Factorizations in Evaluation Monoids

Sophie Zhu
Mentor: Felix Gotti

MIT PRIMES 2021 Conference

October 16, 2021

Monoids

An (additive) **monoid** is a pair $(M, +)$, where M is a set and $+$ is a binary operation on M, such that

- $+$ is both associative and commutative, and
- there exists $0 \in M$ such that $x + 0 = x$.

Examples

- $(\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)$
- $(\{0\} \cup \mathbb{Q}_{\geq 1}, +)$
- $(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}, +)$
- every abelian group

Monoids

An (additive) **monoid** is a pair $(M, +)$, where M is a set and $+$ is a binary operation on M, such that

- $+$ is both associative and commutative, and
- there exists $0 \in M$ such that $x + 0 = x$.

Examples

- $(\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)$
- $(\{0\} \cup \mathbb{Q}_{\geq 1}, +)$
- $(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}, +)$
- every abelian group

Monoids

An (additive) **monoid** is a pair $(M, +)$, where M is a set and $+$ is a binary operation on M, such that

- $+$ is both associative and commutative, and
- there exists $0 \in M$ such that $x + 0 = x$.

Examples

- $(\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)$
- $(\{0\} \cup \mathbb{Q}_{\geq 1}, +)$
- $(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}, +)$
- every abelian group

Monoids

An (additive) **monoid** is a pair $(M, +)$, where M is a set and $+$ is a binary operation on M, such that

- $+$ is both associative and commutative, and
- there exists $0 \in M$ such that $x + 0 = x$.

Examples

- $(\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)$
- $(\{0\} \cup \mathbb{Q}_{\geq 1}, +)$
- $(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}, +)$
- every abelian group

Monoids

An (additive) **monoid** is a pair $(M, +)$, where M is a set and $+$ is a binary operation on M, such that

- $+$ is both associative and commutative, and
- there exists $0 \in M$ such that $x + 0 = x$.

Examples

- $(\mathbb{Z}_{\geq 0}, +), (\mathbb{R}_{\geq 0}, +)$
- $(\{0\} \cup \mathbb{Q}_{\geq 1}, +)$
- $(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}, +)$
- every abelian group

Atoms

For this talk, let $(M, +)$ be an additive monoid with a unique invertible element; namely, 0.

- An integer $p \geq 2$ is a *prime* if $p = a \cdot b$ for any $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.
- A nonzero element a in $(M, +)$ is an **atom** if the equality $a = x + y$ for some $x, y \in M$ implies $x = 0$ or $y = 0$.

We denote the set of atoms in M by $\mathcal{A}(M)$.

Examples

- $\mathcal{A}(\mathbb{Z}_{\geq 0}) = \{1\}$
- $\mathcal{A}(M) = \mathcal{A}(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}) = \{3, 7, 11\}$. For instance, if $7 = x + y$ for $x, y \in M$, then $x = 0$ or $y = 0$ because $3 + 3 = 6$, $3 + 6 = 9$, and $6 + 6 = 12$.

Atoms

For this talk, let $(M, +)$ be an additive monoid with a unique invertible element; namely, 0.

- An integer $p \geq 2$ is a *prime* if $p = a \cdot b$ for any $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.
- A nonzero element a in $(M, +)$ is an **atom** if the equality $a = x + y$ for some $x, y \in M$ implies $x = 0$ or $y = 0$.

We denote the set of atoms in M by $\mathcal{A}(M)$.

Examples

- $\mathcal{A}(\mathbb{Z}_{\geq 0}) = \{1\}$
- $\mathcal{A}(M) = \mathcal{A}(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}) = \{3, 7, 11\}$. For instance, if $7 = x + y$ for $x, y \in M$, then $x = 0$ or $y = 0$ because $3 + 3 = 6$, $3 + 6 = 9$, and $6 + 6 = 12$.

Atoms

For this talk, let $(M, +)$ be an additive monoid with a unique invertible element; namely, 0.

- An integer $p \geq 2$ is a *prime* if $p = a \cdot b$ for any $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.
- A nonzero element a in $(M, +)$ is an **atom** if the equality $a = x + y$ for some $x, y \in M$ implies $x = 0$ or $y = 0$.

We denote the set of atoms in M by $\mathcal{A}(M)$.

Examples

- $\mathcal{A}(\mathbb{Z}_{\geq 0}) = \{1\}$
- $\mathcal{A}(M) = \mathcal{A}(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}) = \{3, 7, 11\}$. For instance, if $7 = x + y$ for $x, y \in M$, then $x = 0$ or $y = 0$ because $3 + 3 = 6$, $3 + 6 = 9$, and $6 + 6 = 12$.

Atoms

For this talk, let $(M, +)$ be an additive monoid with a unique invertible element; namely, 0.

- An integer $p \geq 2$ is a *prime* if $p = a \cdot b$ for any $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.
- A nonzero element a in $(M, +)$ is an **atom** if the equality $a = x + y$ for some $x, y \in M$ implies $x = 0$ or $y = 0$.

We denote the set of atoms in M by $\mathcal{A}(M)$.

Examples

- $\mathcal{A}(\mathbb{Z}_{\geq 0}) = \{1\}$
- $\mathcal{A}(M) = \mathcal{A}(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}) = \{3, 7, 11\}$. For instance, if $7 = x + y$ for $x, y \in M$, then $x = 0$ or $y = 0$ because $3 + 3 = 6$, $3 + 6 = 9$, and $6 + 6 = 12$.

Atoms

For this talk, let $(M, +)$ be an additive monoid with a unique invertible element; namely, 0.

- An integer $p \geq 2$ is a *prime* if $p = a \cdot b$ for any $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.
- A nonzero element a in $(M, +)$ is an **atom** if the equality $a = x + y$ for some $x, y \in M$ implies $x = 0$ or $y = 0$.

We denote the set of atoms in M by $\mathcal{A}(M)$.

Examples

- $\mathcal{A}(\mathbb{Z}_{\geq 0}) = \{1\}$
- $\mathcal{A}(M) = \mathcal{A}(\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}) = \{3, 7, 11\}$. For instance, if $7 = x + y$ for $x, y \in M$, then $x = 0$ or $y = 0$ because $3 + 3 = 6$, $3 + 6 = 9$, and $6 + 6 = 12$.

Atoms

For this talk, let $(M, +)$ be an additive monoid with a unique invertible element; namely, 0.

- An integer $p \geq 2$ is a *prime* if $p = a \cdot b$ for any $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.
- A nonzero element a in $(M, +)$ is an **atom** if the equality $a = x + y$ for some $x, y \in M$ implies $x = 0$ or $y = 0$.

We denote the set of atoms in M by $\mathcal{A}(M)$.

Examples

- $\mathcal{A}(\mathbb{Z}_{\geq 0}) = \{1\}$
- $\mathcal{A}(M) = \mathcal{A}(\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}) = \{3, 7, 11\}$. For instance, if $7 = x + y$ for $x, y \in M$, then $x = 0$ or $y = 0$ because $3 + 3 = 6$, $3 + 6 = 9$, and $6 + 6 = 12$.

Atomicity

- *Fundamental Theorem of Arithmetic*: Every $n \in \mathbb{Z}_{\geq 2}$ factors (uniquely) into primes.
- $(M, +)$ is **atomic** if every nonzero element can be written as a sum of atoms.

Atomicity was first studied in the 1960s by Cohn in the context of commutative ring theory and, since then, has been systematically studied in the abstract context of commutative monoids.

Atomicity

- *Fundamental Theorem of Arithmetic*: Every $n \in \mathbb{Z}_{\geq 2}$ factors (uniquely) into primes.
- $(M, +)$ is **atomic** if every nonzero element can be written as a sum of atoms.

Atomicity was first studied in the 1960s by Cohn in the context of commutative ring theory and, since then, has been systematically studied in the abstract context of commutative monoids.

Atomicity

- *Fundamental Theorem of Arithmetic*: Every $n \in \mathbb{Z}_{\geq 2}$ factors (uniquely) into primes.
- $(M, +)$ is **atomic** if every nonzero element can be written as a sum of atoms.

Atomicity was first studied in the 1960s by Cohn in the context of commutative ring theory and, since then, has been systematically studied in the abstract context of commutative monoids.

Examples of Atomic Monoids

- $\mathbb{Z}_{\geq 0}$ is atomic as $\mathcal{A}(\mathbb{Z}_{\geq 0}) = 1$ and $n = \overbrace{1 + 1 + \cdots + 1}^{n}$.
- For $M = \{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$, recall that $\mathcal{A}(M) = \{3, 7, 11\}$. One can verify that M is atomic; for instance,
    - $6 = 3 + 3$,
    - $9 = 3 + 3 + 3$,
    - $10 = 3 + 7$, and
    - $12 = 3 + 3 + 3 + 3$.

For $A = \{a_i \mid i \in I\} \subseteq M$, we let $\langle A \rangle$, or $\langle a_i \mid i \in I \rangle$, denote the smallest monoid inside M containing A.

- $M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle$ is not atomic because $\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}}$ for each $k \in \mathbb{Z}_{\geq 0}$, and so $\mathcal{A}(M) = \emptyset$.

Examples of Atomic Monoids

- $\mathbb{Z}_{\geq 0}$ is atomic as $\mathcal{A}(\mathbb{Z}_{\geq 0}) = 1$ and $n = \overbrace{1 + 1 + \cdots + 1}^{n}$.
- For $M = \{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$, recall that $\mathcal{A}(M) = \{3, 7, 11\}$. One can verify that M is atomic; for instance,
  - $6 = 3 + 3$,
  - $9 = 3 + 3 + 3$,
  - $10 = 3 + 7$, and
  - $12 = 3 + 3 + 3 + 3$.

For $A = \{a_i \mid i \in I\} \subseteq M$, we let $\langle A \rangle$, or $\langle a_i \mid i \in I \rangle$, denote the smallest monoid inside M containing A.

- $M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle$ is not atomic because $\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}}$ for each $k \in \mathbb{Z}_{\geq 0}$, and so $\mathcal{A}(M) = \emptyset$.

Examples of Atomic Monoids

- $\mathbb{Z}_{\geq 0}$ is atomic as $\mathcal{A}(\mathbb{Z}_{\geq 0}) = 1$ and $n = \overbrace{1 + 1 + \cdots + 1}^{n}$.
- For $M = \{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$, recall that $\mathcal{A}(M) = \{3, 7, 11\}$. One can verify that M is atomic; for instance,
  - $6 = 3 + 3$,
  - $9 = 3 + 3 + 3$,
  - $10 = 3 + 7$, and
  - $12 = 3 + 3 + 3 + 3$.

For $A = \{a_i \mid i \in I\} \subseteq M$, we let $\langle A \rangle$, or $\langle a_i \mid i \in I \rangle$, denote the smallest monoid inside M containing A.

- $M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle$ is not atomic because $\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}}$ for each $k \in \mathbb{Z}_{\geq 0}$, and so $\mathcal{A}(M) = \emptyset$.

Examples of Atomic Monoids

- $\mathbb{Z}_{\geq 0}$ is atomic as $\mathcal{A}(\mathbb{Z}_{\geq 0}) = 1$ and $n = \overbrace{1 + 1 + \cdots + 1}^{n}$.
- For $M = \{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$, recall that $\mathcal{A}(M) = \{3, 7, 11\}$. One can verify that M is atomic; for instance,
    - $6 = 3 + 3$,
    - $9 = 3 + 3 + 3$,
    - $10 = 3 + 7$, and
    - $12 = 3 + 3 + 3 + 3$.

For $A = \{a_i \mid i \in I\} \subseteq M$, we let $\langle A \rangle$, or $\langle a_i \mid i \in I \rangle$, denote the smallest monoid inside M containing A.

- $M = \langle \frac{1}{2^k} \mid k \in \mathbb{Z}_{\geq 0} \rangle$ is not atomic because $\frac{1}{2^k} = \frac{1}{2^{k+1}} + \frac{1}{2^{k+1}}$ for each $k \in \mathbb{Z}_{\geq 0}$, and so $\mathcal{A}(M) = \emptyset$.

Factorizations

- A **factorization** of a nonzero $x \in M$ is a decomposition $x = a_1 + \cdots + a_\ell$, where $a_1, \ldots, a_\ell \in \mathcal{A}(M)$,
- in which case ℓ is called a **length** of x.
- Define $\mathsf{L}(x)$ as the set of all possible lengths of x.

Examples

- In $\mathbb{Z}_{\geq 0}$, the decomposition $n = \overbrace{1 + 1 + \cdots + 1}^{n}$ is a factorization of n of length n. This is unique, so $\mathsf{L}(n) = \{n\}$ for all $n \geq 1$.
- In $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ the decompositions $10 = 3 + 7$ and $21 = 7 + 7 + 7$ are factorizations of 10 and 21 of lengths 2 and 3, resp. This factorization of 10 is unique, so $\mathsf{L}(10) = \{2\}$, but $21 = 3 + \cdots + 3$ (7 times) is also a factorization of 21; indeed, $\mathsf{L}(21) = \{3, 7\}$.

Factorizations

- A **factorization** of a nonzero $x \in M$ is a decomposition $x = a_1 + \cdots + a_\ell$, where $a_1, \ldots, a_\ell \in \mathcal{A}(M)$,
- in which case ℓ is called a **length** of x.
- Define $\mathsf{L}(x)$ as the set of all possible lengths of x.

Examples

- In $\mathbb{Z}_{\geq 0}$, the decomposition $n = \overbrace{1 + 1 + \cdots + 1}^{n}$ is a factorization of n of length n. This is unique, so $\mathsf{L}(n) = \{n\}$ for all $n \geq 1$.
- In $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ the decompositions $10 = 3 + 7$ and $21 = 7 + 7 + 7$ are factorizations of 10 and 21 of lengths 2 and 3, resp. This factorization of 10 is unique, so $\mathsf{L}(10) = \{2\}$, but $21 = 3 + \cdots + 3$ (7 times) is also a factorization of 21; indeed, $\mathsf{L}(21) = \{3, 7\}$.

Factorizations

- A **factorization** of a nonzero $x \in M$ is a decomposition $x = a_1 + \cdots + a_\ell$, where $a_1, \ldots, a_\ell \in \mathcal{A}(M)$,
- in which case ℓ is called a **length** of x.
- Define $\mathsf{L}(x)$ as the set of all possible lengths of x.

Examples

- In $\mathbb{Z}_{\geq 0}$, the decomposition $n = \overbrace{1 + 1 + \cdots + 1}^{n}$ is a factorization of n of length n. This is unique, so $\mathsf{L}(n) = \{n\}$ for all $n \geq 1$.
- In $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ the decompositions $10 = 3 + 7$ and $21 = 7 + 7 + 7$ are factorizations of 10 and 21 of lengths 2 and 3, resp. This factorization of 10 is unique, so $\mathsf{L}(10) = \{2\}$, but $21 = 3 + \cdots + 3$ (7 times) is also a factorization of 21; indeed, $\mathsf{L}(21) = \{3, 7\}$.

Examples of BFMs, FFMs, and UFMs

Let M be an atomic monoid. Then

- M is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $\mathsf{L}(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of n is always bounded above by n.
- M is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$ is also an FFM.
- M is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$.

Examples of BFMs, FFMs, and UFMs

Let M be an atomic monoid. Then

- M is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $\mathsf{L}(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of n is always bounded above by n.
- M is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$ is also an FFM.
- M is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$.

Examples of BFMs, FFMs, and UFMs

Let M be an atomic monoid. Then

- M is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $\mathsf{L}(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of n is always bounded above by n.
- M is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is also an FFM.
- M is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1,0), (0,1)\}$.

Examples of BFMs, FFMs, and UFMs

Let M be an atomic monoid. Then

- M is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $\mathsf{L}(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of n is always bounded above by n.
- M is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \dots\}$ is also an FFM.
- M is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1, 0), (0, 1)\}$.

Examples of BFMs, FFMs, and UFMs

Let M be an atomic monoid. Then

- M is a **bounded factorization monoid** (BFM) if for each nonzero $x \in M$, the set $\mathsf{L}(x)$ is bounded.
  - In a BFM, an element may have infinitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is a BFM. Since its elements lie in $\mathbb{Z}_{\geq 0}$, the length of a factorization of n is always bounded above by n.
- M is a **finite factorization monoid** (FFM) if each nonzero $x \in M$ has finitely many factorizations.
  - $\{0, 3, 6, 7, 9, 10, 11, 12, \ldots\}$ is also an FFM.
- M is a **unique factorization monoid** (UFM) if each nonzero $x \in M$ has exactly one factorization.
  - $\mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM and FFM).
  - $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ is a UFM (thus a BFM & FFM), where $\mathcal{A}(\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}) = \{(1,0),(0,1)\}$.

Question

The phenomenon of non-uniqueness of factorizations naturally appears in algebraic number theory (for instance, the ring of integers $\mathbb{Z}[\sqrt{-5}]$ is not a UFD) and has been the main motivation for the development of factorization theory in the abstract context of commutative monoids. As a crucial part of this development, BFMs and FFMs were introduced in 1992.

Question

What can we say about the existence and non-uniqueness of factorizations in monoids in general?

The following follows directly from the definitions.

$$\textbf{UFM} \Rightarrow \textbf{FFM} \Rightarrow \textbf{BFM} \Rightarrow \textbf{atomicity}$$

Question

The phenomenon of non-uniqueness of factorizations naturally appears in algebraic number theory (for instance, the ring of integers $\mathbb{Z}[\sqrt{-5}]$ is not a UFD) and has been the main motivation for the development of factorization theory in the abstract context of commutative monoids. As a crucial part of this development, BFMs and FFMs were introduced in 1992.

Question

What can we say about the existence and non-uniqueness of factorizations in monoids in general?

The following follows directly from the definitions.

$$\textbf{UFM} \Rightarrow \textbf{FFM} \Rightarrow \textbf{BFM} \Rightarrow \textbf{atomicity}$$

Question

The phenomenon of non-uniqueness of factorizations naturally appears in algebraic number theory (for instance, the ring of integers $\mathbb{Z}[\sqrt{-5}]$ is not a UFD) and has been the main motivation for the development of factorization theory in the abstract context of commutative monoids. As a crucial part of this development, BFMs and FFMs were introduced in 1992.

Question

What can we say about the existence and non-uniqueness of factorizations in monoids in general?

The following follows directly from the definitions.

$$\textbf{UFM} \Rightarrow \textbf{FFM} \Rightarrow \textbf{BFM} \Rightarrow \textbf{atomicity}$$

Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the **(Laurent) evaluation monoid** of α is

$$\begin{aligned} M_\alpha &:= \{f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}]\} \\ &= \{f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_n x^n, c_i \in \mathbb{Z}_{\geq 0}\}. \end{aligned}$$

We discuss the following classes of M_α.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFMs

Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the **(Laurent) evaluation monoid** of α is

$$\begin{aligned} M_\alpha &:= \{f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}]\} \\ &= \{f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_n x^n, c_i \in \mathbb{Z}_{\geq 0}\}. \end{aligned}$$

We discuss the following classes of M_α.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFMs

Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the **(Laurent) evaluation monoid** of α is

$$\begin{aligned} M_\alpha &:= \{f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}]\} \\ &= \{f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_n x^n, c_i \in \mathbb{Z}_{\geq 0}\}. \end{aligned}$$

We discuss the following classes of M_α.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFMs

Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the **(Laurent) evaluation monoid** of α is

$$\begin{aligned} M_\alpha &:= \{f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}]\} \\ &= \{f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_n x^n, c_i \in \mathbb{Z}_{\geq 0}\}. \end{aligned}$$

We discuss the following classes of M_α.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFMs

Overview

Definition

For $\alpha \in \mathbb{R}_{>0}$, the **(Laurent) evaluation monoid** of α is

$$
\begin{aligned}
M_\alpha &:= \{f(\alpha) \mid f(x) \in \mathbb{Z}_{\geq 0}[x, x^{-1}]\} \\
&= \{f(\alpha) \mid f(x) = c_{-n}x^{-n} + \cdots + c_n x^n, c_i \in \mathbb{Z}_{\geq 0}\}.
\end{aligned}
$$

We discuss the following classes of M_α.

1. Atomic monoids
2. Bounded and finite factorization monoids (in connection with the ascending chain condition on principal ideals)
3. A class of FFMs that are not UFMs

Atomicity

Proposition (Z., 2021)

For each $\alpha \in \mathbb{R}_{>0}$, the following statements are equivalent.

(a) $1 \in \mathcal{A}(M_\alpha)$.

(b) $\mathcal{A}(M_\alpha) = \{\alpha^n \mid n \in \mathbb{Z}\}$.

(c) M_α *is atomic.*

If $\alpha \in \mathbb{R}_{>0}$ is transcendental, then M_α is atomic.

Example (M_α *not atomic*)

Consider the monic irreducible polynomial $m(x) = x^3 - 2x^2 + 3x - 7$, which has a real root $\alpha \in (2, 3)$. As $m(x)(x + 2) = x^4 - x^2 - x - 14$, we note $\alpha^4 = \alpha^2 + \alpha + 14$. Then α is not an atom in M, implying M_α is not atomic.

Atomicity

Proposition (Z., 2021)

For each $\alpha \in \mathbb{R}_{>0}$, the following statements are equivalent.

(a) $1 \in \mathcal{A}(M_\alpha)$.

(b) $\mathcal{A}(M_\alpha) = \{\alpha^n \mid n \in \mathbb{Z}\}$.

(c) *M_α is atomic.*

If $\alpha \in \mathbb{R}_{>0}$ is transcendental, then M_α is atomic.

Example (*M_α not atomic*)
Consider the monic irreducible polynomial $m(x) = x^3 - 2x^2 + 3x - 7$, which has a real root $\alpha \in (2, 3)$. As $m(x)(x+2) = x^4 - x^2 - x - 14$, we note $\alpha^4 = \alpha^2 + \alpha + 14$. Then α is not an atom in M, implying M_α is not atomic.

ACCP

One of the most relevant classes of atomic monoids are those satisfying the ACCP.

A monoid $(M, +)$ satisfies the **ascending chain condition on principal ideals** (ACCP) if every sequence $\{x_n\}_{n \in \mathbb{Z}_{>0}} \subseteq M$ satisfying $x_n - x_{n+1} \in M$ for each $n \in \mathbb{N}$, is constant after some point.

Example (*M_α does not satisfy ACCP*)

- $\alpha = 2/3$. Take the sequence $\{x_n\}_{n \in \mathbb{Z}_{>0}}$ defined by $x_n = 2 \cdot (2/3)^n$: $x_n - x_{n+1} = 2 \cdot (2/3)^n - 2 \cdot (2/3)^{n+1}$ $= (2/3)^{n+1} \in M$ for each $n \in \mathbb{Z}_{\geq 0}$, so the sequence does not become constant. Hence, it does not satisfy the ACCP.

ACCP

One of the most relevant classes of atomic monoids are those satisfying the ACCP.

A monoid $(M, +)$ satisfies the **ascending chain condition on principal ideals** (ACCP) if every sequence $\{x_n\}_{n \in \mathbb{Z}_{>0}} \subseteq M$ satisfying $x_n - x_{n+1} \in M$ for each $n \in \mathbb{N}$, is constant after some point.

Example (M_α *does not satisfy ACCP*)

- $\alpha = 2/3$. Take the sequence $\{x_n\}_{n \in \mathbb{Z}_{>0}}$ defined by $x_n = 2 \cdot (2/3)^n$: $x_n - x_{n+1} = 2 \cdot (2/3)^n - 2 \cdot (2/3)^{n+1}$ $= (2/3)^{n+1} \in M$ for each $n \in \mathbb{Z}_{\geq 0}$, so the sequence does not become constant. Hence, it does not satisfy the ACCP.

Nested Classes of Atomic Monoids

The following result is well-known.

Proposition

Every BFM satisfies the ACCP.

Therefore,

$$\textbf{UFM} \Rightarrow \textbf{FFM} \Rightarrow \textbf{BFM} \Rightarrow \textbf{ACCP} \Rightarrow \textbf{atomicity}$$

We established the following main result for the class of Laurent evaluation monoids M_α.

Theorem (Z., 2021)

For $\alpha \in \mathbb{R}_{>0}$, the following holds for M_α.

$$\text{FFM} \Leftrightarrow \text{BFM} \Leftrightarrow \text{ACCP}$$

Nested Classes of Atomic Monoids

The following result is well-known.

Proposition

Every BFM satisfies the ACCP.

Therefore,

$$\textbf{UFM} \Rightarrow \textbf{FFM} \Rightarrow \textbf{BFM} \Rightarrow \textbf{ACCP} \Rightarrow \textbf{atomicity}$$

We established the following main result for the class of Laurent evaluation monoids M_α.

Theorem (Z., 2021)

For $\alpha \in \mathbb{R}_{>0}$, the following holds for M_α.

$$\text{FFM} \Leftrightarrow \text{BFM} \Leftrightarrow \text{ACCP}$$

A Class of FFMs that are not UFMs

Theorem (Z., 2021)

Suppose that α_1 and α_2 are the roots of an irreducible quadratic polynomial in $\mathbb{Q}[x]$ such that $0 < \alpha_1 < 1 < \alpha_2$. Then M_{α_1} is an FFM and, therefore, satisfies the ACCP.

Example (M_α *is FFM but not UFM*)
Consider the polynomial $p(x) := x^2 - 2x + \frac{1}{2}$. It is irreducible, with roots $\alpha_1 := 1 - \frac{\sqrt{2}}{2}$ and $\alpha_2 := 1 + \frac{\sqrt{2}}{2}$. Since $0 < \alpha_1 < 1 < \alpha_2$, the Theorem implies M_α is an FFM. However, it is not a UFM: since M_α is atomic, we have $1, \alpha, \alpha^2 \in \mathcal{A}(M_\alpha)$. Then the two sides of the equality $4\alpha_1 = 2\alpha_1^2 + 1$ yield distinct factorizations of the same element in M_α.

A Class of FFMs that are not UFMs

Theorem (Z., 2021)

Suppose that α_1 and α_2 are the roots of an irreducible quadratic polynomial in $\mathbb{Q}[x]$ such that $0 < \alpha_1 < 1 < \alpha_2$. Then M_{α_1} is an FFM and, therefore, satisfies the ACCP.

Example (*M_α is FFM but not UFM*)
Consider the polynomial $p(x) := x^2 - 2x + \frac{1}{2}$. It is irreducible, with roots $\alpha_1 := 1 - \frac{\sqrt{2}}{2}$ and $\alpha_2 := 1 + \frac{\sqrt{2}}{2}$. Since $0 < \alpha_1 < 1 < \alpha_2$, the Theorem implies M_α is an FFM. However, it is not a UFM: since M_α is atomic, we have $1, \alpha, \alpha^2 \in \mathcal{A}(M_\alpha)$. Then the two sides of the equality $4\alpha_1 = 2\alpha_1^2 + 1$ yield distinct factorizations of the same element in M_α.

Diagram Summarizing Our Results

$$[\textbf{UFM} \;\Leftrightarrow\; \textbf{HFM} \;\Leftrightarrow\; \textbf{LFM}]$$

$$\Downarrow$$

$$[\textbf{FFM} \;\Leftrightarrow\; \textbf{BFM} \;\Leftrightarrow\; \textbf{ACCP}]$$

$$\Downarrow$$

$$\textbf{atomicity}$$

References

- D. D. Anderson, D. F. Anderson, and M. Zafrullah: *Factorization in integral domains*, J. Pure Appl. Algebra **69** (1990) 1–19.
- F. Campanini and A. Facchini: *Factorizations of polynomials with integral non-negative coefficients*, Semigroup Forum **99** (2019) 317–332.
- P. M. Cohn: *Bezout rings and and their subrings*, Proc. Cambridge Philos. Soc. **64** (1968) 251–264.
- J. Correa-Morris and F. Gotti: *On the additive structure of algebraic valuations of cyclic free semirings*. Available on arXiv: https://arxiv.org/pdf/2008.13073.pdf.
- F. Halter-Koch: *Finiteness theorems for factorizations*, Semigroup Forum **44** (1992) 112–117.

Acknowledgements

Many thanks go to

- my mentor Dr. Felix Gotti (MIT) for his invaluable guidance, feedback, and encouragement.
- Dr. Pavel Etingof, Dr. Slava Gerovitch, Dr. Tanya Khovanova, the MIT Math Department, and the MIT PRIMES program, for providing us with the opportunity to work on this project.
- my mother for her constant support.
- you for listening.