On the MCD and MCD-Finite Properties

(joint work with Grant Blitz)

Darren Han and Hengrui Liang

(Mentor: Dr. Felix Gotti)

PRIMES-USA 2025

Summer Workshop for Intrepid Mathematicians
SWIM 2025

August 15

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.

Monoids

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

- **Associativity**: For any $b, c, d \in M$, we have $(b * c) * d = b * (c * d)$.
- **Identity Element**: There exists an element e of M, often denoted by 0 or 1, such that, for any $b \in M$, the following holds: $e * b = b * e = b$.

Let $(M, *)$ be a monoid, and let $N \subseteq M$. Then N is a submonoid of M if it has the following properties:

- $e_M \in N$, and
- N is closed under $*$ (for all $b, c \in N$, we have $b * c \in N$),

Commutativity and Cancellativity

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

Commutativity

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

Cancellativity

- $(M, *)$ 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 are cancellative and commutative.

Examples of Monoids

Examples

1. $(\{e\}, *)$ is a monoid with identity element e.
2. $(\mathbb{N}_0, +)$ is a monoid with identity element 0. We will abuse notation.
    - We use $\mathbb{N}_0$ to denote this monoid when it is clear from context.
    - It is the "prototypical" commutative monoid.
3. $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$ is a submonoid of $\mathbb{N}_0$ with identity element 0.
    - For any element a we have $0 + a = a$, and if $a, b \in \mathbb{N}_{\geq 2}$, then the integer $a + b \geq 4 \geq 2$ so $a + b$ is also an element.
4. $(\mathbb{N}, \cdot)$ is a monoid with identity element 1.
    - We will use $\mathbb{N}$ to denote this monoid.
5. $(\mathbb{Q}_{\geq 0}, +)$ is a monoid with identity element 0.
6. $(\mathbb{Q}_{\geq 1}, \cdot)$ is a monoid with identity element 1.

Units (Invertible Elements)

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

- An element $u \in M$ is called a unit or an invertible element if there exists $u^{-1} \in M$ such that $u * u^{-1}$ is the identity element.
- The set of units is denoted by $\mathcal{U}(M)$.

Examples

1. 0 is the only unit of $\mathbb{N}_0$.
2. 1 is the only unit of $\mathbb{N}$.
3. ± 1 are the units of $(\mathbb{Z}\backslash\{0\}, \cdot)$.

Divisibility and Associates

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

- 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. $3 \mid_{\mathbb{N}} 6$ since $6 = 2 \cdot 3$.
3. In $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$, we have 2 divides 5 (3 is an element), but 4 does not divide 5 (1 is not an element).
4. In $(\mathbb{Z} \backslash \{0\}, \cdot)$, the numbers $-n$ and n are associate for any $n \in \mathbb{N}$ since -1 is a unit.

Abelian Groups

An abelian group $G = (G, *)$ is defined as a commutative monoid with the additional property that every element $b \in G$ is a unit.

Examples

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are groups.
2. $(\mathbb{Z}[x], +)$ is a group.
3. $(\mathbb{Z}/n\mathbb{Z}, +)$, the set of integers modulo n under addition, is a group.
4. $(\mathbb{Z}/p\mathbb{Z}\backslash\{0\}, \cdot)$ (nonzero integers modulo p under multiplication) is a group.
5. $(\mathbb{Q}\backslash\{0\}, \cdot)$ is a group.
6. $(\mathbb{R}\backslash\{0\}, \cdot)$ is a group.

Commutative Rings

A commutative ring with identity 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!).

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

- A commutative ring with identity R is called an integral domain (ID) if there are no non-zero zero divisors. That is, $a \cdot b = 0$ implies that $a = 0$ or $b = 0$.
- We let $R^* = R \backslash \{0\}$ when R is an integral domain.

Examples of Commutative Rings

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 a CRI but not an ID unless $n \in \mathbb{P}$.
   - 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. $(\mathbb{Z}[x], +, \cdot)$ is an ID.
4. Similarly, $(\mathbb{Q}[x], +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$, and $(\mathbb{C}[x], +, \cdot)$ are IDs.

Fields

- A field $(F, +, \cdot)$ is a ring such that every $b \neq 0_F$ in F has a multiplicative inverse.
- This is equivalent to $(F^*, \cdot)$ is a group.

Remark. Every field is an integral domain.

Examples

1. $(\mathbb{Q}, +, \cdot)$ is a field because every nonzero element $r \in \mathbb{Q}$ has multiplicative inverse $\frac{1}{r}$.
2. Similarly, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are fields.
3. $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field for $p \in \mathbb{P}$ since every nonzero residue has a multiplicative inverse modulo p.

Atoms (Irreducible Elements)

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

- A nonunit element b of M is called an atom or an irreducible element if there do not exist nonunits $c, d \in M$ such that $b = c * d$.
- We use $\mathcal{A}(M)$ to denote the set of atoms.

Examples

1. $\mathcal{A}(\mathbb{N}_0) = \{1\}$.
2. $\mathcal{A}(\mathbb{N}) = \mathbb{P}$.
3. $\mathcal{A}((\{0\} \cup \mathbb{N}_{\geq 2}, +)) = \{2, 3\}$.
   - 0 is a unit so it is not an atom.
   - 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 atom.
   - Since 1 is not in the monoid, the only decomposition of 2 is $2 + 0$, but 0 is a unit, so 2 is an atom.
   - Similarly, the only decomposition of 3 is $3 + 0$, so 3 is also an atom.

Atomicity

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

- An element $b \in M \backslash \mathcal{U}(M)$ is called atomic if it can be written as a finite product of atoms.
- If every $b \in M \backslash \mathcal{U}(M)$ 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 since every positive integer can be expressed as a finite product of prime numbers.

The Unique Factorization Property

Let $(M, *)$ be a monoid. For $b \in M$, we let $\mathsf{Z}(b)$ denote the set containing the factorizations of b into atoms.

Remark. Note $(M, *)$ being atomic is equivalent to $|\mathsf{Z}(b)| \geq 1$ for all $b \in M$.

- If $|\mathsf{Z}(b)| = 1$ for all $b \in M$, the monoid M is called a UFM or a unique factorization monoid.

Examples

1. $\mathbb{N}_0$ is a UFM ($n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ 1's}}$).
2. $\mathbb{N}$ is a UFM by the Fundamental Theorem of Arithmetic.
3. $(\mathbb{Z}[i]^*, \cdot)$, called the monoid of Gaussian integers, is also a UFM.

The Finite Factorization Property

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

- In an atomic monoid M, if $\mathsf{Z}(b)$ is finite for all $b \in M$, the monoid M has the FF property and is called a finite factorization monoid (FFM).
- An integral domain R is said to have the FF property if the monoid R^* has the same property.

Remark. Every UFM is an FFM.

Example. The monoid $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$ is an FFM but not a UFM.

- The atoms are $\{2, 3\}$.
- $6 = 2 + 2 + 2 = 3 + 3$, so the monoid is not a UFM.
- For all nonzero n in this monoid, if

$$n = \underbrace{2 + 2 + \cdots + 2}_{a \text{ 2's}} + \underbrace{3 + 3 + \cdots + 3}_{b \text{ 3's}} = 2a + 3b,$$

where $a, b \in \mathbb{N}_0$, then $a \leq n$ and $b \leq n$ so there are at most $(n+1)^2$ distinct factorizations. This is finite so the monoid is an FFM.

The FF Property - Another Example

Example. Let R be the integral domain $\mathbb{Z}[\sqrt{-5}]$.

- We can use the multiplicative map $N\colon R \to \mathbb{N}_0$ defined by $N(a+\sqrt{-5}b) = a^2 + 5b^2$.
  - As a result, if $c \mid_R d$, then $N(c) \mid N(d)$.
- Using the map N, we can argue that R is an FFD (it is well known that a monoid is an FFM if it is atomic and every element has only finitely many irreducible divisors).
- $2, 3, 1 \pm \sqrt{-5}$ are atoms of R.
  - Note that there is no element c such that $N(c) \in \{2, 3\}$.
  - Also, if $N(c) = 1$, then $c \in \{1, -1\} = \mathcal{U}((R, \cdot))$.
  - $N(2) = 4$, so 2 is an atom.
  - Similarly $N(3) = 9$ and $N(1 \pm \sqrt{-5}) = 6$ so these are also atoms.
- Using this, we can show R is not a UFD because $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Greatest Common Divisors (GCD)

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

For a set $S \subseteq M$, an element d is called a common divisor of S if it divides all elements of S.

- The set of units $\mathcal{U}(M)$ are common divisors of every set.

An element d is called the greatest common divisor (GCD) of S if every other common divisor d' of S divides d.

- Note that there is at most one GCD, up to associates.

A monoid M is said to be a GCD monoid if every finite nonempty subset $S \subseteq M$ has a GCD.

Similarly, an integral domain R is said to be a GCD domain if $(R^*, \cdot)$ is a GCD monoid.

More on GCDs

Examples.

1. The monoid $\mathbb{N}$ is a GCD monoid.
2. In the monoid $\mathbb{N}_0$, the GCD of any finite nonempty subset S is $\min(S)$.
   - If d is a common divisor, then $d \leq \min(S)$ so $d \mid_{\mathbb{N}_0} \min(S)$.
3. In the monoid of dyadic rationals $(\mathbb{N}_0[1/2], +)$, where

$$\mathbb{N}_0[1/2] := \{p(1/2) : p(x) \in \mathbb{N}_0[x]\},$$

   the GCD of any finite nonempty subset S is $\min(S)$.
   - For all elements a, b, if $a \leq b$, then $b - a \geq 0$ is also dyadic and therefore is an element of this monoid.
   - Therefore, if d is a common divisor, then $d \leq \min(S)$ and so $d \mid_{\mathbb{N}_0[\frac{1}{2}]} \min(S)$.

Remark. Every UFM is a GCD monoid.

Maximal Common Divisors (MCD)

An element d is called a maximal common divisor (MCD) of S if the set $S/d := \{s/d : s \in S\}$ has no nonunit common divisors.

- A monoid M is said to be a MCD monoid if every finite nonempty subset $S \subseteq M$ has at least one MCD.
- A monoid M is said to be a MCD-finite monoid if every finite nonempty subset $S \subseteq M$ has finitely many MCDs (possibly zero) up to associates.
- A monoid M is a q-GCD monoid if every finite nonempty subset $S \subseteq M$ has at most one MCD (possibly zero) up to associates.

Example. In the monoid $\mathbb{N}$, the numbers $4, 6$ have common divisors $1, 2$, and 2 is the unique GCD and MCD.

Remark. Every FFM is MCD and MCD-finite.

More on Common Divisors

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, but neither of which are GCD.

- 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, note $5 = 3 + 2$ and $6 = 3 + 3$, and the elements 2 and 3 have no nonzero common divisor (both are atoms), so 3 is also an MCD.
- However $2 \nmid_M 3$ and $3 \nmid_M 2$ so neither is a GCD.

Remark. For a set S, if a GCD exists, it is the unique MCD. However, MCDs are not always unique.

Torsion-Free Monoids

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

- We let $a^n = \underbrace{a * a * \cdots * a}_{n\ a's}$ for $a \in M$.
- M is called torsion-free if $a^n = b^n$ for any $n \in \mathbb{N}$ and $a, b \in M$ implies that $a = b$.

Examples

1. $\mathbb{N}_0$ is a torsion-free monoid because if $na = a^n = b^n = nb$ for any $n \in \mathbb{N}$, then we have $a = b$ by dividing out by n as $n \neq 0$.
2. $(\mathbb{Z}/n\mathbb{Z}, +)$ with $n \in \mathbb{N}$ under addition is not a torsion-free monoid as $na = 0 = nb$ for any $a, b \in \mathbb{Z}/n\mathbb{Z}$.

Linearly Orderable Monoids

A monoid $(M, *)$ is linearly orderable if there exists a total order $\preceq$ such that $a \preceq b$ means $a * c \preceq b * c$ for all $a, b, c \in M$.

Theorem (Levi, 1913)

For a commutative monoid M, the following statements are equivalent:

- *M is linearly orderable.*
- *M is cancellative and torsion-free.*

Examples

1. $\mathbb{N}$ under the total order $\leq$. If $a \leq b$, then we have that $a \cdot c \leq b \cdot c$ as $c > 0$.
2. Submonoids of $(\mathbb{Q}_{\geq 0}, +)$, which are called Puiseux monoids with total order $\leq$. If $a \leq b$, then we have $a + c \leq b + c$.
3. Submonoids of $(\mathbb{R}_{\geq 0}, +)$, which are called positive monoids with total order $\leq$.

Valuation Monoids

A monoid $(M, *)$ is called a valuation monoid if, for every $b, c \in M$, either $b \mid_M c$ or $c \mid_M b$.

Remark. Every valuation monoid is also GCD monoid because in a set, there must exist one element that divides all the other elements.

Examples

1. All groups, as every element divides every other element.
2. $\mathbb{N}_0$, as if $a \leq b$, then $b - a \in \mathbb{N}_0$ and so $a \mid_M b$.
3. Similarly, $(\mathbb{Q}_{\geq 0}, +)$ and $(\mathbb{N}_0\left[\frac{1}{2}\right], +)$ are valuation monoids.
4. $G_{\geq 0}$ for some subgroup G of $(\mathbb{R}, +)$, as if $a \leq b$, then $a \mid_M b$ as $b - a \in G$ and $b - a \geq 0$. The last examples are special cases of this example where we took $G \in \left\{\mathbb{Z}, \mathbb{Q}, \mathbb{Z}\left[\frac{1}{2}\right]\right\}$.

Puiseux Valuation Monoids

Theorem (well-known)

Every Puiseux valuation monoid V can be expressed as $V = G_{\geq 0}$ for some subgroup G of $(\mathbb{Q}, +)$.

Remark. This shows that the Puiseux valuation monoids look exactly like the examples we described in the previous slide.

Pre-Schreier Property

Let $(M, *)$ be a monoid. An element $a \in M$ is said to be primal if $a \mid_M b * c$ implies that there exists elements b' and c' in M such that $a = b' * c'$, $b' \mid_M b$, and $c' \mid_M c$.

A monoid $(M, *)$ is said to be pre-Schreier if every element of M is primal.

Examples

1. The monoid $\mathbb{N}_0$ satisfies the pre-Schreier property. Consider $5 \mid_M 3 + 4$. We can write $5 = 2 + 3$ where $2 \mid_M 3$ and $3 \mid_M 4$.
2. The monoid $\{0\} \cup \mathbb{Q}_{\geq 1}$ is not a pre-Schreier monoid. Consider $\frac{3}{2} \mid_M \frac{5}{4} + \frac{7}{4}$. Since $\frac{3}{2}$ is an atom, if $\frac{3}{2} = b' + c'$, one of b' or c' must be $\frac{3}{2}$, so $\frac{3}{2}$ must divide one of the two elements, but this does not happen.

Remark. All GCD monoids are pre-Schreier monoids.

Monoid Algebras

Let R be a commutative ring with identity and M be a linearly orderable monoid. The monoid algebra $R[M]$ is the set of polynomials with coefficients in R and exponents in M, instead of $\mathbb{N}_0$ like a normal polynomial ring.

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

Note that $R[M]$ is a ring under polynomial addition and multiplication.

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

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

$$f \cdot g = x^{\frac{5}{2}} - x^2 + 2x - 2x^{\frac{1}{2}}.$$

Examples of Monoid Algebras

Let R be an integral domain.

Examples

1. The monoid algebra $R[\mathbb{N}_0]$ is equivalent to the standard polynomial ring $R[x]$.
2. The monoid algebra $R[\mathbb{Z}]$ is the ring of Laurent polynomials $R[x^{\pm 1}]$.
3. The monoid algebra $R[\mathbb{N}_0 \times \mathbb{N}_0]$ is the ring of polynomials in two variables, also denoted by $R[x, y]$.

Monoid Algebras that are Integral Domains

Theorem (well-known)

Let R be a commutative ring with identity, and let M be a commutative monoid. Then the following conditions are equivalent.

- *$R[M]$ is an integral domain.*
- *R is an integral domain, and M can be turned into a linearly orderable monoid.*

Ascent of the MCD Property to Monoid Algebras

A property $\mathcal{P}$ is said to ascend to monoid algebras over a field if M satisfies $\mathcal{P}$ implies that the monoid algebra $F[M]$ satisfies $\mathcal{P}$ for any field F.

Question. Does the MCD property ascend to monoid algebras over a field?

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

Let F be a field and let M be a linearly orderable pre-Schreier monoid. If M is an MCD monoid, then $F[M]$ is an MCD domain.

Ascent of the MCD Property – Example

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

Let F be a field and let M be a linearly orderable pre-Schreier monoid. If M is an MCD monoid, then $F[M]$ is an MCD domain.

Example. Let M be the positive monoid $(\mathbb{N}_0 + \mathbb{N}_0\sqrt{2}, +)$.

- Consider a set $S := \{a_1 + b_1\sqrt{2}, \ldots, a_k + b_k\sqrt{2}\}$, then we have that $d := \min\{a_1, \ldots, a_k\} + \min\{b_1, \ldots, b_k\}\sqrt{2}$ must be a maximal common divisor. This is because the minimality guarantees that d is common divisor and S/d either contains 0 or contains a and $b\sqrt{2}$ for $a, b \in \mathbb{N}_0$, which do not share a nonunit common factor. Therefore, M is an MCD monoid.

- If $a_1 + a_2\sqrt{2} \mid_M (b_1 + b_2\sqrt{2}) + (c_1 + c_2\sqrt{2})$, then we have that $a_1 \mid_{\mathbb{N}_0} b_1 + c_1$ and $a_2 \mid_{\mathbb{N}_0} b_2 + c_2$. Since $\mathbb{N}_0$ is pre-Schreier, we can apply the primal property of a_1 and a_2 to find $b_1', b_2', c_1', c_2' \in \mathbb{N}_0$ such that $a_1 + a_2\sqrt{2} = (b_1' + b_2'\sqrt{2}) + (c_1' + c_2'\sqrt{2})$ where $b_1' \mid_M b_1$, $c_1' \mid_M c_1$, etc. Thus, M is a pre-Schreier monoid.

Ascent of the MCD Property – Example (Continued)

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

Let F be a field and let M be a linearly orderable pre-Schreier monoid. If M is an MCD monoid, then $F[M]$ is an MCD domain.

Example. Let M be the positive monoid $(\mathbb{N}_0 + \mathbb{N}_0\sqrt{2}, +)$.

- By our theorem $\mathbb{Q}[M]$ is an MCD domain.
- For instance, consider $S := \{x^{\sqrt{2}+1} + x,\ x^{2\sqrt{2}} + 2x^{\sqrt{2}} + 1\}$, then all common divisors must divide

$$x(x^{2\sqrt{2}} + 2x^{\sqrt{2}} + 1) - x^{\sqrt{2}}(x^{\sqrt{2}+1} + x) = x^{\sqrt{2}+1} + x.$$

  However, x^a cannot divide any common divisor for any $a > 0$, as otherwise, it would not divide the second term. Therefore $x^{\sqrt{2}} + 1$ is the GCD and therefore an MCD.

Ascent of the q-GCD Property to Monoid Algebras

Question. Does the q-GCD property ascend to monoid algebras over a field?

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

Let M be a Puiseux monoid, and let R be a GCD-domain. If M has the q-GCD property, then $R[M]$ also has the q-GCD property.

Ascent of the q-GCD Property – Example

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

Let M be a Puiseux monoid, and let R be a GCD-domain. If M has the q-GCD property, then $R[M]$ also has the q-GCD property.

Example. Let M be the Puiseux monoid $(\mathbb{N}_0\left[\frac{1}{2}\right], +)$.

- M has the q-GCD property: as M is a valuation monoid, $\gcd\{q_1, \ldots, q_n\} = \min\{q_1, \ldots, q_n\}$, for any $q_1, \ldots, q_n \in M$. This is because $a \mid_M b$ when $a \leq b$, so the minimum divides all the term. Now, dividing out by the minimum element gives a set with the identity element which does not have any nonunit divisors.
- $\mathbb{Z}$ is a GCD domain (we have seen this earlier).
- By our theorem, $\mathbb{Z}[M]$ has the q-GCD property.

Ascent of the q-GCD Property – Example (Continued)

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

Let M be a Puiseux monoid, and let R be a GCD-domain. If M has the q-GCD property, then $R[M]$ also has the q-GCD property.

Example. Let M be the Puiseux monoid $(\mathbb{N}_0[\frac{1}{2}], +)$.

- For $S := \{x^{\frac{3}{2}} + x^{\frac{1}{2}}, x^2 + 2x + 1\}$, we have that the common divisors must divide the linear combination

$$(x^2 + 2x + 1) - x^{\frac{1}{2}}(x^{\frac{3}{2}} + x^{\frac{1}{2}}) = x + 1.$$

  Now, we get that $x + 1$ is a common divisor as $S = \{x^{\frac{1}{2}}(x + 1), (x + 1)(x + 1)\}$. Therefore, it must be the greatest common divisor and therefore the set has exactly one MCD.

Ascent of the MCD-finite Property to Monoid Algebras

Question. Does there exist a monoid algebra $F[M]$, where F is a field and M is a Puiseux monoid, that is MCD-finite but not FF?

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

Let F be a field, and let V be a valuation Puiseux monoid that is not atomic. Then $F[V]$ is GCD (and therefore MCD-finite) but not FF.

Ascent of the MCD-finite Property – Example

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

Let F be a field, and let V be a valuation Puiseux monoid that is not atomic. Then $F[V]$ is GCD (and therefore MCD-finite) but not FF.

Example. Let $V = (\mathbb{N}_0[\frac{1}{2}], +)$.

- V is a valuation monoid as seen in an example in a previous slide.
- By our theorem, $\mathbb{Q}[V]$ is an MCD-finite monoid but not FF.
- For $S := \{x^{\frac{3}{2}} - x^{\frac{1}{2}}, x^2 + x^{\frac{3}{2}}\}$, all common divisors must divide

$$(x^2 + x^{\frac{3}{2}}) - x^{\frac{1}{2}}(x^{\frac{3}{2}} - x^{\frac{1}{2}}) = x^{\frac{3}{2}} - x = x(x^{\frac{1}{2}} - 1).$$

  However, we cannot have a factor of x^a with $a > \frac{1}{2}$ as otherwise it would not divide the first term. Therefore, we have that $x - x^{\frac{1}{2}}$ is the GCD and thus, the set has finitely many MCDs.

Ascent of the MCD-finite Property – Example (Continued)

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

Let F be a field, and let V be a valuation Puiseux monoid that is not atomic. Then $F[V]$ is GCD (and therefore MCD-finite) but not FF.

Example. Let $V = (\mathbb{N}_0\left[\frac{1}{2}\right], +)$, and let us consider the monoid algebra $\mathbb{Q}[V]$.

- Since V is a valuation monoid, it is a GCD monoid.
- Hence $\mathbb{Q}[V]$ is a GCD domain.
- x^a is atomic in $\mathbb{Q}[V]$ if and only if a is atomic in V.
- No element of $\mathbb{N}_0\left[\frac{1}{2}\right]$ is atomic: indeed, $a = \frac{a}{2} + \frac{a}{2}$ for all $a \in V$.
- As 1 is not atomic in V, the monomial x is not atomic in $\mathbb{Q}[V]$.
- As $\mathbb{Q}[V]$ is not atomic, it does not have the FF property.

Power Monoids

Let M be a monoid.

Definition. The sumset of two subsets A, B of a monoid M is defined as $A + B := \{a + b : a \in A, b \in B\}$.

Examples

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

Remark. Note that the power monoids are not cancellative as seen by the example above.

Power Monoids

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

Ascent of the MCD-finite Property to Power Monoids

Question. Does the MCD-finite property ascend to finitary power monoids and/or restricted power monoids?

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

For a commutative monoid M, the following statements hold.

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

Ascent of the MCD-finite Property – Example

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

For a commutative monoid M, the following statements hold.

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

Example. Let $M = \{0\} \cup \mathbb{N}_{\geq 2}$.

- We have seen that M is a FFM and thus, an MCD-finite monoid.
- By the theorem, we have that $\mathcal{P}_{\text{fin}}(M)$ is MCD-finite as well.
- For example, let $S := \{\{3, 5\}, \{5, 6\}\}$. It is known that $|A + B| \geq |A| + |B| - 1 \geq |A|$, so the divisors can have at most two elements.
- If the divisor has two elements, then we must be adding them to set of one element to get $\{3, 5\}$ and $\{5, 6\}$. However, adding one element must preserve the difference between the two elements of the divisor, which gives a contradiction as $5 - 3 \neq 6 - 5$.

Ascent of the MCD-finite Property – Example (Continued)

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

For a commutative monoid M, the following statements hold.

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

Example. Let $M = \{0\} \cup \mathbb{N}_{\geq 2}$.

- If the divisor has one element, it must divide $3, 5, 6$ in M, which means it must be 0 or 3. One can check that $\{3\} + \{0, 2\} = \{3, 5\}$ and $\{3\} + \{2, 3\} = \{5, 6\}$ and so $\{3\}$ is a common divisor. For the other case, we have $S/\{0\} = S$ and we have seen that S does indeed have a nonunit common divisor, so $\{0\}$ is not an MCD.
- Since $\{0, 2\}$ and $\{2, 3\}$ can be checked to share no nonunit common divisors, $\text{mcd}(S) = \{\{3\}\}$ which is finite.

Ascent of the MCD-finite Property – Example (Continued)

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

For a commutative monoid M, the following statements hold.

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

Example. Consider the numerical monoid $M = \{0\} \cup \mathbb{N}_{\geq 2}$.

- M is MCD-finite and, by our theorem, $\mathcal{P}_{\text{fin},\mathcal{U}}(M)$ is MCD-finite.
- The common divisors of $S := \{\{0, 2, 3, 4, 5\}, \{0, 2, 4, 6\}\}$ are subsets of the elements, whence every common divisor of S is a subset of $\{0, 2, 4\}$ containing 0.
- Now the maximal term in the sum of two sets must be the sum of the maximal term in both sets.
- If the subset contains 4, then we get that 5 must be the sum of 4 and another element, but this is impossible.

References


J. Coykendall and F. Gotti, *On the atomicity of monoid algebras*, J. Algebra **539** (2019) 138–151.


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. 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,
- **SWIM 2025** for giving us a valuable opportunity to present our research.

End of Presentation

Thank you for your time!