CANCELLATION IN PRIMELY GENERATED REFINEMENT MONOIDS

GARY BROOKFIELD

Abstract. We prove that any primely generated refinement monoid M has separative cancellation, and even strong separative cancellation provided M has no nonzero idempotents. A form of multiplicative cancellation also holds: $na \leq nb$ implies $a \leq b$ for $a, b \in M$ and $n \in \{1, 2, 3, \dots\}$. In addition, M is a semilattice in the sense that, given $c_1, c_2 \in M$, there is an element $d \in M$ such that $c_1, c_2 \leq d$ and, for all $a \in M$, $c_1, c_2 \leq a$ implies $d \leq a$. Finally, we prove that any finitely generated refinement monoid is primely generated; in fact, this holds for any refinement monoid with a set of generators satisfying the descending chain condition.

1. Introduction

In recent years there has been an increasing recognition that certain questions arising in module theory can be usefully reformulated and generalized as questions about the cancellation properties of refinement monoids. Before giving examples of this we define the relevant monoid properties: A commutative monoid M has **refinement** (2.2) if the equation $a_1 + a_2 = b_1 + b_2$ in M implies the existence of $c_{11}, c_{12}, c_{21}, c_{22} \in M$ such that $a_1 = c_{11} + c_{12}$, $a_2 = c_{21} + c_{22}$, $b_1 = c_{11} + c_{21}$, and $b_2 = c_{12} + c_{22}$. There are many cancellation properties that we will discuss in this paper. Two of these are **separativity**: $(\forall a, b \in M)$ $(2a = a + b = 2b \implies a = b)$; and **strong separativity**: $(\forall a, b \in M)$ $(2a = a + b \implies a = b)$.

The clearest example of this use of refinement monoids in module theory appears in the work of P. Ara, K. R. Goodearl, K. C. O'Meara and E. Pardo [1] on exchange rings: For a ring R let R-**Proj** be the category of finitely generated projective left R-modules, and for $P \in R$-**Proj**, let $\langle P \rangle$ be the isomorphism class containing P. Let $V(R)$ be the set of isomorphism classes with operation $+$ induced from the direct sum, that is, $\langle P_1 \rangle + \langle P_2 \rangle = \langle P_1 \oplus P_2 \rangle$ for all $P_1, P_2 \in V(R)$. Then $V(R)$ is an commutative monoid. If R is an exchange ring (see [1, Section 1] for the definition), then $V(R)$ has refinement. Examples of exchange rings are (Von Neumann) regular rings, semiregular rings, and C^*-algebras of real rank 0.

Many important open questions about exchange rings have been reduced to the single (unresolved) question: Is $V(R)$ separative? Thus a module theoretic problem has been reduced to a question about cancellation in refinement monoids.

To discuss the second example of a refinement monoid arising in module theory, we need more definitions: For a monoid M, let $\leq$ be the preorder (2.1) on M defined by $a \leq b$ if and only if there exists $c \in M$ such that $a + c = b$. An element

Date: Oct 28, 2000.
1991 *Mathematics Subject Classification.* Primary 20M14, 20M10; Secondary 06F05.

$p \in M$ is **prime** (2.6) if for all $a_1, a_2 \in M$, $p \leq a_1 + a_2$ implies $p \leq a_1$ or $p \leq a_2$. A monoid is **primely generated** if each of its elements is a sum of primes.

The second example comes from the study of the extensional structure of module categories [2], [3], [4]. The monoid in question, $M(\mathcal{S})$, is defined for any Serre subcategory $\mathcal{S}$ of left R-modules, and has the universal property that any map from $\mathcal{S}$ to a commutative monoid which respects short exact sequences, factors through $M(\mathcal{S})$. As a consequence of the Schreier refinement theorem, $M(\mathcal{S})$ is a refinement monoid. For the details of this construction see, in particular, Section 3 of [3].

Suppose R is commutative Noetherian (or more generally, fully bounded Noetherian), and R-**Noeth** is the Serre subcategory consisting of all Noetherian R-modules. Then $M(R\text{-}\mathbf{Noeth})$ is a primely generated refinement monoid. (In fact, in this case, $M(R\text{-}\mathbf{Noeth})$ is Artinian (6.1) [2, 19.6].)

The module theory part of this claim about $M(R\text{-}\mathbf{Noeth})$ will be developed in a subsequent paper. The purpose of the current paper is to show that refinement monoids which are primely generated have a lot of structure regardless of how they arise.

We will prove, for example, that a primely generated refinement monoid M is separative, and is strongly separative if $2e = e$ in M implies that $e = 0$ (4.5). Also, M has the multiplicative cancellation property (5.11(5)) that $na \leq nb$ implies $a \leq b$ for all $a, b \in M$ and $n \in \mathbb{N} = \{1, 2, 3, \dots\}$. In addition, M is a semilattice (5.16) in the sense that, given $c_1, c_2 \in M$, there is an element $d \in M$ such that $c_1, c_2 \leq d$ and, for all $a \in M$, $c_1, c_2 \leq a$ implies $d \leq a$. These cancellation properties are summarized in 5.19.

We will also show that, if M is cancellative, it has a very simple structure: It must be the direct product of an Abelian group and a free commutative monoid (5.14). Other properties of such monoids appear in Sections 4 and 5.

In Section 6 of the paper we show that any refinement monoid whose generators satisfy the descending chain condition relative to the preorder $\leq$ is primely generated (6.7). In particular, this means that any finitely generated refinement monoid is primely generated, and hence has all of the properties described above.

It should be pointed out that, in general, refinement monoids need not have any of these cancellation properties. This is a consequence of the fact that any commutative monoid can be embedded in a refinement monoid [11], [6, 5.1], [19]. Thus, for example, the non-separative non-refinement monoid $\{0, 1, \infty\}$ of 3.2(2) can be embedded in a refinement monoid which is not separative. From the results of this paper such a non-separative refinement monoid cannot be finitely generated, or more generally, be primely generated. For the question about exchange rings, this provides in a sense a "lower bound" on the complexity of any $V(R)$ which is not separative.

The author thanks Ken Goodearl and Fred Wehrung for their helpful comments during the preparation of this paper.

2. Definitions

All monoids and semigroups in this paper will be commutative, so we will write $+$ for the operation and 0 for the identity element unless this conflicts with existing notation. We refer the reader to [13] and [14] for the standard concepts of monoid theory.

We collect here some notation we will need:

Notation 2.1. *Let M be a monoid and $a, b \in M$.*

- $a \leq b \iff \exists\, c \in M$ *such that* $a + c = b$
- $a \ll b \iff a + b \leq b$
- $a \equiv b \iff a \leq b$ *and* $b \leq a$
- $\{\equiv a\} = \{c \in M \mid c \equiv a\}$
- $a \propto b \iff \exists\, n \in \mathbb{N}$ *such that* $a \leq nb$
- $\{\propto a\} = \{c \in M \mid c \propto a\}$
- $a \asymp b \iff b \propto a \propto b$
- $\{\asymp a\} = \{c \in M \mid c \asymp a\}$

The relation $\leq$ is a preorder on M. (This would not be true if M were merely a semigroup. Without an identity element, $\leq$ need not be reflexive.) For the monoid $(\mathbb{Z}^+, +)$, the set of nonnegative integers, this preorder coincides with the usual order. For the monoid $(\mathbb{Z}, +)$ we have $m \leq n$ for all $m, n \in \mathbb{Z}$. So, for $\mathbb{Z}$, the preorder $\leq$ is not the same as the usual order on the integers.

The relation $\ll$ is transitive, $\propto$ is a preorder, and $\equiv$ and $\asymp$ are congruences. The set $\{\propto a\}$ is a submonoid and $\{\asymp a\}$ is a subsemigroup of M.

Definition 2.2. *Let M be a monoid.*

(1) *M has* **refinement** [17], [6], [7], [18] *if for all $a_1, a_2, b_1, b_2 \in M$ with $a_1 + a_2 = b_1 + b_2$, there exist $c_{11}, c_{12}, c_{21}, c_{22} \in M$ such that*

$$a_1 = c_{11} + c_{12} \qquad a_2 = c_{21} + c_{22}$$
$$b_1 = c_{11} + c_{21} \qquad b_2 = c_{12} + c_{22}.$$

(2) *M has* **decomposition** *if for all $a, b_1, b_2 \in M$ with $a \leq b_1 + b_2$ there exist $a_1, a_2 \in M$ such that $a_1 \leq b_1$, $a_2 \leq b_2$ and $a = a_1 + a_2$.*

It is easy to check that for a monoid M,

$$M \text{ has refinement} \implies M \text{ has decomposition.}$$

Example 3.2(2) shows that the converse is not true.

A simple induction shows that the refinement property extends to equations involving sums of more than two elements: If $a_1 + a_2 + \ldots + a_m = b_1 + b_2 + \ldots + b_n$ in a refinement monoid, then there are c_{ij} such that $a_i = \sum_j c_{ij}$ and $b_j = \sum_i c_{ij}$.

It is convenient to record refinements using matrices. The refinement of $a_1 + a_2 = b_1 + b_2$ from the definition would be written

$$\begin{array}{c} \\ a_1 \\ a_2 \end{array} \begin{array}{c} \begin{array}{cc} b_1 & b_2 \end{array} \\ \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \end{array}.$$

This means that the sum of the entries in each row (column) equals the entry labeling the row (column).

Definition 2.3. *Let M be a semigroup.*

(1) *M is* **cancellative** *if for all $a, b, c \in M$, $a + c = b + c$ implies $a = b$.*
(2) *M is* **strongly separative** [1], [3, 2.3] *if for all $a, b \in M$, $2a = a + b$ implies $a = b$.*
(3) *M is* **separative** [5, Chapter 4.3] *if for all $a, b \in M$, $2a = a + b = 2b$ implies $a = b$.*

Obviously, for a semigroup M we have the implications

$$M \text{ cancellative} \implies M \text{ strongly separative} \implies M \text{ separative}.$$

We should mention one simple but extremely useful fact which will be used without comment throughout this paper: If a, b, c, d are elements of a monoid M such that $a + c = b + c$ and $c \leq d$, then $a + d = b + d$. In particular, if $c \leq a$ then $2a = a + b$, and if $c \leq a, b$ then $2a = a + b = 2b$.

The next two lemmas give conditions which are equivalent to separativity and strong separativity. The proofs are easy.

Lemma 2.4. [1, 2.1], [2, 8.10] *For a decomposition monoid M, the following are equivalent:*

(1) *M is separative.*
(2) $(\forall a, b, c \in M)$ $((a + c = b + c$ *and* $c \propto a, b) \implies a = b)$
(3) $(\forall a \in M)$ $(\{\asymp a\}$ *is cancellative*$)$
(4) $(\forall a, b \in M)(\forall m, n \in \mathbb{N})$ $((ma = mb$ *and* $na = nb) \implies$
$(ka = kb$ *where* $k = \gcd(m, n)))$
(5) $(\forall a, b, c \in M)(\forall n \in \mathbb{N})$ $(a + nc = b + nc \implies a + c = b + c)$
(6) $(\forall a, b, c \in M)$ $((a + c = b + c$ *and* $c \leq a, b) \implies a = b)$

Items 1-4 of this lemma are, in fact, equivalent even when M does not have decomposition.

Lemma 2.5. [3, 2.3] *For a monoid M, the following are equivalent:*

(1) *M is strongly separative.*
(2) $(\forall a, b, c \in M)$ $((a + c = b + c$ *and* $c \leq a) \implies a = b)$
(3) $(\forall a, b, c \in M)(\forall n \in \mathbb{N})$ $(a + (n + 1)c = b + nc \implies a + c = b)$

Definition 2.6. *Let M be a monoid and $p \in M$.*

(1) *p is* **prime** *if for all $a_1, a_2 \in M$, $p \leq a_1 + a_2$ implies $p \leq a_1$ or $p \leq a_2$.*
(2) *p is* **proper** *if $p \not\leq 0$.*
(3) *p is* **regular** *if $2p \leq p$ (equivalently, $2p \equiv p$ or $p \ll p$).*
(4) *p is* **idempotent** *if $2p = p$.*
(5) *p is* **free** *if for all $m, n \in \mathbb{N}$, $mp \leq np$ implies $m \leq n$.*

An element $a \in M$ is **primely generated** *if it is the sum of prime elements of M. The monoid itself is* **primely generated** *if all its elements are primely generated.*

Notice that, by this definition, any element $p \leq 0$ is prime. Also, if $p \equiv q$, then p is prime (regular, free, proper) if and only if q is prime (regular, free, proper). Evidently, a free element is not regular and vice versa, but, in general, a monoid may have elements which are neither as in 3.2(2).

Every idempotent is regular, and every regular element is associated with a unique idempotent by the following lemma.

Lemma 2.7. *If q is a regular element in a monoid, then there is a unique idempotent e in $\{\equiv q\}$, and $\{\equiv q\} = \{\equiv e\}$ is an Abelian group with identity e.*

Proof. Since $2q \leq q$, there is some $s \in M$ such that $2q + s = q$. Set $e = q + s$. It is then routine to confirm that e is the unique idempotent in $\{\equiv q\}$ and that the remaining claims are true. $\square$

We see from this lemma that every regular element in a monoid is associated with an Abelian group. We will actually be able to associate a group with any element of any monoid as follows.

Definition 2.8. *Let u be an element of a monoid M. Define a congruence $\sim_u$ on M by*

$$a \sim_u b \iff u + a = u + b$$

for $a, b \in M$. We will write $[a]_u$ for the $\sim_u$-congruence class containing $a \in M$. Define $G_u = \{[a]_u \mid a \ll u\}$. One can easily show that G_u is the set of all units (invertible elements) of the quotient monoid $M/\sim_u$ and so is an Abelian group.

The following facts about G_u are easy to check:

Lemma 2.9. *Let u, v, e be elements of a monoid M.*

1. *If $v \equiv u$, then $\sim_v$ and $\sim_u$ coincide. In particular, $G_u = G_v$.*
2. *The map $\Omega\colon G_u \to \{\equiv u\}$ defined by $\Omega([x]_u) = u + x$ is a bijection (but not in general a homomorphism). If we define the operation $\Box_u$ on $\{\equiv u\}$ by $a \Box_u b = u + x + y$ where $a = u + x$ and $b = u + y$, then the set $\{\equiv u\}$ with operation $\Box_u$ is a group isomorphic to G_u, with identity u.*
3. *If $e \in M$ is an idempotent, then the operation $\Box_e$ coincides with $+$ on $\{\equiv e\}$, and the map $\Omega\colon G_e \to \{\equiv e\}$ is a group isomorphism.*

From 2, we see that we could have defined G_u to be $(\{\equiv u\}, \Box_u, u)$. The advantage of this is that the elements of the group are then elements of M, rather than congruence classes. The disadvantage is that if $v \equiv u$, then we have $G_u = G_v$ as sets, but the operations $\Box_u$ and $\Box_v$ are, in general, different.

3. Examples

This section provides some examples and special cases of monoids having some of the properties defined previously, and also illustrates the complex relationships between these properties.

Example 3.1. *Let $\mathbb{Z}^*$ be the set of nonzero integers with multiplication as monoid operation. $\mathbb{Z}^*$ is a cancellative refinement monoid for which 1 is the identity element. (Here we must deviate from our convention of additive notation.) The monoid preorder $\leq$ becomes divisibility: ($a \leq b \iff a \mid b$). The only regular elements are 1 and -1. All other elements are free. 1 is the only idempotent. The numbers $\pm 1, \pm 2, \pm 3, \pm 5, \pm 7, \ldots$ are the prime elements. For every element $a \in \mathbb{Z}^*$ we have $G_a \cong \mathbb{Z}/2\mathbb{Z}$.*

Example 3.2.

1. *We will write $\{0, \infty\}$ for the monoid such that $\infty + \infty = \infty$. This is a primely generated refinement monoid which is separative but not strongly separative.*
2. *The monoid $\{0, 1, \infty\}$, where $1 + 1 = 1 + \infty = \infty + \infty = \infty$, has decomposition but not refinement since the equation $1 + 1 = \infty + \infty$ cannot be refined. The defining equation shows that this monoid is not separative. The elements 0 and 1 are prime, so this monoid is primely generated. The element 1 is neither free nor regular.*

The following result is well known. Since its simple proof does not appear elsewhere in print (except perhaps in [8, 2.1] where it is applied to partially ordered Abelian groups) we include it here.

Theorem 3.3. *Let M be a cancellative monoid. Then M has decomposition if and only if it has refinement.*

Proof. Suppose that M has decomposition and there are $a_1, a_2, b_1, b_2 \in M$ such that $a_1+a_2 = b_1+b_2$. Since $a_1 \leq b_1+b_2$, there are $c_{11}, c_{12} \in M$ such that $a_1 = c_{11}+c_{12}$, $c_{11} \leq b_1$ and $c_{12} \leq b_2$. From the inequalities there are c_{21}, c_{22} such that $b_1 = c_{11}+c_{21}$ and $b_2 = c_{12}+c_{22}$. Now we have $a_1+a_2 = b_1+b_2 = c_{11}+c_{21}+c_{12}+c_{22} = a_1+c_{21}+c_{22}$, so cancellation of a_1 gives $a_2 = c_{21} + c_{22}$. Thus we have constructed a refinement of the original equation. □

Example 3.4. *Let $(M, +, 0)$ be an Abelian group. It is easy to see that $a \leq b$ for all $a, b \in M$, and so, in particular, all elements of M are regular primes. This monoid is trivially a decomposition monoid. Since M is cancellative, it is also a refinement monoid. For any element $a \in M$, $G_a \cong M$.*

The above example shows that any theorem that applies to primely generated refinement monoids also applies to Abelian groups. Thus, for example, we will not get cancellation of the form $2a = 2b \implies a = b$ for primely generated refinement monoids, since this is not true for Abelian groups. The fact that Abelian groups have refinement is also a trivial consequence of the next theorem:

Theorem 3.5. *Let M be a monoid such that $(\forall a, b \in M)$ $(a \leq b$ or $b \leq a)$. Then M is separative if and only if M has refinement.*

Proof. Suppose M is separative and we have $a_1 + a_2 = b_1 + b_2$ in M. Using the hypothesis on $\leq$ we can, without loss of generality, assume that $a_1 \leq a_2, b_1, b_2$. In particular, $b_1 = a_1 + x_1$ for some $x_1 \in M$. Thus we have the equation $a_2 + a_1 = (b_2+x_1)+a_1$ with $a_1 \leq a_2, b_2+x_1$. This implies that $2a_2 = a_2+(b_2+x_1) = 2(b_2+x_1)$. Since M is separative, we have $a_2 = b_2 + x_1$ and then

$$\begin{array}{c c} & \begin{matrix} b_1 & b_2 \end{matrix} \\ \begin{matrix} a_1 \\ a_2 \end{matrix} & \begin{pmatrix} a_1 & 0 \\ x_1 & b_2 \end{pmatrix} \end{array}$$

is a refinement of the original equation.

For the converse, we show that $((a + c = b + c \text{ and } c \leq a, b) \implies a = b)$ for $a, b, c \in M$. Since M has refinement, this property is equivalent to separativity (2.4).

We make a refinement of the equation $a + c = b + c$:

$$\begin{array}{c c} & \begin{matrix} b & c \end{matrix} \\ \begin{matrix} a \\ c \end{matrix} & \begin{pmatrix} d_1 & a_1 \\ b_1 & c_1 \end{pmatrix} \end{array}$$

Without loss of generality, we can assume $a_1 \leq b_1$ and hence $b_1 = a_1 + x_1$ for some $x_1 \in M$. We now have $c = c_1 + b_1 = c_1 + a_1 + x_1 = c + x_1$, and, since $c \leq a$, this implies $a = a + x_1$. Finally $b = d_1 + b_1 = d_1 + a_1 + x_1 = a + x_1 = a$. □

The monoids $\mathbb{Z}^+$ and $\mathbb{R}^+$ (the nonnegative real numbers) are totally ordered by $\leq$ and are cancellative, so by the theorem they are refinement monoids.

We now consider examples of monoids which are, in a sense, as far from cancellative as possible: A poset $\mathcal{L}$ is a **semilattice** if for each pair of elements, $a, b \in \mathcal{L}$, the supremum $a \vee b$ exists. A semilattice $\mathcal{L}$ which has a minimum element 0 is called a 0-**semilattice**. In this case, $(\mathcal{L}, \vee, 0)$ is a monoid in which all elements are idempotent.

Conversely [12, 1.3.2], if M is a monoid in which all elements are idempotent, then

$$(\forall a, b \in M)\ (a \leq b \iff a + b = b \iff a \ll b),$$

and $(M, \leq)$ is a 0-semilattice with minimum element 0 in which $+$ and $\vee$ coincide. Though 0-semilattices are not cancellative or strongly separative, they are trivially separative.

The following result is well known [7], [9], but since its proof does not appear elsewhere in print we include it here.

Theorem 3.6. *Let M be a 0-semilattice. Then M has decomposition if and only if it has refinement.*

Proof. Suppose that M has decomposition and there are $a_1, a_2, b_1, b_2 \in M$ such that $a_1 + a_2 = b_1 + b_2$. Since $a_1, a_2 \leq b_1 + b_2$, there are $c_{11}, c_{12}, c_{21}, c_{22} \in M$ such that $a_1 = c_{11} + c_{12}$, $a_2 = c_{21} + c_{22}$, $c_{11}, c_{21} \leq b_1$ and $c_{12}, c_{22} \leq b_2$. Similarly, there are $d_{11}, d_{12}, d_{21}, d_{22} \in M$ such that $b_1 = d_{11} + d_{21}$, $b_2 = d_{12} + d_{22}$, $d_{11}, d_{12} \leq a_1$ and $d_{21}, d_{22} \leq a_2$. It is then easy to check that

$$\begin{array}{c} \\ a_1 \\ a_2 \end{array} \begin{array}{c} \begin{array}{cc} b_1 & \qquad\qquad b_2 \end{array} \\ \begin{pmatrix} c_{11} + d_{11} & c_{12} + d_{12} \\ c_{21} + d_{21} & c_{22} + d_{22} \end{pmatrix} \end{array}$$

is a refinement of the original equation.

We confirm this for a_1: We have $a_1 \leq a_1 + d_{11} + d_{12} = c_{11} + d_{11} + c_{12} + d_{12} \leq 4a_1 = a_1$. Since $\leq$ is a partial order, this implies $c_{11} + d_{11} + c_{12} + d_{12} = a_1$. □

In semilattice theory the decomposition property is called distributivity because a lattice $(\mathcal{L}, \vee, \wedge)$ is distributive if and only if the semilattice $(\mathcal{L}, \vee)$ has decomposition. See [10, p. 99]. An element a in a semilattice $(\mathcal{L}, \vee)$ is **irreducible** if $a = b_1 \vee b_2$ implies $a = b_1$ or $a = b_2$ for all $b_1, b_2 \in \mathcal{L}$. One easily checks that in a decomposition 0-semilattice, an element is irreducible if and only if it is prime. The monoid $\{0, \infty\}$ is a simple example of a primely generated refinement 0-semilattice.

4. Cancellation I

In this section we consider the cancellation properties of a primely generated refinement monoid M. We have seen that M could be a 0-semilattice and hence far from cancellative. We will also see that, if M is cancellative, then M has a very special structure (5.14). So it is perhaps surprising that an arbitrary primely generated refinement monoid has any cancellation properties at all.

To make clear what properties are possible, suppose that we have the equation $a + c = b + c$ in M, and hence also a refinement matrix

$$\begin{array}{c} \\ a \\ c \end{array} \begin{array}{c} \begin{array}{cc} b & c \end{array} \\ \begin{pmatrix} d_1 & a_1 \\ b_1 & c_1 \end{pmatrix} \end{array}$$

Consider the following conditions that the entries of the matrix might satisfy:

A. $a_1 = b_1 = 0$
B. $c = c_1$
C. $c \equiv c_1$

Trivially A $\implies$ B $\implies$ C. Condition A occurs if and only if c cancels from the original equation to give $a = b$. For cancellative monoids B is equivalent to A, but B is attainable for 0-semilattices too: Given the refinement matrix as above, we have $c_1 \leq c$, and so $c_1 + c = c$ and $a_1 + c = a_1 + c_1 + c = 2c = c$. Similarly $b_1 + c = c$. Consequently the entry c_1 in the refinement matrix can simply be replaced by c to yield a refinement matrix satisfying B.

Thus B is a good candidate for a cancellation rule which allows M to be a 0-semilattice. What actually occurs for primely generated refinement monoids is C as the next theorem shows.

Theorem 4.1. *Let M be a refinement monoid, $a, b, c \in M$ with c primely generated. If $a + c = b + c$, then there is a refinement matrix*

$$\begin{array}{c} \\ a \\ c \end{array} \begin{array}{c} \begin{array}{cc} b & c \end{array} \\ \begin{pmatrix} d_1 & a_1 \\ b_1 & c_1 \end{pmatrix} \end{array}$$

with $c \leq c_1$.

Proof. Let $\mathcal{C}$ be the class of all elements $c \in M$ such that $a + c = b + c$ implies the existence of a refinement as above. Clearly $0 \in \mathcal{C}$. We will show that if $c \in \mathcal{C}$ and $p \in M$ is prime, then $c + p \in \mathcal{C}$.

Suppose we have $a + c + p = b + c + p$ for some $c \in \mathcal{C}$ and prime p. Since $c \in \mathcal{C}$, there is a refinement

$$\begin{array}{c} \\ a+p \\ c \end{array} \begin{array}{c} \begin{array}{cc} b+p & c \end{array} \\ \begin{pmatrix} d' & a' \\ b' & c_1 \end{pmatrix} \end{array}$$

with $c \leq c_1$. Refining the equation $b + p = d' + b'$ and then refining the resulting equation involving $a + p$ we get a new refinement matrix, still with c_1 as an entry:

$$\begin{array}{c} \\ a \\ p \\ c \end{array} \begin{array}{c} \begin{array}{ccc} b & p & c \end{array} \\ \begin{pmatrix} d_2 & a_2 & a_3 \\ b_2 & p_1 & p_2 \\ b_3 & p_3 & c_1 \end{pmatrix} \end{array}$$

Note that $p = b_2 + p_1 + p_2 = a_2 + p_1 + p_3$. Now we consider two cases:

- If $p \leq p_1$ or $p \leq p_2$ or $p \leq p_3$, then $c + p \leq c_1 + p_1 + p_2 + p_3$ and

$$\begin{array}{c} \\ a \\ c+p \end{array} \begin{array}{c} \begin{array}{cc} b & c+p \end{array} \\ \begin{pmatrix} d_2 & a_2 + a_3 \\ b_2 + b_3 & c_1 + p_1 + p_2 + p_3 \end{pmatrix} \end{array}$$

  is a refinement of the form we seek.
- If $p \not\leq p_1$ and $p \not\leq p_2$ and $p \not\leq p_3$, then since p is prime we must have $p \leq a_2$ and $p \leq b_2$. Hence $a_2 = p + a_4$ and $b_2 = p + b_4$ for some $a_4, b_4 \in M$, and

$$\begin{array}{c} \\ a \\ c+p \end{array} \begin{array}{c} \begin{array}{cc} b & c+p \end{array} \\ \begin{pmatrix} d_2 + p & a_3 + a_4 \\ b_3 + b_4 & p + c_1 + p_1 + p_2 + p_3 \end{pmatrix} \end{array}$$

  is a refinement of the form we seek.

We have shown therefore that $c + p \in \mathcal{C}$, and by induction, that any primely generated element is in $\mathcal{C}$. $\square$

Corollary 4.2. *Let M be a refinement monoid and $a, b, b_1, b_2, c, c_1, c_2 \in M$ with c, c_1, c_2 primely generated.*

(1) $a + c \leq b + c \implies (\exists a_1 \ll c \text{ such that } a \leq b + a_1)$
(2) $a \ll c_1 + c_2 \implies (\exists a_1, a_2 \text{ such that } a = a_1 + a_2,\ a_1 \ll c_1 \text{ and } a_2 \ll c_2)$
(3) $a \equiv c_1 + c_2 \implies (\exists a_1, a_2 \text{ such that } a = a_1 + a_2,\ a_1 \equiv c_1 \text{ and } a_2 \equiv c_2)$
(4) $a \equiv c \implies a$ *is primely generated*
(5) $c \leq a \leq c + b_1, c + b_2 \implies (\exists b \leq b_1, b_2 \text{ such that } a \equiv c + b)$

Proof.

(1) There is some $x \in M$ such that $a + x + c = b + c$, and then, from 4.1, a refinement matrix

$$\begin{array}{c} \\ a+x \\ c \end{array} \begin{array}{c} \begin{array}{cc} b & c \end{array} \\ \begin{pmatrix} d_1 & a_1 \\ b_1 & c_1 \end{pmatrix} \end{array}$$

with $c \leq c_1$. This implies $a \leq a + x = d_1 + a_1 \leq b + a_1$ with $a_1 \ll c$.

(2) We have $a + c_1 + c_2 \leq c_1 + c_2$. Using 1, there is some $a_2' \ll c_2$ such that $a + c_1 \leq c_1 + a_2'$. Using 1 again, there is some $a_1' \ll c_1$ such that $a \leq a_1' + a_2'$. Decomposing this last inequality, there are $a_1 \leq a_1' \ll c_1$ and $a_2 \leq a_2' \ll c_2$ such that $a = a_1 + a_2$.

(3) We have $c_1 + c_2 \leq a$ so there is some u such that $c_1 + c_2 + u = a \leq c_1 + c_2$. Since $u \ll c_1 + c_2$, by 2, there are u_1, u_2 with $u = u_1 + u_2$, $u_1 \ll c_1$ and $u_2 \ll c_2$. Set $a_1 = c_1 + u_1 \equiv c_1$ and $a_2 = c_2 + u_2 \equiv c_2$, then $a = a_1 + a_2$.

(4) Let $c = p_1 + p_2 + \ldots + p_N$ where $p_1, p_2, \ldots, p_N$ are primes. Using 3 inductively one sees that a can be written $a = p_1' + p_2' + \ldots + p_N'$ where $p_i' \equiv p_i$ for $i = 1, 2, \ldots, N$. Thus a is primely generated.

(5) Let x be such that $a = c + x$. We then have $c + x \leq c + b_1, c + b_2$ so from 1, there are $a_1, a_2 \ll c$ such that $x \leq b_1 + a_1, b_2 + a_2$. Using decomposition, there are $b' \leq b_1$ and $a_3 \leq a_1$ such that $x = b' + a_3$. Since $b' \leq x \leq b_2 + a_2$, there are $b \leq b_2$ and $a_4 \leq a_2$ such that $b' = b + a_4$. We now have $x = b + a_3 + a_4$ with $b \leq b' \leq b_1$, $b \leq b_2$ and $a_3 + a_4 \leq a_1 + a_2 \ll c$. From the last inequality we get $c \equiv c + a_3 + a_4$. Adding b to this yields $b + c \equiv b + c + a_3 + a_4 = c + x = a$.

□

Item 4 of this corollary will be strengthened in 5.18(3).
The cancellation property of item 1,

$$(a + c \leq b + c \implies (\exists a_1 \ll c \text{ such that } a \leq b + a_1)),$$

is called **pseudo-cancellation** by F. Wehrung [18], [19], [20]. Note that claims 2,3 and 5 of this corollary follow from it and decomposition.

We next consider the cancellation of a from the equation $2a = a + b$ in a monoid M. If the monoid has nonzero idempotents, $2a = a + b$ need not imply $a = b$. To see this, suppose $e = 2e \in M$ is an idempotent and $b \in M$ is any element such that $e \not\leq b$, then setting $a = b + e$ we get $2a = a + b$ but $a \neq b$. The next theorem is a generalization of the fact that, for a primely generated refinement monoid, this is the only way that cancellation fails for the equation $2a = a + b$.

Theorem 4.3. *Let M be a refinement monoid and $a, b, c, d \in M$ with c primely generated. If $a + d = b + d$ and $d \propto c \propto a$, then there is a primely generated idempotent $e \in M$ such that $a = b + e$.*

Proof. Since $d \propto c$, there is some $n \in \mathbb{N}$ such that $d \leq nc$. From $a + d = b + d$ we then get $a + nc = b + nc$. Since nc is primely generated and $nc \propto a$, we have reduced our task to proving the following special case: If $a + c = b + c$ with c primely generated and $c \propto a$, then there is a primely generated idempotent e such that $a = b + e$.

Let $\mathcal{C}$ be the class of all elements $c \in M$ such that $a+c = b+c$ and $c \propto a$ implies the existence of a primely generated idempotent $e \in M$ with $a = b + e$. Clearly $0 \in \mathcal{C}$. We will show that if $c \in \mathcal{C}$ and $p \in M$ is prime, then $c + p \in \mathcal{C}$.

Suppose we have $a + c + p = b + c + p$ with $c + p \propto a$ for some $c \in \mathcal{C}$ and prime p. Since $c \in \mathcal{C}$ and $c \propto a \leq a + p$, there is a primely generated idempotent $e \in M$ with $a + p = b + p + e$. From 4.1, there is a refinement matrix

$$\begin{array}{c} \\ a \\ p \end{array} \begin{array}{c} \begin{array}{cc} b+e & p \end{array} \\ \begin{pmatrix} d_1 & a_1 \\ b_1 & p_1 \end{pmatrix} \end{array}$$

with $p \leq p_1$.

Since $p \leq p + c \propto a = d_1 + a_1$ and p is prime, we have $p \leq d_1 + a_1$ and hence two cases to consider:

- If $p \leq d_1$, then $p_1 \leq p \leq d_1$, and the equation $a_1 + p_1 = b_1 + p_1$ implies $a_1 + d_1 = b_1 + d_1$, that is, $a = b + e$.
- If $p \leq a_1$, then $2p \leq a_1 + p_1 = p$, so p is regular. By 2.7, there is some idempotent $f \equiv p$. We have $p \leq f$, and so $a + p = b + e + p$ implies $a + f = b + e + f$. Also $f \leq p \leq a$, and so $f = 2f$ implies $a = f + a$. Consequently $a = b + e + f$. The element f is prime and so $e + f$ is a primely generated idempotent.

We have shown therefore that $c + p \in \mathcal{C}$, and by induction, that any primely generated element is in $\mathcal{C}$. ☐

Corollary 4.4. *Let M be a refinement monoid, $a, b, c, d \in M$ with c primely generated and $n, m \in \mathbb{N}$. Then*

(1) $(a + d = b + d \text{ and } d \propto c \propto a, b) \implies a = b$
(2) $(d \in \{\asymp c\} \text{ and } a + nd = b + nd) \implies a + d = b + d$
(3) $\{\asymp c\}$ *is cancellative*
(4) $(a, b \in \{\asymp c\} \text{ and } ma = mb \text{ and } na = nb) \implies$
$(ka = kb \text{ where } k = \gcd(m, n))$

Proof.

(1) From the theorem we have $a = b + e$ and $b = a + f$ for some idempotents $e, f \in M$. In particular, $e \leq a \leq b$, so from $e+e = e$ we get $b+e = b$. Thus $a = b + e = b$.
(2) We have $(n - 1)d \propto c \propto a + d, b + d$ so this follows from 1.
(3) If $a, b, d \in \{\asymp c\}$ such that $a + d = b + d$, then $d \propto c \propto a, b$ and so, from 1, we get $a = b$.
(4) Without loss of generality, we can assume $m \geq n$ and $m = hn + r$ for suitable $h, r \in \mathbb{Z}^+$ with $r < n$. By the Euclidean algorithm for calculating

the gcd of m and n, it suffices to show that $na = nb$ and $ma = mb$ imply $ra = rb$.

If $r = 0$ there is nothing to prove, so we assume $r \geq 1$. Then $ma = mb$ implies $hna + ra = hnb + rb$ and, since $na = nb$, $hna + ra = hna + rb$. We also have $hna \propto c \propto ra, rb$, so, from 1, $ra = rb$. □

Theorem 4.5. *Any primely generated refinement monoid M is separative. If, in addition, M has no proper idempotents, it is strongly separative.*

Proof. If $2a = a + b = 2b$ for elements $a, b \in M$, then we have $a + a = b + a$ with $a \propto a, b$. Using 4.4(1) we can cancel the a to get $a = b$.

Suppose now that M has no proper idempotents and we have $2a = a + b$ for some $a, b \in M$. Since $a \propto a$, 4.3 provides an idempotent e such that $a = b + e$. By hypothesis we have $e = 0$, so $a = b$. □

We will see in 5.9 that it suffices to check that there are no proper regular prime elements for M to be strongly separative.

There exist separative refinement monoids with no proper idempotents which are not strongly separative. An example of such a monoid is obtained by removing the element $(\infty, 0)$ from the monoid $\{0, \infty\} \times \mathbb{R}^+$. See [2, 9.7] for discussion of this example.

5. Cancellation II

If a is a primely generated element of a refinement monoid M, there will, in general, be many ways of expressing a as a sum of primes. In this section, by being more precise about which expressions are possible for a, we will gain further information about the structure of the monoid.

We will often find it convenient to work with the quotient monoid $M/\equiv$ for which the preorder $\leq$ is, in fact, a partial order, and so we establish some notation that will be in effect throughout this section:

Notation 5.1. *Let M be a monoid. We will write $\overline{M} = M/\equiv$. If $a, b, c, p, q, \ldots$ are elements of M, we will write $\bar{a}, \bar{b}, \bar{c}, \bar{p}, \bar{q}, \ldots$ for the corresponding elements of $\overline{M}$. $\mathbb{P}$ will be set of all proper prime elements of $\overline{M}$. The element 0 is the only nonproper prime in $\overline{M}$ so we write $\mathbb{P}_0$ for the set of all primes of $\overline{M}$.*

It is easy to confirm that $\overline{M}$ is partially ordered by $\leq$ and that, for $a, b \in M$, we have:

- $a \leq b \iff \bar{a} \leq \bar{b}$
- $a \ll b \iff \bar{a} \ll \bar{b} \iff \bar{a} + \bar{b} = \bar{b}$
- $a \equiv b \iff \bar{a} = \bar{b} \iff \bar{a} \equiv \bar{b}$
- $a \propto b \iff \bar{a} \propto \bar{b}$
- $a \asymp b \iff \bar{a} \asymp \bar{b}$
- a is prime (proper,regular, free) $\iff$ $\bar{a}$ is prime (proper,idempotent, free)
- a primely generated $\implies$ $\bar{a}$ primely generated
- M primely generated $\implies$ $\overline{M}$ primely generated

It is an interesting open question whether there is a refinement monoid M such that $\overline{M}$ does not have refinement. At least in the special case under discussion this does not occur:

Theorem 5.2. *If M is a primely generated refinement monoid then so is $\overline{M}$.*

Proof. We have already noted that $\overline{M}$ is primely generated, so we need only show refinement.

Suppose $\bar{a}_1 + \bar{a}_2 = \bar{b}_1 + \bar{b}_2$ in $\overline{M}$, then $a_1 + a_2 \equiv b_1 + b_2$. From 4.2(3), there are a'_1, a'_2 such that, $a_1 \equiv a'_1$, $a_2 \equiv a'_2$ and $a'_1 + a'_2 = b_1 + b_2$. We make a refinement of this equation:

$$\begin{array}{cc} & \begin{array}{cc} b_1 & b_2 \end{array} \\ \begin{array}{c} a'_1 \\ a'_2 \end{array} & \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \end{array}$$

Since $\bar{a}_1 = \bar{a}'_1$ and $\bar{a}_2 = \bar{a}'_2$,

$$\begin{array}{cc} & \begin{array}{cc} \bar{b}_1 & \bar{b}_2 \end{array} \\ \begin{array}{c} \bar{a}_1 \\ \bar{a}_2 \end{array} & \begin{pmatrix} \bar{c}_{11} & \bar{c}_{12} \\ \bar{c}_{21} & \bar{c}_{22} \end{pmatrix} \end{array}$$

is a refinement of the original equation. □

A primely generated refinement monoid for which $\leq$ is a partial order, such as $\overline{M}$, is called **primitive** by R. S. Pierce. Pierce [15] showed how an arbitrary primitive monoid can be described by generators and relations. F. Wehrung [20, Ch. 6] showed, as a consequence, that any primitive monoid embeds into a direct product of copies of the monoid $\mathbb{Z}^\infty$, where $\mathbb{Z}^\infty = \mathbb{Z}^+ \cup \{\infty\}$ with $n + \infty = \infty$ for all $n \in \mathbb{Z}^+$ and $\infty + \infty = \infty$. Thus certain cancellation properties of $\mathbb{Z}^\infty$ are easily proved to be properties of primitive monoids.

Similarly, some properties of a primely generated refinement monoid M are best seen as immediate consequences of the corresponding property of the primitive monoid $\overline{M}$ or of $\mathbb{Z}^\infty$. For example, $\mathbb{Z}^\infty$, and hence primitive monoids, have multiplicative cancellation: $(na = nb \implies a = b)$ for $n \in \mathbb{N}$ and a, b in the monoid. As a consequence, in M, we have $(na \equiv nb \implies a \equiv b)$. See 5.11.

Nonetheless there are some cancellation properties of primely generated refinement monoids which cannot be proved this way. Separativity is an example: The separativity of M does not follow directly from the separativity of $\mathbb{Z}^\infty$ and $\overline{M}$.

In this section we take a more direct route than Pierce and Wehrung from M to $\mathbb{Z}^\infty$ by defining a homomorphism $\phi_p \colon M \to \mathbb{Z}^\infty$ for each proper prime element $p \in M$.

Definition 5.3. *For any element p of a monoid M, define $\phi_p \colon M \to \mathbb{Z}^\infty$ by*

$$\phi_p(a) = \sup\{n \in \mathbb{Z}^+ \mid np \leq a\}$$

for all $a \in M$.

Among the simpler properties of ϕ_p are the following:

- $\phi_p(a) = 0$ if and only if $p \not\leq a$.
- If $a \leq b$, then $\phi_p(a) \leq \phi_p(b)$.
- If $a \equiv b$ and $q \equiv p$, then $\phi_p(a) = \phi_q(b)$.
- $\phi_p(a) = \phi_{\bar{p}}(\bar{a})$.

Since, if $p \equiv q$, we have $\phi_p = \phi_q$, we can label ϕ_p as $\phi_{\bar{p}}$. This causes no ambiguity: $\phi_{\bar{p}}$ is a map from either M or $\overline{M}$ such that $\phi_p(a) = \phi_{\bar{p}}(a) = \phi_{\bar{p}}(\bar{a})$ for all $a \in M$.

Theorem 5.4. *If M is a refinement monoid and $p \in M$ is a proper prime, then ϕ_p is a monoid homomorphism.*

Proof. Since $p \not\leq 0$ we have $\phi_p(0) = 0$, so we need to show only that $\phi_p(a_1 + a_2) = \phi_p(a_1) + \phi_p(a_2)$ for all $a_1, a_2 \in M$.

If $n_1, n_2 \in \mathbb{Z}^+$ such that $n_1 p \leq a_1$ and $n_2 p \leq a_2$, then $(n_1 + n_2)p \leq a_1 + a_2$, so $n_1 + n_2 \leq \phi_p(a_1 + a_2)$. Taking the supremum over all such n_1 and n_2 gives $\phi_p(a_1) + \phi_p(a_2) \leq \phi_p(a_1 + a_2)$.

To show the opposite inequality, suppose $np \leq a_1 + a_2$ for some $n \in \mathbb{Z}^+$. Then there is some $b \in M$ such that $np + b = a_1 + a_2$ and we get the refinement matrix

$$\begin{array}{c} \\ a_1 \\ a_2 \end{array} \begin{array}{c} \begin{array}{ccccc} b & p & p & \dots & p \end{array} \\ \begin{pmatrix} b_1 & x_1 & x_2 & \dots & x_n \\ b_2 & y_1 & y_2 & \dots & y_n \end{pmatrix} \end{array}$$

Since p is prime, for each i, we have either $p \leq x_i$ or $p \leq y_i$. So there are some $n_1, n_2 \in \mathbb{Z}^+$ such that $n = n_1 + n_2$, $n_1 p \leq a_1$ and $n_2 p \leq a_2$. Thus $n \leq \phi_p(a_1) + \phi_p(a_2)$, and taking the supremum over all such n we get $\phi_p(a_1 + a_2) \leq \phi_p(a_1) + \phi_p(a_2)$. □

Remark: This theorem remains true if the hypothesis on M, that it has refinement, is replaced by strong separativity. See [4, 3.3].

Theorem 5.5. *If p and q are primes in a refinement monoid, then $\phi_p(q) \in \{0, 1, \infty\}$ and*

(1) $\phi_p(q) = \infty \iff p \ll q$
(2) $\phi_p(q) = 1 \iff$ ($p \equiv q$ *and* p is free)
(3) $\phi_p(q) = 0 \iff p \not\leq q$

Proof. If $p \leq 0$ then $\phi_p(q) = \infty$ and the claim is trivially true. So it remains to consider the case where $p \not\leq 0$ and hence ϕ_p is a homomorphism:

(1) Notice that if $\phi_p(q) \geq 2$ then $2p \leq q$, so there is some $x \in M$ such that $2p + x = q$. Since q is prime we have either $q \leq x$ or $q \leq p$. In either case we get $q \leq p + x$ and so $q + p \leq 2p + x = q$, that is, $p \ll q$. Conversely, if $p \ll q$, then a simple induction shows that $np + q \leq q$ for all $n \in \mathbb{N}$, so $\phi_p(q) = \infty$.
(2) If $\phi_p(q) = 1$ then $p \leq q$, so there is some $x \in M$ such that $p + x = q$. Since q is prime we have either $q \leq x$ or $q \leq p$. The first case implies $p \ll q$ and hence, from 1, $\phi_p(q) = \infty$, so we must be in the second case, that is $p \equiv q$. To show freeness, suppose $mp \leq np$ for some $m, n \in \mathbb{N}$, then $mq \leq np \leq nq$, and so $m = \phi_p(mq) \leq \phi_p(nq) = n$.

    Conversely, if $q \equiv p$ and p is free, then for any $n \in \mathbb{N}$, we have $np \leq q \iff np \leq p \iff n \leq 1$. Thus $\phi_p(q) = 1$.
(3) This we have already noted.

Finally we note that the argument of 1 shows that $\phi_p(q) \in \{0, 1, \infty\}$. □

One important thing to notice here is that, in contrast to 3.2(2), a prime element p in a refinement monoid is either free or regular: Either $\phi_p(p) = \infty$ and hence p is regular, or $\phi_p(p) = 1$ and p is free. We will soon show (5.9) that this dichotomy extends also to primely generated elements.

Definition 5.6. *Let M be a monoid. For $a \in M$, define*

$$\Gamma_a = \{\bar{p} \in \mathbb{P}_0 \mid \bar{p} \leq \bar{a}\} = \{\bar{p} \in \mathbb{P}_0 \mid \phi_{\bar{p}}(\bar{a}) > 0\}.$$

Then the **support** *of a, $\operatorname{Supp} a$, is the set of maximal elements of Γ_a.*

Clearly $\operatorname{Supp} a$ is **incomparable**, meaning that, for all $\bar{p}_1, \bar{p}_2 \in \operatorname{Supp} a$, $\bar{p}_1 \le \bar{p}_2$ implies $\bar{p}_1 = \bar{p}_2$. If the monoid has refinement then for $\bar{p}_1, \bar{p}_2 \in \operatorname{Supp} a$, we have from 5.5 that

$$\phi_{\bar{p}_1}(\bar{p}_2) = \begin{cases} 0 & \text{if } \bar{p}_1 \ne \bar{p}_2 \\ 1 & \text{if } \bar{p}_1 = \bar{p}_2 \text{ is free} \\ \infty & \text{if } \bar{p}_1 = \bar{p}_2 \text{ is regular} \end{cases}$$

Lemma 5.7. *Let M be a refinement monoid, $a, b \in M$ and $\bar{p} \in \mathbb{P}$.*

(1) $a \asymp b \implies \Gamma_a = \Gamma_b \implies \operatorname{Supp} a = \operatorname{Supp} b$
(2) $\phi_{\bar{p}}(a) \in \mathbb{N} \implies \bar{p} \in \operatorname{Supp} a$

Proof.

(1) This follows very easily from the fact that if, for some prime $\bar{p}$, we have $\bar{p} \le \bar{a} \propto \bar{b}$, then $\bar{p} \le \bar{b}$.
(2) Since $\phi_{\bar{p}}(a) \ne 0$, we have $\bar{p} \le \bar{a}$ and hence $\bar{p} \in \Gamma_a$. Now suppose we have $\bar{q} \in \Gamma_a$ such that $\bar{p} \le \bar{q}$. Then $\bar{q} \le \bar{a}$ and $\phi_{\bar{p}}(\bar{q}) \le \phi_{\bar{p}}(\bar{a}) \in \mathbb{N}$, so that $\phi_{\bar{p}}(\bar{q}) < \infty$. From 5.5 we must have $\phi_{\bar{p}}(\bar{q}) = 1$ and so $\bar{p} = \bar{q}$. Thus $\bar{p}$ is maximal in Γ_a. ☐

Theorem 5.8. *Let c be a primely generated element of a refinement monoid M. Then* $\operatorname{Supp} c$ *is finite and writing* $\operatorname{Supp} c = \{\bar{p}_1, \bar{p}_2, \ldots, \bar{p}_K, \bar{q}_1, \bar{q}_2, \ldots, \bar{q}_L\}$ *with $\bar{p}_i$ free and $\bar{q}_i$ idempotent we get*

$$\bar{c} = n_1\bar{p}_1 + n_2\bar{p}_2 + \ldots + n_K\bar{p}_K + \bar{q}_1 + \bar{q}_2 + \ldots + \bar{q}_L$$

where $n_i = \phi_{\bar{p}_i}(c) \in \mathbb{N}$ for $i = 1, 2, \ldots, K$.

Proof. Suppose $\bar{c} = \bar{p}'_1 + \bar{p}'_2 + \ldots + \bar{p}'_N$ for some primes $\bar{p}'_1, \bar{p}'_2, \ldots, \bar{p}'_N \in \mathbb{P}_0$. Set $\Lambda = \{\bar{p}'_1, \bar{p}'_2, \ldots, \bar{p}'_N\}$. Clearly $\Lambda \subseteq \Gamma_c$, and further, if $\bar{p} \in \Gamma_c$ then $\bar{p} \le \bar{c} = \bar{p}'_1 + \bar{p}'_2 + \ldots + \bar{p}'_N$ and, since $\bar{p}$ is prime, there is some $\bar{p}' \in \Lambda$ such that $\bar{p} \le \bar{p}'$. Since every element of Γ_c is less than or equal to some element of Λ and vice versa, it follows that Γ_c and Λ have the same set of maximal elements. Since Λ is finite, $\operatorname{Supp} c$ is finite.

Next we show that the nonmaximal elements of Λ contribute nothing to the sum $\bar{c} = \bar{p}'_1 + \bar{p}'_2 + \ldots + \bar{p}'_N$. Indeed, if $\bar{p}' \in \Lambda$ is nonmaximal, there is some maximal $\bar{p}'' \in \Lambda$ such that $\bar{p}' \le \bar{p}''$, and hence $\bar{p}' + \bar{b} = \bar{p}''$ for some $\bar{b} \in \overline{M}$. Since $\bar{p}''$ is prime, and $\bar{p}'' \ne \bar{p}'$, we must have $\bar{p}'' = \bar{b}$. Thus $\bar{p}'' = \bar{p}'' + \bar{p}'$, and $\bar{p}'$ can be removed from the sum. Therefore $\bar{c}$ is a sum of elements of $\operatorname{Supp} c$:

$$\bar{c} = n_1\bar{p}_1 + n_2\bar{p}_2 + \ldots + n_K\bar{p}_K + \bar{q}_1 + \bar{q}_2 + \ldots + \bar{q}_L$$

for some $n_1, n_2, \ldots, n_K \in \mathbb{N}$.

Since the set $\operatorname{Supp} c$ is incomparable, applying the homomorphism $\phi_{\bar{p}_i}$ to the above equation yields $n_i = \phi_{\bar{p}_i}(c) \in \mathbb{N}$ for $i = 1, 2, \ldots, K$. ☐

The proof of this theorem shows that if $X = \{\bar{p}_1, \bar{p}_2, \ldots, \bar{p}_K, \bar{q}_1, \bar{q}_2, \ldots, \bar{q}_L\}$ is an incomparable set of primes in $\overline{M}$ such that $\bar{c} = n_1\bar{p}_1 + n_2\bar{p}_2 + \ldots + n_K\bar{p}_K + \bar{q}_1 + \bar{q}_2 + \ldots + \bar{q}_L$ for some $n_1, n_2, \ldots, n_K \in \mathbb{N}$, then $X = \operatorname{Supp} c$.

Translating this into a theorem about M rather than $\overline{M}$ we have the following: If c is a primely generated element of a refinement monoid M, there is an incomparable set of primes $\{p_1, p_2, \ldots, p_K, q_1, q_2, \ldots, q_L\} \subseteq M$ with p_i free and q_i regular such that

$$c \equiv n_1 p_1 + n_2 p_2 + \ldots + n_K p_K + q_1 + q_2 + \ldots + q_L$$

and $n_i = \phi_{p_i}(c) \in \mathbb{N}$ for $i = 1, 2, \ldots, K$. The primes $\{p_1, p_2, \ldots, p_K, q_1, q_2, \ldots, q_L\}$ are unique up to $\equiv$-congruence.

Notice that we do not claim that $c = n_1 p_1 + n_2 p_2 + \ldots + n_K p_K + q_1 + q_2 + \ldots + q_L$. This would be too much to hope for even in the simplest of monoids. For example, let $M = \mathbb{Z}^*$ as in 3.1. The element -4 is primely generated (as is any element), and can be written as $-4 = (-2)(2)$ (multiplicative notation), but here -2 and 2 are $\equiv$-congruent primes, that is, $\{-2, 2\}$ is not incomparable. On the other hand we do have $-4 \equiv 2^2$ which is an expression of the form provided by this theorem.

Corollary 5.9. *Let c be a primely generated element in a refinement monoid. Then c is either free or regular.*

Proof. Let $\bar{c} = n_1 \bar{p}_1 + n_2 \bar{p}_2 + \ldots + n_K \bar{p}_K + \bar{q}_1 + \bar{q}_2 + \ldots + \bar{q}_L$ with $n_i, \bar{p}_i, \bar{q}_i$ as in 5.8. If $K = 0$, then $\bar{c} = \bar{q}_1 + \bar{q}_2 + \ldots + \bar{q}_L$ is idempotent and hence c is regular. Otherwise, given $mc \leq nc$ for some $m, n \in \mathbb{N}$, we apply the monoid homomorphism $\phi_{\bar{p}_1}$ to the inequality to get $mn_1 \leq nn_1$, and so $m \leq n$. Hence c is free. □

Notice that c is regular if and only if it is a sum of regular primes. Thus we can make a slight improvement in 4.5: If M is a primely generated refinement monoid with no proper regular primes, then M is strongly separative.

It is convenient to combine all the homomorphisms $\phi_{\bar{p}}$ for $\bar{p} \in \mathbb{P}$ into a single homomorphism. Thus, we define $\Phi\colon M \to (\mathbb{Z}^\infty)^{\mathbb{P}}$ by

$$\Phi(a) = (\phi_{\bar{p}}(a))_{\bar{p} \in \mathbb{P}}$$

for $a \in M$.

Theorem 5.10. *Let c be a primely generated element in a refinement monoid M. Then for all $a \in M$*

$$c \leq a \iff \Phi(c) \leq \Phi(a) \iff (\forall \bar{p} \in \operatorname{Supp} c)\ (\phi_{\bar{p}}(c) \leq \phi_{\bar{p}}(a)).$$

Proof. The implications

$$c \leq a \implies \Phi(c) \leq \Phi(a) \implies (\forall \bar{p} \in \operatorname{Supp} c)\ (\phi_{\bar{p}}(c) \leq \phi_{\bar{p}}(a))$$

are trivial so we prove that, if $\phi_{\bar{p}}(c) \leq \phi_{\bar{p}}(a)$ for all $\bar{p} \in \operatorname{Supp} c$, then $c \leq a$.

Let $\bar{c} = n_1 \bar{p}_1 + n_2 \bar{p}_2 + \ldots + n_K \bar{p}_K + \bar{q}_1 + \bar{q}_2 + \ldots + \bar{q}_L$ with $n_i, \bar{p}_i, \bar{q}_i$ as in 5.8. Since $\bar{p}_1 \in \operatorname{Supp} c$, we have $n_1 = \phi_{\bar{p}_1}(\bar{c}) \leq \phi_{\bar{p}_1}(\bar{a})$, and so $n_1 \bar{p}_1 \leq \bar{a}$ and there is some $\bar{a}_1 \in \overline{M}$ such that $\bar{a} = n_1 \bar{p}_1 + \bar{a}_1$. Applying the homomorphism $\phi_{\bar{p}_2}$ to this equation gives $\phi_{\bar{p}_2}(\bar{a}_1) = \phi_{\bar{p}_2}(\bar{a})$. Since $n_2 = \phi_{\bar{p}_2}(\bar{c}) \leq \phi_{\bar{p}_2}(\bar{a}) = \phi_{\bar{p}_2}(\bar{a}_1)$, we get $n_2 \bar{p}_2 \leq \bar{a}_1$, and hence $\bar{a} = n_1 \bar{p}_1 + n_2 \bar{p}_2 + \bar{a}_2$ for some $\bar{a}_2 \in M$. This process can be repeated for the remaining free primes and, with obvious modification, for the idempotent primes in $\operatorname{Supp} c$ to give the inequality $n_1 \bar{p}_1 + n_2 \bar{p}_2 + \ldots + n_K \bar{p}_K + \bar{q}_1 + \bar{q}_2 + \ldots + \bar{q}_L \leq \bar{a}$. Thus $\bar{c} \leq \bar{a}$ and $c \leq a$. □

Corollary 5.11. *Let M be a primely generated refinement monoid and $a, b \in M$.*

(1) $a \equiv b \iff \Phi(a) = \Phi(b)$
(2) $\overline{M}$ *embeds via* Φ *in the monoid* $(\mathbb{Z}^\infty)^{\mathbb{P}}$.
(3) $((\forall n \in \mathbb{N})(na \leq b)) \implies a \ll b$
(4) $((\forall n \in \mathbb{N})(na \leq (n+1)b)) \implies a \leq b$

(5) $(\forall n \in \mathbb{N})\ (na \leq nb \implies a \leq b)$
(6) $(\forall n \in \mathbb{N})\ (na \equiv nb \implies a \equiv b)$

Proof. Claims 1 and 2 follow immediately from the theorem. The other claims are true about M because they are true about $\mathbb{Z}^\infty$. For example, we prove 5: If $na \leq nb$, then for all $\bar{p} \in \mathbb{P}$ we have $n\phi_{\bar{p}}(a) \leq n\phi_{\bar{p}}(b)$. In $\mathbb{Z}^\infty$, this implies $\phi_{\bar{p}}(a) \leq \phi_{\bar{p}}(b)$. Therefore $\Phi(a) \leq \Phi(b)$, and so, from the theorem, $a \leq b$. □

See 6.2 for a cancellative refinement monoid which does not have the property of item 3: $((\forall n \in \mathbb{N})\ (na \leq b)) \implies a \ll b$.

The cancellation property of item 5, $(na \leq nb \implies a \leq b)$, is called **unperforation** by F. Wehrung [20, 6.15] who proved it for primitive monoids. For such monoids it implies also **multiplicative cancellation**: $(na = nb \implies a = b)$.

The following example shows that a cancellative refinement monoid need not be unperforated.

Example 5.12. [2, 11.17] *Let M be the submonoid obtained by deleting the element $(0,1)$ from the cancellative monoid $\mathbb{R}^+ \times \mathbb{Z}_2$. (We write $\mathbb{Z}_2 = \{0,1\}$ for the two element group.)*

M is a refinement monoid. Easily checked is that for $(r_1,x_1),(r_2,x_2) \in M$

$$(r_1,x_1) \leq (r_2,x_2) \iff (r_1 = r_2 \text{ and } x_1 = x_2) \text{ or } r_1 < r_2.$$

Set $a = (1,0)$ and $b = (1,1)$. Then we have $2a = 2b$ but $a \not\leq b$.

The refinement monoid $\{0,\infty\}$ is not cancellative but is unperforated. So these examples show the independence of the two types of cancellation.

As we have already noted, we do not expect multiplicative cancellation to occur in primely generated refinement monoids because it does not occur in the special case of Abelian groups. For an Abelian group G, let

$$\tau(G) = \{a \in G \mid \exists n \in \mathbb{N} \text{ such that } na = 0\},$$

the torsion subgroup. Then it is easy to see that G has multiplicative cancellation if and only if $\tau(G) = 0$. This result extends very easily to primely generated refinement monoids.

Theorem 5.13. *Let M be a primely generated refinement monoid. Then M has multiplicative cancellation if and only if $\tau(G_a) = 0$ for all $a \in M$.*

Proof. Suppose that $na = nb$ for some $a, b \in M$ and $n \in \mathbb{N}$, and that $\tau(G_a) = 0$. From 5.11(6) and $na = nb$ we get $a \equiv b$, so there is some $x \ll a$ such that $b = a + x$, and hence $na = na + nx$. Using 4.4(2) we can cancel $(n-1)a$ from this to get $a = a + nx$, that is, $n[x]_a = 0$ in G_a. Since $\tau(G_a) = 0$, this implies $[x]_a = 0$, and so $b = a + x = a$.

Conversely, suppose M has multiplicative cancellation and $a \in M$. If we have $n[x]_a = 0$ in G_a for some $x \ll a$ and $n \in \mathbb{N}$, then $a = a + nx$ and so $na = n(a + x)$. Using multiplicative cancellation, we get $a = a + x$, and hence $[x]_a = 0$. Thus $\tau(G_a) = 0$ □

As mentioned in the introduction, a cancellative primely generated refinement monoid M is the direct product of an Abelian group and a free commutative monoid. In the proof of this fact, the full strength of cancellation is not actually needed. What suffices is the rule $(\forall c, x \in M)\ (c + x = c \implies x = 0)$. Monoids with this property are called **stably finite**.

We remind the reader that from 2.8, G_0 is the group of all invertible elements of M, that is, $G_0 = \{x \in M \mid x \leq 0\}$. Since $[x]_0 = \{x\}$ for all $x \in M$, we drop the notation $[x]_0$.

Theorem 5.14. *Let M be a stably finite primely generated refinement monoid. Then $\overline{M}$ is isomorphic to the free commutative monoid on $\mathbb{P}$ and $M \cong \overline{M} \times G_0$. In particular, M is cancellative.*

Proof. First we note the following simple fact: If $c, x, y \in M$ such that $c + x = c + y \leq c$, then there is some $z \in M$ such that $c + x + z = c + y + z = c$. Since M is stably finite, this implies $x + z = y + z = 0$, that is, $x, y, z \in G_0$. Since G_0 is a group, it follows that $x = y$.

Thus we have the following:

(1) If $x \ll c$ for $c, x \in M$, then $x \in G_0$. If $\bar{x} \ll \bar{c}$ for $\bar{c}, \bar{x} \in \overline{M}$, then $\bar{x} = 0$.
(2) All regular elements of M are in G_0. The only regular element of $\overline{M}$ is 0. In particular $\mathbb{P}$ contains only free primes.
(3) From 5.5 and 1, if $\bar{p} \in \mathbb{P}$, then $\phi_{\bar{p}}(\bar{q}) \in \{0, 1\}$ for all primes $\bar{q} \in \overline{M}$. Hence $\phi_{\bar{p}}(\bar{c}) < \infty$ for all $\bar{c} \in \overline{M}$.
(4) If $a \equiv b$ for $a, b \in M$, then $a = b + x$ for some unique $x \in G_0$.

If $0 \neq \bar{c} \in \overline{M}$ then, using 5.8, and 2, we have $\bar{c} = n_1\bar{p}_1 + n_2\bar{p}_2 + \ldots + n_K\bar{p}_K$ for some $\bar{p}_1, \bar{p}_2, \ldots, \bar{p}_K \in \mathbb{P}$ with $n_i = \phi_{\bar{p}_i}(\bar{c})$ for $i = 1, 2, \ldots, K$. In fact, since $\phi_{\bar{p}}(\bar{c})$ is nonzero for only a finite number of primes $\bar{p} \in \mathbb{P}$, we can write $\bar{c} = \sum_{\bar{p} \in \mathbb{P}} \phi_{\bar{p}}(\bar{c})\bar{p}$ for all $\bar{c} \in \overline{M}$. Thus $\overline{M}$ is isomorphic to the free commutative monoid on the set $\mathbb{P}$.

Let $\mathbb{P}' \subseteq M$ be a set of representatives of the elements of $\mathbb{P}$. Then for $c \in M$ we have $c \equiv \sum_{p \in \mathbb{P}'} \phi_p(c)p$ and hence, by 4, $c = \sum_{p \in \mathbb{P}'} \phi_p(c)p + x$ where $x \in G_0$ is uniquely determined. It is then easy to check that the map $\Lambda \colon M \to \overline{M} \times G_0$ defined by $\Lambda(c) = (\bar{c}, x)$ where $x \in G_0$ is determined as above, is a monoid isomorphism. Since $\overline{M}$ and G_0 are cancellative, so is M. ☐

The simplest example of this theorem is the monoid $M = \mathbb{Z}^*$ of 3.1. This monoid is a cancellative primely generated refinement monoid. We have $G_0 = \{1, -1\}$ and we can choose $\mathbb{P}' = \{2, 3, 5, 7, 11, \ldots\}$. Then any element $c \in M$ can be expressed uniquely in the form $c = p_1^{n_1} p_2^{n_2} \ldots p_K^{n_K} x$ (multiplicative notation) with $p_1, p_2, \ldots, p_K$ distinct elements of $\mathbb{P}'$, $n_1, n_2, \ldots n_K \in \mathbb{N}$ and $x \in G_0$.

We now set into place the context in which the remaining theorems of this section will be proved. This will involve notation which depends on a choice of representatives X of the elements of $\operatorname{Supp} c$ where c is a fixed primely generated element in a refinement monoid M.

Specifically, let $X = \{p_1, p_2, \ldots, p_K, q_1, q_2, \ldots, q_L\} \subseteq M$ be such that $\operatorname{Supp} c = \{\bar{p}_1, \bar{p}_2, \ldots, \bar{p}_K, \bar{q}_1, \bar{q}_2, \ldots, \bar{q}_L\}$ with $\bar{p}_i$ free and $\bar{q}_i$ idempotent as in 5.8. From 2.7, we can assume that $q_1, q_2, \ldots, q_L$ are idempotents. It is easy to check that $\{\propto c\} = \{\propto (p_1 + p_2 + \ldots + p_K + q_1 + q_2, \ldots + q_L)\}$.

Our goal is to define a homomorphism $\Psi_X \colon \{\propto \Phi(c)\} \to \{\propto c\}$ which serves almost as a one-sided inverse for Φ restricted to $\{\asymp c\}$. To do so we will need to make the convention that if $q \in M$ is an idempotent, then $\infty q = q$. With this convention, the map $\mu \mapsto \mu q$ from $\mathbb{Z}^\infty$ to M is a homomorphism.

Suppose we have $\gamma = (\gamma_{\bar{p}})_{\bar{p} \in \mathbb{P}} \in (\mathbb{Z}^\infty)^{\mathbb{P}}$ such that $\gamma \propto \Phi(c)$. Then for all $p \in X$ we have $\gamma_{\bar{p}} \propto \phi_{\bar{p}}(c)$. In particular, for $i = 1, 2, \ldots, K$, we have $\gamma_{\bar{p}_i} \propto \phi_{\bar{p}_i}(c) \in \mathbb{N}$, and so $\gamma_{\bar{p}_i} < \infty$. Consequently, with the above convention on the idempotents $\{q_1, q_2, \dots, q_L\}$, we can define a homomorphism $\Psi_X \colon \{\propto \Phi(c)\} \to M$ by

$$\Psi_X(\gamma) = \sum_{p \in X} \gamma_{\bar{p}} p.$$

If $a \propto c$ then $\Phi(a) \propto \Phi(c)$, and to shorten our notation we will write

$$a^* = \Psi_X(\Phi(a)) = \sum_{p \in X} \phi_{\bar{p}}(a)\ p.$$

Notice that, by construction and 5.8, we have $c \equiv c^*$.

We check that the image of Ψ_X is contained in $\{\propto c\}$: Suppose $\gamma \propto \Phi(c)$. Then applying the homomorphism Ψ_X yields $\Psi_X(\gamma) \propto \Psi_X(\Phi(c)) = c^* \equiv c$. Thus $\Psi_X(\gamma) \propto c$.

The next lemma says that Ψ_X is a one-sided inverse for Φ when restricted to $\{\asymp \Phi(c)\}$. This follows from the facts that $\mathbb{Z}^\infty$ has only three $\asymp$-congruence classes: $\{0\}$, $\mathbb{N}$ and $\{\infty\}$; and that $\phi_{\bar{p}}(c) \in \mathbb{N}$ for only a finite set of primes $\bar{p} \in \mathbb{P}$.

Lemma 5.15. *Let M be a refinement monoid with $c \in M$ and Ψ_X as above. Let $\gamma = (\gamma_{\bar{p}})_{\bar{p} \in \mathbb{P}} \in (\mathbb{Z}^\infty)^{\mathbb{P}}$.*

(1) $\gamma \asymp \Phi(c) \iff (\forall \bar{p} \in \mathbb{P})\ (\gamma_{\bar{p}} \asymp \phi_{\bar{p}}(c))$
$\iff (\gamma_{\bar{p}} \in \mathbb{N}$ *for* $\bar{p} \in \{\bar{p}_1, \bar{p}_2, \dots, \bar{p}_K\}$ *and* $\gamma_{\bar{p}} = \phi_{\bar{p}}(c)$ *otherwise*$)$
(2) $\gamma \asymp \Phi(c) \implies \Psi_X(\gamma) \asymp c$ *and* $\Phi(\Psi_X(\gamma)) = \gamma$
(3) $\Phi(\{\asymp c\}) = \{\asymp \Phi(c)\} \cong \mathbb{N}^K$

Proof.

(1) If $\gamma \asymp \Phi(c)$, we have $\gamma_{\bar{p}} \asymp \phi_{\bar{p}}(c)$ for all $\bar{p} \in \mathbb{P}$. From 5.7(2), we see that $\phi_{\bar{p}}(c) \in \mathbb{N}$ if and only if $\bar{p} \in \{\bar{p}_1, \bar{p}_2, \dots, \bar{p}_K\}$. Thus we have the conditions $\gamma_{\bar{p}} \in \mathbb{N}$ for $\bar{p} \in \{\bar{p}_1, \bar{p}_2, \dots, \bar{p}_K\}$ and $\gamma_{\bar{p}} = \phi_{\bar{p}}(c)$ otherwise. Since $\phi_{\bar{p}}(c) \in \mathbb{N}$ for only a finite set of primes $\bar{p} \in \mathbb{P}$, one readily confirms that any $\gamma \in (\mathbb{Z}^\infty)^{\mathbb{P}}$ satisfying these conditions also satisfies $\gamma \asymp \Phi(c)$.
(2) Applying the homomorphism Ψ_X to $\gamma \asymp \Phi(c)$ yields $\Psi_X(\gamma) \asymp c^* \equiv c$. Thus $\Psi_X(\gamma) \asymp c$. From this we have $\phi_{\bar{p}}(\Psi_X(\gamma)) \asymp \phi_{\bar{p}}(c)$ for all $\bar{p} \in \mathbb{P}$. For all primes $\bar{p} \notin \{\bar{p}_1, \bar{p}_2, \dots, \bar{p}_K\}$ we have $\phi_{\bar{p}}(c) \in \{0, \infty\}$ and hence, with 1, $\phi_{\bar{p}}(\Psi_X(\gamma)) = \phi_{\bar{p}}(c) = \gamma_{\bar{p}}$. For all primes $\bar{p} \in \{\bar{p}_1, \bar{p}_2, \dots, \bar{p}_K\}$, a direct calculation from the definition of $\Psi_X(\gamma)$ gives $\phi_{\bar{p}}(\Psi_X(\gamma)) = \gamma_{\bar{p}}$. Thus $\Phi(\Psi_X(\gamma)) = \gamma$.
(3) Since Φ is a homomorphism, we have $\Phi(\{\asymp c\}) \subseteq \{\asymp \Phi(c)\}$. The opposite inclusion is clear from 2. The claim that $\{\asymp \Phi(c)\} \cong \mathbb{N}^K$ follows from 1. □

Notice that $\mathbb{Z}^\infty$ is a semilattice with $\mu \vee \nu = \max\{\mu, \nu\}$ for $\mu, \nu \in \mathbb{Z}^\infty$. It is easy to check that $\mu \vee \nu \asymp \mu + \nu$ for all $\mu, \nu \in \mathbb{Z}^\infty$. This fact enables us to show that a primely generated refinement monoid is also a semilattice (with appropriate accommodation of the fact that M is preordered rather than partially ordered):

Theorem 5.16. *Let M be a refinement monoid. Then, given primely generated elements $c_1, c_2 \in M$, there exists a primely generated element $d \in M$ such that $c_1, c_2 \leq d$ and, for all $a \in M$, $c_1, c_2 \leq a$ implies $d \leq a$.*

Proof. Let $\gamma = \Phi(c_1) \vee \Phi(c_2)$. For each $\bar{p} \in \mathbb{P}$ we have

$$\gamma_{\bar{p}} = \phi_{\bar{p}}(c_1) \vee \phi_{\bar{p}}(c_2) \asymp \phi_{\bar{p}}(c_1) + \phi_{\bar{p}}(c_2) = \phi_{\bar{p}}(c_1 + c_2).$$

The element $c = c_1 + c_2$ is primely generated so, from 5.15(1), we get $\gamma \asymp \Phi(c)$. From 5.15(2), there is a primely generated element $d = \Psi_X(\gamma)$ such that $\Phi(d) = \gamma = \Phi(c_1) \vee \Phi(c_2)$. We have $\Phi(c_1), \Phi(c_2) \leq \Phi(d)$ so, from 5.10, $c_1, c_2 \leq d$.

If $c_1, c_2 \leq a$, then $\Phi(c_1), \Phi(c_2) \leq \Phi(a)$, so that $\Phi(d) = \Phi(c_1) \vee \Phi(c_2) \leq \Phi(a)$. From 5.10 we get $d \leq a$. □

If M is a primely generated refinement monoid, then $\overline{M}$ is a primely generated refinement monoid which is partially ordered by $\leq$, so $\overline{M}$ is a semilattice in the usual sense: Given $\bar{c}_1, \bar{c}_2 \in \overline{M}$, there exists $\bar{d} = \bar{c}_1 \vee \bar{c}_2$. In contrast to 0-semilattices, the operations $\vee$ and $+$ may be different.

Corollary 5.17. *Let M be a refinement monoid. Then, given $a, b_1, b_2, c \in M$ with a and c primely generated such that $a \leq c + b_1, c + b_2$, there exists $b \leq b_1, b_2$ such that $a \leq c + b$.*

Proof. We have $a, c \leq c+b_1, c+b_2$ with a, c primely generated, so from the theorem, there is an element $d \in M$ such that $a, c \leq d \leq c + b_1, c + b_2$. Applying 4.2(5) to the inequalities $c \leq d \leq c + b_1, c + b_2$, we get some $b \leq b_1, b_2$ such that $d \equiv b + c$. Since $a \leq d$, we have also $a \leq b + c$ □

The property discussed in this corollary,

$$(a \leq c + b_1, c + b_2 \implies \exists b \leq b_1, b_2 \text{ such that } a \leq c + b,)$$

is called the **interval axiom** by F. Wehrung who proved it for primitive monoids [20, 6.16].

One of the most surprising things about a primely generated element c in a refinement monoid is that it has considerable influence on elements in $\{\asymp c\}$. For example, the next theorem shows that all of these neighboring elements must be primely generated. Here we use the definitions and conventions established for 5.15.

Theorem 5.18. *Let c be a primely generated element in a refinement monoid M.*

(1) *If $a \asymp c$, then $\sim_a$ and $\sim_c$ coincide. In particular, $G_a = G_c$ and for all $x \in M$, $x \ll a$ if and only if $x \ll c$.*
(2) $a \asymp c \implies a^* \equiv a$ *and* $\Phi(a^*) = \Phi(a)$
(3) $a \asymp c \implies a$ *is primely generated*
(4) $\{\asymp c\} \cong \mathbb{N}^K \times G_c$ *where K is the number of free primes in* $\operatorname{Supp} c$.

Proof.

(1) Suppose $x \sim_a y$, that is, $a + x = a + y$. We have $c + a + x = c + a + y$ with $a \propto c \propto c + x, c + y$, and so, from 4.4(1), $c + x = c + y$. Thus $x \sim_c y$.

Conversely, if $x \sim_c y$, that is, $c + x = c + y$, then $c + a + x = c + a + y$ with $c \propto c \propto a + x, a + y$ and so, from 4.4(1), $a + x = a + y$. Thus $x \sim_a y$.

(2) Since $a \asymp c$, there are $b \in M$ and $m \in \mathbb{N}$ such that $a+b = mc$. Adding c to b and 1 to m if necessary, we can assume that $b \asymp c$. Thus $\Phi(a), \Phi(b) \asymp \Phi(c)$. From 5.15(2) we have $a^*, b^* \asymp c$ with $\Phi(a) = \Phi(a^*)$ and $\Phi(b) = \Phi(b^*)$, and hence, from 5.10, $a^* \leq a$ and $b^* \leq b$. Since Φ and Ψ_X are homomorphisms, we have $a^* + b^* = mc^* \equiv mc$, and so

$$a + mc \leq a + a^* + b^* \leq a + a^* + b = a^* + mc$$

with $mc \propto c \propto a, a^*$. Using 4.4(1) we can cancel mc from this inequality to give $a \leq a^*$. Thus $a \equiv a^*$ as claimed.

(3) Since $a \equiv a^*$ and a^* is primely generated, the claim follows from 4.2(4).

(4) Let $S = \Phi(\{\asymp c\})$. From 5.15(3), we have $S \cong \mathbb{N}^K$, so it suffices to show that $\{\asymp c\} \cong S \times G_c$. Let $\tau\colon S \times G_c \to \{\asymp c\}$ be defined by $\tau(\gamma, [x]_c) = \Psi_X(\gamma) + x$, and $\sigma\colon \{\asymp c\} \to S \times G_c$ be defined by $\sigma(a) = (\Phi(a), [x]_c)$ where x is determined by $a = a^* + x$. Using 1, 2 and 5.15, the reader can confirm that these maps are well defined inverse semigroup homomorphisms. □

In the next theorem we summarize all the cancellation properties of primely generated refinement monoids that we have proved:

Theorem 5.19. *Let M be a primely generated refinement monoid.*

P1. $(\forall a, b, c \in M)$ $(a + c = b + c \implies (\exists$ *refinement*

$$\begin{array}{c} \\ a \\ c \end{array}\begin{array}{c} \begin{array}{cc} b & c \end{array} \\ \begin{pmatrix} d_1 & a_1 \\ b_1 & c_1 \end{pmatrix} \end{array}$$

with $c \le c_1))$

P2. $(\forall a, b, c \in M)$ $(a + c \le b + c \implies (\exists a_1 \ll c$ *such that* $a \le b + a_1))$ *–pseudo-cancellation*

P3. $(\forall a, c_1, c_2 \in M)$ $(a \ll c_1 + c_2 \implies$
$(\exists a_1, a_2$ *such that* $a = a_1 + a_2,\ a_1 \ll c_1$ *and* $a_2 \ll c_2))$

P4. $(\forall a, c_1, c_2 \in M)$ $(a \equiv c_1 + c_2 \implies$
$(\exists a_1, a_2$ *such that* $a = a_1 + a_2,\ a_1 \equiv c_1$ *and* $a_2 \equiv c_2))$

P5. $(\forall a, b_1, b_2, c \in M)$ $(c \le a \le c + b_1, c + b_2 \implies (\exists b \le b_1, b_2$ *such that* $a \equiv c + b))$

T. $(\forall a, b, c \in M)$ $((a + c = b + c$ *and* $c \propto a) \implies$
$(\exists e$ *such that* $2e = e$ *and* $a = b + e))$

S1. $(\forall a, b \in M)$ $((2a = a + b = 2b) \implies a = b)$ *–separativity*

S2. $(\forall a, b, c \in M)$ $((a + c = b + c$ *and* $c \propto a, b) \implies a = b)$

S3. $(\forall a \in M)$ $(\{\asymp a\}$ *is cancellative*$)$

S4. $(\forall a, b \in M)(\forall m, n \in \mathbb{N})$ $((ma = mb$ *and* $na = nb) \implies$
$(ka = kb$ *where* $k = \gcd(m, n)))$

S5. $(\forall a, b, c \in M)(\forall n \in \mathbb{N})$ $(a + nc = b + nc \implies a + c = b + c)$

S6. $(\forall a, b, c \in M)$ $((a + c = b + c$ *and* $c \le a, b) \implies a = b)$

Z1. $(\forall a, b \in M)$ $(((\forall n \in \mathbb{N})(na \le b)) \implies a \ll b)$

Z2. $(\forall a, b \in M)$ $(((\forall n \in \mathbb{N})(na \le (n+1)b)) \implies a \le b)$

Z3. $(\forall a, b \in M)(\forall n \in \mathbb{N})$ $(na \le nb \implies a \le b)$ *–unperforation*

Z4. $(\forall a, b \in M)(\forall n \in \mathbb{N})$ $(na \equiv nb \implies a \equiv b)$

U1. $(\forall c_1, c_2 \in M)$ $(\exists d$ *such that* $c_1, c_2 \le d$ *and* $(\forall a \in M)$ $(c_1, c_2 \le a \implies d \le a))$ *–semilattice property*

U2. $(\forall a, b_1, b_2, c \in M)$ $((a \le c + b_1, c + b_2) \implies (\exists b \le b_1, b_2$ *such that* $a \le c + b))$ *–interval axiom*

Proof. P1 is from 4.1. P2-5 are from 4.2. T is from 4.3. S1 is from 4.5. S2-5 are from 4.4 or from S1 and 2.4. Z1-4 are from 5.11. U1 is from 5.16. U2 is from 5.17. □

There are of course many connections among these properties. For example, we have seen in the proof of 4.2 that, for decomposition monoids, P1 implies P2, and that P2 implies P3-5. From the proof of 4.5 we see that T implies S1. By 2.4, S1-4 are equivalent even without refinement, and S5-6 are equivalent to S1-4 in decomposition monoids.

We end this section by proving one other connection:

Theorem 5.20. *Let M be a refinement monoid. Then*

$$\text{P1} \iff \text{P2 } \textit{(pseudo-cancellation)} \implies \text{S1-6 } \textit{(separativity)}.$$

Proof. The implication P1 $\implies$ P2 is proved exactly as 4.2(1), so we prove only that P2 $\implies$ P1:

Suppose M has pseudo-cancellation (P2) and we have $a + c = b + c$ for some $a, b, c \in M$. We make a refinement of this equation:

$$\begin{array}{cc} & \begin{array}{cc} b & c \end{array} \\ \begin{array}{c} a \\ c \end{array} & \begin{pmatrix} d_1 & a_1 \\ b_1 & c_1 \end{pmatrix} \end{array}$$

We have $a_1+c_1 = b_1+c_1$ so, using P2, there is some $x_1 \ll c_1$ such that $a_1 \leq b_1+x_1$. Decomposing this inequality we get $a' \leq b_1$ and $x' \leq x_1 \ll c_1$ such that $a_1 = a'+x'$. Since $a' \leq b_1$, there is some $y' \in M$ such that $b_1 = a' + y'$. this gives us the refinement matrix

$$\begin{array}{cc} & \begin{array}{cc} b & c \end{array} \\ \begin{array}{c} a \\ c \end{array} & \begin{pmatrix} d_1 + a' & x' \\ y' & c_1 + a' \end{pmatrix} \end{array}$$

and, since $x' \ll c_1$, we also have $c = c_1 + a_1 = c_1 + a' + x' \leq c_1 + a'$ as required.

We show next that P1 implies S6. Since M has refinement, S6 is equivalent to S1-5.

Suppose then that we have $a + c = b + c$ in M with $c \leq a, b$. From P1, there is a refinement matrix

$$\begin{array}{cc} & \begin{array}{cc} b & c \end{array} \\ \begin{array}{c} a \\ c \end{array} & \begin{pmatrix} d_1 & a_1 \\ b_1 & c_1 \end{pmatrix} \end{array}$$

with $c \leq c_1$. Since $c \leq a, b$, there are $a_2, b_2 \in M$ such that $a = a_2+c$ and $b = b_2+c$. Thus $a_2 + c + b_1 = a + b_1 = d_1 + a_1 + b_1 = b + a_1 = b_2 + c + a_1$, and since $c \leq c_1$, we get $a_2 + c_1 + b_1 = b_2 + c_1 + a_1$. But $c_1 + b_1 = c_1 + a_1 = c$ and so $a_2 + c = b_2 + c$, that is, $a = b$. □

6. Artinian Refinement Monoids

The purpose of this section is to show that refinement monoids which satisfy certain descending chain conditions are primely generated. This provides a large class of refinement monoids to which the cancellation results of the previous sections can be applied. Since $\leq$ is a preorder, not a partial order on monoids, we have to extend the usual definitions used for partially ordered sets as follows:

Definition 6.1. *Let $\mathcal{L}$ be a preordered set and $X \subseteq \mathcal{L}$. Then an element $x \in X$ is* **minimal** *in X if for all $y \in X$, $y \leq x$ implies that $x \leq y$. A* **maximal** *element of X is, of course, defined dually.*

The subset X is **Artinian** *if every nonempty subset of X has a minimal element. The equivalent chain condition definition is that X is Artinian if and only if for every decreasing sequence $a_0 \geq a_1 \geq a_2 \geq \ldots$ in X, there is some $N \in \mathbb{N}$ such that $a_n \geq a_N$ for all $n \in \mathbb{Z}^+$.*

If I is a submonoid of M then the preorder of I as a subset of M may be different than its preorder as an independent monoid. Thus a submonoid of an Artinian monoid may not be Artinian.

Example 6.2. [2, 14.2] *Let I be the submonoid of the Artinian monoid $M = \mathbb{Z}^+ \times \mathbb{Z}$ obtained by removing the set $\{(0, m) \mid m \in \mathbb{N}\}$. I is a cancellative refinement monoid. Set $c = (0, -1)$ and $a_m = (1, m)$ for $m \in \mathbb{Z}^+$. One can easily check that $a_0 \geq a_1 \geq a_2 \geq \ldots$ has no minimal element so that the monoid I is not Artinian.*

Note also that $a_0 = a_n + nc$ for $n \in \mathbb{Z}^+$. Thus $nc \leq a_0$ for all $n \in \mathbb{N}$ but $c \not\ll a_0$.

Conversely, a submonoid I which is Artinian with its minimum preorder may not be an Artinian subset of M.

Example 6.3. *The preorder $\leq$ on $\mathbb{R}^+$ is the same as the usual order on real numbers, so $\mathbb{R}^+$ is not Artinian. Let $I = \{0\} \cup [1, \infty) \subseteq \mathbb{R}^+$. Then I is a submonoid which is not an Artinian subset of $\mathbb{R}^+$. Nonetheless, with its own preorder, I is an Artinian monoid.*

The motivation for our discussion of Artinian monoids is the following:

Theorem 6.4. *Any Artinian decomposition monoid is primely generated.*

Proof. Let M be an Artinian decomposition monoid and let $\mathcal{D}$ be the set of elements of M which are not primely generated. If $\mathcal{D}$ is not empty it has a minimal element p. We will show that p is prime, contradicting $p \in \mathcal{D}$.

Suppose $p \leq a_1 + a_2$ for some $a_1, a_2 \in M$, then there are $p_1, p_2 \in M$ such that $p_1 \leq a_1$, $p_2 \leq a_2$ and $p = p_1 + p_2$. Either p_1 or p_2 must be in $\mathcal{D}$ otherwise p would be a sum of primes. But the minimality of p in $\mathcal{D}$ then implies that either $p \leq p_1 \leq a_1$ or $p \leq p_2 \leq a_2$, thus p is prime. □

We will show in 6.7 that a decomposition monoid is Artinian if and only if it has a set of generators which form an Artinian subset. To do so, it is convenient to reformulate the Artinian property in terms of decreasing functions from $\mathbb{Z}^+$ into the monoid:

Definition 6.5. *Let $\mathcal{K}, \mathcal{L}$ be preordered sets. A function $f\colon \mathcal{K} \to \mathcal{L}$ is* **decreasing** *if for all $x, y \in \mathcal{K}$, $x \leq y$ implies $f(x) \geq f(y)$. We will say a decreasing function f* **converges** *if the image of f has a minimal element, and* **diverges** *otherwise.*

If $f, g\colon \mathcal{K} \to \mathcal{L}$ are two functions we will write $f \leq g$ if $f(x) \leq g(x)$ for all $x \in \mathcal{K}$. The relation $\leq$ is, in general, a preorder on functions.

Evidently, a monoid M is Artinian if and only if every decreasing function $f\colon \mathbb{Z}^+ \to M$ converges.

Lemma 6.6. *Let M be a decomposition monoid and $f\colon \mathbb{Z}^+ \to M$ a divergent decreasing function. Suppose $f(n) = x_1 + x_2 + \ldots + x_k$ for some $n \in \mathbb{Z}^+$, $k \in \mathbb{N}$ and $x_1, x_2, \ldots, x_k \in M$. Then there is a divergent decreasing function $f'\colon \mathbb{Z}^+ \to M$ such that*

(1) $f'(n) \in \{x_1, x_2, \ldots, x_k\}$
(2) $f' \leq f$

Proof. We define functions $f_1, f_2, \ldots, f_k\colon \mathbb{Z}^+ \to M$ such that for all $m \geq n$, $f(m) = f_1(m) + f_2(m) + \ldots + f_k(m)$:

For all $m \leq n$ and $i \in \{1, 2, \ldots, k\}$, set $f_i(m) = x_i$. Notice that $f(n) = f_1(n) + f_2(n) + \ldots + f_k(n)$.

To define these functions for $m > n$ we proceed inductively. Assume then that $f_1(m), f_2(m), \ldots, f_k(m)$ have been defined. We have $f(m+1) \leq f(m) = f_1(m) + f_2(m) + \ldots + f_k(m)$, so using the decomposition property, we can define $f_i(m+1)$ for $i \in \{1, 2, \ldots, k\}$ so that $f_i(m+1) \leq f_i(m)$ and

$$f(m+1) = f_1(m+1) + f_2(m+1) + \ldots + f_k(m+1).$$

It is easy to see that each of the functions $f_1, f_2, \ldots, f_k$ is decreasing and satisfies 1 and 2. If all of these functions converge, then there is some $N \in \mathbb{N}$ such that $f_i(m) \geq f_i(N)$ for all $m \geq N$ and $i \in \{1, 2, \ldots, k\}$, and hence $f(m) \geq f(N)$ for $m \geq \max\{n, N\}$. This contradicts our hypothesis that f diverges.

Therefore there must be some index $i \in \{1, 2, \ldots, k\}$ such that f_i diverges. Set $f' = f_i$. □

Theorem 6.7. *Let M be a decomposition monoid with a set of generators $X \subseteq M$. If X is Artinian then M is Artinian.*

Proof. We prove the contrapositive by assuming that there is a divergent decreasing function $f\colon \mathbb{Z}^+ \to M$, and showing this leads to a divergent decreasing function $g\colon \mathbb{Z}^+ \to X$.

Using induction we will construct a sequence of divergent decreasing functions $f \geq f_0 \geq f_1 \geq \ldots$ such that $f_m(m) \in X$ for all $m \in \mathbb{Z}^+$:

Since X generates M, there are $x_1, x_2, \ldots, x_k \in X$ such that $f(0) = x_1 + x_2 + \ldots + x_k$. The lemma then provides a divergent decreasing function f_0 such that $f_0(0) \in X$ and $f \geq f_0$. Suppose now that f_m has been defined as required. Then $f_m(m+1)$ is a finite sum of elements of X and so using the lemma as before, there is a divergent decreasing function $f_{m+1} \leq f_m$ such that $f_{m+1}(m+1) \in X$.

Define the function $g\colon \mathbb{Z}^+ \to X$ by $g(m) = f_m(m)$ for $m \in \mathbb{Z}^+$. Then g is decreasing: If $m \leq n$ in $\mathbb{Z}^+$ then $g(m) = f_m(m) \geq f_n(m) \geq f_n(n) = g(n)$.

Suppose g converges, that is, for some $N \in \mathbb{Z}^+$ we have $g(n) \geq g(N)$ for all $n \geq N$. Then for all $n \geq N$ we get $f_N(n) \geq f_n(n) = g(n) \geq g(N) = f_N(N)$, that is, f_N converges. This is a contradiction and so g must diverge. □

As an immediate consequence of this theorem and 6.4 we get

Corollary 6.8. *Let M be a refinement monoid with a set of generators $X \subseteq M$. If X is Artinian, then M is primely generated. In particular, any finitely generated refinement monoid is primely generated.*

This corollary provides a large class of primely generated refinement monoids, and hence a large class of monoids having the cancellation properties described in the previous two sections.

References

[1] P. Ara, K. R. Goodearl, K. C. O'Meara and E. Pardo, *Separative Cancellation for Projective Modules over Exchange Rings*, Israel J. Math. **105**, (1998), 105-137.
[2] G. Brookfield, *Ph.D. Dissertation*, University of California, Santa Barbara, (1997).
[3] G. Brookfield, *Direct Sum Cancellation of Noetherian Modules*, J. Algebra **200**, (1998), 207-224.
[4] G. Brookfield, *The Grothendieck Group and the Extensional Structure of Noetherian Module Categories*, preprint, (1999).
[5] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups, Vol. I,* Math. Surveys of the A.M.S. **7**, (1961)

[6] H. Dobbertin, *Refinement Monoids, Vaught Monoids and Boolean Algebras,* Math. Ann. **265**, (1983), 475-487.

[7] H. Dobbertin, *Primely Generated Regular Refinement Monoids,* J. Algebra **91**, (1984), 166-175.

[8] K. R. Goodearl, *Partially Ordered Abelian Groups with Interpolation,* A.M.S., (1986).

[9] K. R. Goodearl and F. Wehrung, *Representations of Distributive Semilattices by Dimension Groups, Regular Rings, C^*-Algebras, and Complemented Modular Lattices,* preprint, (1998).

[10] G. Grätzer, *General Lattice Theory,* Academic Press, (1978).

[11] P. A. Grillet, *Interpolation Properties and Tensor Products of Semigroups,* Semigroup Forum **1**, (1970), 162-168.

[12] J. M. Howie, *Fundamentals of Semigroup Theory,* Oxford Univ. Press, (1995).

[13] T. W. Hungerford, *Algebra,* Springer Verlag, (1974).

[14] N. Jacobson, *Basic Algebra I, 2nd ed.*, W.H. Freeman, (1985).

[15] R. S. Pierce, *Countable Boolean Algebras,* in *Handbook of Boolean Algebras*, edited by J. D. Monk with R. Bonnet, Elsevier, (1989), 775-876

[16] R. M. Shortt and F. Wehrung, *Common Extensions of Semigroup-Valued Charges,* J. of Math. Anal. Appl. **187** No. 1, (1994), 235-258.

[17] A. Tarski, *Cardinal Algebras,* Oxford Univ. Press, (1949).

[18] F. Wehrung, *Injective Positively Ordered Monoids I,* J. of Pure and App. Algebra **83**, (1992), 43-82.

[19] F. Wehrung, *Embedding Simple Commutative Monoids into Simple Refinement Monoids,* Semigroup Forum **56**, (1998), 104-129.

[20] F. Wehrung, *The Dimension Monoid of a Lattice,* Algebra Univers. **40**, (1998), 247-411.

Department of Mathematics, University of Iowa, Iowa City IA 52242-1419
E-mail address: `gbrookfi@math.uiowa.edu`