Atomicity in Algebra and Combinatorics

Felix Gotti
fgotti@mit.edu

Massachusetts Institute of Technology

IAP Mathematics Lecture Series
January 13, 2021

Atomicity in Commutative Monoids

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Monoids

Notation: $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ and $\mathbb{N}_0 := \{0\} \cup \mathbb{N}$.

Definition: A pair $(M, *)$, where M is a set and $*$ is a binary operation on M (that is, a function $* : S \times S \to S$ where $(x, y) \mapsto x * y$), is called a monoid if

1. $*$ is associative: $x * (y * z) = (x * y) * z$ for all $x, y, z \in M$, and
2. M has an identity element: there is $1 \in M$ such that $1 * x = x * 1 = x$ for all $x \in M$.

- We often write just M, rather than $(M, *)$.
- A monoid M is a group if every $x \in M$ is invertible (that is, there exists $y \in M$ such that $x * y = y * x = 1$).

Remark: We will assume that every monoid we mention here is

- commutative: $x * y = y * x$ for all $x, y \in M$, and
- cancellative: $x * y = x * z$ implies $y = z$ for all $x, y, z \in M$.

Examples

1. $\mathbb{N}_0$, $\mathbb{Q}_{\geq 0}$, and $\{m/2^n : m, n \in \mathbb{N}_0\}$ are monoids with the standard addition.
2. $\mathbb{N}$ is a monoid under the standard multiplication.
3. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the standard addition.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

Atomic Monoids

Definition (atomic monoid)

Let $(M, *)$ be a monoid.

- A non-invertible $a \in M$ is an atom if for all $x, y \in M$, the equality $a = x * y$ implies that either x or y is invertible.
- The monoid M is atomic if every non-invertible element of M can be expressed as a product of atoms.
- We let $\mathcal{A}(M)$ denote the set of atoms of M.

Examples

1. $(\mathbb{N}_0, +)$ is atomic and its only atom is 1.
2. For every $d \in \mathbb{N}$, the monoid $(\mathbb{N}_0^d, +)$ is atomic.
3. For every $r \in \mathbb{Q}_{>0}$, the monoid $(\{0\} \cup \mathbb{Q}_{\geq r}, +)$ is atomic with set of atoms $[r, 2r) \cap \mathbb{Q}$.
4. $(\mathbb{N}, \cdot)$ is atomic with set of atoms $\mathbb{P}$, the set of prime numbers.
5. The additive monoid $M = \{m/2^n : m, n \in \mathbb{N}_0\}$ is not atomic: $x = x/2 + x/2$ for all $x \in M \setminus \{0\}$.

ACCP Monoids

Definition: Let $(M, *)$ be a monoid.

- For each $x \in M$, the set $x * M := \{x * y : y \in M\}$ is called a principal ideal of M.
- M satisfies the ascending chain condition on principal ideals (ACCP) if for every sequence $(x_n * M)_{n \in \mathbb{N}}$ of principal ideals of M, there exists $k \in \mathbb{N}$ such that $x_n * M = x_k * M$ for every $n \geq k$.

Proposition

Every monoid that satisfies the ACCP is atomic.

ACCP Monoids

Definition: Let $(M, *)$ be a monoid.

- For each $x \in M$, the set $x * M := \{x * y : y \in M\}$ is called a principal ideal of M.
- M satisfies the ascending chain condition on principal ideals (ACCP) if for every sequence $(x_n * M)_{n \in \mathbb{N}}$ of principal ideals of M, there exists $k \in \mathbb{N}$ such that $x_n * M = x_k * M$ for every $n \geq k$.

Proposition

Every monoid that satisfies the ACCP is atomic.

ACCP Monoids

Definition: Let $(M, *)$ be a monoid.

- For each $x \in M$, the set $x * M := \{x * y : y \in M\}$ is called a principal ideal of M.
- M satisfies the ascending chain condition on principal ideals (ACCP) if for every sequence $(x_n * M)_{n \in \mathbb{N}}$ of principal ideals of M, there exists $k \in \mathbb{N}$ such that $x_n * M = x_k * M$ for every $n \geq k$.

Proposition

Every monoid that satisfies the ACCP is atomic.

ACCP Monoids

Definition: Let $(M, *)$ be a monoid.

- For each $x \in M$, the set $x * M := \{x * y : y \in M\}$ is called a principal ideal of M.
- M satisfies the ascending chain condition on principal ideals (ACCP) if for every ascending sequence $(x_n * M)_{n\in\mathbb{N}}$ of principal ideals of M, there exists $k \in \mathbb{N}$ such that $x_n * M = x_k * M$ for every $n \geq k$.

Proposition

Every monoid that satisfies the ACCP is atomic. Exercise.

Proof: Let M be ACCP. Sps BWOC that $\exists\, x_0 \in M \setminus M^\times$ ($M^\times$ = set of invertible elements of M). is not the product of elements in $M \setminus M^\times$. Then $\exists\, x_1, y_1 \in M \setminus M^\times : x_0 = x_1 y_1$, where WLOG x_1 is NOT the prod. of non-invert. elements. Inductively, $\exists\, (x_n)$ and (y_n) : $x_n = x_{n+1} y_{n+1}$ and x_n is NOT the prod. of non-invertible. Now the seq $(x_n M)$ is an asc. chain of princ. ideals, and so $\exists\, k \in \mathbb{N}$: $x_k M = x_{k+1} M$. Then $y_{k+1} \in M^\times$. Therefore we get a contr. $\blacksquare$

Factorizations in Monoids

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \ldots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.
2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi\colon \{1, \ldots, k\} \to \{1, \ldots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).
3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Factorizations in Monoids

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \dots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.

2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi\colon \{1, \dots, k\} \to \{1, \dots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).

3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.

4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Factorizations in Monoids

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \dots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.
2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi\colon \{1, \dots, k\} \to \{1, \dots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).
3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Factorizations in Monoids

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \dots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.
2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi\colon \{1, \dots, k\} \to \{1, \dots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).
3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Factorizations in Monoids

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \dots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.
2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi \colon \{1, \dots, k\} \to \{1, \dots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).
3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \dots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.
2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi \colon \{1, \dots, k\} \to \{1, \dots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).
3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Factorizations in Monoids

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \dots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.
2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi\colon \{1, \dots, k\} \to \{1, \dots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).
3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Factorizations in Monoids

Let $(M, *)$ be an atomic monoid.

1. If $x = a_1 * \cdots * a_\ell$ for atoms $a_1, \dots, a_\ell \in M$, then the formal expression $a_1 * \cdots * a_\ell$ is a factorization of x.
2. Two factorizations $a_1 * \cdots * a_\ell$ and $b_1 * \cdots * b_k$ are the same if $k = \ell$ and there is a bijection $\varphi \colon \{1, \dots, k\} \to \{1, \dots, k\}$ such that a_j and $b_{\varphi(j)}$ are associates (i.e., $b_{\varphi(j)} = a_j u$ for some invertible element $u \in M$).
3. For each $x \in M$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
4. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in M$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Ex: $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$, $6 = 2+2+2 = 3+3 \Rightarrow \mathsf{L}(6) = \{2,3\}$.

Definition

Let M be an atomic monoid.

- M is a unique factorization monoid (UFM) if $|\mathsf{Z}(x)| = 1$ for all $x \in M$.
- M is a half-factorial monoid (HFM) if $|\mathsf{L}(x)| = 1$ for all $x \in M$.
- M is a finite factorization monoid (FFM) if $|\mathsf{Z}(x)| < \infty$ for all $x \in M$.
- M is a bounded factorization monoid (BFM) if $|\mathsf{L}(x)| < \infty$ for all $x \in M$.

Factorizations in Monoids (continuation)

We have the following chain of implications.

UFM $\Rightarrow$ [FFM, HFM] $\Rightarrow$ BFM $\Rightarrow$ atomic monoid

Examples

① $M = \{0\} \cup \{2, 3, \ldots\}$ is NOT a HFM as $L(6) = \{2, 3\}$.
However, M is a FFM. [HFM $\not\Rightarrow$ FFM] and also [HFM $\not\Rightarrow$ UFM]

② $M = (\{0\} \cup \mathbb{Q}_{\geq 2}, +)$ with $\mathcal{A}(M) = [2, 4) \cap \mathbb{Q}$. We have

$$5 = \underbrace{\left(2 + \tfrac{1}{n}\right) + \left(3 - \tfrac{1}{n}\right)}_{\in\, Z(5)}$$

for all $n \in \mathbb{N}$.

$\Longrightarrow$ M is NOT a FFM. However it is NOT difficult to see that M is a BFM.

Factorizations in Monoids (continuation)

We have the following chain of implications.

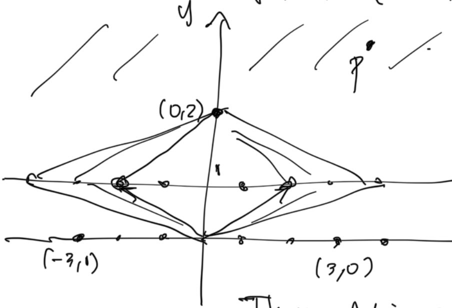
$$\textbf{UFM} \Rightarrow \textbf{[FFM, HFM]} \Rightarrow \textbf{BFM} \Rightarrow \textbf{atomic monoid}$$

Remark: None of the implications above is reversible.

③ Take $M = (\mathbb{Z} \times \mathbb{N}_0, +)$. Then M is atomic and $\mathcal{A}(M) = \{(a,1) : a \in \mathbb{Z}\}$. Note

$(0,2) = (-n,1) + (n,1) \Rightarrow |\mathsf{Z}(0,2)| = \infty$

$\mathsf{L}(0,2) = \{2\}$.



$\longrightarrow$ atoms

$\longrightarrow$ invertible elements

Thus, M is a HFM.

Atomicity in Commutative Rings

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

Integral Domains: Definition and Examples

Definition: A triple $(R, +, \cdot)$ is a commutative ring if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are monoids and the following conditions hold:

- the monoid $(R, +)$ is a group: every element in $(R, +)$ is invertible;
- $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- $1a = a$ for all $a \in R$.

In addition, R is an integral domain if for all $a, b \in R$, the equality $ab = 0$ implies that either $a = 0$ or $b = 0$.

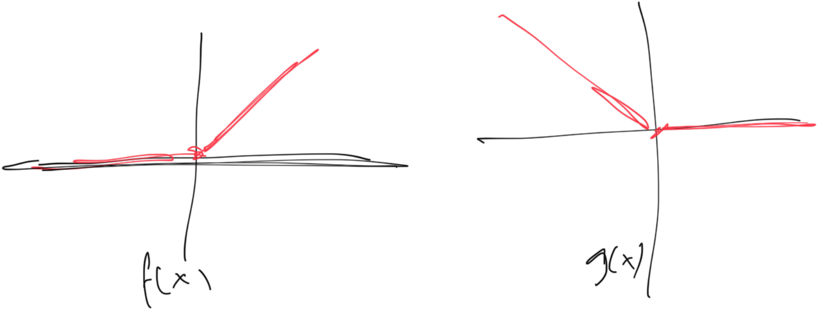
Notation

- We will write R instead of the more cumbersome notation $(R, +, \cdot)$.
- For an integral domain R, we call $(R \setminus \{0\}, \cdot)$ the multiplicative monoid of R, and we denote it by R^*.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are integral domains.
- $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ is an integral domain.

A Non-Example: The set $C(\mathbb{R})$ consisting of all continuous functions on $\mathbb{R}$ is a commutative ring that is not an integral domain.



$$f(x) \cdot g(x) = 0$$

Atomic Domains

Definition

An integral domain is called atomic or an atomic domain if R^* is an atomic monoid.

Examples of atomic domains

- $\mathbb{Z}$ is an atomic domain
- $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ are atomic domains
- $\mathbb{R}[x]$ is an atomic domain
- Noetherian domains and, in particular, the ring of integers of every number field are atomic domains

Examples of a non-atomic domain: Let $\bar{\mathbb{Z}}_{\mathbb{C}}$ denote the set of all complex numbers α such that there exists a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$. The set $\bar{\mathbb{Z}}_{\mathbb{C}}$ is an integral domain that is not atomic.

Definition

An integral domain is called atomic or an atomic domain if R^* is an atomic monoid.

Examples of atomic domains

- $\mathbb{Z}$ is an atomic domain
- $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ are atomic domains
- $\mathbb{R}[x]$ is an atomic domain
- Noetherian domains and, in particular, the ring of integers of every number field are atomic domains

Examples of a non-atomic domain: Let $\bar{\mathbb{Z}}_{\mathbb{C}}$ denote the set of all complex numbers α such that there exists a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$. The set $\bar{\mathbb{Z}}_{\mathbb{C}}$ is an integral domain that is not atomic.

Atomic Domains

Definition

An integral domain is called atomic or an atomic domain if R^* is an atomic monoid.

Examples of atomic domains

- $\mathbb{Z}$ is an atomic domain
- $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ are atomic domains
- $\mathbb{R}[x]$ is an atomic domain
- Noetherian domains and, in particular, the ring of integers of every number field are atomic domains

Examples of a non-atomic domain: Let $\bar{\mathbb{Z}}_{\mathbb{C}}$ denote the set of all complex numbers α such that there exists a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$. The set $\bar{\mathbb{Z}}_{\mathbb{C}}$ is an integral domain that is not atomic.

Atomic Domains

Definition

An integral domain is called atomic or an atomic domain if R^* is an atomic monoid.

Examples of atomic domains

- $\mathbb{Z}$ is an atomic domain
- $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ are atomic domains
- $\mathbb{R}[x]$ is an atomic domain
- Noetherian domains and, in particular, the ring of integers of every number field are atomic domains

Examples of a non-atomic domain: Let $\bar{\mathbb{Z}}_{\mathbb{C}}$ denote the set of all complex numbers α such that there exists a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$. The set $\bar{\mathbb{Z}}_{\mathbb{C}}$ is an integral domain that is not atomic.

Atomic Domains

Definition

An integral domain is called atomic or an atomic domain if R^* is an atomic monoid.

Examples of atomic domains

- $\mathbb{Z}$ is an atomic domain
- $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ are atomic domains
- $\mathbb{R}[x]$ is an atomic domain
- Noetherian domains and, in particular, the ring of integers of every number field are atomic domains

Examples of a non-atomic domain: Let $\bar{\mathbb{Z}}_{\mathbb{C}}$ denote the set of all complex numbers α such that there exists a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$. The set $\bar{\mathbb{Z}}_{\mathbb{C}}$ is an integral domain that is not atomic.

Atomic Domains

Definition

An integral domain is called atomic or an atomic domain if R^* is an atomic monoid.

Examples of atomic domains

- $\mathbb{Z}$ is an atomic domain
- $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ are atomic domains
- $\mathbb{R}[x]$ is an atomic domain
- Noetherian domains and, in particular, the ring of integers of every number field are atomic domains

Examples of a non-atomic domain: Let $\bar{\mathbb{Z}}_{\mathbb{C}}$ denote the set of all complex numbers α such that there exists a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$. The set $\bar{\mathbb{Z}}_{\mathbb{C}}$ is an integral domain that is not atomic.

Atomic Domains

Definition

An integral domain is called atomic or an atomic domain if R^* is an atomic monoid.

Examples of atomic domains

- $\mathbb{Z}$ is an atomic domain
- $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ are atomic domains
- $\mathbb{R}[x]$ is an atomic domain
- Noetherian domains and, in particular, the ring of integers of every number field are atomic domains

Examples of a non-atomic domain: Let $\bar{\mathbb{Z}}_{\mathbb{C}}$ denote the set of all complex numbers α such that there exists a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$. The set $\bar{\mathbb{Z}}_{\mathbb{C}}$ is an integral domain that is not atomic.

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Unique Factorization Domains

Definition. An integral domain R is a unique factorization domain (or a UFD) if R^* is a UFM.

Remark: Every UFD is an atomic domain.

Examples of UFDs

- $\mathbb{Z}$ is a UFD (this is the Fundamental Theorem of Arithmetic).
- $\mathbb{Z}[i]$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD.

Examples of integral domains that are not UFDs

- $\bar{\mathbb{Z}}_{\mathbb{C}}$ is not atomic, and so it is not a UFD.
- $\mathbb{Z}[\sqrt{-5}]$ is an atomic domain that is not a UFD: for instance, $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$

Atomic Integral Domains

Definition. Let R be an integral domain. Then

- R is a finite factorization domain (FFD) if R^* is an FFM,
- R is a half-factorial domain (HFD) if R^* is an HFM, and
- R is a bounded factorization domain (BFD) if R^* is a BFM.

As for monoids, we have the following chain of implications.

$$\textbf{UFD} \Rightarrow \textbf{[FFD, HFD]} \Rightarrow \textbf{BFD} \Rightarrow \textbf{atomic domain}$$

Examples

1. $\mathbb{Z}[\sqrt{-5}]$ is both an FFD and an HFD but it is not a UFD (Exercise).
2. The subring $\mathbb{Z}[x^2, x^3]$ of $\mathbb{Z}[x]$ is a BFD that is not an HFD (Exercise).
3. The subring $\mathbb{R} + \mathbb{C}[x]$ of $\mathbb{C}[x]$ is a BFD that is not an FFD (Exercise).

Atomic Integral Domains

Definition. Let R be an integral domain. Then

- R is a finite factorization domain (FFD) if R^* is an FFM,
- R is a half-factorial domain (HFD) if R^* is an HFM, and
- R is a bounded factorization domain (BFD) if R^* is a BFM.

As for monoids, we have the following chain of implications.

$$\textbf{UFD} \Rightarrow \textbf{[FFD, HFD]} \Rightarrow \textbf{BFD} \Rightarrow \textbf{atomic domain}$$

Examples

1. $\mathbb{Z}[\sqrt{-5}]$ is both an FFD and an HFD but it is not a UFD (Exercise).
2. The subring $\mathbb{Z}[x^2, x^3]$ of $\mathbb{Z}[x]$ is a BFD that is not an HFD (Exercise).
3. The subring $\mathbb{R} + \mathbb{C}[x]$ of $\mathbb{C}[x]$ is a BFD that is not an FFD (Exercise).

Atomic Integral Domains

Definition. Let R be an integral domain. Then

- R is a finite factorization domain (FFD) if R^* is an FFM,
- R is a half-factorial domain (HFD) if R^* is an HFM, and
- R is a bounded factorization domain (BFD) if R^* is a BFM.

As for monoids, we have the following chain of implications.

$$\textbf{UFD} \Rightarrow \textbf{[FFD, HFD]} \Rightarrow \textbf{BFD} \Rightarrow \textbf{atomic domain}$$

Examples

1. $\mathbb{Z}[\sqrt{-5}]$ is both an FFD and an HFD but it is not a UFD (Exercise).
2. The subring $\mathbb{Z}[x^2, x^3]$ of $\mathbb{Z}[x]$ is a BFD that is not an HFD (Exercise).
3. The subring $\mathbb{R} + \mathbb{C}[x]$ of $\mathbb{C}[x]$ is a BFD that is not an FFD (Exercise).

Atomic Integral Domains

Definition. Let R be an integral domain. Then

- R is a finite factorization domain (FFD) if R^* is an FFM,
- R is a half-factorial domain (HFD) if R^* is an HFM, and
- R is a bounded factorization domain (BFD) if R^* is a BFM.

As for monoids, we have the following chain of implications.

$$\text{UFD} \Rightarrow [\text{FFD, HFD}] \Rightarrow \text{BFD} \Rightarrow \text{atomic domain}$$

Examples

1. $\mathbb{Z}[\sqrt{-5}]$ is both an FFD and an HFD but it is not a UFD (Exercise).
2. The subring $\mathbb{Z}[x^2, x^3]$ of $\mathbb{Z}[x]$ is a BFD that is not an HFD (Exercise).
3. The subring $\mathbb{R} + \mathbb{C}[x]$ of $\mathbb{C}[x]$ is a BFD that is not an FFD (Exercise).

Atomic Integral Domains

Definition. Let R be an integral domain. Then

- R is a finite factorization domain (FFD) if R^* is an FFM,
- R is a half-factorial domain (HFD) if R^* is an HFM, and
- R is a bounded factorization domain (BFD) if R^* is a BFM.

As for monoids, we have the following chain of implications.

$$\textbf{UFD} \Rightarrow \textbf{[FFD, HFD]} \Rightarrow \textbf{BFD} \Rightarrow \textbf{atomic domain}$$

Examples

1. $\mathbb{Z}[\sqrt{-5}]$ is both an FFD and an HFD but it is not a UFD (Exercise).
2. The subring $\mathbb{Z}[x^2, x^3]$ of $\mathbb{Z}[x]$ is a BFD that is not an HFD (Exercise).
3. The subring $\mathbb{R} + \mathbb{C}[x]$ of $\mathbb{C}[x]$ is a BFD that is not an FFD (Exercise).

Atomic Integral Domains

Definition. Let R be an integral domain. Then

- R is a finite factorization domain (FFD) if R^* is an FFM,
- R is a half-factorial domain (HFD) if R^* is an HFM, and
- R is a bounded factorization domain (BFD) if R^* is a BFM.

As for monoids, we have the following chain of implications.

$$\textbf{UFD} \Rightarrow \textbf{[FFD, HFD]} \Rightarrow \textbf{BFD} \Rightarrow \textbf{atomic domain}$$

Examples

1. $\mathbb{Z}[\sqrt{-5}]$ is both an FFD and an HFD but it is not a UFD (Exercise).
2. The subring $\mathbb{Z}[x^2, x^3]$ of $\mathbb{Z}[x]$ is a BFD that is not an HFD (Exercise).
3. The subring $\mathbb{R} + \mathbb{C}[x]$ of $\mathbb{C}[x]$ is a BFD that is not an FFD (Exercise).

Atomic Integral Domains

Definition. Let R be an integral domain. Then

- R is a finite factorization domain (FFD) if R^* is an FFM,
- R is a half-factorial domain (HFD) if R^* is an HFM, and
- R is a bounded factorization domain (BFD) if R^* is a BFM.

As for monoids, we have the following chain of implications.

$$\textbf{UFD} \Rightarrow \textbf{[FFD, HFD]} \Rightarrow \textbf{BFD} \Rightarrow \textbf{atomic domain}$$

Examples

1. $\mathbb{Z}[\sqrt{-5}]$ is both an FFD and an HFD but it is not a UFD (Exercise).
2. The subring $\mathbb{Z}[x^2, x^3]$ of $\mathbb{Z}[x]$ is a BFD that is not an HFD (Exercise).
3. The subring $\mathbb{R} + x\mathbb{C}[x]$ of $\mathbb{C}[x]$ is a BFD that is not an FFD (Exercise).

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$. $M = \{ \alpha_1 \frac{1}{p_1} + \cdots + \alpha_k \frac{1}{p_k} : \alpha_1, \dots, \alpha_k \in \mathbb{N} \text{ and } p_1, \dots, p_k \in \mathbb{P} \}$
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$.
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$.
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$.
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$.
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$.
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$.
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

A Non-BFD Atomic Domain

Example

1. Let $\mathbb{P}$ be the set of primes, and consider the submonoid M of $(\mathbb{Q}_{\geq 0}, +)$ generated by $\{1/p : p \in \mathbb{P}\}$.
2. The monoid M satisfies the ACCP and $\mathcal{A}(M) = \{1/p : p \in \mathbb{P}\}$ (Exercise).
3. Now let R be the set of polynomial expressions with rational coefficients and exponents in M.
4. R can be checked to be an integral domain.
5. Since M satisfies the ACCP, one can easily check that R also satisfies the ACCP.
6. Therefore R is an atomic domain.
7. Since $x = \left(x^{\frac{1}{p}}\right)^p$ for every $p \in \mathbb{P}$, the integral domain R is not a BFD.

Remark: There are atomic domains that do not satisfy the ACCP. The first one was constructed by A. Grams in 1974.

Atomicity in Lattices

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho\colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Definition of a Poset

Definition. A partially ordered set (or poset) is a pair $(P, \leq)$ consisting of a set P and a binary relation $\leq$ satisfying the following properties.

1. Reflexivity: $x \leq x$ (for all $x \in P$).
2. Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$ (for all $x, y \in P$).
3. Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$ (for all $x, y, z \in P$).

We write P instead of $(P, \leq)$. Let P be a poset.

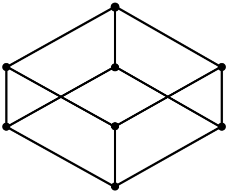
- P has a $\hat{0}$ if there exists $\hat{0} \in P$ such that $\hat{0} \leq x$ for all $x \in P$.
- We write $x \lessdot y$ when $x < y$ and $x \leq z \leq y$ for some z implies that $z = x$ or $z = y$, in which case we say that y covers x.
- P is graded if there is a rank function $\rho \colon P \to \mathbb{N}_0$ such that for all $x, y \in P$

  (a) $x < y$ implies that $\rho(x) < \rho(y)$,

  (b) $x \lessdot y$ implies that $\rho(x) + 1 = \rho(y)$.

Examples of Posets

1. A totally ordered set is a poset where any two elements are comparable. For instance, $\mathbb{N}$ or $[n] := \{1, 2, \ldots, n\}$ for every $n \in \mathbb{N}$.
2. The power sets $2^{\mathbb{N}} := \{S : S \subseteq \mathbb{N}\}$ and $2^{[n]} := \{S : S \subseteq [n]\}$ are posets under inclusion.
3. For each $n \in \mathbb{N}$, the set D_n of all divisors of n is a poset if $a \le b$ means that a divides b as integers.
4. A finite poset P can be represented by its Hasse diagram: a graph whose vertices are the elements of P and whose edges are the covered relations such that if $s < t$, then s is drawn below t with respect to the y-axis. Below are the Hasse diagrams of $2^{[3]}$:



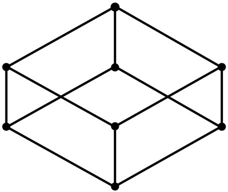
Examples of Posets

1. A totally ordered set is a poset where any two elements are comparable. For instance, $\mathbb{N}$ or $[n] := \{1, 2, \dots, n\}$ for every $n \in \mathbb{N}$.

2. The power sets $2^{\mathbb{N}} := \{S : S \subseteq \mathbb{N}\}$ and $2^{[n]} := \{S : S \subseteq [n]\}$ are posets under inclusion.

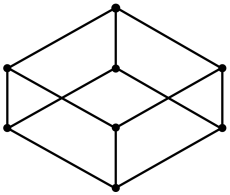
3. For each $n \in \mathbb{N}$, the set D_n of all divisors of n is a poset if $a \le b$ means that a divides b as integers.

4. A finite poset P can be represented by its Hasse diagram: a graph whose vertices are the elements of P and whose edges are the covered relations such that if $s < t$, then s is drawn below t with respect to the y-axis. Below are the Hasse diagrams of $2^{[3]}$:



Examples of Posets

1. A totally ordered set is a poset where any two elements are comparable. For instance, $\mathbb{N}$ or $[n] := \{1, 2, \dots, n\}$ for every $n \in \mathbb{N}$.
2. The power sets $2^{\mathbb{N}} := \{S : S \subseteq \mathbb{N}\}$ and $2^{[n]} := \{S : S \subseteq [n]\}$ are posets under inclusion.
3. For each $n \in \mathbb{N}$, the set D_n of all divisors of n is a poset if $a \le b$ means that a divides b as integers.
4. A finite poset P can be represented by its Hasse diagram: a graph whose vertices are the elements of P and whose edges are the covered relations such that if $s < t$, then s is drawn below t with respect to the y-axis. Below are the Hasse diagrams of $2^{[3]}$:



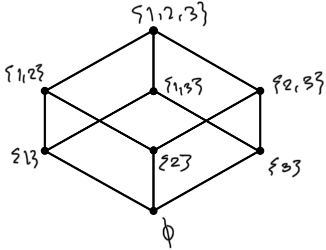
Examples of Posets

1. A totally ordered set is a poset where any two elements are comparable. For instance, $\mathbb{N}$ or $[n] := \{1, 2, \dots, n\}$ for every $n \in \mathbb{N}$.

2. The power sets $2^{\mathbb{N}} := \{S : S \subseteq \mathbb{N}\}$ and $2^{[n]} := \{S : S \subseteq [n]\}$ are posets under inclusion.

3. For each $n \in \mathbb{N}$, the set D_n of all divisors of n is a poset if $a \le b$ means that a divides b as integers.

4. A finite poset P can be represented by its Hasse diagram: a graph whose vertices are the elements of P and whose edges are the covered relations such that if $s < t$, then s is drawn below t with respect to the y-axis. Below are the Hasse diagrams of $2^{[3]}$:



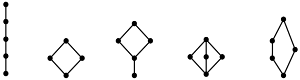
Lattice: Definition and Examples

Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \operatorname{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram  is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.



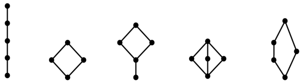
Lattice: Definition and Examples

Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \mathrm{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram  is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.



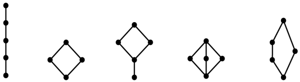
Lattice: Definition and Examples

Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \mathrm{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram  is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.



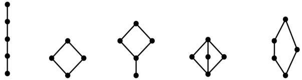
Lattice: Definition and Examples

Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \mathrm{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram  is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.



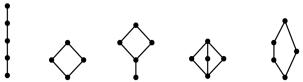
Lattice: Definition and Examples

Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \mathrm{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram  is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.



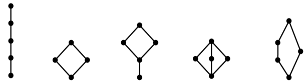
Lattice: Definition and Examples

Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \mathrm{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram  is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.



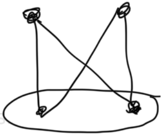
Lattice: Definition and Examples

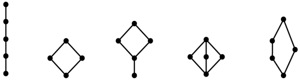
Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \mathrm{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram $\bowtie$ is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.





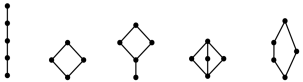
Lattice: Definition and Examples

Definition: Let P be a poset.

- If $S := \{s_1, \dots, s_n\} \subseteq P$ has a least upper bound (resp., a greatest lower bound) in P, we denote it by $\vee S := s_1 \vee \cdots \vee s_n$ (resp., $\wedge S := s_1 \wedge \cdots \wedge s_n$) and call it the join (resp., meet) of $s_1, \dots, s_n$.
- The poset P is called a lattice if every finite subset of P has both a join and a meet.

Examples

1. $[n]$ and $\mathbb{N}$ are lattices, where $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.
3. D_n is a lattice, where $a \vee b = \mathrm{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$.
4. The poset with Hasse diagram  is not a lattice.
5. Below are the Hasse diagrams of the lattices with five elements.



Atomic Lattices

Definition

Let L be a lattice with $\hat{0}$.

- An element $r \in L$ is an atom if it covers $\hat{0}$.
- If every element of L is the join of atoms, then L is atomic.

Example of Atomic Lattices

1. The lattice with Hasse diagram  is atomic while the lattice with Hasse diagram  is not.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.

Atomic Lattices

Definition

Let L be a lattice with $\hat{0}$.

- An element $r \in L$ is an atom if it covers $\hat{0}$.
- If every element of L is the join of atoms, then L is atomic.

Example of Atomic Lattices

1. The lattice with Hasse diagram  is atomic while the lattice with Hasse diagram  is not.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.

Atomic Lattices

Definition

Let L be a lattice with $\hat{0}$.

- An element $r \in L$ is an atom if it covers $\hat{0}$.
- If every element of L is the join of atoms, then L is atomic.

Example of Atomic Lattices

1. The lattice with Hasse diagram  is atomic while the lattice with Hasse diagram  is not.
2. $2^{[n]}$ and $2^{\mathbb{N}}$ are lattices, where $A \vee B = A \cup B$ and $A \wedge B = A \cap B$.

NOT atomic.

atomic

Factorizations in Lattices

Let L be an atomic lattice.

1. If $x = a_1 \vee \cdots \vee a_\ell$ for atoms $a_1, \dots, a_\ell \in L$, then the formal expression $a_1 \vee \cdots \vee a_\ell$ is a factorization of x if it is irredundant, that is, $\vee A < x$ for each $A \subsetneq \{a_1, \dots, a_\ell\}$. For $x \in L$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
2. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in L$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let L be an atomic lattice.

- is a unique factorization lattice (UFL) if $|\mathsf{Z}(x)| = 1$ for all $x \in L$.
- is a half-factorial lattice (HFL) if $|\mathsf{L}(x)| = 1$ for all $x \in L$.
- is a finite factorization lattice (FFL) if $|\mathsf{Z}(x)| < \infty$ for all $x \in L$.
- is a bounded factorization lattice (BFL) if $|\mathsf{L}(x)| < \infty$ for all $x \in L$.

Factorizations in Lattices

Let L be an atomic lattice.

1. If $x = a_1 \vee \cdots \vee a_\ell$ for atoms $a_1, \dots, a_\ell \in L$, then the formal expression $a_1 \vee \cdots \vee a_\ell$ is a factorization of x if it is irredundant, that is, $\vee A < x$ for each $A \subsetneq \{a_1, \dots, a_\ell\}$. For $x \in L$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.

2. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in L$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let L be an atomic lattice.

- is a unique factorization lattice (UFL) if $|\mathsf{Z}(x)| = 1$ for all $x \in L$.
- is a half-factorial lattice (HFL) if $|\mathsf{L}(x)| = 1$ for all $x \in L$.
- is a finite factorization lattice (FFL) if $|\mathsf{Z}(x)| < \infty$ for all $x \in L$.
- is a bounded factorization lattice (BFL) if $|\mathsf{L}(x)| < \infty$ for all $x \in L$.

Let L be an atomic lattice.

1. If $x = a_1 \vee \cdots \vee a_\ell$ for atoms $a_1, \dots, a_\ell \in L$, then the formal expression $a_1 \vee \cdots \vee a_\ell$ is a factorization of x if it is irredundant, that is, $\vee A < x$ for each $A \subsetneq \{a_1, \dots, a_\ell\}$. For $x \in L$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.

2. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in L$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let L be an atomic lattice.

- is a unique factorization lattice (UFL) if $|\mathsf{Z}(x)| = 1$ for all $x \in L$.
- is a half-factorial lattice (HFL) if $|\mathsf{L}(x)| = 1$ for all $x \in L$.
- is a finite factorization lattice (FFL) if $|\mathsf{Z}(x)| < \infty$ for all $x \in L$.
- is a bounded factorization lattice (BFL) if $|\mathsf{L}(x)| < \infty$ for all $x \in L$.

Factorizations in Lattices

Let L be an atomic lattice.

1. If $x = a_1 \vee \cdots \vee a_\ell$ for atoms $a_1, \dots, a_\ell \in L$, then the formal expression $a_1 \vee \cdots \vee a_\ell$ is a factorization of x if it is irredundant, that is, $\vee A < x$ for each $A \subsetneq \{a_1, \dots, a_\ell\}$. For $x \in L$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.
2. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in L$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let L be an atomic lattice.

- is a unique factorization lattice (UFL) if $|\mathsf{Z}(x)| = 1$ for all $x \in L$.
- is a half-factorial lattice (HFL) if $|\mathsf{L}(x)| = 1$ for all $x \in L$.
- is a finite factorization lattice (FFL) if $|\mathsf{Z}(x)| < \infty$ for all $x \in L$.
- is a bounded factorization lattice (BFL) if $|\mathsf{L}(x)| < \infty$ for all $x \in L$.

Factorizations in Lattices

Let L be an atomic lattice.

1. If $x = a_1 \vee \cdots \vee a_\ell$ for atoms $a_1, \dots, a_\ell \in L$, then the formal expression $a_1 \vee \cdots \vee a_\ell$ is a factorization of x if it is irredundant, that is, $\vee A < x$ for each $A \subsetneq \{a_1, \dots, a_\ell\}$. For $x \in L$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.

2. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in L$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let L be an atomic lattice.

- is a unique factorization lattice (UFL) if $|\mathsf{Z}(x)| = 1$ for all $x \in L$.
- is a half-factorial lattice (HFL) if $|\mathsf{L}(x)| = 1$ for all $x \in L$.
- is a finite factorization lattice (FFL) if $|\mathsf{Z}(x)| < \infty$ for all $x \in L$.
- is a bounded factorization lattice (BFL) if $|\mathsf{L}(x)| < \infty$ for all $x \in L$.

Factorizations in Lattices

Let L be an atomic lattice.

1. If $x = a_1 \vee \cdots \vee a_\ell$ for atoms $a_1, \dots, a_\ell \in L$, then the formal expression $a_1 \vee \cdots \vee a_\ell$ is a factorization of x if it is irredundant, that is, $\vee A < x$ for each $A \subsetneq \{a_1, \dots, a_\ell\}$. For $x \in L$, we let $\mathsf{Z}(x)$ denote the set of factorizations of x.

2. The length of a factorization z is the number of atoms it involves and is denoted by $|z|$, and for $x \in L$ we set $\mathsf{L}(x) := \{|z| : z \in \mathsf{Z}(x)\}$.

Definition

Let L be an atomic lattice.

- is a unique factorization lattice (UFL) if $|\mathsf{Z}(x)| = 1$ for all $x \in L$.
- is a half-factorial lattice (HFL) if $|\mathsf{L}(x)| = 1$ for all $x \in L$.
- is a finite factorization lattice (FFL) if $|\mathsf{Z}(x)| < \infty$ for all $x \in L$.
- is a bounded factorization lattice (BFL) if $|\mathsf{L}(x)| < \infty$ for all $x \in L$.

Factorizations in Lattices (continuation)

As in the case of monoids and rings, we have the following chain of implications.

$$\textbf{UFL} \Rightarrow [\textbf{FFL, HFL}] \Rightarrow \textbf{BFL} \Rightarrow \textbf{atomic lattice}$$

Examples None of the above implications is reversible.

Factorizations in Lattices (continuation)

As in the case of monoids and rings, we have the following chain of implications.

$$\textbf{UFL} \Rightarrow \textbf{[FFL, HFL]} \Rightarrow \textbf{BFL} \Rightarrow \textbf{atomic lattice}$$

Examples

Finite Geometric Lattice

Definition: A finite lattice L is called a geometric lattice if it satisfies the following two conditions.

- L is atomic.
- For all $x, y \in L$ such that both x and y cover $x \wedge y$, the join $x \vee y$ covers both x and y.

Remark: Geometric lattices are in natural bijection with matroids, which are objects well studied in combinatorics.

Theorem

Every geometric lattice is an HFL.

Finite Geometric Lattice

Definition: A finite lattice L is called a geometric lattice if it satisfies the following two conditions.

- L is atomic.
- For all $x, y \in L$ such that both x and y cover $x \wedge y$, the join $x \vee y$ covers both x and y.

Remark: Geometric lattices are in natural bijection with matroids, which are objects well studied in combinatorics.

Theorem

Every geometric lattice is an HFL.

Finite Geometric Lattice

Definition: A finite lattice L is called a geometric lattice if it satisfies the following two conditions.

- L is atomic.
- For all $x, y \in L$ such that both x and y cover $x \wedge y$, the join $x \vee y$ covers both x and y.

Remark: Geometric lattices are in natural bijection with matroids, which are objects well studied in combinatorics.

Theorem

Every geometric lattice is an HFL.

Finite Geometric Lattice

Definition: A finite lattice L is called a geometric lattice if it satisfies the following two conditions.

- L is atomic.
- For all $x, y \in L$ such that both x and y cover $x \wedge y$, the join $x \vee y$ covers both x and y.

Remark: Geometric lattices are in natural bijection with matroids, which are objects well studied in combinatorics.

Theorem

Every geometric lattice is an HFL.

References

- D. D. Anderson, D. F. Anderson, and M. Zafrullah: *Factorization in integral domains*, J. Pure Appl. Algebra **69** (1990) 1–19.
- A. Geroldinger and F. Halter-Koch: *Non-unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics Vol. 278, Chapman & Hall/CRC, Boca Raton, 2006.
- A. Grams: *Atomic rings and the ascending chain condition for principal ideals*, Math. Proc. Cambridge Philos. Soc. **75** (1974) 321–329.
- F. Halter-Koch: *Finiteness theorems for factorizations*, Semigroup Forum **44** (1992) 112–117.
- M. Roitman: *Polynomial extensions of atomic domains*, J. Pure Appl. Algebra **87** (1993) 187–199.
- R. P. Stanley, Enumerative Combinatorics, Vol. 1, Cambridge University Press, New York, 2011.

End of Presentation

THANK YOU!