# SILLY DIRECT-SUM DECOMPOSITIONS

ROGER WIEGAND
RESEARCH/EXPOSITORY TALK
TRIBHUVAN UNIVERSITY

In this talk we explore the analogy between factorization in integral domains and direct-sum decompositions of modules. Also, we give examples of strange direct-sum decompositions.

sec:analogy

## 1. The analogy

We begin by recalling some basic terminology and notation from factorization theory.

def:factor-terminology **Definition 1.1.** Let $D$ be a commutative integral domain.

(a) Let $x, y \in D$. We say that $x$ *divides* $y$ and write $x \mid y$ provided there exists $z \in D$ such that $xz = y$.

(b) An element $p \in D$ is *irreducible* provided $p \neq 0$, $p$ is not a unit of $D$, and $p = xy \implies$ either $x$ or $y$ is a unit.

(c) An element $p \in D$ is *prime* provided $p \neq 0$, $p$ is not a unit of $D$, and $p \mid xy \implies p \mid x$ or $p \mid y$.

(d) We say elements $x$ and $y$ are *associates*, and we write $x \sim y$, provided there is a unit $u$ of $D$ such that $ux = y$.

(e) The domain $D$ is a *unique factorization domain* (UFD) provided

(i) every non-zero non-unit of $D$ can be expressed as a finite product of irreducible elements; and

(ii) if $p_1 \cdots p_r = q_1 \cdots q_s$ with each $p_i$ and each $q_j$ irreducible, then $r = s$ and, after renumbering, $p_i \sim q_i$ for each $i$.

ex:prime-irred **Exercise 1.2.** Prove that every prime element is irreducible. Assume that every non-zero non-unit is a product of finitely many irreducible elements. Prove that $R$ is a UFD if and only if every irreducible element is prime.

eg:non-ufd **Example 1.3.** The standard example of a non-UFD is the ring $\mathbb{Z}[\sqrt{-5}]$ of integers in the quadratic number field $\mathbb{Q}(\sqrt{-5})$. In this domain the element 6 has two factorizations: $2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. (One has to check that all four elements are irreducible and that 2 is not an associate of either element on the righthand side of the equation.) There are easier examples: in the ring $\mathbb{Q}[t^2, t^3]$ of polynomials with no linear term, the element $t^{60}$ has factorizations of different lengths (something that does not happen in the ring $\mathbb{Z}[\sqrt{-5}]$): the elements $t^2$ and $t^3$ are irreducible, and $(t^2)^{30} = (t^3)^{20}$.

ex:irred-not-prime **Exercise 1.4.** In the domains $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Q}[t^2, t^3]$, respectively, show that 2 and $t^2$ are not prime.

*Date*: 20 April, 2015.

notation:modules

**Notation 1.5.** Now let $R$ be a ring and $\mathcal{C}$ a non-empty class of $R$-modules closed under finite direct sums, direct summands, and isomorphism. That is, if $M$, $N$, $V$ are $R$-modules with $M \oplus N \cong V$, one has $V \in \mathcal{C}$ if and only if $M \in \mathcal{C}$ and $N \in \mathcal{C}$. Assume, moreover, that $\mathrm{V}(\mathcal{C})$, the collection of isomorphism classes of modules in $\mathcal{C}$, is a *set* (not a proper class). Thus, for example, $\mathcal{C}$ might be the class $R$-mod of all finitely generated modules. The class $R$-Mod of *all* modules, however, would not be allowed. We make $\mathrm{V}(\mathcal{C})$ into an additive semigroup using $\oplus$ as an operation: letting $[M]$ denote the isomorphism class of $M$, we write $[M] + [N] = [M \oplus N]$. The (additive) identity element is of course $[0]$, and this is the *only* unit of $V(\mathcal{C})$, since $M \oplus N \cong 0 \implies M \cong N \cong 0$. Therefore the analog of "associates" is pretty boring: equality in $V(\mathcal{C})$ and isomorphism in $\mathcal{C}$.

Here are the module-theoretic analogs of the concepts (other than (d)) in Definition **??**. (The terminology is somewhat different, since the terms "irreducible module" and "prime module" have been usurped and mean something quite different and irrelevant to our discussion.)

def:module-terminology

**Definition 1.6.** Let $R$ and $\mathcal{C}$ be as in Notation **??**.

(a) Let $X, Y \in \mathcal{C}$. We say that $X$ *divides* $Y$ and write $X \mid Y$ provided there exists $Z \in \mathcal{C}$ such that $X \oplus Z \cong Y$.

(b) A module $P \in \mathcal{C}$ is *indecomposable* provided $P \cong X \oplus Y$ (with $X, Y \in \mathcal{C}$), implies $X = 0$ or $Y = 0$.

(c) A module $P \in \mathcal{C}$ is *prime-like* provided $P \mid X \oplus Y$ (with $X, Y \in C$) implies $P \mid X$ or $P \mid Y$.

(e) The class $\mathcal{C}$ has the *Krull-Remak-Schmidt* property (KRS) provided

(i) every non-zero element of $\mathcal{C}$ can be expressed as a finite direct sum of indecomposable modules; and

(ii) if $P_1 \cdots P_r \cong Q_1 \cdots Q_s$ with each $P_i$ and each $Q_j$ indecomposable, then $r = s$ and, after renumbering, $P_i \cong Q_i$ for each $i$.

ex:prime-like-indec

**Exercise 1.7.** State the analog of Exercise **??**, and do it.

sec:not-KRS

## 2. Failure of KRS

**Assumption 2.1.** Assume from now on that $R$ is a commutative Noetherian ring and that $\mathcal{C} \subseteq R$-mod. Now every element of $\mathcal{C}$ is a direct sum of finitely many indecomposable elements of $\mathcal{C}$. (Exercise: Prove this.)

Here is a family of examples where KRS fails (see [**?**, Example 2.3]).

**Example 2.2.** Let $R$ be an integral domain with two non-principal ideals $I$ and $J$ satisfying $I + J = R$. (For example, take $R = \mathbb{Q}[x, y]$, and let $I$ and $J$ be the maximal ideals $Rx + Ry$ and $Rx + R(y - 1)$.) Then

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

All four modules are indecomposable, neither $I$ nor $J$ is isomorphic to $R$.

That's too easy, and the reason is that the ring $R$ above has more than one maximal ideal. For this reason we will assume from now on that $R$ is a *local* ring, that is, a Noetherian ring just one maximal ideal $\mathfrak{m}$. Now *cancellation* holds [**?**], that is, $M \oplus X \cong M \oplus Y \implies X \cong Y$. (Recall that we are assuming $\mathcal{C} \subseteq R$-mod, that is, all modules under consideration are finitely generated. Without this assumption there are trivial counterexamples to cancellation: take, for example, $M$ to be a free module of infinite rank, let $X = 0$, and let $Y = R$.)

Even with these restrictions (finitely generated modules over a local ring), the semigroup $\mathrm{V}(R\text{-mod})$ is too large to to allow a reasonable description, except in very special cases (for example, when $R$ is a principal ideal ring). We will focus on a small piece of $R$-mod. Fix a finitely generated module $M$, and let $\operatorname{add} M$ denote the set of isomorphism classes of direct summands of direct sums of finitely many copies of $M$. Thus $[X] \in \operatorname{add} M$ if and only if there exist $Y \in R$-mod) and $n \in \mathbb{N}$ such that $X \oplus Y \cong M^{(n)}$.

sec:Diophantine

## 3. Diophantine semigroups: Realization

def:diophantine

**Definition 3.1.** An additive semigroup $H$ is *Diophantine* provided there exist positive integers $n$ and $t$ and an $n \times t$ integer matrix $\varphi$ such that $H \cong (\ker \varphi) \cap \mathbb{N}_0^{(t)}$. Thus $H$ is the set of non-negative integer solutions to $n$ homogeneous linear equations in $t$ variables.

The next two theorems were proved in my 2001 paper [**?**]. The second "realization theorem" is the more difficult of the two.

thm:diophantine

**Theorem 3.2.** *Let $R$ be a Noetherian local ring, and let $M$ be a finitely generated $R$-module. Then $\operatorname{add} M$ is a Diophantine semigroup.*

thm:realization

**Theorem 3.3.** *Let $H$ be a Diophantine semigroup, say $H = (\ker \varphi) \cap \mathbb{N}_0^{(t)}$, where $\varphi$ is an $n \times t$ integer matrix. Assume that $H$ has an "order-unit", that is, an element $\alpha = \begin{bmatrix} a_1 \\ \vdots \\ a_t \end{bmatrix} \in H$ with $a_i > 0$ for each $i$. Then there exist a local domain $R$, a finitely generated torsion-free $R$-module $M$, and a semigroup isomorphism $H \cong \operatorname{add} M$, taking $\alpha$ to $[M]$.*

ex:order

**Exercise 3.4.** Using the representation $H = (\ker \varphi) \cap \mathbb{N}_0^{(t)}$, we have $H$ embedded in $\mathbb{N}_0^{(t)}$, which we endow with the *product partial ordering*: $\begin{bmatrix} a_1 \\ \vdots \\ a_t \end{bmatrix} \le \begin{bmatrix} b_1 \\ \vdots \\ b_t \end{bmatrix} \iff a_i \le b_i$ for each $i$. Prove that $\alpha \mid \beta$ (i.e., there exists $\gamma \in H$ such that $\alpha + \gamma = \beta$) if and only if $\alpha \le \beta$ in $\mathbb{N}_0^{(t)}$.

ex:order-unit

**Exercise 3.5.** Let $H$ be any non-zero Diophantine semigroup, say $H = (\ker \varphi) \cap \mathbb{N}_0^{(t)}$, where $\varphi$ is an $n \times t$ integer matrix. Choose an element $\alpha = \begin{bmatrix} a_1 \\ \vdots \\ a_t \end{bmatrix}$ with the maximum number of positive coordinates. We may assume, without changing the isomorphism class of $H$, that $a_1, \dots, a_s$ are positive and $a_{s+1} = \cdots = a_t = 0$. Show that if $\beta = \begin{bmatrix} b_1 \\ \vdots \\ b_t \end{bmatrix}$ is an arbitrary element of $H$, then $b_{s+1} = \cdots = b_t = 0$. Deduce that $H \cong (\ker \psi) \cap \mathbb{N}_0^{(s)}$, where $\psi$ is the $n \times s$ matrix obtained from $\varphi$ by deleting the last $t - s$ columns. Moreover, $(\ker \psi) \cap \mathbb{N}_0^{(s)}$ has an order-unit, namely, the column vector obtained from $\alpha$ by deleting the $t - s$ zeroes at the bottom. Thus, up to isomorphism, the assumption that $H$ contains an order-unit is no restriction.

The first counterexamples to KRS in the local case were due to Swan in the sixties (see [**?**]). The key idea in Swan's example is that the integral closure of a local domain need not be local. The argument in the realization theorem above uses this same idea, together with a delicate construction of indecomposable modules over the completion (which I will talk about in my next lecture).

The local domain $R$ in Theorem **??** is easy to describe, though finding the requisite module is much more difficult. Fix a Diophantine semigroup $H$ as in the theorem. The number $n$ (the number of defining equations) in the theorem plays a key role. Let $\mathsf{k}$ be any field with at least $n+1$ elements, and let $c_0, \dots, c_n$ be distinct elements of $\mathsf{k}$. Let $\mathsf{k}(x)$ be the ring of rational functions (quotients of polynomials) in one variable, and let $R$ be the subring of $\mathsf{k}(x)$ consisting of those rational functions $f(x) = \frac{p(x)}{q(x)}$ (here $p(x)$ and $q(x)$ are polynomials) such that

(a) $f(x)$ is defined at each $c_i$ (that is, $q(c_0), \dots, q(c_n)$ are all non-zero),

(b) $f(c_0) = \cdots = f(c_n)$, and

(c) the first, second, and third derivatives $f'(x), f''(x)$, and $f'''(x)$ all vanish at each $c_i$.

Then $R$ is a local domain, and there is a finitely generated torsion-free $R$ module $M$ such that $\operatorname{add} M \cong H$. One might hope to find a single local that can accommodate *all* Diophantine semigroups, but in fact the dependence on the number of defining equations is essential. Karl Kattchee [**?**] has shown that there is no fixed local ring over which every Diophantine semigroup can be realized.

Thanks to the realization theorem, if we want to find silly direct-sum decompositions, all we have to do is to find semigroups with silly decompositions into atoms. (An *atom* of a Diophantine semigroup is a non-zero element $\alpha$ with the property that $\alpha = \beta + \gamma \implies \beta = 0$ or $\gamma = 0$.) Of course, if we have an isomorphism between $\operatorname{add} M$ and $H$, the indecomposable modules in $\operatorname{add} M$ correspond to the atoms of $H$.

Here is an example of behavior similar to that of the ring $\mathbb{Z}[\sqrt{-5}]$ in Example **??**:

ex:quad **Exercise 3.6.** Let $H = \{ \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \in \mathbb{N}_0^{(4)} \mid a + b = c + d \}$, a Diophantine semigroup defined by one equation. Show that $H$ has exactly four atoms, namely:

$$\alpha := \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \qquad \beta := \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \qquad \gamma := \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad \delta := \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

We have the obvious relation $\alpha + \beta = \gamma + \delta$. By the realization theorem, there is a local domain $R$ with pairwise non-isomorphic indecomposable finitely generated modules $A, B, C, D$ satisfying the relation $A \oplus B \cong C \oplus D$.

We can get much worse behavior:

ex:83 **Exercise 3.7.** Let $H = \{ \begin{bmatrix} a \\ b \\ c \end{bmatrix} \in \mathbb{N}_0^{(3)} \mid a + 82b = 83c \}$. Show that $H$ has exactly three atoms, namely:

$$\alpha := \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \qquad \beta := \begin{bmatrix} 83 \\ 0 \\ 1 \end{bmatrix} \qquad \gamma := \begin{bmatrix} 0 \\ 83 \\ 82 \end{bmatrix}$$

These satisfy the obvious relation $\beta + \gamma = 83\alpha$. By the realization theorem, there is a local ring with pairwise non-isomorphic indecomposable modules $A, B, C$ satisfying the relation $B \oplus C \cong A^{(83)}$. An innocent bystander looking at direct sums of copies of $A$ would notice that $A^{(2)}$, $A^{(3)}$, ..., $A^{(82)}$ have only the obvious decompositions into direct sums of indecomposables. Then all of a sudden $A^{(83)}$ comes along with a decomposition as a direct sum of just two indecomposables!

In each of these examples, the Diophantine semigroup is defined by just *one* equation and hence can be realized over the subring of $\mathsf{k}(x)$ consisting of rational functions $f$ such that $f(0) = f(1)$ and whose first three derivatives vanish at 0 and 1. Semigroups with more than one defining equation can exhibit even more bizarre behavior. See [**?**] for more examples of silly direct-sum behavior.

Can we find modules over a local ring that emulate the two factorizations of $t^{60}$ in Example **??**? That is, are there finitely generated indecomposable modules $A$ and $B$ over a local ring, such that $A^{(30)} \cong B^{(20)}$. If there were such modules, then, by Theorem **??**, we would have a Diophantine semigroup $H$ with distinct atoms $a$ and $b$ such that $30a = 20b$. As in Exercise **??**, we have $H \hookrightarrow \mathbb{N}^{(t)}$. The relation obviously implies that $a \leq b$ (in the product partial ordering on $\mathbb{N}^{(t)}$). But this means that $a \mid b$ in $H$, an obvious contradiction. Thus such a relation is *not* possible in the context of modules!

Please consult the expository paper [**?**] for a leisurely, reasonably self-contained presentation of many of the ideas discussed in this talk.

## References

[1] N. Baeth and R. Wiegand, Factorization theory and decompositions of modules, *Amer. Math. Monthly* **1**20 (2013), 3–34.
[2] E. G. Evans, Jr., Krull-Schmidt and cancellation over local rings, *Pacific J. Math.* **4**6 (1973), 115–121.
[3] K. Kattchee Monoids and direct-sum decompositions over local rings *J. Algebra* **2**56 (2002), 51–65.
[4] R. Wiegand Direct-sum decompositions over local rings, *J. Algebra* **2**40 (2001), 83–97.