One-Sided Ideal Factorization Theory in Hereditary Noetherian Prime Rings

Daniel Vitas

UNIVERSITY OF LJUBLJANA
Faculty of Mathematics and Physics

Institute of Mathematics, Physics and Mechanics

June 17, 2026

Multiplying integers

Multiplication in $\mathbb{Z}$

$$12 \cdot 27 =$$

Multiplying integers

Multiplication in $\mathbb{Z}$

$$12 \cdot 27 = 324$$

Multiplying integers

Multiplication in $\mathbb{Z}$

$$12 \cdot 27 = 324$$
$$2^2\,3^1 \cdot 2^0\,3^3 = 2^2\,3^4$$

Multiplying integers

Multiplication in $\mathbb{Z}$

$$12 \cdot 27 = 324$$
$$2^2\, 3^1 \cdot 2^0\, 3^3 = 2^2\, 3^4$$

is actually just addition of tuples

$$(2, 1, 0, \ldots) + (0, 3, 0, \ldots) = (2, 4, 0, \ldots)$$

Multiplying algebraic integers

The ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ is a bit more interesting:

$$\frac{3+\sqrt{-23}}{2} \cdot \frac{3-\sqrt{-23}}{2} = 8$$

Multiplying algebraic integers

The ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ is a bit more interesting:

$$\frac{3+\sqrt{-23}}{2} \cdot \frac{3-\sqrt{-23}}{2} = 8$$

$$2 \cdot 2 \cdot 2 = 8$$

Multiplying algebraic integers

The ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ is a bit more interesting:

$$\frac{3+\sqrt{-23}}{2} \cdot \frac{3-\sqrt{-23}}{2} = 8$$

$$2 \cdot 2 \cdot 2 = 8$$

The elements 2, $\frac{3+\sqrt{-23}}{2}$, and $\frac{3-\sqrt{-23}}{2}$ are irreducible and aren't associated, so we have

$$(1,1,0,0,\ldots) = (0,0,3,0,\ldots)$$

Multiplying algebraic integers

The ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ is a bit more interesting:

$$\frac{3+\sqrt{-23}}{2} \cdot \frac{3-\sqrt{-23}}{2} = 8$$

$$2 \cdot 2 \cdot 2 = 8$$

The elements 2, $\frac{3+\sqrt{-23}}{2}$, and $\frac{3-\sqrt{-23}}{2}$ are irreducible and aren't associated, so we have

$$(1,1,0,0,\ldots) = (0,0,3,0,\ldots) \qquad \text{bad!}$$

Multiplying algebraic integers

The ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ is a bit more interesting:

$$\begin{aligned} \frac{3+\sqrt{-23}}{2} \cdot \frac{3-\sqrt{-23}}{2} &= 8 \\ 2 \cdot 2 \cdot 2 &= 8 \end{aligned}$$

The elements 2, $\frac{3+\sqrt{-23}}{2}$, and $\frac{3-\sqrt{-23}}{2}$ are irreducible and aren't associated, so we have

$$(1,1,0,0,\dots) = (0,0,3,0,\dots) \qquad \text{bad!}$$

Working with ideals instead:

$P, Q \lhd \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ certain prime ideals

$$\begin{aligned} (2) &= PQ \\ \left(\frac{3+\sqrt{-23}}{2}\right) &= P^3 \\ \left(\frac{3-\sqrt{-23}}{2}\right) &= Q^3 \end{aligned}$$

Multiplying algebraic integers

The ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ is a bit more interesting:

$$P^3 \cdot Q^3 \quad = \frac{3+\sqrt{-23}}{2} \cdot \frac{3-\sqrt{-23}}{2} = 8$$

$$PQ \cdot PQ \cdot PQ = \quad 2 \cdot 2 \cdot 2 \quad = 8$$

The elements 2, $\frac{3+\sqrt{-23}}{2}$, and $\frac{3-\sqrt{-23}}{2}$ are irreducible and aren't associated, so we have

$$(1,1,0,0,\ldots) = (0,0,3,0,\ldots) \qquad \text{bad!}$$

Working with ideals instead:

$P, Q \vartriangleleft \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ certain prime ideals

$$(2) = PQ$$

$$\left(\frac{3+\sqrt{-23}}{2}\right) = P^3$$

$$\left(\frac{3-\sqrt{-23}}{2}\right) = Q^3$$

Dedekind domains and divisors

A commutative domain R is a *Dedekind domain* if it is **hereditary**:

$$\text{every ideal } I \lhd D \text{ is projective}$$

Dedekind domains and divisors

A commutative domain R is a *Dedekind domain* if it is **hereditary**:

$$\text{every ideal } I \lhd D \text{ is projective}$$

Example

Rings of algebraic integers $\mathcal{O}_K$ of a number field K.

Dedekind domains and divisors

A commutative domain R is a *Dedekind domain* if it is **hereditary**:

$$\text{every ideal } I \lhd D \text{ is projective}$$

Example

Rings of algebraic integers $\mathcal{O}_K$ of a number field K.

A *divisor* of a non-zero ideal $I \lhd R$ is

$$\partial I = \sum_{P \text{ prime}} m_P P \in \bigoplus_{P \text{ prime}} \mathbb{Z}_{\geq 0} P$$

$m_P =$ the multiplicity of P appearing in the factorization of I

Dedekind domains and divisors

A commutative domain R is a *Dedekind domain* if it is **hereditary**:

$$\text{every ideal } I \lhd D \text{ is projective}$$

Example

Rings of algebraic integers $\mathcal{O}_K$ of a number field K.

A *divisor* of a non-zero ideal $I \lhd R$ is

$$\partial I = \sum_{P \text{ prime}} m_P P \in \bigoplus_{P \text{ prime}} \mathbb{Z}_{\geq 0} P$$

For ideals I and J, we have

$$\boxed{\partial IJ = \partial I + \partial J.}$$

$m_P =$ the multiplicity of P appearing in the factorization of I

Dedekind domains and divisors

A commutative domain R is a *Dedekind domain* if it is **hereditary**:

$$\text{every ideal } I \lhd D \text{ is projective}$$

Example

Rings of algebraic integers $\mathcal{O}_K$ of a number field K.

A *divisor* of a non-zero ideal $I \lhd R$ is

$$\partial I = \sum_{P \text{ prime}} m_P P \in \bigoplus_{P \text{ prime}} \mathbb{Z}_{\geq 0} P$$

For ideals I and J, we have

$$\partial IJ = \partial I + \partial J.$$

$m_P =$ the multiplicity of P appearing in the factorization of I

$$P \lhd R \text{ prime} \iff U = R/P \text{ simple } R\text{-module}$$

Dedekind domains and divisors

A commutative domain R is a *Dedekind domain* if it is **hereditary**:

$$\text{every ideal } I \lhd D \text{ is projective}$$

Example

Rings of algebraic integers $\mathcal{O}_K$ of a number field K.

A *divisor* of a non-zero ideal $I \lhd R$ is

$$\partial I = \sum_{U \text{ simple}} m_U\, U \in \bigoplus_{U \text{ simple}} \mathbb{Z}_{\geq 0}\, U$$

For ideals I and J, we have

$$\partial IJ = \partial I + \partial J.$$

m_U = the multiplicity of U appearing in the Jordan-Hölder decomposition of R/I

$$P \lhd R \text{ prime} \iff U = R/P \text{ simple } R\text{-module}$$

Maximal orders

Let R be a *noncommutative maximal* $\mathbb{Z}$*-order*, i.e., a subring of a CSA over $\mathbb{Q}$, f.g. as a $\mathbb{Z}$-module, and maximal such.

Maximal orders

Let R be a *noncommutative maximal* $\mathbb{Z}$*-order*, i.e., a subring of a CSA over $\mathbb{Q}$, f.g. as a $\mathbb{Z}$-module, and maximal such.

Examples

$$M_2(\mathbb{Z}), \quad \mathbb{H}_{\mathbb{Z}} + \tfrac{1}{2}(1 + i + j + k)\,\mathbb{Z}$$

Maximal orders

Let R be a *noncommutative maximal $\mathbb{Z}$-order*, i.e., a subring of a CSA over $\mathbb{Q}$, f.g. as a $\mathbb{Z}$-module, and maximal such.

Examples

$$M_2(\mathbb{Z}), \quad \mathbb{H}_{\mathbb{Z}} + \tfrac{1}{2}(1+i+j+k)\,\mathbb{Z}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I + \partial J.$$

∂ is bijective

Maximal orders

Let R be a *noncommutative maximal $\mathbb{Z}$-order*, i.e., a subring of a CSA over $\mathbb{Q}$, f.g. as a $\mathbb{Z}$-module, and maximal such.

Examples

$$M_2(\mathbb{Z}), \quad \mathbb{H}_{\mathbb{Z}} + \tfrac{1}{2}(1+i+j+k)\,\mathbb{Z}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I + \partial J.$$

∂ is bijective

The problem with one-sided ideals:

$$a = bc$$

$$aR = (b\,cRc^{-1})\,cR$$

Right ideals over different rings!

Maximal orders

Let R be a *noncommutative maximal $\mathbb{Z}$-order*, i.e., a subring of a CSA over $\mathbb{Q}$, f.g. as a $\mathbb{Z}$-module, and maximal such.

Examples

$$M_2(\mathbb{Z}), \quad \mathbb{H}_{\mathbb{Z}} + \tfrac{1}{2}(1+i+j+k)\,\mathbb{Z}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I + \partial J.$$

∂ is bijective

The problem with one-sided ideals:

$$a = bc$$

$$aR = (b\,cRc^{-1})\,cR$$

Right ideals over different rings!

There is a canonical bijection between simple modules.

Maximal orders

Let R be a *noncommutative maximal $\mathbb{Z}$-order*, i.e., a subring of a CSA over $\mathbb{Q}$, f.g. as a $\mathbb{Z}$-module, and maximal such.

Examples

$$M_2(\mathbb{Z}), \quad \mathbb{H}_{\mathbb{Z}} + \tfrac{1}{2}(1+i+j+k)\,\mathbb{Z}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I + \partial J.$$

Also works for **one-sided** ideals!

∂ is bijective

The problem with one-sided ideals:

$$a = bc$$

$$aR = (b\,cRc^{-1})\,cR$$

Right ideals over different rings!

There is a canonical bijection between simple modules.

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

HNP Rings

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

Example

Hereditary $\mathbb{Z}$-orders in a CSA over $\mathbb{Q}$, e.g.

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

HNP Rings

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

Example

Hereditary $\mathbb{Z}$-orders in a CSA over $\mathbb{Q}$, e.g.

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

HNP Rings

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

Example

Hereditary $\mathbb{Z}$-orders in a CSA over $\mathbb{Q}$, e.g.

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

$$I = \begin{bmatrix} p\mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

HNP Rings

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

Example

Hereditary $\mathbb{Z}$-orders in a CSA over $\mathbb{Q}$, e.g.

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

$$I = \begin{bmatrix} p\mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

$$I^2 = I \implies \partial I \circ \partial I = \partial I$$

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

Example

Hereditary $\mathbb{Z}$-orders in a CSA over $\mathbb{Q}$, e.g.

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

$$I = \begin{bmatrix} p\mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

$$J = \begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & p\mathbb{Z} \end{bmatrix}$$

$$I^2 = I \implies \partial I \circ \partial I = \partial I$$

$$\partial IJ = \partial I + 2\partial J$$

$$\partial JI = 2\partial I + \partial J$$

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

Example

Hereditary $\mathbb{Z}$-orders in a CSA over $\mathbb{Q}$, e.g.

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

∂ injective, but **not** surjective!

$$I = \begin{bmatrix} p\mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

$$J = \begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & p\mathbb{Z} \end{bmatrix}$$

$$I^2 = I \implies \partial I \circ \partial I = \partial I$$

$$\partial IJ = \partial I + 2\partial J$$

$$\partial JI = 2\partial I + \partial J$$

HNP Rings

A ring R is an *HNP ring* if it is **hereditary**, **noetherian**, and **prime**.

Example

Hereditary $\mathbb{Z}$-orders in a CSA over $\mathbb{Q}$, e.g.

$$\begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

For two-sided ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J,$$

where $\circ$ is given by... (Rump-Yang 2016)

∂ injective, but **not** surjective!

$$I = \begin{bmatrix} p\mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}$$

$$J = \begin{bmatrix} \mathbb{Z} & p\mathbb{Z} \\ \mathbb{Z} & p\mathbb{Z} \end{bmatrix}$$

$$I^2 = I \implies \partial I \circ \partial I = \partial I$$

$$\partial IJ = \partial I + 2\partial J$$

$$\partial JI = 2\partial I + \partial J$$

One-sided ideals

Theorem (V. 2026)

There **is** exactly one operation $\circ$ on the divisors such that for **one-sided** ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

One-sided ideals

Theorem (V. 2026)

There **is** exactly one operation $\circ$ on the divisors such that for **one-sided** ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

Proof. Given ∂I and ∂J, we want to describe

$$\partial IJ = R/IJ$$

Theorem (V. 2026)

There **is** exactly one operation $\circ$ on the divisors such that for **one-sided** ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

Proof. Given ∂I and ∂J, we want to describe

$$\begin{aligned} \partial IJ &= R/IJ \\ &= J/IJ + R/J \end{aligned}$$

$$\begin{tikzcd} R \arrow[d, dash] \\ J \arrow[d, dash] \\ IJ \end{tikzcd}$$

One-sided ideals

Theorem (V. 2026)

There **is** exactly one operation $\circ$ on the divisors such that for **one-sided** ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

Proof. Given ∂I and ∂J, we want to describe

$$\begin{aligned} \partial IJ &= R/IJ \\ &= J/IJ + R/J \\ &= \partial I \otimes J + \partial J \end{aligned}$$

$$\begin{tikzcd} R \arrow[d, dash] \\ J \arrow[d, dash] \\ IJ \end{tikzcd}$$

One-sided ideals

Theorem (V. 2026)

There **is** exactly one operation $\circ$ on the divisors such that for **one-sided** ideals I and J, we have

$$\partial IJ = \partial I \circ \partial J.$$

Proof. Given ∂I and ∂J, we want to describe

$$\begin{aligned} \partial IJ &= R/IJ \\ &= J/IJ + R/J \\ &= \partial I \otimes J + \partial J \end{aligned}$$

$$\begin{array}{c} R \\ | \\ J \\ | \\ IJ \end{array}$$

- For a maximal ideal J, this follows from the structure of HNP rings. (using idealizers)

One-sided ideals

Theorem (V. 2026)

There **is** exactly one operation $\circ$ on the divisors such that for **one-sided** ideals I and J, we have
$$\partial IJ = \partial I \circ \partial J.$$

Proof. Given ∂I and ∂J, we want to describe

$$\begin{aligned} \partial IJ &= R/IJ \\ &= J/IJ + R/J \\ &= \partial I \otimes J + \partial J \end{aligned}$$

$$\begin{tikzcd} R \arrow[d, dash] \\ J \arrow[d, dash] \\ IJ \end{tikzcd}$$

- For a maximal ideal J, this follows from the structure of HNP rings. (using idealizers)
- We describe a general right ideal J using maximal ideals. (first enlarge the right order, and shrink the left order)