# Length-Factoriality and Pure Irreducibility

Alan Bu Joseph Vulakh Alex Zhao
Mentor: Dr. Felix Gotti

MIT PRIMES Conference
October 15–16, 2022

# Monoids

A commutative, cancellative monoid is a set $M$ endowed with an operation, denoted as multiplication or addition. A multiplicative monoid satisfies the following properties:

- $a \cdot b \in M$ for all $a, b \in M$.
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in M$.
- There exists an identity 1 such that $1 \cdot a = a$ for all $a \in M$.
- $a \cdot b = b \cdot a$ for all $a, b \in M$.
- For all $a, b, c \in M$, if $a \cdot c = b \cdot c$ then $a = b$.

For the rest of this presentation, we abbreviate to just monoid.

**Examples**

- The nonzero integers are a monoid under multiplication.
- The integers are a monoid under addition.

A monoid with inverses is called an abelian group.

# Divisibility in Monoids

Let $M$ be a multiplicative monoid.

Given elements $a, b \in M$, we say $b$ divides $a$ if there exists $c$ in $M$ such that $a = bc$.

An element $u \in M$ is called a unit if $u$ divides 1.

**Examples**

- In $\mathbb{Z} \setminus \{0\}$ under multiplication, 2 divides 6 because $6 = 2 \cdot 3$. The units in this monoid are $\pm 1$.
- $\mathbb{Q} \setminus \{0\}$ under multiplication is a monoid. Every element divides every other element: $a = b \cdot (\frac{a}{b})$. Furthermore, every element is a unit: $a \cdot (\frac{1}{a}) = 1$.
- $\mathbb{N}_0 \setminus \{1\}$ under addition is a monoid. In this monoid, $b$ divides $a$ if $b + 2 \leq a$ or $b = a$. The only unit is 0.

# Divisibility in Monoids, cont.

Again, let $M$ be a multiplicative monoid.

Two elements are associates if one is a unit multiple of the other.

A nonunit $a \in M$ is an atom if for any $b, c \in M$ satisfying $a = bc$, either $b$ or $c$ is a unit.

**Examples**

- In $\mathbb{Z} \setminus \{0\}$ under multiplication, for each $n$, the elements $\pm n$ are associates. The atoms are $\pm p$ for primes $p$.
- In $\mathbb{Q} \setminus \{0\}$ under multiplication, any two elements are associates, and there are no atoms.
- In $\mathbb{N}_0 \setminus \{1\}$ under addition, no two distinct elements are associates because its only unit is 0. The set of atoms is $\{2, 3\}$.

# Integral Domains

An integral domain is a set $R$ with two operations, addition and multiplication, satisfying the following properties:

- $R$ is an abelian group under addition, with identity 0.
- $R \backslash \{0\}$ is a monoid under multiplication, with identity 1.
- Multiplication in $R$ distributes over addition; that is, for all $a, b, c \in R$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

We refer to divisibility properties (atoms, units, divisibility) of the multiplicative monoid of $R$ as properties of $R$ itself.

**Examples**

- The sets of integers, rational numbers, and real numbers are all integral domains.
- The Gaussian integers $a + bi$ for integers $a, b$ form an integral domain.

# Fundamental Theorem of Arithmetic

## Fundamental Theorem of Arithmetic

For any $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, there is a **unique** factorization of $n$ as a product of atoms, up to order and associates.

## Example

The element 6 can only be factored as $2 \cdot 3$, $3 \cdot 2$, $(-2) \cdot (-3)$, or $(-3) \cdot (-2)$. These factorizations differ only in the order of the factors and unit multiples of atoms.

Can this be generalized?

# Unique Factorization Domains

An integral domain $R$ is called a unique factorization domain (UFD) if every nonzero nonunit element $r$ satisfies the following two properties:

- $r$ can be written as a finite product of atoms of $R$: $r = p_1 \dots p_n$.
- This factorization is unique up to order and associates. In other words, if $r = q_1 \dots q_m$, with all $q_i$ atoms, then $m = n$, the $q_i$ can be reordered so that for all $i$, $p_i$ is associate to $q_i$.

**Examples**

- The Fundamental Theorem of Arithmetic states that $\mathbb{Z}$ is a UFD.
- The integral domain of the Gaussian integers (complex numbers of the form $a + bi$ with $a, b \in \mathbb{Z}$) is a UFD.

# Nonunique Factorization

The integral domain $\mathbb{Z}[\sqrt{-5}]$ consists of numbers of the form $a + b\sqrt{-5}$, where $a, b$ are integers. In this integral domain, every element can be written as a finite product of atoms, but some elements have multiple factorizations.

**Example**

The element 6 can be written as $2 \cdot 3$ or $(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. The elements $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all atoms, and no two are associates. Thus these two factorizations are distinct, and $\mathbb{Z}[\sqrt{-5}]$ does not satisfy the unique factorization property.

# Factorization Properties

Since factorization in integral domains uses only one operation, the concept can be extended from the multiplicative monoids of integral domains to arbitrary monoids.

## Definition (Atomic Monoid)

A monoid is atomic if every nonunit element has a factorization as a product of atoms.

## Examples

- The multiplicative monoid of a unique factorization domain is atomic.
- The multiplicative monoid of $\mathbb{Z}[\sqrt{-5}]$ is atomic.
- The additive monoid of nonnegative integers is atomic (1 is the only atom).
- The additive monoid $\{0\} \cup \mathbb{R}_{\geq 1}$ is atomic (elements of $[1, 2)$ are the atoms).

# Factorization Properties, cont.

We call the number of (not necessarily distinct) atoms in a factorization its length. For the following definition, the monoid $M$ is assumed to be atomic.

**Definition (Length-Factorial Monoid)**

A monoid is length-factorial if no two distinct factorizations of the same element have the same length. We abbreviate length-factorial monoid to LFM.

**Example**

The additive monoid $M = \mathbb{N}_0 \setminus \{1\}$ is an LFM with atoms 2 and 3.

**Theorem (Coykendall, Smith, 2011)**

*Any integral domain whose multiplicative monoid is an LFM is a unique factorization domain.*

# Pure Atoms

**Remark**

In $M = \mathbb{N}_0 \setminus \{1\}$, for any two distinct factorizations of the same element, one is longer than the other. Then the longer one has more 2s and the shorter one has more 3s.

This motivates the following definition:

**Definition (Pure Atoms)**

An atom $a$ is purely long if for any two factorizations of the same element of $M$, if one contains $a$ and the other does not contain $a$, then $a$ is in the longer factorization, with the condition that at least one such pair of factorizations exists. A purely short atom is defined similarly.

# Factorization in Length-Factorial Monoids

**Theorem (Bu, Vulakh, Zhao, 2022)**

*Every nonunit element of an LFM has only finitely many distinct factorizations.*

**Example**

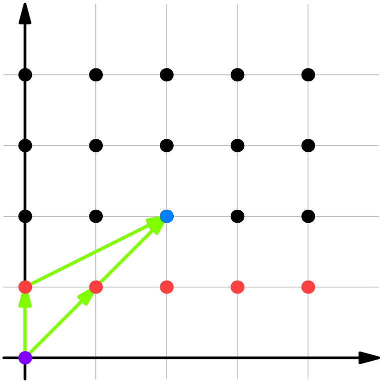
The monoid $M = \mathbb{N}_0 \setminus \{1\}$ is an LFM.
Every element of $M$ has only finitely many distinct factorizations.

Does the converse hold?

# Factorization in Length-Factorial Monoids, cont.

**Example**

Every element of $M = \{(0,0)\} \cup (\mathbb{N}_0 \times \mathbb{N})$ has only finitely many distinct factorizations.
$M$ is not an LFM: $(2,2) = (0,1) + (2,1) = (1,1) + (1,1)$.



# Pure Atoms in Length-Factorial Monoids

**Theorem (Bu, Vulakh, Zhao, 2022)**

*For any $(m, n) \in \mathbb{N}^2$, there exists an LFM with exactly $m$ purely long atoms and exactly $n$ purely short atoms.*

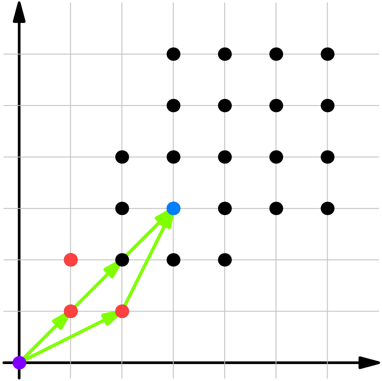
**Example**

For $(m, n) = (1, 1)$, the monoid $\mathbb{N}_0 \setminus \{1\}$ has one purely long atom, 2, and one purely short atom, 3.

# Pure Atoms in Length-Factorial Monoids, cont.

## Example

For $(m, n) = (1, 2)$, the submonoid of $\mathbb{Z}^2$ generated by $(1, 1)$, $(2, 1)$, and $(1, 2)$ is an LFM with $(1, 1)$ purely long and $(2, 1)$ and $(1, 2)$ purely short.



# Pure Atoms in Monoid Domains

**Definition (Monoid Domain)**

Given an integral domain $R$ and an additive monoid $M$, we denote by $R[x; M]$ the ring of polynomial expressions in $x$ with coefficients in $R$ and exponents in $M$, and call it the monoid domain of $M$ over $R$.

We abbreviate this by $R[M]$.

**Theorem (Bu, Vulakh, Zhao, 2022)**

*Let $F$ be a field, and $M$ an atomic additive submonoid of $\mathbb{Q}_{\geq 0}$, the nonnegative rational numbers. Then the monoid domain $F[M]$ contains no pure atoms.*

# Acknowledgements

Many thanks to

- Our mentor, Dr. Felix Gotti
- MIT PRIMES organizers
- Our parents

# References


S. T. Chapman, J. Coykendall, F. Gotti, and W. W. Smith: *Length-factoriality in commutative monoids and integral domains*, J. Algebra **578** (2021) 186–212.

P. M. Cohn: *Bezout rings and and their subrings*, Proc. Cambridge Philos. Soc. **64** (1968) 251–264.

J. Coykendall and W. W. Smith: *On unique factorization domains*, J. Algebra **332** (2011) 62–70.

D. Dummit and R. Foote: *Abstract Algebra*, Prentice Hall, 2003.