subspace of $K[N]$ generated by $Gs \cup Gt$, and let W be the subspace generated by all the other orbits in N, so that $K[N] = V \oplus W$. If $x_i \in Gs \cup Gt$, then $q_0 x_i$ is a linear combination of elements of Gx_i and hence $q_0 x_i \in V$; similarly, $x_i \notin Gs \cup Gt$ implies $q_0 x_i \in W$. Also, $s - t \in V$.

If in addition $s, t \neq z$, then $z \in W$, and

$$s - t = \lambda z + q_0 u = \left(\sum_{x_i \in Gs \cup Gt} \lambda_i q_0 x_i \right) + \left(\lambda z + \sum_{x_i \notin Gs \cup Gt} \lambda_i q_0 x_i \right)$$

implies, by the result above, that

$$s - t = \sum_{x_i \in Gs \cup Gt} \lambda_i q_0 x_i \, .$$

If we assume $Gs \neq Gt$, then $Gs \cap Gt = \emptyset$, and we can use a similar argument on the subspaces of V generated by Gs and Gt to deduce from

$$s - t = \left(\sum_{x_i \in Gs} \lambda_i q_0 x_i \right) + \left(\sum_{x_i \in Gt} \lambda_i q_0 x_i \right)$$

that $s = \sum_{x_i \in Gs} \lambda_i q_0 x_i$ (and similarly for t), which by (iii) is impossible. Therefore $Gs = Gt$, so that $t \in Gs$ and $s - t = \sum_{x_i \in Gs} \lambda_i q_0 x_i$, which by (ii) implies $s = t$.

If s and t are not both different from z, then either both are equal to z, which implies $s = t$, or, say, $s \neq z$ and $t = z$. In this case we argue as above, but with V generated by Gs and W generated by all other orbits in N (so that $z \in W$): from the relation

$$s - t = \left(\sum_{x_i \in Gs} \lambda_i q_0 x_i \right) + \left(\lambda z + \sum_{x_i \notin Gs} \lambda_i q_0 x_i \right)$$

we conclude that $s = \sum_{x_i \in Gs} \lambda_i q_0 x_i$, which by (ii) is impossible. ■

We now resume the proof of the theorem, and we consider the third case in this proof, namely that G is cyclic of order $n > 1$. By the hypothesis on S, every nonzero orbit Gx has precisely n elements, namely $x, ax, \cdots, a^{n-1}x$, which must all be distinct. In this case, we let $q_0 = (a - \omega e)^m$, where $m > 0$ and ω is a primitive nth root of 1 in K, and we let $\mathfrak{q}$ be the principal ideal (q_0) of $K[S]$. Since $(1 - \omega)^m z = q_0 z$, we see that $z \in \mathfrak{q}$ and hence our lemma can be applied to $\mathfrak{q}$. [In this case we could let $m = 1$, but the added generality will be useful in the next cases.]

From Section 2 we recall that $a - \omega e$ generates a maximal ideal of $K[G]$. The radical of $\mathfrak{q}$ contains $K[N]$ (since $z \in \mathfrak{q}$) and $a - \omega e$, and hence it is a maximal ideal of $K[S]$. Therefore $\mathfrak{q}$ is primary. To show that $\mathfrak{q}$ separates S, we verify conditions (i), (ii), (iii) of the lemma. That (i) holds follows from Lemma 2.8, since in $K[G]$ we have the relation $(q_0) \subseteq (a - \omega e)$. To prove (ii) and (iii), let $x \in N$ and

$x \neq z$. Since $x, ax, \cdots, a^{n-1}x$ are linearly independent in $K[S]$, we see that $u \in K[G]$, $ux = 0$ implies $u = 0$. Now assume $x' = a^k x \in Gx$ is such that $x' - x = \sum_{i=0}^{n-1} \lambda_i(a - \omega e)^m a^i x$, with $\lambda_i \in K$; then

$$(a^k - e)x = \left(\sum_{i=0}^{n-1} \lambda_i(a - \omega e)^m a^i \right) x;$$

by the argument above, $a^k - e = \sum_{i=0}^{n-1} \lambda_i(a - \omega e)^m a^i$ (since both are in $K[G]$); by (i), $a^k = e$; hence $x' = x$, which proves (ii). Similarly, assume

$$x = \sum_{i=0}^{n-1} \lambda_i(a - \omega e)^m a^i x;$$

again, this implies $e = \sum_{i=0}^{n-1} \lambda_i(a - \omega e)^m a^i$; by (i), e must be a zero element of G; this forces G to be trivial, a contradiction that proves (iii). Thus the theorem is true in this case also.

There remain the cases where $G \cong \mathbb{Z}$ and there are finite nonzero orbits. By the hypothesis on S, these all have the same number n of elements. The fourth case is when $n > 1$. Here we again let $\mathfrak{q}$ be the principal ideal (q_0) of $K[S]$, with $q_0 = (a - \omega e)^m$; but now we require $m > 1$. Again we see that $z \in \mathfrak{q}$ and that $\mathfrak{q}$ is primary. Condition (i) of Lemma 3.7 is proved as follows. Every nonzero element u of $K[G] \cong K[\mathbb{Z}]$ can be uniquely written in the form $u = a^k f(a)$, where $k \in \mathbb{Z}$ and $f \in K[X]$ is a polynomial with nonzero constant coefficient; k is the least power of a that appears in u. If we assume that $a^r - a^s = q_0 u$ for some $u \in K[G]$, with, say, $r > s$, then $a^s(a^{r-s} - e) = a^k(a - \omega e)^m f(a)$, which implies $s = k$ and $X^{r-s} - 1 = (X - \omega)^m f(X)$ in $K[X]$. The latter equality is impossible, since K has characteristic 0 and hence no $X^t - 1$ has multiple roots in K. Therefore (i) holds.

Let $x \in N$ and $x \neq z$. In case the orbit of x is infinite, the elements $a^k x$ ($k \in \mathbb{Z}$) are pairwise distinct, and as above we see that $u \in K[G]$ and $ux = 0$ implies $u = 0$. The proof of (ii) and (iii) is then the same as in the third case (we use (i)). Now assume that the orbit of x is finite; then it consists of $x, ax, \cdots, a^{n-1}x$, and these are all distinct. We make the subspace V of $K[S]$ generated by Gx into a $K[\mathbb{Z}(n)]$-module, exactly as in the proof of Lemma 2.9, with $\alpha \cdot v = av$ for all $v \in V$ (where α is the generator of $\mathbb{Z}(n)$). Again we see that $\upsilon \in K[\mathbb{Z}(n)]$ and $\upsilon \cdot x = 0$ implies $\upsilon = 0$. Because the principal ideal $((\alpha - \omega\varepsilon)^m) \subseteq (\alpha - \omega\varepsilon)$ of $K[\mathbb{Z}(n)]$ separates $\mathbb{Z}(n)$, by Lemma 2.8, we can again prove (ii) and (iii) exactly as in the third case, replacing a by α and e by ε, and using the module action, whenever necessary.

The fifth and last case to consider for the theorem is the case where $G \cong \mathbb{Z}$ and the finite orbits in N all have only one element. In this case, we let $\mathfrak{q}$ be generated by $q_0 = (a - e)^m$ (where $m > 1$) and z; we must include z, since this time $q_0 z = 0$. The verification that $\mathfrak{q}$ is primary and that (i) holds is carried out as in the fourth case; the same is true of (ii) and (iii) in case x has infinite orbit. If now $x \in N \setminus z$ has finite orbit, then (ii) is trivial. For (iii), we note that when x has trivial orbit, $ax = x = ex$ and hence $q_0 x = 0$; hence $x = \sum_{y \in Gx} \lambda_y q_0 y$; that is, $x = \lambda q_0 x$ is clearly impossible. ■

4. Unfortunately, the author has found no way to extend this theorem to the case where, say, G is finitely generated. It is clear that the previous proof is articulated around the possible actions of G on each orbit, and these are not so easily dealt with if G is not cyclic.

As it stands, Theorem 3.6 still gives a complete characterization of finite primary semigroups:

COROLLARY 3.8. *Let* K *be a field of characteristic* 0 *containing all* n*th roots of unity, and let* S *be a finite semigroup. Then* S *is* K-*primary if and only if it is either a nilsemigroup or a cyclic group or a homogeneous elementary semigroup with cyclic group of units.*

Proof. A finite cancellative (subelementary) semigroup must be a group (be elementary), and hence the direct part follows from Proposition 1.7, Corollary 3.4, and Lemma 3.5 (and the remarks preceding Theorem 3.6). The converse follows from Proposition 3.2 and Theorems 3.3 and 3.6. ■

REFERENCES

1. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*. Vol. I. Mathematical Surveys, No. 7. Amer. Math. Soc., Providence, R.I., 1961.

2. I. G. Connell, *On the group ring*. Canad. J. Math. 15 (1963), 650-685.

3. P. Dubreil and M. L. Dubreil-Jacotin, *Leçons d' algèbre moderne*. Deuxième édition. Dunod, Paris, 1964.

4. P. A. Grillet, *Primary semigroups*. Semigroup Forum 4 (1972), 237-241.

5. ———, *Subdirect decompositions of finitely generated commutative semigroups*. Semigroup Forum 4 (1972), 242-247.

6. ———, *A completion theorem for finitely generated commutative semigroups*. J. Algebra (to appear).

7. S. Lang, *Algebra*. Addison-Wesley, Reading, Mass., 1965.

8. P. Lefebvre, *Sur les demi-groupes de fractions*. C. R. Acad. Sci. Paris Sér. A-B 265 (1967), A329-A332.

9. I. S. Ponizovskiĭ, *A remark on commutative semigroups*. (Russian) Dokl. Akad. Nauk SSSR 142 (1962), 1258-1260.

Tulane University
New Orleans, Louisiana 70118