

Factorization theory and decompositions of modules

Nicholas R. Baeth¹ and Roger A. Wiegand²

October 4, 2011

Abstract

Let R be a commutative ring with identity. It often happens that $M_1 \oplus M_2 \oplus \cdots \oplus M_s \cong N_1 \oplus N_2 \oplus \cdots \oplus N_t$ for indecomposable R -modules M_1, M_2, \dots, M_s and N_1, N_2, \dots, N_t with $s \neq t$. This behavior can be captured by studying the commutative monoid $\{[M] \mid M \text{ is an indecomposable } R\text{-module}\}$ with operation given by $[M] + [N] = [M \oplus N]$. In this mostly self-contained exposition, we introduce the reader to the interplay between the the study of direct-sum decompositions of modules and the study of factorizations in commutative monoids.

1 Introduction

Our goal is to study direct-sum decompositions of finitely generated modules over local rings. Unlike the case of vector spaces (modules over fields), a module can decompose as a direct sum of indecomposable modules in several different ways. For example, it is possible to have pairwise non-isomorphic indecomposable modules A, B and C such that $A \oplus B \cong C \oplus C \oplus C$, so even the *number* of indecomposable summands need not be invariant. On the other hand, there *are* a few rules. For instance, one cannot have $A \oplus C \cong B \oplus C$, or $A \oplus A \cong B \oplus B \oplus B$. Information of this sort is encoded in the monoid of isomorphism classes. We will focus mainly on rings of dimension one, and in that context we will determine exactly which semigroups can be realized as semigroups of isomorphism classes. A recurring theme in the paper will be the analogy between direct-sum decompositions of modules and factorization in integral domains.

2 Rings and modules

Throughout this paper R will denote a commutative, Noetherian ring with identity. “Noetherian” means that there is no infinite strictly ascending chain $I_1 \subset I_2 \subset I_3 \subset \dots$ of ideals in R . More generally, an R -module is *Noetherian* provided it has no infinite strictly ascending chain of submodules. Equivalently, every non-empty set of submodules has a maximal element. An R -module M is *finitely generated* if it has a finite subset $\{m_1, \dots, m_t\}$ such that $M = Rm_1 + \cdots + Rm_t$, that is, every element $m \in M$ can be expressed as an R -linear combination of the m_i .

Just as for vector spaces, one can form the direct sum $M_1 \oplus \cdots \oplus M_t$ of a family of modules. This is just the set of t -tuples (x_1, \dots, x_t) with $x_i \in M_i$, and with the obvious coordinate-wise operations. (We will, however, usually write elements of the direct sum as column vectors, in order to allow matrices to operate on the left.) Alternatively, starting with a module M , we can seek an “internal decomposition” of M . We write $M = M_1 \oplus \cdots \oplus M_t$ provided

- (i) each M_i is a submodule of M ,
- (ii) $M_1 + \cdots + M_t = M$, and
- (iii) $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_t) = 0$ for each i .

¹Department of Mathematics and Computer Science, University of Central Missouri, Warrensburg, MO 64093, baeth@ucmo.edu

²Department of Mathematics, University of Nebraska–Lincoln, Lincoln, NE 68588-0130, rwiegand@math.unl.edu

A non-zero R -module M is *decomposable* provided there exist non-zero R -modules M_1, M_2 such that $M \cong M_1 \oplus M_2$; otherwise M is *indecomposable*. (The symbol “ \cong ” denotes isomorphism. Note that the 0 module is not considered to be indecomposable, for the same reason that 1 is not regarded as a prime: it’s useless as a building block!) Sometimes, e.g., in the proof of Proposition 2.1 below, it’s better to work with internal decompositions: a module M is decomposable if and only if there exist non-zero submodules M_1 and M_2 of M such that $M = M_1 \oplus M_2$.

Let \mathcal{C} be a class of finitely generated R -modules. We’ll say that \mathcal{C} is *closed under direct sums, direct summands, and isomorphism*, provided the following holds: Whenever $M, M_1,$ and M_2 are finitely generated R -modules with $M \cong M_1 \oplus M_2$, we have $M \in \mathcal{C} \iff M_1, M_2 \in \mathcal{C}$. Given such a class \mathcal{C} , we will say that \mathcal{C} satisfies the Krull-Remak-Schmidt-Azumaya theorem (KRSA for short), provided the following holds:

(KRSA) If $M_1 \oplus \cdots \oplus M_t \cong N_1 \oplus \cdots \oplus N_u$, where the M_i and N_j are indecomposable modules in \mathcal{C} , then $t = u$ and, after renumbering, $M_i \cong N_i$ for each i .

For example, if K is a field, the class \mathcal{C} of finite-dimensional vector spaces clearly satisfies KRSA: up to isomorphism, the one-dimensional vector space K is the only indecomposable vector space, and a vector space has dimension n if and only if it is isomorphic to a direct sum of n copies of K . For a more interesting example, let R be any commutative principal ideal domain. Then the class \mathcal{C} of finitely generated R -modules satisfies KRSA, by the elementary divisor theorem. The indecomposable modules in \mathcal{C} are the cyclic modules R and $R/(p^n)$, where p is an irreducible element and $n \geq 1$.

One usually includes in KRSA the condition that every module in \mathcal{C} is a direct sum of indecomposable modules. The next two propositions guarantee that in our context (finitely generated modules over Noetherian rings) this condition is automatically satisfied.

Proposition 2.1. *Let M be a non-zero Noetherian module. Then M is a direct sum of finitely many indecomposable modules.*

Proof. We show first that M has an indecomposable direct summand. Suppose not. Then M is decomposable, say, $M = X_1 \oplus Y_1$, with both summands non-zero. Now write $X_1 = X_2 \oplus Y_2$, $X_2 = X_3 \oplus Y_3$, $X_3 = X_4 \oplus Y_4, \dots$, with all of the X_i and Y_i non-zero. For each n we have $X_n \oplus Y_n \oplus Y_{n-1} \oplus \cdots \oplus Y_2 \oplus Y_1 = M$. We get a strictly ascending chain $Y_1 \subset Y_1 \oplus Y_2 \subset Y_1 \oplus Y_2 \oplus Y_3 \subset \dots$ of submodules of M , contradicting the assumption that M is Noetherian.

To complete the proof, choose any indecomposable direct summand Z_1 of M , and write $M = Z_1 \oplus W_1$. If $W_1 = 0$, we’re done; otherwise (by the first paragraph applied to W_1), W_1 has an indecomposable direct summand, say, $W_1 = Z_2 \oplus W_2$, with Z_2 indecomposable. If $W_2 \neq 0$, write $W_2 = Z_3 \oplus W_3$, with Z_3 indecomposable. The chain $Z_1 \subset Z_1 \oplus Z_2 \subset Z_1 \oplus Z_2 \oplus Z_3 \subset \dots$ has to terminate, and eventually we get $M = Z_1 \oplus \cdots \oplus Z_t$. \square

In this paper all of our modules will be finitely generated and therefore, by the next proposition, Noetherian.

Proposition 2.2. *Every finitely generated module over a Noetherian ring is a Noetherian module. Every submodule of a Noetherian module is finitely generated.*

Proof. Given an R -module M and a submodule N , one checks easily that M is Noetherian if and only if both N and M/N are Noetherian. Since $(M_1 \oplus M_2)/(M_1 \oplus 0) \cong M_2$, it follows that the direct sum of two Noetherian modules is again Noetherian, and hence that a free module $R^{(t)}$ is Noetherian if R is a Noetherian ring. Since a module generated by t elements is a homomorphic image of $R^{(t)}$, the result follows. For the last statement, observe that if N were a non-finitely generated submodule of a module M , a doomed but persistent attempt to find a finite generating set $\{x_i\}$ for N would yield an infinite strictly ascending chain $Rx_1 \subset Rx_1 + Rx_2 \subset Rx_1 + Rx_2 + Rx_3 \subset \dots$ of submodules of M . \square

A recurring theme in this paper is the analogy between decompositions of modules and factorization in integral domains. In a Noetherian domain the factorization process for a given element has to terminate. Analogously, the decomposition process of a Noetherian module has to stop in a finite number of steps. One cannot keep splitting off direct summands *ad infinitum*. In the ring of integers, for example, every integer $n \geq 2$ is a finite product of prime numbers. A typical approach to proving this is to show first that n is divisible by some prime p and then to argue, by induction, that $\frac{n}{p}$ is a product of primes. The proof of Proposition 2.1 is in the same spirit.

Here is a family of examples where KRSA fails.

Example 2.3. Let R be a commutative integral domain with two non-principal ideals I and J satisfying $I + J = R$. (For a concrete example, take $R = \mathbb{C}[x, y]$, the polynomial ring in two variables, and let I and J be the maximal ideals $Rx + Ry$ and $Rx + R(y - 1)$.) Then

$$I \oplus J \cong R \oplus (I \cap J).$$

To see this, choose $a \in I$ and $b \in J$ such that $a + b = 1$. Define R -homomorphisms $\varphi : I \oplus J \rightarrow R \oplus (I \cap J)$ and $\psi : R \oplus (I \cap J) \rightarrow I \oplus J$ as follows:

$$\varphi : \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} x + y \\ bx - ay \end{bmatrix} \qquad \psi : \begin{bmatrix} r \\ s \end{bmatrix} \mapsto \begin{bmatrix} ar + s \\ br - s \end{bmatrix}.$$

One checks that φ and ψ are inverses of each other. Since R is a domain, every non-zero ideal is indecomposable as an R -module. Moreover, neither I nor J is isomorphic to R (since, by assumption, neither is a principal ideal). \square

This example indicates that the existence of comaximal proper ideals is likely to lead to failure of KRSA. For this reason we will usually restrict our attention to modules over commutative *local* rings — commutative rings with just one maximal ideal. Notice that a commutative ring is local if and only if the sum of any two non-units is again a non-unit. This observation motivates the following definition:

Definition 2.4. A ring Λ (not necessarily commutative) is said to be *local* provided $\Lambda \neq 0$, and the sum of any two non-units of Λ is again a non-unit.

(The trivial ring in which $1 = 0$ is disqualified, since we want the set of non-units to include 0.) By the way, a *unit* of Λ is an element that has a *two-sided* inverse. An element can have a left inverse without being a unit. For example, in the endomorphism ring Λ of an infinite-dimensional vector space V with basis $\{v_1, v_2, v_3, \dots\}$, consider the unilateral shifts: $\varphi : v_i \mapsto v_{i+1}$ and $\psi : v_{i+1} \mapsto v_i$ (with $\psi(x_1) = 0$). Then $\psi\varphi = 1_V$, but neither φ nor ψ is an automorphism of V .

Proposition 2.5. *Let Λ be a local ring. Then the set J of non-units of Λ is a two-sided ideal of Λ .*

Proof. We begin with three observations. First, $\Lambda \setminus J$ is closed under multiplication, since the product of two units is a unit. Second, if an element x has a left inverse and a right inverse, say, $yx = 1$ and $xz = 1$, then $y = y(xz) = (yx)z = z$, so x is a unit. Third, if $x \in J$ then $x^2 \in J$, for if x^2 were a unit then x would have both a left and a right inverse. Now let $x \in J$ and $\lambda \in \Lambda$. We will show that $\lambda x \in J$; an appeal to symmetry will then imply that $x\lambda \in J$. Suppose $\lambda x \notin J$. Then $\lambda \in J$, else $x = \lambda^{-1}(\lambda x) \notin J$ by our first observation. Also, $x\lambda \in J$, else x would have both a left and a right inverse. In the equation

$$\lambda x = (x + \lambda)^2 - x^2 - x\lambda - \lambda^2,$$

all terms on the right-hand side are in J . Since J is closed under addition, this forces $\lambda x \in J$, contradiction. \square

The reason we're discussing non-commutative rings is that we will need to study endomorphism rings of modules. Given an R -module M , we denote by $\text{End}_R(M)$ the ring of endomorphisms of M , that is, R -homomorphisms from M to M . The addition is pointwise, and the product of f and g is the composition $f \circ g$. Endomorphism rings are rarely commutative. For example, for a vector space V over a field F , $\text{End}_F(V)$ commutes if and only if $\dim(V) \leq 1$. We now observe that the structure of the endomorphism ring of a module determines whether or not the module is indecomposable. We write 1_M (or 1 if there is no ambiguity) to denote the identity map $1_M(m) = m$ for all $m \in M$. Similarly, 0_M (or 0) denotes the map $0_M(m) = 0$ for all $m \in M$.

Proposition 2.6. *Let M be a non-zero R -module. Then M is indecomposable if and only if 0 and 1 are the only idempotents of $\text{End}_R(M)$.*

Proof. Suppose e is an idempotent of $\text{End}_R(M)$ and $e \neq 0, 1$. If $x \in e(M) \cap \text{Ker}(e)$, write $x = e(y)$. Then $x = e^2(y) = e(x) = 0$; thus $e(M) \cap \text{Ker}(e) = (0)$. Also, given any $z \in M$, we have $z = e(z) + (z - e(z)) \in e(M) + \text{Ker}(e)$. We have shown that $M = e(M) \oplus \text{Ker}(e)$. Moreover, $e(M) \neq (0)$ since $e \neq 0$. Choosing any $z \in M$ with $e(z) \neq z$, we have $0 \neq z - e(z) \in \text{Ker}(e)$, and M is decomposable.

Conversely, if $M = M_1 \oplus M_2$, with both summands non-zero, the projection map $x_1 + x_2 \mapsto x_1$ (for $x_i \in M_i$) is a non-trivial idempotent in $\text{End}_R(M)$. \square

Indecomposable modules behave, with respect to direct-sum decompositions, like irreducible elements in an integral domain: They cannot be broken down further. The key to proving unique factorization in a principal ideal domain is to show that irreducible elements enjoy a stronger property. Recall that a non-zero non-unit p in an integral domain D is *prime* provided $p \mid ab \implies p \mid a$ or $p \mid b$. Borrowing notation from factorization theory, we write $X \mid Y$, for R -modules X and Y to indicate that there is an R -module Z such that $X \oplus Z \cong Y$. Soon we will verify KRSA in situations where the indecomposable direct summands all have local endomorphism rings, modeling the proof after unique factorization in \mathbb{Z} . The following lemma says that modules with local endomorphism rings behave like prime elements in a domain and, further, that they can be cancelled from direct-sum relations.

Lemma 2.7. *Let R be a commutative, Noetherian ring, and let M, X, Y , and Z be R -modules. Assume that $E := \text{End}_R(M)$ is a local ring.*

- (i) *If $M \mid X \oplus Y$, then $M \mid X$ or $M \mid Y$ (“primelike”).*
- (ii) *If $M \oplus Z \cong M \oplus Y$, then $Z \cong Y$ (“cancellation”).*

Proof. We’ll prove (i) and (ii) sort of simultaneously. In (i) we have a module Z such that $M \oplus Z \cong X \oplus Y$. In the proof of (ii) we set $X = M$ and again get an isomorphism $M \oplus Z \cong X \oplus Y$. Notice that showing that $M \mid X$ amounts to producing homomorphisms $\alpha : M \rightarrow X$ and $\pi : X \rightarrow M$ such that $\pi\alpha = 1_M$. (See Lemma 3.3.)

Choose reciprocal isomorphisms $\varphi : M \oplus Z \rightarrow X \oplus Y$ and $\psi : X \oplus Y \rightarrow M \oplus Z$. Write

$$\varphi = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \quad \text{and} \quad \psi = \begin{bmatrix} \mu & \nu \\ \sigma & \tau \end{bmatrix},$$

where $\alpha : M \rightarrow X$, $\beta : Z \rightarrow X$, $\gamma : M \rightarrow Y$, $\delta : Z \rightarrow Y$, $\mu : X \rightarrow M$, $\nu : Y \rightarrow M$, $\sigma : X \rightarrow Z$ and $\tau : Y \rightarrow Z$. Since $\psi\varphi = 1_{M \oplus Z} = \begin{bmatrix} 1_M & 0 \\ 0 & 1_Z \end{bmatrix}$, we have $\mu\alpha + \nu\gamma = 1_M$. Therefore, as $\text{End}_{\mathcal{A}}(M)$ is local, either $\mu\alpha$ or $\nu\gamma$ must be an automorphism of M . Assuming that $\mu\alpha$ is an automorphism, we let $\pi = (\mu\alpha)^{-1}\mu : X \rightarrow M$. Then $\pi\alpha = 1_M$, and so $M \mid X$. Similarly, the assumption that $\nu\gamma$ is an isomorphism forces M to be a direct summand of Y . This proves (i).

To prove (ii) we assume that $X = M$. Suppose first that α is a unit of E . We use α to diagonalize φ :

$$\begin{bmatrix} 1 & 0 \\ -\gamma\alpha^{-1} & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & -\alpha^{-1}\beta \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & -\gamma\alpha^{-1}\beta + \delta \end{bmatrix} =: \xi.$$

Since all the matrices on the left are invertible, so must be ξ , and it follows that $-\gamma\alpha^{-1}\beta + \delta : Z \rightarrow Y$ is an isomorphism.

Suppose, on the other hand, that $\alpha \in J := \{\text{non-units of } E\}$. Then $\nu\gamma \notin J$ (as $\mu\alpha + \nu\gamma = 1_M$), and it follows that $\alpha + \nu\gamma \notin J$. We define a new map

$$\psi' := \begin{bmatrix} 1_M & \nu \\ \sigma & \tau \end{bmatrix} : M \oplus Y \rightarrow M \oplus Z,$$

which we claim is an isomorphism. Assuming the claim, we diagonalize ψ' as we did before to φ , obtaining, in the lower-right corner, an isomorphism from Y onto Z . To prove the claim, we use the equation $\psi\varphi = 1_{M \oplus Z}$ to get

$$\psi'\varphi = \begin{bmatrix} \alpha + \nu\gamma & \beta + \nu\gamma \\ 0 & 1_Z \end{bmatrix}.$$

As $\alpha + \nu\gamma$ is an automorphism of M , $\psi'\varphi$ is clearly an automorphism of $M \oplus Z$. Therefore $\psi' = (\psi'\varphi)\varphi^{-1}$ is an isomorphism. \square

We can now prove KRSA for the class \mathcal{C} , provided the indecomposable modules in \mathcal{C} have local endomorphism rings. The reader will notice that the structure of the proof is identical to the proof of unique factorization in the ring of integers. In Section 2.1 this result will be applied to the situation where R is a complete local ring.

Theorem 2.8. *Let R be a commutative Noetherian ring, and let \mathcal{C} be a class of finitely generated modules, closed under direct sums, isomorphism, and direct summands. Assume that $\text{End}_R(M)$ is a local ring for every indecomposable module $M \in \mathcal{C}$. Then KRSA holds in \mathcal{C} .*

Proof. Let t and u be positive integers, and suppose $M_1 \oplus M_2 \oplus \cdots \oplus M_t \cong N_1 \oplus N_2 \oplus \cdots \oplus N_u$, where the M_i and N_j are indecomposable modules in \mathcal{C} . We will use induction on t to verify the conclusion of KRSA. The case $t = 1$ is clear, since M_1 is assumed to be indecomposable. Proceeding inductively, assume that $t \geq 2$. Now $M_t \mid N_1 \oplus \cdots \oplus N_u$. Since $\text{End}_R M_t$ is local, (i) of Lemma 2.7 implies that $M_t \mid N_j$ for some j . But N_j is indecomposable, so in fact $M_t \cong N_j$. After reordering the N_j , we may assume that $j = u$. Using (ii) of Lemma i, we have $M_1 \oplus \cdots \oplus M_{t-1} \cong N_1 \oplus \cdots \oplus N_{u-1}$. The inductive hypothesis now implies that $t - 1 = u - 1$ (so $t = u$), and, after reordering, that $M_i \cong N_i$ for each i . \square

2.1 Completions and a Krull-Remak-Schmidt-Azumaya Theorem

In this section we will see that KSRA holds over any complete local ring. Then, in Section 3, we will get a handle on direct-sum decompositions over arbitrary local rings by analyzing what happens to modules on passage to the completion. For the rest of the paper, we let R be a commutative, Noetherian local ring. Then R has exactly one maximal ideal, and we often denote the ring by the pair (R, \mathfrak{m}) to signal the important role played by the maximal ideal \mathfrak{m} . We can make R into a metric space by declaring two elements x and y to be close to each other provided their difference is in a high power of \mathfrak{m} . More generally, let M be a finitely generated R -module. The Krull Intersection Theorem [Mat86, Theorem 8.10], which we shall not prove here, states that $\bigcap_{n=1}^{\infty} \mathfrak{m}^n M = 0$. Thus, if $x \neq y$ there is an integer n such that $x - y \in \mathfrak{m}^n M \setminus \mathfrak{m}^{n+1} M$. In this case we let $d(x, y) = 2^{-n}$, and we let $d(x, x) = 0$. Note that R is a metric space with metric d . In fact, the triangle inequality holds, in the stronger form $d(x, z) \leq \max\{d(x, y), d(y, z)\}$ for $x, y, z \in M$. The ring R , respectively, the R -module M , is said to be *complete* provided every Cauchy sequence in R , respectively M , converges. Whenever we use the terminology “complete local ring”, it is tacitly assumed that the ring is commutative and Noetherian.

Proposition 2.9. *If (R, \mathfrak{m}) is a complete local ring, then every finitely generated R -module is complete.*

Proof. Given a generating $\{m_1, \dots, m_t\}$ for M , we get a surjective R -homomorphism from the free R -module $R^{(t)}$ onto M by sending the standard basis elements e_i to m_i . Now a direct sum of two complete modules is easily seen to be complete, and it follows by induction that $R^{(r)}$ is complete. Since completeness carries over to homomorphic images, we see that M is complete. \square

The completion \widehat{R} , respectively \widehat{M} , of (R, \mathfrak{m}) , respectively M , with respect to this metric is called the *\mathfrak{m} -adic completion* of R (respectively M). The completion \widehat{M} can be built as the collection of equivalence classes of Cauchy sequences in M , and alternatively as the inverse limit of the modules $M/\mathfrak{m}^n M$, with respect to the natural surjections $\pi_n : M/\mathfrak{m}^{n+1} M \rightarrow M/\mathfrak{m}^n M$. (The inverse limit is the submodule of the direct product $\prod_{n=1}^{\infty} (M/\mathfrak{m}^n M)$ consisting of sequences (x_n) satisfying $\pi_n(x_{n+1}) = x_n$ for each n .) Either viewpoint makes it clear that \widehat{R} is a commutative ring and that \widehat{M} is a finitely generated \widehat{R} -module. It is not hard to show that \widehat{R} is local with maximal ideal $\widehat{\mathfrak{m}} = \mathfrak{m}\widehat{R}$. In fact, $(\widehat{R}, \widehat{\mathfrak{m}})$ is Noetherian, though the proof of this fact is far from trivial. We refer the reader to [AM69, Chapter 10] for the basic theory of completions. For those who like tensor products, we mention that \widehat{M} can be naturally identified with $\widehat{R} \otimes_R M$.

For a familiar example of completion, consider the polynomial ring $F[x]$ in one variable with coefficients in a field F . The ring R of rational functions defined at 0 is then a local ring with maximal ideal $\mathfrak{m} := \{f \in R \mid f(0) = 0\}$. The \mathfrak{m} -adic completion \widehat{R} of R is then the ring $F[[x]]$ of formal power series. Similarly, the completion of the ring of rational numbers with denominators prime to p is the ring of p -adic integers.

Our goal in this section is to prove KRSA for finitely generated modules over a complete local ring. In view of Theorem 2.8 it will be enough to show that indecomposable finitely generated modules have local endomorphism rings. The proof requires a few preliminary results on the Jacobson radical $\mathcal{J}(\Lambda)$ of a ring Λ . This is the intersection of the maximal left ideals of Λ . (One can check that if Λ is a local ring then $\mathcal{J}(\Lambda)$ is exactly the set of non-units of Λ .) We refer the reader to [Lam01, Chapter 2] for a nice treatment of the basics, which we summarize in the next proposition. Recall that an *R -algebra* is ring Λ together with a ring homomorphism $\varphi : R \rightarrow \Lambda$ that carries R into the center of Λ (that is, $(\varphi(r))\lambda = \lambda(\varphi(r))$ for each $r \in R$ and each $\lambda \in \Lambda$). If Λ is an R -algebra and is finitely generated as an R -module (via the structure given by $r\lambda := \varphi(r)\lambda$), then we call Λ a *module-finite R -algebra*.

Proposition 2.10. *Let Λ be a ring, and let $J = \mathcal{J}(\Lambda)$.*

- (i) J is the intersection of the maximal right ideals of Λ and therefore is a two-sided ideal of Λ .
- (ii) $\mathcal{J}(\Lambda/J) = 0$.
- (iii) If (R, \mathfrak{m}) is a commutative local ring and Λ is a module-finite R -algebra, then $\mathfrak{m}\Lambda \subseteq J$.
- (iv) If Λ has the descending chain condition on left ideals (in particular, if Λ is a finite-dimensional algebra over a field), then J is nilpotent.

Given an ideal I of a ring Λ , we say that *idempotents lift modulo I* provided for every idempotent e of Λ/I there is an idempotent \tilde{e} of Λ such that $\tilde{e} + I = e$. Similarly, given a surjective ring homomorphism $\Lambda \twoheadrightarrow \Gamma$, we say that idempotents lift from Γ to Λ provided every idempotent of Γ comes from an idempotent of Λ . (Notice, for example, that the idempotent $\bar{3}$ in $\mathbb{Z}/(6)$ does not lift to an idempotent of \mathbb{Z} .) It is well known that idempotents lift modulo any nil ideal (an ideal in which every element is idempotent). A typical proof of this fact actually yields the following more general result:

Proposition 2.11. *Let I be a two-sided ideal of a (possibly non-commutative) ring Λ , and let e be an idempotent of Λ/I . Given any positive integer n , there is an element $x \in \Lambda$ such that $x + I = e$ and $x \equiv x^2 \pmod{I^n}$.*

Proof. Start with an arbitrary element $u \in \Lambda$ such that $u + I = e$, and let $v = 1 - u$. In the binomial expansion of $(u + v)^{2n-1}$, let x be the sum of the first n terms: $x = u^{2n-1} + \dots + \binom{2n-1}{n-1} u^n v^{n-1}$. Putting $y = 1 - x$ (the other half of the expansion), we see that $x - x^2 = xy \in \Lambda(uv)^n \Lambda$. Since $uv = u(1 - u) \in I$, we have $x - x^2 \in I^n$. \square

Proposition 2.12. *Let (R, \mathfrak{m}) be a complete local ring, and let Λ be a module-finite R -algebra. Then idempotents lift modulo $\mathcal{J}(\Lambda)$.*

Proof. Let $F = R/\mathfrak{m}$, the residue field of R , and put $\bar{\Lambda} = \Lambda/\mathfrak{m}\Lambda$. By Proposition 2.10, $\mathfrak{m}\Lambda \subseteq J := \mathcal{J}(\Lambda)$, and we see that $\mathcal{J}(\bar{\Lambda}) = \bar{J} := J/\mathfrak{m}\Lambda$. Now $\bar{\Lambda}$ is a finite-dimensional F -algebra, and thus \bar{J} is nilpotent, by Proposition 2.10. Now $\Lambda/J \cong (\Lambda/\mathfrak{m}\Lambda)/(J/\mathfrak{m}\Lambda) = \bar{\Lambda}/\bar{J}$ (by the ‘‘Third Isomorphism Theorem’’ [DF04, Sec. 10.2]). We have factored our homomorphism $\Lambda \twoheadrightarrow \Lambda/J$ as the composite $\Lambda \twoheadrightarrow \bar{\Lambda} \twoheadrightarrow \bar{\Lambda}/\bar{J}$, thereby dividing the heavy lifting into two stages. Proposition 2.11 takes care of the first stage, from $\bar{\Lambda}/\bar{J}$ to $\bar{\Lambda}$. Therefore it will suffice to show that every idempotent e of $\bar{\Lambda} = \Lambda/\mathfrak{m}\Lambda$ lifts to an idempotent of Λ .

Using Proposition 2.11, we can choose, for each positive integer n , an element $x_n \in \Lambda$ such that $x_n + \mathfrak{m}\Lambda = e$ and $x_n \equiv x_n^2 \pmod{\mathfrak{m}^n \Lambda}$. (Of course $\mathfrak{m}^n \Lambda = (\mathfrak{m}\Lambda)^n$.) We claim that (x_n) is a Cauchy sequence for the \mathfrak{m} -adic topology on Λ . To see this, let n be an arbitrary positive integer. Given any $m \geq n$, put $z = x_m + x_n - 2x_m x_n$. Then $z \equiv z^2 \pmod{\mathfrak{m}^n \Lambda}$. Also, since $x_m \equiv x_n \pmod{\mathfrak{m}\Lambda}$, we see that $z \equiv 0 \pmod{\mathfrak{m}\Lambda}$, so $1 - z$ is a unit of Λ . Since $z(1 - z) \in \mathfrak{m}^n \Lambda$, it follows that $z \in \mathfrak{m}^n \Lambda$. Thus we have

$$x_m + x_n \equiv 2x_m x_n, \quad x_m \equiv x_m^2, \quad x_n \equiv x_n^2 \pmod{\mathfrak{m}^n \Lambda}.$$

Multiplying the first congruence, in turn, by x_m and by x_n , we learn that $x_m \equiv x_m x_n \equiv x_n \pmod{\mathfrak{m}^n \Lambda}$. If, now, $\ell \geq n$ and $m \geq n$, we see that $x_\ell \equiv x_m \pmod{\mathfrak{m}^n \Lambda}$. This verifies the claim. Since, by Proposition 2.9, Λ is \mathfrak{m} -adically complete, we let x be the limit of the sequence (x_n) .

Let’s check that x is an idempotent lifting e . Given any $n \geq 1$, choose $m \geq n$ such that $x \equiv x_m \pmod{\mathfrak{m}^n \Lambda}$. Then $x^2 \equiv x_m^2 \pmod{\mathfrak{m}^n \Lambda}$. By construction, $x_m - x_m^2 \in \mathfrak{m}^n \Lambda$, and since $\mathfrak{m}^m \Lambda \subseteq \mathfrak{m}^n \Lambda$, we see that $x \equiv x^2 \pmod{\mathfrak{m}^n \Lambda}$. Since n was arbitrary, the distance between x and x^2 is 0, that is, $x = x^2$. Taking $n = 1$ and choosing m as above, we have $x \equiv x_m \pmod{\mathfrak{m}\Lambda}$; thus $x + \mathfrak{m}\Lambda = x_m + \mathfrak{m}\Lambda = e$. \square

Theorem 2.13. *Let (R, \mathfrak{m}) be a complete local ring. Then KSRA holds for the class of finitely generated R -modules.*

Proof. By Theorem 2.8 it will suffice to show that $\Lambda := \text{End}_R(M)$ is local whenever M is an indecomposable finitely generated R -module. Note that $\text{End}_R(M)$ is an R -algebra via the ring homomorphism $r \mapsto$ (multiplication by r). Moreover, one can show, since R is Noetherian and M is finitely generated, that $\text{End}_R(M)$ is module-finite over R . (See Lemma 3.2 for a more general result.)

Since M is indecomposable, Λ has no idempotents other than 0 and 1. Now Proposition 2.12 implies that $\Lambda/\mathcal{J}(\Lambda)$ has no interesting idempotents either. By Proposition 2.10, $\mathfrak{m}\Lambda \subseteq J := \mathcal{J}(\Lambda)$, so Λ/J is a homomorphic

image of the finite-dimensional algebra $\Lambda/\mathfrak{m}\Lambda$ over the field $F := R/\mathfrak{m}$. Therefore Λ/J has the descending chain condition on left ideals; and $\mathcal{J}(\Lambda/J) = 0$ by Proposition 2.10. By the Wedderburn-Artin Theorem [Lam01, Theorem 3.5], Λ/J is isomorphic to a direct product $\mathbb{M}_{n_1}(D_1) \times \cdots \times \mathbb{M}_{n_r}(D_r)$ of full matrix rings over division rings D_1, \dots, D_r . But since 0 and 1 are the only idempotents of Λ/J , we see that $r = 1$ and $n_1 = 1$, that is, Λ/J is a division ring. It follows that J is exactly the set of non-units of Λ , and hence that Λ is a local ring. \square

3 Monoids of Modules

For our purposes, a *monoid* is a commutative, additive semigroup with identity element. In keeping with the additive notation, we denote the identity element by “0”. We will consider two additional conditions one might impose on a monoid:

- i) A monoid Λ is *cancellative* provided $a + c = b + c \implies a = b$ for all $a, b, c \in \Lambda$.
- ii) A monoid Λ is *reduced* provided $a + b = 0 \implies a = b = 0$ for all $a, b, c \in \Lambda$.

For a Noetherian local ring (R, \mathfrak{m}) , we define $\mathcal{M}(R)$ to be the set of isomorphism classes $[M]$ of finitely generated R -modules M , endowed with the monoid structure given by the direct sum: $[M] + [N] = [M \oplus N]$. Obviously $\mathcal{M}(R)$ is commutative and reduced, and we’ll see below, in Corollary 3.7, that $\mathcal{M}(R)$ is cancellative. In the next definition, we formulate several concepts we will need in the language of monoids.

Definition 3.1. An element x of a monoid is an *atom* provided (i) $x \neq 0$, and (ii) $x = y + z \implies y = 0$ or $z = 0$. A monoid Λ is *atomic* provided it is reduced and cancellative, and every non-zero element of Λ is a finite sum of atoms. A *factorial* monoid is an atomic monoid in which the representation as a sum of atoms is unique up to order of the summands. In detail: If x_i and y_j are atoms of Λ and $x_1 + \cdots + x_m = y_1 + \cdots + y_n$, then $m = n$, and, after a permutation of $\{1, \dots, m\}$, $x_i = y_i$ for $i = 1, \dots, m$. A monoid homomorphism $\varphi : \Lambda \rightarrow \Gamma$ is a *divisor homomorphism* provided $x \mid y \iff \varphi(x) \mid \varphi(y)$ for all $x, y \in \Lambda$. Here, $x \mid y$ means there is $z \in \Lambda$ with $x + z = y$.

In an atomic monoid Λ , let H be the set of atoms. Since every element of Λ is uniquely an \mathbb{N}_0 -linear combination of elements of H , we see that Λ is a free monoid with basis H . In particular, $\Lambda \cong \mathbb{N}_0^{(\Omega)}$, where Ω is an index set of cardinality $|H|$. In what follows, we will use the terms “factorial monoid” and “free monoid” interchangeably.

For reduced, cancellative monoids, divisor homomorphisms are injective: If $\varphi(x) = \varphi(y)$, then $x \mid y$ and $y \mid x$, say, $x + a = y$ and $y + b = x$. Then $x + a + b = x + 0$, whence $a + b = 0$. Therefore $a = b = 0$, so $x = y$.

A finitely generated R -module M is indecomposable if and only if $[M]$ is an atom of $\mathcal{M}(R)$. Expressing a finitely generated R -module M as a direct sum of indecomposable modules amounts to writing $[M]$ as a sum of atoms of $\mathcal{M}(R)$. Given a submonoid Λ of $\mathcal{M}(R)$ closed under direct summands, finite direct sums, and isomorphism, we see that Λ is factorial if and only if Λ satisfies KRSA. (Remember we are tacitly assuming that R is Noetherian, so Proposition 2.2 and Proposition 2.1 ensure that $\mathcal{M}(R)$ and Λ are atomic.) In particular, $\mathcal{M}(R)$ is factorial if (R, \mathfrak{m}) is a complete local ring. This suggests that we should try to understand the monoid homomorphism $\Phi : \mathcal{M}(R) \rightarrow \mathcal{M}(\widehat{R})$ taking $[M]$ to $[\widehat{M}]$. This approach is used in virtually every area of mathematics: To understand obstreperous behavior, pass to a structure where the behavior is well understood, and then see how much information is lost in the passage. As it turns out, the homomorphism Φ is a divisor homomorphism (Theorem 3.6) and, in particular, is injective. What is sometimes lost is indecomposability: it can happen that M is indecomposable but \widehat{M} is not. This phenomenon is the source of the fun we’ll have when studying the monoids $\mathcal{M}(R)$.

The proof that Φ is a divisor homomorphism involves several little tricks, the first of which is to describe the relation $M \mid N$ in terms of homomorphisms. We let $\text{Hom}_R(M, N)$ denote the set of R -homomorphisms from M to N . This is an abelian group with pointwise operations. In fact, it’s also an R -module: If $f \in \text{Hom}_R(M, N)$ and $r \in R$, the product rf is defined by $(rf)(x) = rf(x)$. (Notice that the fact that rf is an R -homomorphism depends on the fact that R is commutative!)

Lemma 3.2. *Let M and N be finitely generated modules over a commutative Noetherian ring A . Then $\text{Hom}_A(M, N)$ is finitely generated as an A -module.*

Proof. Let $\{x_1, \dots, x_t\}$ be a set of generators for N , and define an R -homomorphism $\varphi : \text{Hom}_A(M, N) \rightarrow N^{(t)}$ by

$$\varphi(f) = \begin{bmatrix} f(x_1) \\ \vdots \\ f(x_t) \end{bmatrix}.$$

Then φ is injective. Since, by Proposition 2.2, $N^{(t)}$ is Noetherian, $\text{Hom}_A(M, N)$ is finitely generated. \square

Lemma 3.3. *Let M and N be finitely generated R -modules. Then $M \mid N$ if and only if there are homomorphisms $\alpha \in \text{Hom}_R(M, N)$ and $\beta \in \text{Hom}_R(N, M)$ such that $\beta\alpha = 1_M$.*

Proof. If $\beta\alpha = 1_M$, then α is injective, so $\alpha(M) \cong M$. One checks easily that $N = \alpha(M) \oplus \text{Ker}(\beta)$. For the converse, suppose $M \oplus X \cong N$. Choose reciprocal isomorphisms

$$\begin{bmatrix} \alpha & \sigma \end{bmatrix} : M \oplus X \rightarrow N \quad \text{and} \quad \begin{bmatrix} \beta \\ \tau \end{bmatrix} : N \rightarrow M \oplus X.$$

Then

$$\begin{bmatrix} 1_M & 0 \\ 0 & 1_X \end{bmatrix} = \begin{bmatrix} \beta \\ \tau \end{bmatrix} \begin{bmatrix} \alpha & \sigma \end{bmatrix} = \begin{bmatrix} \beta\alpha & \beta\sigma \\ \tau\alpha & \tau\sigma \end{bmatrix},$$

and the top left corner yields the equation we want. \square

Here is one of the most useful results in all of commutative algebra:

Lemma 3.4 (Nakayama's Lemma). *Let (A, \mathfrak{m}) be a commutative local ring, M a finitely generated A -module, and N a submodule of M . If $N + \mathfrak{m}M = M$, then $N = M$.*

Proof. By passing to M/N , we may assume that $N = 0$. Suppose, by way of contradiction, that $M \neq 0$. Let $\{x_1, \dots, x_t\}$ be a minimal generating set; then $t \geq 1$. Since $M = \mathfrak{m}M$, we can write $x_t = a_1x_1 + \dots + a_{t-1}x_{t-1} + a_t x_t$. Let $u = 1 - a_t$. Since $u \notin \mathfrak{m}$, u is a unit of A , and we have $x_t = u^{-1}(a_1x_1 + \dots + a_{t-1}x_{t-1})$. (By convention, the right-hand side is 0 if $t = 1$). It follows that $M = Ax_1 + \dots + Ax_{t-1}$, and this contradicts minimality of the original generating set. \square

Lemma 3.5. *Let M be a Noetherian R -module. Every surjective R -endomorphism of M is an automorphism.*

Proof. Let $f : M \rightarrow M$, and put $L_n = \text{Ker}(f^n)$ for $n \geq 1$. The sequence $L_1 \subseteq L_2 \subseteq L_3 \subseteq \dots$ has to stabilize. Choose any $n \geq 1$ such that $L_n = L_{2n}$, and let x be an arbitrary element of L_n . Since f^n is surjective, there is an element $y \in M$ with $f^n(y) = x$. Then $f^{2n}(y) = f^n(x) = 0$, so $y \in L_{2n} = L_n$, and hence $x = 0$. This shows that $L_n = 0$, whence $L_1 = 0$. \square

Theorem 3.6. *Let (R, \mathfrak{m}) be a commutative Noetherian local ring, and let M and N be finitely generated R -modules. Then $M \mid N \iff \widehat{M} \mid \widehat{N}$. In other words, the homomorphism $\Phi : \mathcal{M}(R) \rightarrow \mathcal{M}(\widehat{R})$, taking $[M]$ to $[\widehat{M}]$, is a divisor homomorphism.*

Proof. If $M \mid N$, say, $M \oplus X \cong N$, then $\widehat{M} \oplus \widehat{X} \cong \widehat{N}$, so $\widehat{M} \mid \widehat{N}$. For the converse, we choose, using Lemma 3.3, homomorphisms $\alpha \in \text{Hom}_{\widehat{R}}(\widehat{M}, \widehat{N})$ and $\beta \in \text{Hom}_{\widehat{R}}(\widehat{N}, \widehat{M})$ such that $\beta\alpha = 1_{\widehat{M}}$. Put $H = \text{Hom}_R(M, N)$, a finitely generated R -module by Lemma 3.2. Every $h \in H$ induces an element $\widehat{h} \in \text{Hom}_{\widehat{R}}(\widehat{M}, \widehat{N})$. Moreover, $\text{Hom}_{\widehat{R}}(\widehat{M}, \widehat{N})$ is naturally isomorphic to the completion \widehat{H} [Mat86, Theorems 7.11 and 8.14]. This means that α can be approximated to any order by elements of H . Taking a first-order approximation, we obtain $f \in H$ such that $(\widehat{f} - \alpha)(\widehat{M}) \subseteq \widehat{\mathfrak{m}}\widehat{N}$. Similarly, we find $g \in \text{Hom}_R(N, M)$ such that $(\widehat{g} - \beta)(\widehat{N}) \subseteq \widehat{\mathfrak{m}}\widehat{M}$. Now $\widehat{g}\widehat{f} - 1_{\widehat{M}} = \widehat{g}\widehat{f} - \beta\alpha = (\widehat{g} - \beta)\alpha + (\widehat{g}\widehat{f} - \beta\alpha)$, and it follows that $(\widehat{g}\widehat{f} - 1_{\widehat{M}})(\widehat{M}) \subseteq \widehat{\mathfrak{m}}\widehat{M}$. Therefore $\widehat{M} = \widehat{g}\widehat{f}(\widehat{M}) + \widehat{\mathfrak{m}}\widehat{M}$, and now Nakayama's Lemma implies that $\widehat{g}\widehat{f}(\widehat{M}) = \widehat{M}$. From the view of \widehat{M} as the inverse limit of the modules M/\mathfrak{m}^t , we see that the endomorphisms of $M/\mathfrak{m}^t M$ induced by the composition gf are surjective for each t . Another application of Nakayama's Lemma shows that gf is itself surjective and hence, by Lemma 3.5, an automorphism of M . Letting $h = (gf)^{-1}g : N \rightarrow M$, we see that $hf = 1_M$, and now Lemma 3.3 implies that $M \mid N$. \square

The following easy corollary of Theorem 3.6 will be useful as we consider examples in Section 4.2.

Corollary 3.7. *Let (R, \mathfrak{m}) be a commutative Noetherian local ring, and let M and N be finitely generated R -modules. If $\widehat{M} \cong \widehat{N}$, then $M \cong N$. The monoid $\mathcal{M}(R)$ is reduced and cancellative.*

Proof. If $\widehat{M} \cong \widehat{N}$, then trivially $\widehat{M} \mid \widehat{N}$ and $\widehat{N} \mid \widehat{M}$. Applying Theorem 3.6, we see $M \mid N$ and $N \mid M$. Therefore $N \cong M \oplus X$ and $M \cong N \oplus Y$ for some finitely generated R -modules X and Y , and hence $N \cong N \oplus Y \oplus X$. Passing to finite-dimensional vector spaces over the field R/\mathfrak{m} , we have $N/\mathfrak{m}N \cong N/\mathfrak{m}N \oplus Y/\mathfrak{m}Y \oplus X/\mathfrak{m}X$, whence $Y/\mathfrak{m}Y = X/\mathfrak{m}X = 0$. Now Nakayama's Lemma implies that $X = Y = 0$. This shows that $M \cong N$.

Obviously $\mathcal{M}(R)$ is reduced. To verify that it is cancellative, suppose A, B and C are finitely generated R -modules with $A \oplus C \cong B \oplus C$. Passing to the completion, we have $\widehat{A} \oplus \widehat{C} \cong \widehat{B} \oplus \widehat{C}$. Writing each of these \widehat{R} -modules as a direct sum of indecomposable modules, and using KRSA (Theorem 2.13), we easily deduce that $\widehat{A} \cong \widehat{B}$, and now the first part of the corollary implies that $A \cong B$. \square

Assumption 3.8. From now on, all of our monoids will be assumed to be reduced and cancellative.

Except in special situations, $\mathcal{M}(R)$ is too big and complex to afford a precise description. We will focus on little pieces of the monoid, whose descriptions will still give us enough information to determine whether or not KRSA uniqueness holds, or how badly it fails. We fix a finitely generated R -module M and then look at the smallest submonoid of $\mathcal{M}(R)$ that contains $[M]$ and is closed under direct summands and finite direct sums.

Notation 3.9. For a finitely generated R -module M , $\text{add}(M)$ consists of isomorphism classes $[N]$ of finitely generated modules N that are direct summands of direct sums of finitely many copies of M .

Thus $[N] \in \text{add}(M)$ if and only if there exist a module V and a positive integer t such that $N \oplus V \cong M^{(t)}$. If, for example, we want to understand the direct-sum relations among modules M_1, \dots, M_s , we might take $M = M_1 \oplus \dots \oplus M_s$. All of these relations are encoded in the monoid structure of $\text{add}(M)$.

Similarly, for an element x in a monoid H , we can define $\text{add}(x)$: an element $h \in H$ belongs to $\text{add}(x)$ if and only if there exist an element $y \in H$ and a positive integer n such that $h + y = nx$.

3.1 $\text{add}(M)$ as a submonoid of $\mathbb{N}_0^{(t)}$

Let M be a non-zero finitely generated module over a commutative, Noetherian local ring (R, \mathfrak{m}) . Write $\widehat{M} = V_1^{(n_1)} \oplus \dots \oplus V_t^{(n_t)}$, where

- (i) each V_i is an indecomposable \widehat{R} -module,
- (ii) each n_i is a positive integer, and
- (iii) $V_i \not\cong V_j$ if $i \neq j$.

We preserve this fixed ordering of the indecomposable direct summands V_i of \widehat{M} . Given any $[N] \in \text{add}(M)$, we clearly have $[\widehat{N}] \in \text{add}(\widehat{M})$; therefore $\widehat{N} \cong V_1^{(a_1)} \oplus \dots \oplus V_t^{(a_t)}$, where the a_i are non-negative integers. Let \mathbb{N}_0 denote the additive monoid of non-negative integers. We have a monoid homomorphism $\Psi : \text{add}(M) \rightarrow \mathbb{N}_0^{(t)}$ taking $[N]$ to the t -tuple $[a_1 \dots a_t]$. In fact, this is a divisor homomorphism: If $[N_1]$ and $[N_2]$ are in $\text{add}(M)$ and $\Psi([N_1]) \mid \Psi([N_2])$, then clearly $\widehat{N}_1 \mid \widehat{N}_2$. Now Theorem 3.6 implies that $N_1 \mid N_2$, that is, $[N_1] \mid [N_2]$. We can identify $\text{add}(M)$ with its image $\Gamma(M) := \Psi(\text{add}(M))$, a submonoid of $\mathbb{N}_0^{(t)}$. In the monoid $\mathbb{N}_0^{(t)}$, we have $\alpha \mid \beta$ if and only if $\alpha \leq \beta$ with the coordinate-wise partial ordering: $[a_1 \dots a_t] \leq [b_1 \dots b_t]$ if and only if $a_i \leq b_i$ for each i . After making this identification, we see that

$$N_1 \mid N_2 \text{ if and only if } [N_1] \leq [N_2] \text{ with respect to the coordinate-wise partial ordering on } \mathbb{N}_0^{(t)}. \quad (3.1)$$

Definition 3.10. A *full* submonoid of a monoid Γ is a submonoid Γ' such that the inclusion $\Gamma' \hookrightarrow \Gamma$ is a divisor homomorphism.

In summary, we have proved the following:

Theorem 3.11. *Let M be a finitely generated module over a commutative, Noetherian local ring (R, \mathfrak{m}) . Let t be the number of non-isomorphic indecomposable \widehat{R} -modules in the (unique) decomposition of \widehat{M} as a direct sum of indecomposables. Then Ψ provides an isomorphism between $\text{add}(M)$ and the full submonoid $\Gamma(M)$ of $\mathbb{N}_0^{(t)}$. The module M is indecomposable if and only if $\Psi([M])$ is a minimal element of $\Gamma(M) - \{[0 \ 0 \ \dots \ 0]\}$.*

Using this perspective, we can explain a comment in the introduction: One cannot have finitely generated modules A and B over a local ring such that A is indecomposable and $A \oplus A \cong B \oplus B \oplus B$. Suppose the contrary, and let $M = A \oplus B$. Note that $a := [A]$ and $b := [B]$ are non-zero elements of $\text{add}(M)$. We have $2a = 3b$, so $b \leq a$. But then $b \mid a$ by (3.1). Since a is indecomposable and $b \neq 0$, we have $b = a$. But then the relation $2a = 3a$ forces $a = 0$, a contradiction.

Monoids admitting a full embedding into a free monoid $\mathbb{N}_0^{(t)}$ are the subject of intense study and go by several different names. People working in the factorization theory of monoids refer to them as “finitely generated Krull monoids” or “Diophantine monoids” (more on that later). They also figure prominently in applications of commutative algebra to simplicial topology. See, e.g., the book by Bruns and Herzog [BH93], where they are called “positive normal affine monoids”.

3.2 One-dimensional rings and Diophantine monoids

The *dimension* of a commutative ring A is the supremum of integers r for which A has a chain $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r$ of prime ideals. It can be shown [BH93] that for a local Noetherian ring (R, \mathfrak{m}) , the ring R and its completion \widehat{R} have the same dimension. Soon we will restrict our attention to one-dimensional local rings (R, \mathfrak{m}) . With this restriction we will be able to describe exactly how $\mathcal{M}(R)$ sits inside $\mathcal{M}(\widehat{R})$, that is, exactly which \widehat{R} -modules come from R -modules. (We say, informally, that a finitely generated \widehat{R} -module N comes from an R -module provided there is a finitely generated R -module M such that $\widehat{M} \cong N$. We will soon make this concept formal.)

A *Diophantine* monoid is a monoid isomorphic to the monoid of non-negative integer solutions to a finite system of homogeneous linear equations with integer coefficients. Thus H is Diophantine if and only if there exist positive integers s and t and an $s \times t$ integer matrix φ such that $H \cong (\text{Ker}(\varphi)) \cap \mathbb{N}_0^{(t)}$. In this case we see that H is a full submonoid of $\mathbb{N}_0^{(t)}$. In fact the converse holds: If H is a full submonoid of some $\mathbb{N}_0^{(r)}$ then in fact H is Diophantine (though one might have to take the integer t in the definition strictly larger than r). A proof of this fact, attributed to M. Hochster, is outlined in Exercise 6.1.10 on page 263 of [BH93]. The big theorem we are heading toward is a *realization theorem*, which says that given any Diophantine monoid H there is a one-dimensional local Noetherian integral domain (R, \mathfrak{m}) and a finitely generated R -module M such that $\Gamma(M) \cong H$.

In dimension one, the *rank* of an \widehat{R} -module N , defined in terms of the localizations at the minimal prime ideals, is the key to determining whether or not N comes from an R -module. Let A be any commutative ring, not necessarily local. If P is a prime ideal of A , then A_P denotes the set of formal fractions $\frac{a}{s}$ where $a \in A$ and $s \in A \setminus P$, with the following equivalence relation: $\frac{a}{s} = \frac{a'}{s'}$ iff there exists $t \in A \setminus P$ such that $t(as' - a's) = 0$. The familiar operations $\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$ and $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$ then make A_P into a local ring, called the “localization of A at P ”. (The maximal ideal is the set of fractions whose numerators are in P .) If A is an integral domain and we take $P = (0)$, then A_P is the quotient field of A . For another example, let $A = \mathbb{R}[x]$, fix a point $p \in \mathbb{R}$, and let P be the maximal ideal consisting of polynomials f for which $f(p) = 0$. Then A_P is the ring of rational functions that are defined near p (whence the term “local”). The prime ideals of A_P are exactly the ideals QA_P , where Q is a prime ideal of A and $Q \subseteq P$.

We will be particularly interested in localizations at *minimal primes*. These are the prime ideals P that contain no prime ideal properly. More generally, given an ideal I of A , a *minimal prime* of I is a prime ideal P such that $I \subseteq P$ and there is no prime ideal Q with $I \subseteq Q \subsetneq P$. The minimal primes of A are thus the minimal primes of the ideal (0) .

We can localize modules too: For an A -module M and a prime ideal P of A , M_P is the set of formal fractions $\frac{m}{s}$ where $m \in M$ and $s \in A \setminus P$ (with a similar equivalence relation). The multiplication $(a/s)(m/t) = (am)/(st)$ makes M_P into an A_P -module. If M is finitely generated as an A -module, then M_P is a finitely generated R_P -module: if m_1, \dots, m_t generate M over A , then the fractions $m_i/1$ generate M_P over A_P .

Proposition 3.12. *If A is a Noetherian ring, then A has only finitely many minimal primes.*

Proof. The proof is a quintessential example of a process called “Noetherian induction”. We will prove the formally stronger statement that every ideal has only finitely many minimal primes. Suppose this fails. Then, since A is Noetherian, there is an ideal I maximal with respect to having infinitely many minimal primes. Then I is certainly not a prime ideal, so there are elements $x, y \in A - I$ such that $xy \in I$. The ideals $K := I + Ax$ and $L := I + Ay$ each have only finitely many minimal primes, since they contain I properly. Now every minimal prime P of I must contain either K or L and must therefore be either a minimal prime of K or a minimal prime of L , an obvious contradiction. \square

In a commutative ring A , the set $\text{Nil}(A)$ of nilpotent elements is exactly the intersection of the prime ideals of A . (If $x \notin \text{Nil}(A)$, Zorn’s Lemma provides an ideal P maximal with respect to containing no power of x , and a little fiddling shows that P is a prime ideal.) We say that A is *reduced* provided $\text{Nil}(A) = (0)$. (The word “reduced” here has little to do with the property defined above for monoids; it’s just one of those unfortunate collisions of terminology.)

Lemma 3.13. *Let P be a minimal prime ideal in a commutative reduced ring A . Then A_P is a field.*

Proof. Suppose x is a non-unit of A_P ; our goal is to show that $x = 0$. We have $xA_P \subsetneq A_P$, and Zorn’s Lemma implies that xA_P is contained in some maximal ideal \mathfrak{m} of A_P . Since P is a minimal prime, PA_P is the unique prime ideal of A_P and therefore must equal $\text{Nil}(A_P)$. An easy computation shows that $\text{Nil}(A_P) = (0)$, so (0) is the unique prime ideal of A_P . Since maximal ideals are prime, we have $\mathfrak{m} = (0)$, whence $x = 0$. \square

Assume, now, that (R, \mathfrak{m}) is reduced (and Noetherian and local as always), and let M be a finitely generated R -module. For a minimal prime ideal P of R , let $\text{rank}_P(M)$ denote the dimension of M_P as a vector space over the field R_P . If P_1, \dots, P_s are all of the minimal primes of R , the *rank* of M is the s -tuple (r_1, \dots, r_s) , where $r_i = \text{rank}_{P_i}(M)$. If $r_i = r_j$ for all i, j , we say that M has *constant rank*.

Suppose, for example, that R has three minimal primes P_1, P_2 , and P_3 . Then the R -module R has rank $(1, 1, 1)$. The R -module R/P_1 has rank $(1, 0, 0)$, and $R/(P_1 \cap P_2)$ has rank $(1, 1, 0)$. One can show easily that R/\mathfrak{m} has rank $(0, 0, 0)$.

In general, suppose that P_1, P_2, \dots, P_s are the minimal primes of R , and let $E \subseteq \{1, 2, \dots, s\}$. Then

$$\text{rank} \left(\frac{R}{\bigcap_{i \in E} P_i} \right) = (r_1, \dots, r_s), \text{ where } r_i = \begin{cases} 1, & i \in E \\ 0, & i \notin E \end{cases} .$$

It follows that *every* s -tuple of zeros and ones can be realized as the rank of a cyclic R -module. Moreover, every non-zero cyclic module R/I over a local ring (R, \mathfrak{m}) is indecomposable. We’ll refer to s -tuples of zeros and ones as *boring* s -tuples. Soon we will see how to build indecomposable modules with more interesting ranks. As we shall see in Interlude 3.19, however, even modules with boring ranks sometimes suffice to demonstrate failure of KRSA.

Assumptions 3.14. From now on (R, \mathfrak{m}) is a local noetherian ring of dimension one, and its minimal primes are P_1, \dots, P_s . We assume further that \widehat{R} is reduced (so of course R is reduced as well).

We now return to the question of which \widehat{R} -modules come from R -modules. We’ll also need to know which \widehat{R} -modules come from *indecomposable* R -modules. We’ll call a non-zero finitely generated \widehat{R} -module N *extended* if $N \cong \widehat{M}$ for some finitely generated R -module M , and *minimally extended* if, in addition, no non-zero proper direct summand of M is extended.

Let’s rephrase Theorem 3.11 in these terms.

Corollary 3.15. *Let M be a finitely generated R -module. These are equivalent:*

- (i) M is indecomposable.
- (ii) \widehat{M} is minimally extended.
- (iii) $\Psi([M])$ is a minimal element of $\Gamma(M) - \{[0 \ 0 \ \dots \ 0]\}$.

For one-dimensional rings, we have the following result due to L. S. Levy and C. Odenthal [LO96, Theorem 6.2], which tells us exactly which \widehat{R} -modules are extended. There is a partial result for certain two-dimensional rings, but there is no such result for rings of dimension greater than two; in fact, the general question of which modules over the completion of a local ring A come from A -modules seems to be extremely difficult.

Proposition 3.16. *Let (R, \mathfrak{m}) be a one-dimensional Noetherian local ring. Let \widehat{R} denote the \mathfrak{m} -adic completion of R , and assume \widehat{R} is reduced. Let M be a finitely generated \widehat{R} -module. Then M is extended from an R -module if and only if $\text{rank}_P(M) = \text{rank}_Q(M)$ whenever P and Q are minimal prime ideals of \widehat{R} with $P \cap R = Q \cap R$. \square*

We will not prove this result here, but refer the reader to [LO96, Theorem 6.2]. If R is a domain, then 0 is the only minimal prime ideal of R , and Proposition 3.16 takes the following form:

Corollary 3.17. *Let (R, \mathfrak{m}) be a one-dimensional Noetherian local integral domain. Let \widehat{R} denote the \mathfrak{m} -adic completion of R , and assume \widehat{R} is reduced. Let M be a finitely generated \widehat{R} -module. Then M is extended from an R -module if and only if M has constant rank. \square*

Given a finitely generated R -module M , we know that $\text{add}(M)$ can be viewed as a full submonoid of some $\mathbb{N}_0^{(t)}$. Using Proposition 3.16, we can, in fact, represent $\text{add}(M)$ as a Diophantine monoid. (Although this follows purely formally from Theorem 3.11 and the fact [BH93, Exercise 6.1.10] that full submonoids of $\mathbb{N}_0^{(t)}$ are always Diophantine, it is instructive to see exactly where the defining equations come from.)

Theorem 3.18. *Let (R, \mathfrak{m}) be a one-dimensional local ring with reduced completion \widehat{R} , and let M be a finitely generated R -module. Then $\text{add}(M)$ is a Diophantine monoid.*

Proof. By Theorem 3.11 it will suffice to show that $\Gamma(M)$ is a Diophantine monoid. Let P_1, \dots, P_s be the minimal prime ideals of \widehat{R} . As in Section 3.1, write $\widehat{M} = V_1^{(n_1)} \oplus \dots \oplus V_t^{(n_t)}$, where the V_j are non-isomorphic indecomposable \widehat{R} -modules and the n_j are positive integers. Let $r_{ij} = \dim_{R/P_i}((V_j)_{P_i})$, so that $(r_{1j}, \dots, r_{sj}) = \text{rank}(V_j)$.

Suppose $a = [a_1 \ \dots \ a_t] \in \mathbb{N}_0^{(t)}$, and let $N = V_1^{(a_1)} \oplus \dots \oplus V_t^{(a_t)}$. Then $a \in \Gamma(M)$ if and only if N comes from an R -module. (We need Theorem 3.6 here to conclude that if $N \cong \widehat{V}$, where V is a finitely generated R -module, then $[V] \in \text{add}(M)$.) Notice that $\text{rank}(N) = (\rho_1, \dots, \rho_s)$, where $\rho_i = \sum_{j=1}^t r_{ij} a_j$. Let $S = \{(i, l) \mid 1 \leq i < l \leq s \text{ and } P_i \cap R = P_l \cap R\}$. By Proposition 3.16 we see that $a \in \Gamma(M)$ if and only if $\rho_i = \rho_l$ whenever $(i, l) \in S$. Thus $\Gamma(M)$ is the solution set of a family of $|S|$ homogeneous linear equations with integer coefficients. (If $S = \emptyset$, that is, if the P_i lie over distinct prime ideals of R , then there are no relations, and $\Gamma(M)$ is the free monoid $\mathbb{N}_0^{(t)}$.) \square

Interlude 3.19. At this point we describe a couple of “warmup” examples, to illustrate the general method we will use to demonstrate failure of KRSA. Suppose, for example, that (R, \mathfrak{m}, k) is a one-dimensional Noetherian local domain whose completion \widehat{R} has three minimal prime ideals P_1, P_2, P_3 . We assume, as always, that \widehat{R} is reduced. For $i = 1, 2, 3$, let $X_i = R/P_i$ and $Y_i = R/\bigcap_{j \neq i} P_j$. Then $\text{rank}(X_i \oplus Y_i) = (1, 1, 1)$, so Corollary 3.17 provides a finitely generated R -module A_i such that $\widehat{A}_i \cong X_i \oplus Y_i$. Similarly, there are finitely generated R -modules B and C such that $X_1 \oplus X_2 \oplus X_3 \cong \widehat{B}$ and $Y_1 \oplus Y_2 \oplus Y_3 \cong \widehat{C}$, since the given \widehat{R} -modules have constant ranks $(1, 1, 1)$ and $(2, 2, 2)$ respectively. It is easy to see that \widehat{B}, \widehat{C} and the \widehat{A}_i are minimal extended. By Corollary 3.15, the corresponding R -modules B, C, A_i are indecomposable. Moreover, Corollary 3.7 implies that $A_1 \oplus A_2 \oplus A_3$ and $B \oplus C$ are isomorphic, since their completions are both isomorphic to $X_1 \oplus X_2 \oplus X_3 \oplus Y_1 \oplus Y_2 \oplus Y_3$.

In order to obtain examples such as the one mentioned in the introduction, we will need \widehat{R} -modules with more interesting rank functions. Still assuming R is a domain, suppose \widehat{R} has two minimal primes P_1 and P_2 . Fix an integer $n \geq 2$, and suppose we can build indecomposable finitely generated \widehat{R} -modules E, F and G with respective ranks $(2n+1, n+1)$, $(n+2, n+1)$ and $(0, n+1)$. Given $[a \ b \ c] \in \mathbb{N}_0^{(3)}$, let $N(a, b, c) = E^{(a)} \oplus F^{(b)} \oplus G^{(c)}$, an \widehat{R} -module of rank $((2n+1)a + (n+2)b, (n+1)(a+b+c))$. Using Corollary 3.17, we see that $N(a, b, c)$ is extended an R -module $M(a, b, c)$ if and only if $(2n+1)a + (n+2)b = (n+1)(a+b+c)$, that is, if and only if $[a \ b \ c]$ belongs to the Diophantine monoid $H := \{[x \ y \ z] \in \mathbb{N}_0^{(3)} \mid nx + y = (n+1)z\}$. Noting that $[1 \ 1 \ 1] \in H$, we put $C = M(1, 1, 1)$. Then $\widehat{C} \cong E \oplus F \oplus G$, and $\text{add}(C) \cong \Gamma(C) = H$. Clearly $[1 \ 1 \ 1]$ is an atom of H , as are $[n+1 \ 0 \ n]$ and $[0 \ n+1 \ 1]$. Letting $A = M(n+1, 0, n)$ and $B = M(0, n+1, 1)$, we see that A, B and C are indecomposable

R -modules. Moreover, we have the relation $A \oplus B \cong C^{(n+1)}$. (The example mentioned in the introduction is the case $n = 2$.) An innocent bystander analyzing powers of C would not detect the silly direct-sum behavior until the $n + 1^{\text{st}}$ step, since $C^{(n)}$ has only one representation as a direct sum of indecomposable modules.

These examples suggest that in order to realize an arbitrary Diophantine monoid as a monoid of the form $\Gamma(M)$, we need to find examples where, first of all, \widehat{R} has more minimal primes than R does, and second, \widehat{R} has finitely generated modules with interesting rank functions. The next theorem [Wie01, (2.3) and (2.4)] fits the bill perfectly. Moreover the requisite ring can always be chosen to be an integral domain, and the module M to be torsion-free. (Over an integral domain R , a module M is *torsion-free* provided $rm \neq 0$ when r and m are non-zero elements of R and M , respectively.)

Theorem 3.20. *Fix an integer $s \geq 2$, and let (r_1, \dots, r_s) be an arbitrary non-trivial s -tuple of non-negative integers. Choose real numbers $q_1 < \dots < q_s$. Let R be the subring of the field $\mathbb{R}(x)$ of rational functions in one variable consisting of functions $f(x)$ satisfying the following conditions:*

- (i) $f(q_1) = \dots = f(q_s)$
- (ii) $f^{(i)}(q_j) = 0$ for $j \in \{1, 2, \dots, s\}$ and $i \in \{1, 2, 3\}$. (Here $f^{(i)}$ denotes the i^{th} derivative of $f(x)$.)

Then

- (a) R is a one-dimensional local ring,
- (b) \widehat{R} is reduced and has exactly s minimal prime ideals, and
- (c) there exists a finitely generated torsion-free \widehat{R} -module N with $\text{rank}(N) = (r_1, \dots, r_s)$.

There's nothing special about the field of real numbers here. All we need is a field with at least s distinct elements q_1, \dots, q_s . The construction of the module M and the proof of indecomposability are quite technical and use ideas going back to a 1967 paper of Drozd and Roiter [DR67] on the classification of one-dimensional rings of finite representation type. While we won't say anything more about the module M we will say a little bit about the ring and where the various maximal ideals of \widehat{R} come from. The maximal ideal of R is $\mathfrak{m} := \{f \in R \mid f(q_1) = \dots = f(q_s) = 0\}$. The ring R is a subring of the ring S consisting of rational functions that are defined at each q_i . The ring S has exactly s maximal ideals, namely, $\mathfrak{m}_i := \{f \in S \mid f(q_i) = 0\}$, $i = 1, \dots, s$. One can show that S is finitely generated as an R -module, so that \widehat{S} is a finitely generated \widehat{R} -module. The ring $\widehat{S}/\mathfrak{m}\widehat{S}$ has a family of orthogonal idempotents, one for each maximal ideal $\mathfrak{m}_i\widehat{S}$, and by Propositions 2.10 and 2.12 these lift to idempotents of \widehat{S} . These idempotents give a decomposition $\widehat{S} = D_1 \times \dots \times D_s$, in which each D_i is a one-dimensional local domain. Then $Q_i := \prod_{j \neq i} D_j$ is a minimal prime ideal of \widehat{S} , and the prime ideals $P_i := Q_i \cap \widehat{R}$ are exactly the minimal prime ideals of \widehat{R} .

Theorem 3.21 (Realization Theorem for Diophantine Monoids). *Let $H \subseteq \mathbb{N}_0^{(t)}$ be any Diophantine monoid containing an element $\alpha := [a_1 \dots a_t]$ in which each a_i is positive. Then there exist a one-dimensional local domain R and a finitely generated torsion-free R -module M such that $\Gamma(M) = H$, with $\Psi([M]) = \alpha$ (in the notation of Theorem 3.11).*

Proof. Assume H is defined by m homogeneous linear equations. Then we can write $H = \mathbb{N}_0^{(t)} \cap \text{Ker}(\Phi)$, where $\Phi : \mathbb{Q}^t \rightarrow \mathbb{Q}^m$ is a linear transformation. We regard Φ as an $m \times t$ matrix $[q_{ij}]$, and we can assume, by clearing denominators, that the entries q_{ij} are integers. Choose a positive integer h such that $q_{ij} + h \geq 0$ for all i, j . Let R be the ring of Theorem 3.20 with $s = m + 1$. (The number of minimal primes of \widehat{R} is one more than the number of defining equations of the monoid.)

For $j = 1, \dots, t$, choose, using Theorem 3.20, an indecomposable, finitely generated, torsion-free \widehat{R} -module N_j such that

$$\text{rank}(N_j) = (q_{1j} + h, \dots, q_{mj} + h, h), \quad j = 1, \dots, t. \tag{3.2}$$

Suppose now that $\beta = [b_1 \dots b_t] \in \mathbb{N}_0^{(t)}$. If $N = N_1^{(b_1)} \oplus \dots \oplus N_t^{(b_t)}$, then

$$\text{rank}(N) = \left(\sum_{j=1}^t (q_{1j} + h)b_j, \dots, \sum_{j=1}^t (q_{mj} + h)b_j, \left(\sum_{j=1}^t b_j \right) h \right). \tag{3.3}$$

By Corollary 3.17, N comes from an R -module if and only if $\sum_{j=1}^t (q_{ij} + h)b_j = \left(\sum_{j=1}^t b_j\right)h$ for $1 \leq i \leq m$, that is, if and only if $\beta \in \mathbb{N}_0^{(t)} \cap \text{Ker}(\Phi) = H$.

Let M be the finitely generated R -module (unique up to isomorphism) such that $\widehat{M} \cong L_1^{(a_1)} \oplus \cdots \oplus L_t^{(a_t)}$. Then $\Gamma(M) = H$, and the isomorphism Ψ of Theorem 3.11 carries $[M]$ to the element α . \square

4 Measuring Failure of KRSA

In this section we describe invariants that are useful in determining the extent to which direct-sum decompositions can be non-unique.

4.1 More on Monoids

We briefly leave the world of direct-sum decompositions and recall some basic concepts of factorization in commutative monoids. We will return later to monoids of modules and use these tools to describe how badly KRSA can fail over Noetherian local rings of dimension one.

Throughout, let H denote a monoid satisfying (i) and (ii) of §3.

Definition 4.1. A *Krull monoid* is a monoid admitting a divisor homomorphism $\varphi : H \rightarrow F$, where F is a free monoid. A *divisor theory* is a divisor homomorphism $\varphi : H \hookrightarrow \mathbb{N}_0^{(\Omega)}$ such that every element of $\mathbb{N}_0^{(\Omega)}$ is the greatest lower bound (in the usual product partial ordering) of some non-empty finite set of elements in $\varphi(H)$. Note (cf. [HK98, 20.4]) that if $\varphi : H \rightarrow F$ and $\varphi' : H \rightarrow F'$ are divisor theories for H , then there is a monoid isomorphism $\psi : F \rightarrow F'$ such that $\varphi' = \psi \circ \varphi$.

In fact [GHK06, Theorem 2.4.8], every Krull monoid has a divisor theory. Although we will not prove this here, we will need this fact when we discuss the divisor class group of a Krull monoid.

Our next task is to show that all Krull monoids are atomic. The key to proving Theorem 4.3, as well as Theorem 4.4, is to appeal to the descending chain condition on $\mathbb{N}_0^{(t)}$, with respect to the product (coordinate-wise) partial ordering: $[a_1 \dots a_t] \leq [b_1 \dots b_t] \iff a_i \leq b_i$ for each i . A poset X satisfies DCC provided there is no infinite strictly descending chain $x_1 > x_2 > x_3 > \dots$ in X . One verifies easily that if X and Y both have DCC then so does $X \times Y$. Since \mathbb{N}_0 has DCC, an induction argument shows the following:

Lemma 4.2. *Let r be any positive integer. Then $\mathbb{N}_0^{(r)}$ satisfies DCC.* \square

Proposition 4.3. *If H is a Krull monoid, then H is atomic.*

Proof. We may assume that H is a full submonoid of $\mathbb{N}_0^{(I)}$ for some (possibly infinite) index set I . Let x be a non-zero element of H . Then $x \in \mathbb{N}_0^{(F)}$ for some finite subset F of I . One checks easily that $\text{add}(x)$ is also a full submonoid of $\mathbb{N}_0^{(F)}$. (Technically, we should write either “ $\text{add}_H(x)$ ” or “ $\text{add}_{\mathbb{N}_0^{(I)}}(x)$ ”, but they are the same, since H is a full submonoid of $\mathbb{N}_0^{(I)}$.) For elements $y, z \in \text{add}(x)$, we have $y \mid z$ in $\text{add}(x)$ if and only if $y \leq z$ in $\mathbb{N}_0^{(F)}$, that is, if and only if $y \leq z$ in the product ordering on $\mathbb{N}_0^{(I)}$. Moreover, if $h_1 + h_2 \in \text{add}(x)$, with $h_i \in H$, then $h_1, h_2 \in \text{add}(x)$; it follows that every atom of $\text{add}(x)$ is actually an atom of H . Therefore it will suffice to show that x is a sum of atoms of $\text{add}(x)$. By Lemma 4.2, $\mathbb{N}_0^{(F)}$, and hence H , satisfies DCC.

We will show, in fact, that *every* non-zero element of $\text{add}(x)$ is a sum of atoms. If not, the set B of non-zero elements of $\text{add}(x)$ that *cannot* be expressed as a sum of atoms of $\text{add}(x)$ is non-empty. By the descending chain condition, B has a minimal element b . Certainly b is not an atom, so $b = c + d$, where c and d are non-zero elements of $\text{add}(x)$. Then $c < b$ and $d < b$, so neither c nor d is in B . Writing c and d as sums of atoms makes b a sum of atoms, contradicting the fact that $b \in B$. This contradiction shows that $B = \emptyset$, and the proof is complete. \square

Moreover, if H is a full submonoid to $\mathbb{N}_0^{(t)}$ for some positive integer t , in particular, if H is a Diophantine monoid, then H has only finitely many atoms, as we shall see in Corollary 4.5 below. (Recall that the atoms are the minimal elements of $H \setminus \{0\}$.) Given any poset X , we define a *clutter* to be a subset S of X with no order relations among its elements. In other words, if $x, y \in S$, then neither $x < y$ nor $y < x$. (The less colorful term “antichain” is often used in the literature.)

Theorem 4.4. *Let t be a positive integer. Then $\mathbb{N}_0^{(t)}$ has no infinite clutters. For any subset Y of $\mathbb{N}_0^{(t)}$, $\min(Y)$ is finite.*

Proof. The second statement follows from the first, since $\min(Y)$ is a clutter. To prove the first statement, we use induction on t , the case $t = 1$ being trivial. Suppose, now, that $t \geq 2$, and let M be a clutter in $\mathbb{N}_0^{(t)}$. If $M = \emptyset$, then M is very finite, so we assume that $M \neq \emptyset$ and fix an element $[a_1 \dots a_n]$ in M .

For each pair of integers i and j with $1 \leq i \leq n$ and $0 \leq j \leq a_i$, define $M_{ij} = \{[x_1 x_2 \dots x_t] \in M \mid x_i = j\}$ and $B_{ij} = \{[x_1 x_2 \dots x_{t-1}] \in \mathbb{N}_0^{t-1} \mid [x_1 \dots x_{i-1} j x_i \dots x_{t-1}] \in M_{ij}\}$. For each i and j , the bijection $M_{ij} \leftrightarrow B_{ij}$, given by $[x_1 \dots x_{i-1} j x_{i+1} \dots x_t] \leftrightarrow [x_1 \dots x_{i-1} x_{i+1} \dots x_t]$, shows that B_{ij} is a clutter. The inductive hypothesis now guarantees that each set B_{ij} is finite, and hence that each M_{ij} is finite. Since there are only finitely many sets M_{ij} , we need only show that $M \subseteq \bigcup M_{ij}$. Let $[x_1 x_2 \dots x_t] \in M$. If $a_i < x_i$ for all i , then $[a_1 a_2 \dots a_t] < [x_1 x_2 \dots x_t]$, contradicting the assumption that M is a clutter. Thus there exists $i \in \{1, 2, \dots, n\}$ with $x_i \leq a_i$, and $[x_1 x_2 \dots x_n] \in M_{ix_i}$. \square

Alternatively, one can prove Theorem 4.4 by verifying a more general result: If A and B are posets, each with DCC, and each having no infinite clutters, then $A \times B$ has no infinite clutters.

Corollary 4.5. *Let H be a full submonoid of $\mathbb{N}_0^{(t)}$ for some positive integer t . Then H has only finitely many atoms. In particular, every Diophantine monoid has only finitely many atoms.* \square

Corollary 4.6. *Let x be an element of a Krull monoid H . Then x has only finitely many distinct factorizations as sums of atoms.*

Proof. By choosing a suitable divisor homomorphism, we may assume that H is a full submonoid of $\mathbb{N}_0^{(\Omega)}$ for some index set Ω . Choose a finite subset F of Ω such that $x \in \mathbb{N}_0^{(F)}$. Then $\text{add}(x)$ is a full submonoid of $\mathbb{N}_0^{(F)}$. Now every atom of H that divides x is actually an atom of $\text{add}(x)$, which, by Corollary 4.5, has only finitely many atoms. Thus there are only finitely many atoms p_1, \dots, p_n that divide x . The decompositions of x are all of the form $x = e_1 p_1 + \dots + e_n p_n$, for suitable non-negative integers e_i , and our task is to show that there are only finitely many sequences (e_1, \dots, e_n) arising in this way. It will suffice to establish a bound on each e_i . Suppose, by way of contradiction, that there is an atom p of H such that $ep \mid x$ for every positive integer e . Then, in the coordinate-wise partial ordering on $\mathbb{N}_0^{(t)}$, we have $ep \leq x$ for each e . Write $p = [a_1 \dots a_t]$ and $x = [b_1 \dots b_t]$, as elements of $\mathbb{N}_0^{(t)}$. Since $p \neq 0$ we have $a_j > 0$ for some j . Then $b_j \geq ea_j$ for every e , an obvious contradiction. \square

Given a Krull monoid H , we let $\mathcal{Q}(H)$ denote the *quotient group*, which consists of formal differences $\{x - y \mid x, y \in H\}$. If $\varphi: H \rightarrow \mathbb{N}_0^{(\Omega)}$ is a divisor theory, we have an induced quotient homomorphism $\mathcal{Q}(\varphi): \mathcal{Q}(H) \rightarrow \mathcal{Q}(\mathbb{N}_0^{(\Omega)})$ defined by $\mathcal{Q}(\varphi)(x - y) = \varphi(x) - \varphi(y)$. This gives rise to the *divisor class group* $\text{Cl}(H)$, which is defined to be the cokernel of the map $\mathcal{Q}(\varphi)$. Elements of $\text{Cl}(H)$ are called *divisor classes*. Noting that $\mathcal{Q}(\mathbb{N}_0^{(\Omega)}) = \mathbb{Z}^{(\Omega)}$, we see that a divisor class is a coset $z + L$, where $z \in \mathbb{Z}^{(\Omega)}$ and L is the image of the homomorphism $\mathcal{Q}(\varphi)$. We let $\pi: \mathbb{Z}^{(\Omega)} \rightarrow \text{Cl}(H)$ be the canonical surjection. An element $z \in \mathbb{Z}^{(\Omega)}$ belongs to $\text{Ker}(\pi)$ if and only if there are elements $x, y \in H$ such that $\varphi(x) - \varphi(y) = z$. Moreover, we claim that

$$\text{Ker}(\pi) \cap \mathbb{N}_0^{(\Omega)} = \varphi(H). \tag{4.1}$$

Of course $\text{Ker}(\pi) \cap \mathbb{N}_0^{(\Omega)} \supseteq \varphi(H)$. To verify the reverse inclusion, suppose $z \in \text{Ker}(\pi) \cap \mathbb{N}_0^{(\Omega)}$, and write $z = \varphi(x) - \varphi(y)$, with $x, y \in H$. Then $z + \varphi(y) = \varphi(x)$, so $\varphi(y) \mid \varphi(x)$. Therefore $y \mid x$, as φ is a divisor homomorphism, say, $y + h = x$. Now $\varphi(h) = \varphi(x) - \varphi(y) = z$. This shows that $\text{Ker}(\pi) \cap \mathbb{N}_0^{(\Omega)} \subseteq \varphi(H)$.

The divisor class group gives a crude measure of failure of unique factorization:

Proposition 4.7. *Let H be a Krull monoid. Then H is free if and only if $\text{Cl}(H)$ is trivial.*

Proof. Let $\varphi: H \rightarrow \mathbb{N}_0^{(\Omega)}$ be a divisor theory, and let $\pi: \mathbb{Z}^{(\Omega)} \rightarrow \text{Cl}(H)$ be the canonical surjection.

Suppose $\text{Cl}(H)$ is trivial. Then $\mathbb{N}_0^{(\Omega)} \subseteq \text{Ker}(\pi)$, and now (4.1) implies that $\varphi(H) = \mathbb{N}_0^{(\Omega)}$. Since all divisor homomorphisms are injective, $H \cong \mathbb{N}_0^{(\Omega)}$, and thus H is free. Conversely, if H is free, then the identity map $\iota: H \rightarrow H$ is a divisor theory. The induced map $\mathcal{Q}(\iota): \mathcal{Q}(H) \rightarrow \mathcal{Q}(H)$ is also the identity map, and $\text{Cl}(H) = \mathcal{Q}(H)/\mathcal{Q}(H) = 0$. \square

Let H denote a Krull monoid with divisor theory $\varphi: H \rightarrow \mathbb{N}_0^{(\Omega)}$. We refer to the standard basis elements $e_\omega \in \mathbb{N}_0^{(\Omega)}$ as *primes*, and we say that an element $g \in \text{Cl}(H)$ *contains a prime* if $g = \pi(e_\omega)$ for some prime $e_\omega \in \mathbb{N}_0^{(\Omega)}$. (Here $\pi: \mathbb{Z}^{(\Omega)} \rightarrow \text{Cl}(H)$ is the canonical projection.) As we shall see in Theorem 4.13, if $\text{Cl}(H)$ is infinite and every divisor class contains a prime, then factorization in H is wildly non-unique. The reader should note that the elements e_ω are exactly the atoms, equivalently, prime elements, of the free monoid $\mathbb{N}_0^{(\Omega)}$. It might be seem more consistent to say that a divisor class *contains an atom*, but the terminology above is ubiquitous in the literature, and we will stick with it.

In the following theorem [BS] we require the matrix \mathcal{A} to contain certain columns of zeros and ones and observe that the natural inclusion $\text{Ker}(\mathcal{A}) \cap \mathbb{N}_0^{(\Omega)} \subseteq \mathbb{N}_0^{(\Omega)}$ is nearly always a divisor theory. In Section 4.2 we will use the existence of certain boring ranks to acquire these additional columns. We also determine the divisor class groups of such Diophantine monoids and consider which divisor classes contain primes. More general results for finitely generated Diophantine monoids can be found in [CKO02].

Theorem 4.8. *Fix an integer $q \geq 1$ and let I_q denote the $q \times q$ identity matrix. Let $\mathcal{D} = [D_1 \mid D_2 \mid D_3]$, where*

$$D_1 = [I_q \mid -I_q],$$

$$D_2 = \left[\begin{array}{c|c} 1 & -1 \\ 1 & -1 \\ \vdots & \vdots \\ 1 & -1 \end{array} \right],$$

and D_3 is an arbitrary integer matrix with q rows (and possibly infinitely many columns). Let $H = \text{Ker}(\mathcal{D}) \cap \mathbb{N}_0^{(\Omega)}$, where Ω is the cardinality of the set of columns of \mathcal{D} .

- (i) *The natural inclusion $H \hookrightarrow \mathbb{N}_0^{(\Omega)}$ is a divisor theory.*
- (ii) *$\text{Cl}(H) \cong \mathbb{Z}^{(q)}$.*
- (iii) *Each column of \mathcal{D} corresponds, via the isomorphism in (ii), to a divisor class that contain a prime.*

Proof. We begin by showing that the inclusion $H \hookrightarrow \mathbb{N}_0^{(\Omega)}$ is a divisor homomorphism. Suppose $\alpha, \gamma \in H$ with $\alpha \leq \gamma$ in $\mathbb{N}_0^{(\Omega)}$; that is, there is an element $\beta \in \mathbb{N}_0^{(\Omega)}$ with $\alpha + \beta = \gamma$. Since $\mathcal{D}(\alpha + \beta) = 0$ and $\mathcal{D}\alpha = 0$, we see that $\mathcal{D}\beta = 0$ as well, and thus $\beta \in H$. Therefore $H \hookrightarrow \mathbb{N}_0^{(\Omega)}$ is a divisor homomorphism. For an element $\beta \in \mathbb{N}_0^{(\Omega)}$, write $-\mathcal{D}\beta = [d_1 \ \cdots \ d_q]^T$ where each d_i is an integer, and set $M = \max\{0, d_1, \dots, d_q\}$ and $m = \min\{0, d_1, \dots, d_q\}$. For each $i \in \{1, \dots, 2q+2\}$, let ε_i denote the standard basis vector in $\mathbb{N}_0^{(\Omega)}$ with 1 in the i th coordinate and 0 elsewhere; note that $\mathcal{D}\varepsilon_i$ is precisely the i th column of \mathcal{D} . Define

$$\beta_1 := \sum_{i=1}^q (d_i - m)\varepsilon_i - m\varepsilon_{2q+2} \in \mathbb{N}_0^{(\Omega)} \text{ and } \beta_2 := \sum_{i=1}^q (M - d_i)\varepsilon_{q+i} + M\varepsilon_{2q+1} \in \mathbb{N}_0^{(\Omega)}.$$

One checks that $\beta + \beta_1$ and $\beta + \beta_2$ are in $\mathbb{N}_0^{(\Omega)} \cap \text{Ker}(\mathcal{D}) = H$ and that β is the greatest lower bound of $\{\beta + \beta_1, \beta + \beta_2\}$. Therefore the inclusion $H \hookrightarrow \mathbb{N}_0^{(\Omega)}$ is a divisor theory.

For each $i \in \{1, 2, \dots, q\}$, the standard basis vector e_i occurs as a column of \mathcal{D} , and thus $\mathcal{D}: \mathbb{Z}^{(\Omega)} \rightarrow \mathbb{Z}^{(q)}$ is surjective. Therefore

$$\mathbb{Z}^{(\Omega)} / \text{Ker}(\mathcal{D}) \cong \mathbb{Z}^{(q)}. \tag{4.2}$$

Clearly $\mathcal{Q}(H) \subseteq \text{Ker}(\mathcal{D})$, and we now show the reverse inclusion. Let $\alpha \in \text{Ker}(\mathcal{D})$, and write $\alpha = \beta - \gamma$ for some $\beta, \gamma \in \mathbb{N}_0^{(\Omega)}$. As in the previous paragraph, find $\beta_1 \in \mathbb{N}_0^{(\Omega)}$ with $\beta + \beta_1 \in H$. Then $\gamma + \beta_1 = \beta + \beta_1 - \alpha \in \mathbb{N}_0^{(\Omega)} \cap \text{Ker}(\mathcal{D}) = H$, and so $\alpha = (\beta + \beta_1) - (\gamma + \beta_1) \in \mathcal{Q}(H)$. Therefore $\mathcal{Q}(H) = \text{Ker}(\mathcal{D})$, and now $\text{Cl}(H) = \mathbb{Z}^{(\Omega)} / \mathcal{Q}(H) = \mathbb{Z}^{(\Omega)} / \text{Ker}(\mathcal{D}) \cong \mathbb{Z}^{(q)}$ by (4.2). This proves (ii).

For (iii), we observe that, for an element $z \in \mathbb{Z}^{(\Omega)}$, the isomorphism in (ii) carries the divisor class $\pi(z)$ to the matrix product $\mathcal{D}z \in \mathbb{Z}^{(q)}$. Suppose now that c is the ω^{th} column of \mathcal{D} . Then $c = \mathcal{D}e_\omega$, which corresponds, via the isomorphism in (ii), to the divisor class $\pi(e_\omega)$. Since this divisor class contains the prime e_ω , the proof is complete. \square

Let H be a Krull monoid and h a non-zero element of H . The *set of lengths* of h is $\mathsf{L}(h) := \{n \mid h = a_1 + \cdots + a_n \text{ for atoms } a_i \in H\}$. The *elasticity* of $h \in H$ is $\rho(h) := \sup \mathsf{L}(h) / \inf \mathsf{L}(h)$. Since, by Corollary 4.6, h has only finitely many distinct factorizations, the elasticity $\rho(h)$ is finite. If H is free, then factorization is unique, and hence $\rho(h) = 1$ for every non-zero element $h \in H$. The converse can fail, as we see in the following example.

Example 4.9. Consider the monoid $H = \{[w \ x \ y \ z] \in \mathbb{N}_0^{(4)} \mid w + x = y + z\}$. The atoms are $\alpha_1 = [1 \ 0 \ 1 \ 0]$, $\alpha_2 = [1 \ 0 \ 0 \ 1]$, $\alpha_3 = [0 \ 1 \ 1 \ 0]$, and $\alpha_4 = [0 \ 1 \ 0 \ 1]$. One can then verify that if $\sum_{i=1}^4 a_i \alpha_i = \sum_{i=1}^4 b_i \alpha_i$ for nonnegative integers $a_1, a_2, a_3, a_4, b_1, b_2, b_3,$ and b_4 , then $a_1 + a_2 + a_3 + a_4 = b_1 + b_2 + b_3 + b_4$, and hence $\rho(H) = 1$. However, since $\alpha_1 + \alpha_4 = \alpha_2 + \alpha_3$, it is clear that H is not factorial.

We say that a monoid H is *half-factorial* if $|\mathsf{L}(h)| = 1$ for every non-zero element $h \in H$ (equivalently, H is atomic and any two representations of an element of H as a sum of atoms have the same length). We put $\rho(H) := \sup\{\rho(h) \mid h \in H \setminus \{0\}\}$, the *elasticity* of H . The monoid H is *fully elastic* provided every rational number in the closed interval $[1, \rho(H)]$ occurs as the elasticity of some element of H . (Note that if $\rho(H) = \infty$, we say H is fully elastic if every rational number in $[1, \infty)$ occurs as the elasticity of some element in H .)

We now introduce the block monoid of a Krull monoid. This object is often easier to study, yet it carries a great deal of information about the original monoid.

Definition 4.10 (block monoid). Let G be an abelian group, let P be any subset of G , and let $\mathcal{F}(P)$ be the free abelian monoid with basis P . Thus $\mathcal{F}(P)$ consists of formal \mathbb{N}_0 -linear combinations of elements in the set P with the obvious binary operation. We express an element b of $\mathcal{F}(P)$ as follows:

$$b = n_1 p_1 \oplus \cdots \oplus n_t p_t,$$

where the p_i are in P and the n_i are non-negative integers and \oplus denotes a formal sum in $\mathcal{F}(P)$. Consider the map

$$\begin{array}{ccc} \sigma: \mathcal{F}(P) & \longrightarrow & G \\ n_1 p_1 \oplus \cdots \oplus n_t p_t & \mapsto & n_1 p_1 + \cdots + n_t p_t \end{array}$$

taking the formal sum in $\mathcal{F}(P)$ to the actual sum in G . The submonoid $\mathcal{B}(G, P) = \{s \in \mathcal{F}(P) : \sigma(s) = 0\}$ of $\mathcal{F}(P)$ is called the *block monoid of G* with respect to P . In other words, the block monoid is the set of formal sums that add up to 0 in the group G . (In the literature, the free monoid $\mathcal{F}(P)$ and the block monoid $\mathcal{B}(G, P)$ are usually written multiplicatively, but the additive notation seems more appropriate to our situation.)

We are particularly interested in the following situation:

- (i) H is a Krull monoid,
- (ii) $G = \mathcal{Cl}(H)$, and
- (iii) P is the subset of G consisting of divisor classes that contain primes.

In this situation, we refer to $\mathcal{B}(G, P)$ as the *block monoid of H* and denote it simply by $\mathcal{B}(H)$.

Before describing how $\mathcal{B}(H)$ is useful in studying factorization in the Krull monoid H , we need to define a type of monoid homomorphism that preserves basic factorization properties.

Definition 4.11 (transfer homomorphism). Let H and K be monoids (reduced and cancellative as always). A homomorphism $\varphi : H \rightarrow K$ is a *transfer homomorphism* provided

- (i) φ is surjective,
- (ii) $\varphi(z) \neq 0$ for each non-zero $z \in H$, and
- (iii) whenever $\varphi(z) = a + b$ in K , there exist $x, y \in H$ such that $\varphi(x) = a$, $\varphi(y) = b$, and $x + y = z$ in H .

Suppose that $\varphi : H \rightarrow K$ is a transfer homomorphism. Given $z \in H$, one checks easily that z is an atom of H if and only if $\varphi(z)$ is an atom of K . In fact, φ preserves the basic structure of factorizations in H . In particular, $L(z) = L(\varphi(z))$ (and consequently $\rho(z) = \rho(\varphi(z))$ and $\rho(H) = \rho(K)$) [Ger88], and we can study sets of lengths and elasticities in H by studying these same invariants in K . We take this approach when H is a Krull monoid and K is the block monoid $\mathcal{B}(H)$. In the next result (proved in more generality in [Ger88]) we establish a transfer homomorphism $\beta : H \rightarrow \mathcal{B}(H)$. But first we set the stage by building a commutative diagram that shows the various homomorphisms involved.

Let H be a Krull monoid with divisor theory $\varphi : H \hookrightarrow \mathbb{N}_0^{(\Omega)}$. Let $\pi : \mathbb{Z}^{(\Omega)} \rightarrow \mathcal{Cl}(H)$ denote the canonical surjection onto the divisor class group of H , and let P be the set of divisor classes that contain primes. Thus $P = \{\pi(e_\omega)\}_{\omega \in \Omega}$ where the set $\{e_\omega\}_{\omega \in \Omega}$ is the standard basis for the free monoid $\mathbb{N}_0^{(\Omega)}$, and $\mathcal{B}(H) = \mathcal{B}(\mathcal{Cl}(H), P)$. We define the monoid homomorphism $\bar{\beta} : \mathbb{N}_0^{(\Omega)} \rightarrow \mathcal{F}(P)$ on the basis of $\mathbb{N}_0^{(\Omega)}$ by $e_\omega \mapsto \pi(e_\omega)$. (Warning: Although the homomorphism $\bar{\beta}$ is obviously surjective, it is not necessarily injective.) Recall also the map $\sigma : \mathcal{F}(P) \rightarrow \mathcal{Cl}(H)$ from Definition 4.10 and that $\mathcal{B}(H) = \{z \in \mathcal{F}(P) \mid \sigma(z) = 0\}$. For an element $x \in \mathbb{N}_0^{(\Omega)}$ one checks, using (4.1) that

$$x \in \varphi(H) \iff \bar{\beta}(x) \in \mathcal{B}(H). \tag{4.3}$$

Thus $\bar{\beta}$ induces a surjective monoid homomorphism $\beta : H \rightarrow \mathcal{B}(H)$ making the following diagram commute:

$$\begin{array}{ccccc} H & \xrightarrow{\varphi} & \mathbb{N}_0^{(\Omega)} & \xrightarrow{\subseteq} & \mathbb{Z}^{(\Omega)} \\ \beta \downarrow & & \downarrow \bar{\beta} & & \downarrow \pi \\ \mathcal{B}(H) & \xrightarrow{\subseteq} & \mathcal{F}(P) & \xrightarrow{\sigma} & \mathcal{Cl}(H) \end{array} \tag{4.4}$$

Theorem 4.12. *The map $\beta : H \rightarrow \mathcal{B}(H)$ is a transfer homomorphism.*

Proof. On replacing H by an isomorphic copy, we may assume that $H \subseteq \mathbb{N}_0^{(\Omega)}$ and that the map φ in the (4.4) is the inclusion map.

We have already verified (i) in Definition 4.11. In order to check (ii) and (iii), we establish some notation to allow for the fact that the homomorphism $\bar{\beta}$ may not be injective. Given an element $z \in \mathbb{N}_0^{(\Omega)}$, write $z = \sum_{\omega \in F} m_\omega \omega$, where F is a finite subset of Ω and the m_ω are non-negative integers. Let p_1, \dots, p_s be the distinct elements of $\{\pi(e_\omega)\}_{\omega \in F}$. For $i = 1, \dots, s$, let $F_i = \{\omega \in F \mid \pi(e_\omega) = p_i\}$, and put $n_i = \sum_{\omega \in F_i} m_\omega$. Then $\beta(z) = \bar{\beta}(z) = n_1 p_1 \oplus \dots \oplus n_s p_s \in \mathcal{F}(P)$.

Suppose now that z is a non-zero element of H . Choose $\omega \in \Omega$ such that $m_\omega > 0$, and suppose $\omega \in F_i$. Then $n_i > 0$, whence $\beta(z) \neq 0$. This proves (ii). For (iii), suppose $\beta(z) = a + b$, with $a, b \in \mathcal{B}(H)$. Since $\beta(z) = n_1 p_1 \oplus \dots \oplus n_s p_s$ and the p_i are distinct basis elements of the free monoid $\mathcal{F}(P)$, it follows that $a = k_1 p_1 \oplus \dots \oplus k_s p_s$ and $b = \ell_1 p_1 \oplus \dots \oplus \ell_s p_s$, where $0 \leq k_i \leq n_i$ and $k_i + \ell_i = n_i$ for each i . In order to decompose z in a manner that is compatible with the decomposition of $\beta(z)$, we fix an index i for the moment and recall that $\sum_{\omega \in F_i} m_\omega = k_i + \ell_i$. We can choose, for each $\omega \in F_i$, a non-negative integer $u_\omega \leq m_\omega$ in such a way that $\sum_{\omega \in F_i} u_\omega = k_i$. Put $v_\omega = m_\omega - u_\omega$. Now, letting i vary, we have $u_\omega + v_\omega = m_\omega$ for all $\omega \in F$. Putting $x = \sum_{\omega \in F} u_\omega e_\omega$ and $y = \sum_{\omega \in F} v_\omega e_\omega$, we see that $\bar{\beta}(x) = a$, $\bar{\beta}(y) = b$, and $x + y = z$. Finally, (4.3) implies that x and y are in H , since their images under $\bar{\beta}$ are in $\mathcal{B}(H)$. \square

We state without proof the following amazing result on sets of lengths in a Krull monoid with infinite divisor class group. This theorem shows how dreadful factorization can be in certain monoids.

Theorem 4.13 ([Kai99], Theorem 1). *Let H be a Krull monoid with infinite divisor class group, and assume that every divisor class contains a prime. Then, for any non-empty finite set $L \subseteq \{n \in \mathbb{N} \mid n \geq 2\}$, there exists an element $h \in H$ such that $L(h) = L$.*

Thus, for example, there's an element $h \in H$ with the following property: h is a sum n atoms if and only if $n \in \{7, 33, 9268\}$. An immediate corollary of Kainrath's theorem is that any monoid satisfying the hypotheses of Theorem 4.13 has infinite elasticity — a result we will apply in Example 4.17.

Corollary 4.14. *Let H be a Krull monoid with infinite divisor class group G , and assume that every divisor class contains a prime. Then $\rho(H) = \infty$, and H is fully elastic.*

Proof. Given a rational number $p \geq 1$, write $p = \frac{a}{b}$ with $a, b \in \mathbb{N}$. By Theorem 4.13, there is an element $h \in H$ with $L(h) = \{2b, 2a\}$, and thus $\rho(h) = \frac{2a}{2b} = p$. \square

4.2 Back to Direct-sum Decompositions

Suppose R is a one-dimensional reduced commutative Noetherian local ring. By Propositions 2.1 and 4.3, $\mathcal{M}(R)$ is an atomic Krull monoid. Also, by Theorem 3.6, the map $[M] \mapsto [\widehat{M}]$ gives a divisor homomorphism $\mathcal{M}(R) \rightarrow \mathcal{M}(\widehat{R})$. By Theorem 2.13, $\mathcal{M}(\widehat{R})$ is isomorphic to the free monoid $\mathbb{N}_0^{(\Omega)}$, where Ω is the set of isomorphism classes of indecomposable finitely generated \widehat{R} -modules. In this section we apply the tools from Section 4.1 to demonstrate spectacular failure of KRSA over one-dimensional Noetherian local rings.

Given the set of ranks of all indecomposable modules over the ring \widehat{R} , and a description of how minimal primes of \widehat{R} lie over the minimal primes of R , we can completely describe $\mathcal{M}(R)$ as a Diophantine monoid.

Let P_1, \dots, P_s denote the minimal primes of R , and for each $i \in \{1, \dots, s\}$ let $Q_{i,1}, \dots, Q_{i,t_i}$ denote the minimal prime ideals of \widehat{R} with $Q_{i,j} \cap R = P_i$. Let $q = |\text{Spec}(\widehat{R})| - |\text{Spec}(R)|$. Since the minimal primes in a one-dimensional local ring are the ones different from the maximal ideal, q is the difference between the number of minimal primes of \widehat{R} and the number of minimal primes of R . Note that $q = (t_1 - 1) + (t_2 - 1) + \dots + (t_s - 1) = \sum_{i=1}^s t_i - s$. (By the way, we are using the fact [Mat86, Theorem 7.3] that the map $\text{Spec}(\widehat{R}) \rightarrow \text{Spec}(R)$, taking P to $P \cap R$, is surjective.) Then $\mathcal{M}(R) \cong \text{Ker}(\mathcal{A}) \cap \mathbb{N}_0^{(\Omega)}$, where Ω is the set of indecomposable finitely generated \widehat{R} -modules, and where the matrix \mathcal{A} is the $q \times \Omega$ matrix defined by the following scheme:

For an indecomposable \widehat{R} -module M , let $(r_{1,1}, \dots, r_{1,t_1}, \dots, r_{s,1}, \dots, r_{s,t_s})$ denote its rank, where $r_{i,j} = \text{rank}_{Q_{i,j}}(M)$, the rank of M at $Q_{i,j}$. The column indexed by the isomorphism class $[M]$ is the transpose of the vector

$$\begin{bmatrix} r_{1,1} - r_{1,2} & \cdots & r_{1,1} - r_{1,t_1} & r_{2,1} - r_{2,2} & \cdots & r_{2,1} - r_{2,t_2} & \cdots & r_{s,1} - r_{s,2} & \cdots & r_{s,1} - r_{s,t_s} \end{bmatrix}.$$

If Q_1, Q_2, \dots, Q_t are the minimal primes of \widehat{R} , and $I \subseteq \{1, 2, \dots, t\}$, then $\widehat{R} / \cap_{i \in I} Q_i$ is an indecomposable finitely generated \widehat{R} -module of rank (r_1, r_2, \dots, r_t) where $r_i = 1$ if $i \in I$ and $r_i = 0$ if $i \notin I$. Thus the matrix \mathcal{A} contains, as a submatrix, the matrix $[D_1 | D_2]$ as in Theorem 4.8. Moreover, if $\alpha \in \text{Cl}(\mathcal{M}(R))$, then α contains a prime if $\alpha = \mathcal{A}e_\omega$ for some atom e_ω in $\mathbb{Z}^{(\Omega)}$. Since $\mathcal{A}e_\omega$ is the ω th column of \mathcal{A} , the elements in $\text{Cl}(\mathcal{M}(R)) \cong \mathbb{Z}^{(\Omega)}$ that contain primes correspond to the distinct columns of \mathcal{A} . Therefore the block monoid is $\mathcal{B}(\mathcal{M}(R)) \cong \text{Ker}(\mathcal{A}') \cap \mathbb{N}_0^{(\Omega')}$ where \mathcal{A}' denotes the matrix formed by eliminating all repeated columns in \mathcal{A} . In the following examples, we construct the matrix \mathcal{A} and apply factorization-theoretic techniques to the study of direct-sum decomposition over certain one-dimensional local rings.

We also use this strategy to investigate direct-sum decompositions of restricted classes of modules, e.g., the class of all finitely generated torsion-free modules. In this context we note that an extended finitely generated torsion-free \widehat{R} -module is necessarily extended from a finitely generated torsion-free R -module. In the first example we consider a possibly incomplete list of ranks to exhibit failure of KRSA and give bounds on the elasticity of $\mathcal{M}(R)$.

Example 4.15. Suppose that R is an integral domain and that its completion \widehat{R} has two minimal primes P_1 and P_2 . Recall that the indecomposable \widehat{R} -module \widehat{R}/P_1 has rank $(1, 0)$ and the indecomposable \widehat{R} -module \widehat{R}/P_2 has rank $(0, 1)$. Let M and N be indecomposable \widehat{R} -modules with ranks (m_1, m_2) and (n_1, n_2) respectively. Suppose further that $a := m_1 - m_2$ and $b := n_2 - n_1$ are positive, and let c denote the least common multiple of a and b . Since $a, b > 0$, neither M nor N is extended. However, one checks that $M^{(c/a)} \oplus N^{(c/b)}$ is minimally extended and is thus the completion of an indecomposable R -module Z . We note also that $M \oplus (\widehat{R}/P_2)^{(a)}$, $N \oplus (\widehat{R}/P_1)^{(b)}$, and $\widehat{R}/P_1 \oplus \widehat{R}/P_2$ are also minimally extended and hence are the completions of indecomposable R -modules X, Y , and W respectively. Since

$$\left(M^{(c/a)} \oplus N^{(c/b)} \right) \oplus (\widehat{R}/P_1 \oplus \widehat{R}/P_2)^{(c)} \cong \left(M \oplus (\widehat{R}/P_2)^{(a)} \right)^{(c/a)} \oplus \left(N \oplus (\widehat{R}/P_1)^{(b)} \right)^{(c/b)},$$

it follows that $L := Z \oplus W^{(c)}$ is isomorphic to $X^{(c/a)} \oplus Y^{(c/b)}$ as R -modules. This illustrates the failure of KRSA. Note that the R -module L can be expressed both as the direct sum of $c + 1$ indecomposable R -modules and as the direct sum of $(c/a) + (c/b)$ indecomposable R -modules. Therefore $\rho(L) \geq \frac{c+1}{(c/a)+(c/b)}$ in

the monoid $\mathcal{M}(R)$. If $a, b > 1$, then $\frac{c+1}{(c/a)+(c/b)} > 1$ and hence $\rho(\mathcal{M}(R)) > 1$. If the sets $\{a \mid a = \text{rank}_{P_1}(M) - \text{rank}_{P_2}(M) \text{ for some indecomposable } M_R\}$ and $\{b \mid b = \text{rank}_{P_2}(M) - \text{rank}_{P_1}(M) \text{ for some indecomposable } M_R\}$ are unbounded, then there is no bound on $\{\rho([L] \mid L \text{ is an } R\text{-module})\}$, and thus $\rho(\mathcal{M}(R)) = \infty$.

Giving a complete list of ranks of indecomposable \widehat{R} -modules would allow a more precise calculation of elasticity. Unfortunately, acquiring this set of ranks is a difficult problem in general. However, in certain cases, the ranks of all indecomposable modules are known. As the construction of indecomposables with various ranks is rather technical, we simply provide the ranks and go from there. In the next example, we describe the non-uniqueness of direct-sum decompositions of torsion-free modules over a ring which has *finite representation type*, i.e., it has, up to isomorphism, only finitely many indecomposable torsion-free modules.

Example 4.16. Fix a positive integer n . Suppose R is a local domain whose \mathfrak{m} -adic completion \widehat{R} is isomorphic to $\mathbb{C}[[x, y]]/(x^2y - y^{2n+1})$. (We know that such a ring exists by a theorem of Lech [Lec86].) Note that \widehat{R} has exactly three minimal primes, namely $y\widehat{R}$, $(x - y^n)\widehat{R}$, and $(x + y^n)\widehat{R}$.

We first consider *all* finitely generated R and \widehat{R} modules, even those with torsion. Let r be any positive integer, and set $s = 1 + 2 + \dots + r$. For each $i \in \{1, 2, \dots, r, s\}$, there exist, by [HRKW08], indecomposable finitely generated \widehat{R} -modules M_i and N_i of rank $(0, 0, i)$ and $(i, i, 0)$, respectively. (These modules are not necessarily torsion-free.) Since R is a domain, none of these modules is extended. However, $M_1 \oplus N_1, \dots, M_r \oplus N_r, (\bigoplus_{i=1}^r M_i) \oplus N_s$, and $(\bigoplus_{i=1}^r N_i) \oplus M_s$ are extended. Moreover, these modules are minimally extended and are thus extended from indecomposable R -modules. Since

$$\begin{aligned} M &= \left(\left(\bigoplus_{i=1}^r M_i \right) \oplus N_s \right) \oplus \left(\left(\bigoplus_{i=1}^r N_i \right) \oplus M_s \right) \\ &\cong \bigoplus_{i=1}^r (M_i \oplus N_i) \oplus (M_s \oplus N_s) \end{aligned}$$

we see that $2, r + 1 \in L([M])$, and hence the elasticity of the element $[M] \in \mathcal{M}(R)$ is at least $\frac{r+1}{2}$. As r was arbitrary, the elasticity of $\mathcal{M}(R)$ is infinite.

The direct-sum behavior of finitely generated *torsion-free* modules over R isn't so crazy. In fact, R and \widehat{R} have finite representation type. The following table (cf. [Yos90], [Bae07]) gives a list, up to isomorphism, of all indecomposable finitely generated torsion-free \widehat{R} -modules, along with their ranks at the three minimal primes. (Note that there are $4n + 5$ indecomposable \widehat{R} -modules.)

module	rank	module	rank
A	$(1, 0, 0)$	E	$(1, 0, 1)$
B	$(0, 1, 0)$	F_j	$(0, 1, 1) \quad 1 \leq j \leq n$
C	$(0, 0, 1)$	G_j	$(2, 1, 1) \quad 1 \leq j \leq n - 1$
D	$(1, 1, 0)$	H_j	$(1, 1, 1) \quad 1 \leq j \leq 2n + 1$

We now use this information to describe direct-sum behavior of finitely generated torsion-free modules over R . Since we are dealing only with torsion-free modules, we refer to the monoids $\mathfrak{C}(\widehat{R})$ and $\mathfrak{C}(R)$ of finitely generated torsion-free modules over \widehat{R} and R , respectively. Since KRSA holds for the class of all finitely generated \widehat{R} modules, $\mathfrak{C}(R) \subseteq \mathfrak{C}(\widehat{R}) \cong \mathbb{N}_0^{(4n+5)}$. If M is any finitely generated torsion-free \widehat{R} -module, we have

$$M \cong A^a \oplus B^b \oplus C^c \oplus D^d \oplus E^e \oplus \left(\bigoplus_{j=1}^n F_j^{f_j} \right) \oplus \left(\bigoplus_{j=1}^{n-1} G_j^{g_j} \right) \oplus \left(\bigoplus_{j=1}^{2n+1} H_j^{h_j} \right).$$

Since R is a domain, L is extended if and only if $\text{rank}(L)$ is constant; i.e., if and only if

$$\sum_{j=1}^{n-1} g_j + a + e = \sum_{j=1}^n f_j + b \quad \text{and} \quad b + d = c + e.$$

Thus, represented as a Diophantine monoid, $\mathfrak{C}(R) = (\text{Ker}(\mathcal{A}) \cap \mathbb{N}_0^{2n+4}) \oplus \mathbb{N}_0^{2n+1}$ where

$$\mathcal{A} = \begin{bmatrix} 1 & -1 & 0 & 0 & 1 & -1 & -1 & \dots & -1 & 1 & \dots & 1 \\ 0 & 1 & -1 & 1 & -1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}.$$

This is a $2 \times (2n + 4)$ matrix whose columns correspond to the “unknowns” $a, b, c, d, e, f_1, \dots, f_n, g_1, \dots, g_{n-1}$. The divisor classes containing primes are the images of the standard basis vectors of \mathbb{N}_0^{2n+2} , that is the six distinct columns of \mathcal{A} . Thus the block monoid of $\mathfrak{C}(R)$ is

$$\mathcal{B}(\mathfrak{C}(R)) \cong \text{Ker} \begin{bmatrix} 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 1 & -1 & 1 & -1 & 0 \end{bmatrix} \cap \mathbb{N}_0^6. \tag{4.5}$$

The irreducible elements of this monoid are:

$$\begin{aligned} h_1 &= [1 \ 0 \ 0 \ 0 \ 0 \ 1] & h_2 &= [0 \ 1 \ 0 \ 0 \ 1 \ 0] & h_3 &= [0 \ 0 \ 1 \ 1 \ 0 \ 0] \\ h_4 &= [1 \ 1 \ 1 \ 0 \ 0 \ 0] & h_5 &= [0 \ 0 \ 0 \ 1 \ 1 \ 1] \end{aligned}$$

Note that $h_1 + h_2 + h_3 = h_4 + h_5$, and hence this monoid is not half-factorial. To show that the elasticity is exactly $3/2$, begin with $\sum_{i=1}^6 a_i h_i = \sum_{i=1}^6 b_i h_i$ with each a_i and b_i nonnegative integers. We leave it as an exercise to show that assuming $(\sum_{i=1}^6 a_i) / (\sum_{i=1}^6 b_i) > 3/2$ leads to a contradiction. Alternatively, one can apply an algorithm from [Kat04] to compute the elasticity of $\mathfrak{C}(R)$. Even though KRSA fails for the class of torsion-free modules over R , the failure is fairly mild: If an R -module M can be expressed as the direct sum of s indecomposable modules and as the direct sum of t indecomposable modules, then the ratio t/s never exceeds $3/2$. As we will see in further examples, much worse direct-sum behavior can occur.

In the final example, we investigate the highly non-unique direct-sum decompositions that can occur with torsion-free modules over a ring with infinite representation type. In stark contrast with the ring in Example 4.16, the elasticity is infinite.

Example 4.17. Let (R, \mathfrak{m}) be a one-dimensional Noetherian local domain whose \mathfrak{m} -adic completion \widehat{R} is isomorphic to the ring

$$\widehat{R} \cong \frac{\mathbb{C}[[x, y]]}{y(x^3 - y^7)}.$$

In this example we apply the same tricks as in Example 4.16. The minimal prime ideals of \widehat{R} are $(x^3 - y^7)\widehat{R}$ and $y\widehat{R}$. To illustrate how badly KRSA fails over R , we need only consider direct-sum relations on *some* of the finitely generated torsion-free modules. It was shown in [Sac10] and [BS] that, for each positive integer n , there exist a positive integer t and an indecomposable finitely generated torsion-free \widehat{R} -module M_n of rank $(0, n)$, and also an indecomposable finitely generated torsion-free \widehat{R} -module N_n of rank $(t + n, n)$. Therefore

$$\text{Ker} ([0 \ 1 \ -1 \ 2 \ -2 \ 3 \ -3 \ \dots]) \cap \mathbb{N}_0^{(\mathbb{N}_0)}$$

is a submonoid of $\mathfrak{C}(R)$.

By Theorem 4.8 $\mathcal{Cl}(\mathfrak{C}(R)) \cong \mathbb{Z}$. Moreover, every element of \mathbb{Z} appears as a column of the defining matrix. Therefore Theorem 4.13 implies that, given any non-empty finite subset S of integers greater than 1, there exists a finitely generated torsion-free R -module M that can be expressed, for every $s \in S$, as the direct sum of s indecomposable finitely generated torsion-free R -modules. By Corollary 4.14, $\rho(\mathfrak{C}(R)) = \infty$.

Calculations similar to those in Examples 4.16 and 4.17 have been done for all one-dimensional local rings with finite representation type (cf. [Bae07] and [BL]) and for some one-dimensional local rings with infinite representation type (cf. [BS]).

5 Questions

In this final section, we give a list of questions related to describing the direct-sum decomposition of modules via the study of certain commutative monoids. Questions (1) and (2) can certainly be approached by interested undergraduates, while Questions (3) and (4) are likely to be very difficult problems.

- (1) What monoids can be realized as Diophantine monoids whose defining matrices consist only of entries in the set $\{-1, 0, 1\}$, and what properties to such monoids have? Since it is easy to construct indecomposable modules corresponding to columns of this form, how can this information be used to describe direct-sum decompositions?

- (2) Certain invariants of the monoid $\mathcal{M}(R)$, such as elasticity and the divisor class group, have been studied. In the study of commutative monoids, other important invariants such as the ω invariant, catenary degree, critical number, and delta sets are used to further refine descriptions of factorization. What do these invariants tell us about direct-sum decompositions?
- (3) In order to get a complete description of all possible direct-sum decompositions of torsion-free modules over one-dimensional local rings, one needs to have a description of all ranks that can occur for indecomposable torsion-free modules over complete rings of this type. All ranks have been computed when R — equivalently \widehat{R} — has finite representation type. At the other extreme, when \widehat{R}/P has infinite representation type for every minimal prime ideal P , Crabbe and Saccon [CS] have shown that *every* tuple occurs as the rank of some indecomposable torsion-free module. Partial results are known in some of the intermediate cases, where \widehat{R} has infinite representation type but \widehat{R}/P has finite representation type for at least one minimal prime P . Given a one-dimensional local Noetherian ring with reduced completion \widehat{R} , what tuples occur as ranks of indecomposable \widehat{R} -modules?
- (4) Much of our focus has been on one-dimensional rings. However, the same tools from factorization theory can be applied to study direct-sum decompositions over a ring R of dimension larger than one if it can determine which \widehat{R} -modules are extended from R -modules. This information is known for certain classes of two-dimensional local integral domains and, in this setting, the monoid $\mathcal{M}(R)$ was considered in [Bae09]. Are there other classes of local rings for which we can determine which \widehat{R} -modules are extended from R -modules? If so, what factorization-theoretic information can be gleaned from this structure?

References

- [AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802 (39 #4129)
- [Bae07] Nicholas R. Baeth, *A Krull-Schmidt theorem for one-dimensional rings of finite Cohen-Macaulay type*, J. Pure Appl. Algebra **208** (2007), no. 3, 923–940.
- [Bae09] N. R. Baeth, *Direct sum decompositions over two-dimensional local domains*, Comm. Algebra **37** (2009), no. 5, 1469–1480.
- [BH93] Winfried Bruns and Jürgen Herzog, *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, Cambridge, 1993. MR 1251956
- [BL] Nicholas R. Baeth and Melissa R. Lucas, *Monoids of torsion-free modules over rings with finite representation type*, preprint.
- [BS] N. Baeth and S. Saccon, *Monoids of modules over rings with infinite Cohen-Macaulay type*, to appear in J. Comm. Algebra.
- [CKO02] S.T. Chapman, U. Krause, and E. Oeljeklaus, *On Diophantine monoids and their class groups*, Pacific J. Math. **207** (2002), no. 1, 125–147.
- [CS] Andrew Crabbe and Silvia Saccon, *Ranks of indecomposable maximal Cohen-Macaulay modules*, in preparation.
- [DF04] David S. Dummit and Richard M. Foote, *Abstract Algebra*, third ed., John Wiley & Sons Inc., Hoboken, NJ, 2004. MR 2286236 (2007h:00003)
- [DR67] Ju. A. Drozd and A. V. Roïter, *Commutative rings with a finite number of indecomposable integral representations*, Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967), 783–798. MR 0220716 (36 #3768)
- [Ger88] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. **197** (1988), 505–529.

- [GHK06] Alfred Geroldinger and Franz Halter-Koch, *Non-unique Factorizations*, Pure and Applied Mathematics (Boca Raton), vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006, Algebraic, combinatorial and analytic theory.
- [HK98] F. Halter-Koch, *Ideal Systems*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 211, Marcel Dekker, 1998.
- [HRKW08] W. Hassler, R. Karr, L. Klingler, and R. Wiegand, *Indecomposable modules of large rank over Cohen-Macaulay local rings*, Trans. Amer. Math. Soc. **360** (2008), no. 3, 1391–1406.
- [Kai99] Florian Kainrath, *Factorization in Krull monoids with infinite class group*, Colloq. Math. **80** (1999), no. 1, 23–30.
- [Kat04] K. Kattchee, *Elasticities of Krull domains with finite divisor class group*, Linear Algebra Appl. **384** (2004), 171–185.
- [Lam01] T. Y. Lam, *A First Course in Noncommutative Rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001. MR 1838439 (2002c:16001)
- [Lec86] Christian Lech, *A method for constructing bad Noetherian local rings*, Algebra, algebraic topology and their interactions (Stockholm, 1983), Lecture Notes in Mathematics, vol. 1183, Springer-Verlag, New York-Berlin, 1986, pp. 241–247.
- [LO96] Lawrence S. Levy and Charles J. Odenthal, *Package deal theorems and splitting orders in dimension 1*, Trans. Amer. Math. Soc. **348** (1996), no. 9, 3457–3503. MR 1351493
- [Mat86] Hideyuki Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Math., vol. 8, Cambridge University Press, Cambridge, 1986.
- [Sac10] S. Saccon, *One-dimensional local rings of infinite Cohen-Macaulay type*, Ph.D. thesis, University of Nebraska–Lincoln, Department of Mathematics, 2010.
- [Wie01] Roger Wiegand, *Direct-sum decompositions over local rings*, J. Algebra **240** (2001), no. 1, 83–97. MR 1830544
- [Yos90] Yuji Yoshino, *Cohen-Macaulay modules over Cohen-Macaulay rings*, London Mathematical Society Lecture Note Series, vol. 146, Cambridge University Press, Cambridge, 1990.