# Maximal Common Divisors (MCDs) in Monoids and Rings

Grant Blitz, Darren Han, and Hengrui Liang

(Research Mentor: Dr. Felix Gotti)

PRIMES-USA 2025

Fall-Term PRIMES Conference

October 18

# Table of Contents

# General Notation

- $\mathbb{N} := \{1, 2, 3, \ldots\}$.
- $\mathbb{N}_0 := \{0, 1, 2, \ldots\} = \{0\} \cup \mathbb{N}$.
- $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the set of rational numbers, real numbers, and complex numbers, respectively.
- $\mathbb{P}$ denotes the set of prime numbers.

# What is a Monoid?

**Definition.** A monoid $M = (M, *)$ is defined as a nonempty set with a binary operation $* : M \times M \to M$ satisfying the following.

- **It Is Associative**: For any $b, c, d \in M$, we have $(b * c) * d = b * (c * d)$.
- **It Has an Identity**: There exists an element $e$ of $M$ (often denoted by 0 or 1) such that $e * b = b * e = b$ for all $b \in M$.

**Examples.**

1. $(\mathbb{N}, \cdot)$ is a monoid with identity element 1.
2. $(\mathbb{N}_0, +)$ is a monoid with identity element 0.
3. $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$ is a monoid with identity 0.

# Commutativity and Cancellativity

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

**Definitions.**

- $(M, *)$ is said to be commutative if $b * c = c * b$ for all $b, c \in M$.
- $(M, *)$ is said to be cancellative if $a * c = b * c$ implies $a = b$ for all $a, b, c \in M$.

**Remark.** From now on, we tacitly assume that all monoids we deal with here are *commutative* and, unless we say otherwise, *cancellative*.

# Examples of Monoids

**Examples.**

1. $(\mathbb{N}_0, +)$ is a monoid under the standard addition.
   - We use $\mathbb{N}_0$ to denote this monoid when it is clear from context.
2. $(\mathbb{N}_0, \cdot)$ is a monoid under the standard multiplication.
   - It is **not** cancellative because $0 \cdot 1 = 0 \cdot 2 = 0$, but $1 \neq 2$.
3. $(\mathbb{N}, \cdot)$ is a monoid.
   - We will use $\mathbb{N}$ to denote this monoid.
4. $(4\mathbb{N}_0 + 1, \cdot)$ consists of the positive integers that are $1 \pmod 4$.

# Units and Abelian Groups

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

**Definitions.**

- An element $u \in M$ is called a unit if there exists $u^{-1} \in M$ such that $u * u^{-1}$ is the identity element. The set of units is denoted by $\mathcal{U}(M)$.
- An abelian group $G = (G, *)$ is a commutative monoid with the additional property that every element $b \in G$ is a unit.

**Examples.**

1. $0$ is the only unit of $\mathbb{N}_0$.
2. $1$ is the only unit of $\mathbb{N}$.
3. $\pm 1$ are the units of $(\mathbb{Z} \backslash \{0\}, \cdot)$.
4. $(\mathbb{Z}/p\mathbb{Z} \backslash \{0\}, \cdot)$ (nonzero integers modulo $p$ under multiplication) is a group.

# Divisibility and Associates

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

**Definitions.**

- An element $a$ is said to divide an element $b$ if there exists an element $c \in M$ such that $a * c = b$. This is denoted by $a \mid_M b$.
- Two elements $b, c \in M$ are associates if and only if there exists a $u \in \mathcal{U}(M)$ such that $b = c * u$. This is equivalent to $b \mid_M c$ and $c \mid_M b$.

**Examples.**

1. For any $a, b \in \mathbb{N}_0$ we have $a \mid_{\mathbb{N}_0} b$ if and only if $a \leq b$.
2. In $M := (\{0\} \cup \mathbb{N}_{\geq 2}, +)$, we have 2 divides 5 (as $3 \in M$), but 4 does not divide 5 (as $1 \notin M$).
3. In $(\mathbb{Z} \backslash \{0\}, \cdot)$, the numbers $-n$ and $n$ are associates for any $n \in \mathbb{N}$ since $-1$ is a unit.

# Integral Domain

**Definition.** An integral domain is a triple $(R, +, \cdot)$ consisting of a nonempty set and two binary operations satisfying the following:

- $(R, +)$ forms an abelian group with identity $0_R$.
- $R$ is closed under multiplication, the operation $\cdot$ is associative, and $(R, \cdot)$ has $1_R$ as an identity element.
- The identity $a \cdot (b + c) = a \cdot b + a \cdot c$ holds for all $a, b, c \in R$ (the distributive law holds!).
- There are no nonzero zero-divisors or, equivalently, if $a \cdot b = 0$ for some $a, b \in R$, then either $a = 0$ or $b = 0$.

**Remark.** We assume that $0_R \neq 1_R$ in any integral domain $R$ as otherwise $R$ is trivial (i.e., $R$ contains exactly one element).

# Examples of Integral Domains

**Examples.**

1. $(\mathbb{Z}, +, \cdot)$ is the prototypical integral domain.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ for $n \in \mathbb{N}_{\geq 2}$ is an integral domain if and only if $n \in \mathbb{P}$.
   - For $n \in \mathbb{P}$ and any $a, b \in \mathbb{Z}/n\mathbb{Z}$, we have that $ab \equiv 0 \pmod{n}$ implies $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.
   - For $n$ composite, there exist positive integers $a, b \in (1, n)$ such that $ab = n$ so $ab \equiv 0 \pmod{n}$, but $a, b \not\equiv 0 \pmod{n}$.
3. $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$, called the ring of Gaussian integers, is also an integral domain under the standard complex addition and multiplication.

# Irreducibles

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

**Definition.**

- A nonunit element $b$ of $M$ is called an irreducible if there do not exist nonunits $c, d \in M$ such that $b = c * d$.

**Examples.**

1. The only irreducible of $\mathbb{N}_0$ is 1.
2. The irreducibles of $\mathbb{N}$ are $\mathbb{P}$.
3. The irreducibles of $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$ are $\{2, 3\}$.
    - 0 is a unit so it is not an irreducible.
    - For $n \geq 4$, we have $n = 2 + (n - 2)$, and $n - 2 \geq 2$ so $n - 2 \in \mathbb{N}_{\geq 2}$. This means $n$ is not an irreducible.
    - Since 1 is not in the monoid, the only decomposition of 2 is $2 + 0$, but 0 is a unit, so 2 is an irreducible.
    - Similarly, the only decomposition of 3 is $3 + 0$, so 3 is also an irreducible.

# Atomicity

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

**Definition.**

- An element $b \in M \setminus \mathcal{U}(M)$ is called atomic if it can be written as a finite product of irreducibles.
- If every $b \in M \setminus \mathcal{U}(M)$ is atomic, the monoid $M$ is called an atomic monoid.

**Example.** $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$ is atomic since every positive even integer can be expressed as

$$2n = \underbrace{2 + 2 + \cdots + 2}_{n \text{ 2's}},$$

and every positive odd integer at least 3 can be expressed as

$$2n + 3 = 3 + \underbrace{2 + 2 + \cdots + 2}_{n \text{ 2's}}.$$

**Example.** $\mathbb{N}$ is atomic by the Fundamental Theorem of Arithmetic.

# Maximal Common Divisors

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

**Definition.** An element $d \in M$ is called a maximal common divisor (MCD) of subset $S \subseteq M$ if the set $S - d := \{s - d : s \in S\}$ has no nonunit common divisors. We let $\mathrm{mcd}(S)$ denote the set of MCDs of $S$.

**Example.** In the monoid $M := (\{0\} \cup \mathbb{N}_{\geq 2}, +)$, the set $\{5, 6\}$ has nonzero common divisors $2, 3$, both of which are MCDs.

- 5 has divisors $0, 2, 3, 5$.
- 6 has divisors $0, 2, 3, 4, 6$.
- The common divisors are $0, 2, 3$.
- Since $5 = 2 + 3$ and $6 = 2 + 4$, and the elements 3 and 4 have no nonzero common divisor, then 2 is an MCD of $\{5, 6\}$.
- Similarly $5 = 3 + 2$ and $6 = 3 + 3$, and the elements 2 and 3 have no nonzero common divisor (both are irreducibles), so 3 is also an MCD.

# The MCD and MCD-finite Properties

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

**Recall.** An element $d \in M$ is an MCD of a nonempty subset $S$ of $M$ if $S - d := \{s - d : s \in S\}$ has no nonunit common divisors.

**Definitions.**

- $M$ is called an MCD monoid if every finite nonempty subset $S \subseteq M$ has at least one MCD.
- $M$ is called an MCD-finite monoid if every finite nonempty subset $S \subseteq M$ has finitely many MCDs (possibly zero) up to associates.

**Examples.**

1. $\mathbb{N}_0$ is both an MCD and MCD-finite monoid as $a \,|_M\, b$ if $a \leq b$, so $\mathrm{mcd}(S) = \min(S)$, so every set has exactly one MCD.
2. $\mathbb{N}$ is both an MCD and an MCD-finite monoid as $\mathrm{mcd}(S) = \gcd(S)$, so every set has exactly one MCD.

# Finitary Power Monoids

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

**Definition.** The sumset of two subsets $A, B$ of $M$ is defined as

$$A + B := \{a + b : (a, b) \in A \times B\}.$$

**Example.** Let $M = \mathbb{N}_0$.

1. $\{2\} + \{1, 3\} = \{3, 5\}$.
2. $\{1, 2\} + \{1, 3\} = \{2, 3, 4, 5\}$.

**Definition.** $\mathcal{P}_{\text{fin}}(M)$ denotes the finitary power monoid of $M$, which is the monoid containing all the finite nonempty subsets of $M$ with the sumset operation.

# Restricted Power Monoids

**Definition.** $\mathcal{P}_{\text{fin},\mathcal{U}}(M)$ denotes the restricted power monoid of $M$, which is the monoid containing all the finite nonempty subsets of $M$ such that every subset contains an element of $\mathcal{U}(M)$ under the sumset operation.

**Example.** Let $M = \mathbb{N}_0$.

1. $\{0, 1, 2\} + \{0, 1\} = \{0, 1, 2, 3\}$.
2. $\{0, 2\} + \{0, 1\} = \{0, 1, 2, 3\}$.

**Remark.** Power monoids are not necessarily cancellative. In the example above, $\{0, 1\}$ cannot be canceled.

# MCD and MCD-finite Property in Power Monoids

**Question.** If $M$ is an MCD monoid, must $\mathcal{P}_{\text{fin}}(M)$ be an MCD monoid?

**Theorem (Dani-Gotti-Hong-Li-Schlessinger, 2025)**

*If $M$ is an MCD monoid, so is $\mathcal{P}_{\text{fin}}(M)$.*

**Question.** If $M$ is an MCD-finite monoid, must $\mathcal{P}_{\text{fin}}(M)$ be an MCD-finite monoid?

**Theorem (Blitz-Han-Gotti-Liang, 2025)**

*If $M$ is an MCD-finite monoid, so is $\mathcal{P}_{\text{fin}}(M)$.*

**Question.** If $M$ is an MCD-finite monoid, must $\mathcal{P}_{\text{fin},\mathcal{U}}(M)$ be an MCD-finite monoid?

**Theorem (Blitz-Han-Gotti-Liang, 2025)**

*If $M$ is an MCD-finite monoid, so is $\mathcal{P}_{\text{fin},\mathcal{U}}(M)$.*

# What Is a Monoid Algebras

**Definition.** Let $R$ be an integral domain and $M$ be a monoid. The monoid algebra of $M$ over $R$ is the set of polynomial expressions with coefficients in $R$ and exponents in $M$:

$$R[M] := \left\{ \sum_{i=1}^{n} r_i x^{m_i} : r_i \in R, m_i \in M \text{ for all } 1 \leq i \leq n \right\}.$$

**Remark.** $R[M]$ is a integral domain under the standard polynomial-like addition and multiplication.

# Operations in Monoid Algebras

**Example.** Consider the monoid algebra $\mathbb{Z}[\mathbb{Q}_{\geq 0}]$ and elements $f = x^2 + 2x^{\frac{1}{2}}$ and $g = x^{\frac{1}{2}} - 1$.

$$\begin{aligned} f + g &= x^2 + 2x^{\frac{1}{2}} + x^{\frac{1}{2}} - 1 \\ &= x^2 + 3x^{\frac{1}{2}} - 1. \end{aligned}$$

$$\begin{aligned} f \cdot g &= (x^2 + 2x^{\frac{1}{2}})(x^{\frac{1}{2}} - 1) \\ &= x^2 \cdot x^{\frac{1}{2}} - x^2 \cdot 1 + 2x^{\frac{1}{2}} \cdot x^{\frac{1}{2}} - 2x^{\frac{1}{2}} \cdot 1 \\ &= x^{\frac{5}{2}} - x^2 + 2x - 2x^{\frac{1}{2}}. \end{aligned}$$

# Atomicity in Polynomial Domains

**Definition.** $R[x]$ denotes the integral domain of polynomials with coefficients in $R$: it is indeed the monoid algebra $R[\mathbb{N}_0]$ of $\mathbb{N}_0$ over $R$.

**Question.** If $R$ is an atomic integral domain, must the polynomial extension $R[x]$ also be an atomic integral domain?

**Theorem (Roitman, 1993)**

*There exists an atomic integral domain $R$ such that its polynomial extension $R[x]$ is not atomic.*

**Theorem (Roitman, 1993)**

*If $R$ is an atomic and MCD integral domain, then the polynomial extension $R[x]$ also an atomic integral domain.*

# Atomicity in Monoid Algebras

**Question.** If a monoid $M$ is atomic, must the monoid algebra $R[M]$ be atomic for every integral domain $R$?

**Theorem (Gotti-Rabinovitz, 2025)**

*There exists an atomic monoid M such that the monoid algebra R[M] is not atomic for any integral domain R.*

**Question.** What if we restrict our attention to MCD monoids $M$?

**Theorem (Blitz-Han-Gotti-Liang, 2025)**

*There exists an atomic and MCD monoid M such that $\mathbb{F}_p[M]$ is not atomic for any prime p ($\mathbb{F}_p$ is the field of p elements).*

# References


- J. Dani, F. Gotti, L. Hong, B. Li, and S. Schlessinger, *On finitary power monoids of linearly orderable monoids*, ArXiv, arxiv.org/abs/2501.03407.

- S. Eftekhari and M. R. Khorsandi, *MCD-finite domains and ascent of IDF-property in polynomial extensions*, Comm. Algebra **46** (2018) 3865–3872.

- R. Gilmer and T. Parker, *Divisibility properties in semigroup rings*, Michigan Math. J. **21** (1974) 65–86.

- V. Gonzalez, E. Li, H. Rabinovitz, P. Rodriguez, and M. Tirador, *On the atomicity of power monoids of Puiseux monoids*, Internat. J. Algebra Comput. **35** (2025) 167–181.

- F. Gotti and H. Rabinovitz, *On the ascent of atomicity to monoid algebras*, J. Algebra **663** (2025) 857–881.

- F. W. Levi, *Arithmetische Gesetze im Gebiete diskreter Gruppen*, Rend. Circ. Mat. Palermo **35** (1913) 225–236.

- M. Roitman, *Polynomial extensions of atomic domains*, J. Pure Appl. Algebra **87** (1993) 187–199.

# Acknowledgments

The authors would like to thank

- **Dr. Felix Gotti** for mentoring this project,
- **PRIMES-USA** for allowing us to conduct rewarding mathematical research.

# End of Presentation

**Thank you for your time!**