On the Ascent of Divisibility Properties to Monoid Algebras

Mingyang Cen, Eric Guo, and Patrek Ragnarsson

Research Mentor: Dr. Felix Gotti

PRIMES-USA 2026

Fall-Term PRIMES Conference

October 24, 2026

Motivation (I)

Classical problem in algebra:

For this slide, let us work with polynomials with integer coefficients: call these simply *polynomials*.

We can multiply together polynomials like $(x-1)(x+1) = x^2 - 1$, just like we multiply integers.

Let an irreducible polynomial be a polynomial like $x - 1$ or $x^2 + 1$ that cannot be split into a product of polynomials, besides 1 or -1.

Motivation (II)

Key property of the integers: Any positive integer can be factored uniquely into the product of prime numbers.

Q: Can we uniquely factorize polynomials into irreducible polynomials?

A (Gauss, 1801): Yes, this factorization can be done uniquely.

However, we can gain more insight by generalizing even further.

Motivation (III)

Insight: Encapsulate the integers into an object called a ring, where addition, subtraction, and multiplication can be done. As a ring, the integers are denoted $\mathbb{Z}$.

The ring of polynomials $\mathbb{Z}[X]$ contains all the polynomials with integer coefficients. We can go even further and encapsulate the concept of polynomial rings, using what is called a monoid algebra $R[M]$.

The unique factorization property asserts that every nonzero nonunit element of a ring can be uniquely factored into atoms (elements that cannot be split into a product).

Rephrasing the previous question: Since $\mathbb{Z}$ satisfies the unique factorization property, does $\mathbb{Z}[X]$ satisfy this property as well?

Go even further: If R is a ring satisfying a certain property, will a monoid algebra $R[M]$ satisfy that property as well?

Notation

Notation.

- $\mathbb{N} := \{1, 2, 3, \ldots\}$
- $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$
- For a set S and a real number x, define $S_{\geq x} := \{s \in S : s \geq x\}$.
- Similarly, define $S_{>x} := \{s \in S : s > x\}$.

Monoids

Definition. A (commutative cancellative) monoid $M = (M, *)$ is a set with an operation $*\colon M \times M \to M$, satisfying the following.

- There exists an **identity** element e such that $e * a = a * e = a$ for all $a \in M$.
- It is **associative**: $(a * b) * c = a * (b * c)$ for any $a, b, c \in M$.
- It is **commutative**: $a * b = b * a$ for any $a, b \in M$.
- It is **cancellative**: $a * b = c * b$ implies $a = c$ for any $a, b, c \in M$.

Remark. Monoids under addition have identity elements denoted by 0, while monoids under multiplication have identity elements denoted by 1.

Examples of monoids

Examples.

- $(\mathbb{N}, \cdot)$ is a monoid with identity 1. Here, $2 \cdot 3 = 6$.
- $(\mathbb{N}_0, +)$ is a monoid with identity 0. Here, $2 + 3 = 5$.
- The additive monoid $\mathbb{N}_0 \setminus \{1\} = \{0, 2, 3, 4, 5, 6, \ldots\}$.
- $(\mathbb{Q}_{\geq 0}, +)$ is a monoid with identity element 0.

Definition. A submonoid of a monoid M is a subset of M that is also a monoid, under the same operation and identity as M.

Definition. We call a submonoid of $(\mathbb{Q}_{\geq 0}, +)$ a Puiseux monoid.

- These are commonly considered due to their elementary yet nontrivial structure.

Elementary divisibility definitions on monoids

Let $(M, \cdot)$ be a monoid. Consider any $a, b \in M$.

Definitions.

- We say that a divides b if there exists $c \in M$ such that $a \cdot c = b$. We write $a \mid_M b$.
- We say that a is a unit if there exists an inverse element $a^{-1} \in M$ with $a \cdot a^{-1} = 1$.
- We say that M is a group if every element is a unit.
- We call any nonunit element a an atom if it is not the product of any two nonunits in M. This is the analog of an irreducible element of a ring.

  The atoms of $(\mathbb{N}, \cdot)$ are precisely the primes.

Remark. Although most terminology comes from the multiplicative case, it is applied equivalently to additive monoids.

Examples of divisibility

Examples.

- In $(\mathbb{N}_0, +)$, we have $1 + 2 = 3$, so $2 \mid_{\mathbb{N}_0} 3$. The only atom is 1.
- In $(\mathbb{N}_0 \setminus \{1\}, +)$, we see that $2 \nmid_{\mathbb{N}_0 \setminus \{1\}} 3$, as 1 is not an element. The atoms are 2 and 3.
- In both monoids above, the only unit is 0.
- Every element in the monoid $(\mathbb{Z}, +)$ is a unit.

Rings

Definitions.

- A ring is a set with additive group structure and multiplicative monoid structure (not necessarily cancellative), where the distributive law holds.
- An integral domain is a commutative ring where $0 \neq 1$ and there are no nonzero zero divisors.
- If P is a property of monoids, we say that an integral domain R satisfies P if its multiplicative monoid $(R \setminus \{0\}, \cdot)$ satisfies P.

Examples.

- The prototypical example of a ring is $\mathbb{Z}$. This is also an integral domain.
- Let $i = \sqrt{-1}$. The Gaussian integers $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ form a more complicated example of a ring.

Fields

Definitions.

- A field is an integral domain where multiplicative inverses exist for every nonzero element.
- The fraction field of an integral domain R is the field consisting of quotients of the form a/b, where $a, b \in R$ and $b \neq 0$.

Examples.

- The prototypical example of a field is $\mathbb{Q}$, the fraction field of $\mathbb{Z}$.
- The fraction field of $\mathbb{Z}[i]$ is the field $\mathbb{Q}[i] := \{a + bi : a, b \in \mathbb{Q}\}$.

Monoid algebras and the ascent problem

Definition

Let R be an integral domain, and let M be a monoid. The monoid algebra $R[M]$ is the set of polynomials with coefficients in R and exponents in M:

$$R[M] := \left\{ r_1 X^{m_1} + r_2 X^{m_2} + \cdots + r_n X^{m_n} : \quad r_i \in R,\ m_i \in M \quad \forall i \right\}.$$

Remarks.

- $R[M]$ is a ring: addition and multiplication are defined as with ordinary polynomials.
- If M is torsion-free ($na = nb \implies a = b$), then $R[M]$ is an integral domain.

We will assume all monoids are torsion-free from now on.

Examples of monoid algebras

Examples.

- $R[\mathbb{N}_0]$ equals the ring of polynomials with coefficients in R, denoted $R[X]$.
- $R[\mathbb{Z}]$ is known as the Laurent polynomial ring. Each element is like a polynomial, but the exponents can be negative, as in

$$r_2X^2 + r_1X + r_0 + r_{-1}X^{-1} + r_{-2}X^{-2}.$$

Ascent problem

Question (Ascent problem)

Choose a certain property P of monoids. Let M be a monoid satisfying P, and let R be an integral domain satisfying P. Does $R[M]$ satisfy property P?

If not, which extra conditions can we impose on R and M to guarantee $R[M]$ satisfies P?

Maximal common divisors

Definition. Let M be a monoid. A common divisor $d \in M$ of a finite nonempty subset $S \subseteq M$ is a maximal common divisor (MCD) if the set

$$S - d := \{s - d : s \in S\}$$

has no nonunit common divisors.

Remark. A subset may have multiple MCDs, or no MCDs.

Example. Take the monoid $M := \{0\} \cup \mathbb{N}_{\geq 2} = \{0, 2, 3, 4, 5, \ldots\}$.

1. Take the subset $S = \{5, 6\}$ of M.
2. The set of common divisors is $\{0, 2, 3\}$, yet only 2 and 3 are MCDs.
   - The set $S - 0 = \{5, 6\}$ has the nonunit common divisor 2, and hence 0 is not an MCD.
   - The set $S - 2 = \{3, 4\}$ has no nonunit common divisors, and hence 2 is an MCD (similarly for 3).

The MCD-finite property

Definition. A monoid M is called an MCD-finite monoid if every nonempty finite subset of M has finitely many (possibly none) MCDs up to multiples by units.

Examples.

1. Every monoid N that is a subset of $\mathbb{N}_0$ is MCD-finite, as for any finite nonempty subset S of N, every MCD of S must be at most $\min S$.
   - Thus, the monoid $M := \{0\} \cup \mathbb{N}_{\geq 2}$ defined previously is MCD-finite.
2. The additive Puiseux monoid $M := \{0\} \cup \mathbb{Q}_{\geq 1}$ is not MCD-finite.
   - Take $S = \{3, 7/2\}$ and any $d \in \mathbb{Q}$ with $1 < d \leq 2$.
   - As $S - d = \{3 - d, 7/2 - d\} \subseteq M$, d is a common divisor of S.
   - Since $3 - d \in [1, 2)$, its only nonzero divisor is itself, but
   $$(7/2 - d) - (3 - d) = 1/2 \notin M.$$
   - Hence, $S - d$ has no nonzero common divisors, so d is an MCD of S.

MCD-finite ascent question

Given this new property, it is natural to ask the following:

Question (MCD-finite ascent)

Does the MCD-finite property ascend to monoid algebras? In particular, if a monoid M satisfies the MCD-finite property, must $R[M]$ also satisfy it for an MCD-finite integral domain R?

We show a stronger negative result, even when restricted to the class of Puiseux monoids.

Theorem (Cen–Gotti–Guo–Ragnarsson, 2026)

The MCD-finite property does not ascend from a monoid to its monoid algebra over the class of Puiseux monoids. In particular, there exists a Puiseux monoid M satisfying the MCD-finite property such that, for any integral domain R, $R[M]$ is not an MCD-finite domain.

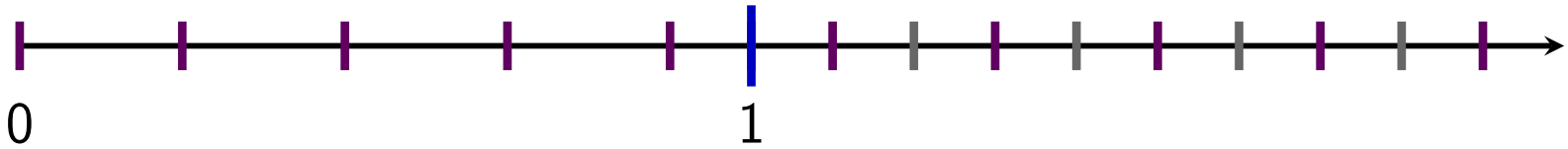
Non-ascent of the MCD-finite property over Puiseux monoids

Theorem (Cen–Gotti–Guo–Ragnarsson, 2026)

The MCD-finite property does not ascend from a monoid to its monoid algebra over the class of Puiseux monoids.

Construction. Below, $\mathbb{N}_0[1/3] := \{a/3^n : a, n \in \mathbb{N}_0\}$.

- Set $M := 2\mathbb{N}_0\,[1/3] \cup \mathbb{N}_0\,[1/3]_{\geq 1}$ and take any finite nonempty subset S.
  - Below 1, only elements with even numerators are allowed.



- Every element of $M \setminus \{0, 1\}$ can be reduced by a sufficiently small element $2/3^n$ while remaining in M. Let d be an MCD of S.
- If $s - d \notin \{0, 1\}$ for every $s \in S$, then for some large n we have $(s - d) - 2/3^n \in M$ for each $s \in S$: d can then be enlarged.
- Thus, $d \in S \cup (S - 1)$, and there are only finitely many possible MCDs.

Non-ascent of the MCD-finite property over Puiseux monoids

Recall. $M := 2\mathbb{N}_0\,[1/3] \cup \mathbb{N}_0\,[1/3]_{\geq 1}$.

Example. $R = \mathbb{Z}$.

1. Take $f = X^2 + X^3$ and $g = X^{7/3} + X^{10/3}$ with the family of common divisors
$$d_n = X + X^{1+3^{-n}} \ (n \in \mathbb{N}).$$
Write $f_n = f/d_n$ and $g_n = g/d_n$ as the quotients, with $f_n, g_n \in \mathbb{Z}[M]$.
2. **Maximality.** It suffices to show that every common divisor c of f_n and g_n is a unit.
   - The lowest exponents of f_n and g_n are 1 and $4/3$; as 1 cannot split into two nonzero elements in M, the lowest exponent of c is 0 or 1.
   - Yet, it cannot be 1 as this would force g_n/c to have lowest exponent $4/3 - 1 = 1/3 \notin M$: it must be 0.
   - **Parity structure.** The restriction of even numerators below 1 in M forces c to be constant to divide f_n. As f_n has coefficient one, c is a unit.
3. $\mathbb{Z}[M]$ **is not MCD-finite.** The only units are ± 1. No two d_n differ by a sign, and hence we exhibit infinitely many MCDs.

The D-property

Definition. A monoid M has the D-property if, for all $a, b, c \in M$,

$$\left.\begin{array}{l} a \mid_M bc, \\ a \text{ and } b \text{ have no nonunit common divisor} \end{array}\right\} \implies a \mid_M c.$$

The D-property generalizes Euclid's lemma.

Counterexample. The additive monoid

$$M = \{0, 2, 3, 4, \ldots\}$$

does not have the D-property:

- $2 \mid_M 3 + 3$, since $6 - 2 = 4 \in M$.
- The only common divisor of 2 and 3 is 0, the identity.
- But $2 \nmid_M 3$, since $3 - 2 = 1 \notin M$.

Ascent of the D-property over fields and Puiseux monoids

Definition. A monoid M is a valuation monoid if, for any two $a, b \in M$, we have $a \mid_M b$ or $b \mid_M a$.

Theorem (Cen–Gotti–Guo–Ragnarsson, 2026)

For a Puiseux monoid M and field F, the following are equivalent.

(a) *The monoid algebra $F[M]$ satisfies the D-property.*

(b) *The monoid M is a valuation monoid.*

Failure of D-ascent: There exists a Puiseux monoid M with the D-property that is not a valuation monoid. Thus $F[M]$ fails the D-property for every field F.

Polynomial rings: Since $\mathbb{N}_0$ is a valuation monoid, $F[\mathbb{N}_0] \cong F[X]$ has the D-property.

Insufficiency of previous criterion over integral domains

Question

For what integral domains R and nontrivial Puiseux monoids M is the monoid algebra $R[M]$ a D-domain?

Lemma (Cen–Gotti–Guo–Ragnarsson, 2026)

Let R be an integral domain and M a Puiseux monoid such that the monoid algebra $R[M]$ satisfies the D-property. Then M is a valuation monoid.

Theorem (Cen–Gotti–Guo–Ragnarsson, 2026)

There exists a D-domain R such that $R[X] \cong R[\mathbb{N}_0]$ does not satisfy the D-property.

Introducing the FC-property

Two elements of a domain are said to be coprime if they share no nonunit common divisor.

Let R be an integral domain with fraction field K, and let M be a monoid.

Definition. The pair (R, M) has the FC-property if, for all $f, g \in R[M]$,

$$f, g \text{ are coprime in } R[M] \implies f, g \text{ are coprime in } K[M].$$

Example. Let $R = \mathbb{Z}$ and $M = \mathbb{N}_0$. The fraction field K of R is $\mathbb{Q}$. We know by Gauss' lemma that coprime elements in $\mathbb{Z}[\mathbb{N}_0] \cong \mathbb{Z}[X]$ remain coprime in $\mathbb{Q}[\mathbb{N}_0] \cong \mathbb{Q}[X]$, which proves that (R, M) has the FC-property.

Main characterization of D-property ascent

Theorem (Cen–Gotti–Guo–Ragnarsson, 2026)

Let R be an integral domain and M a nontrivial Puiseux monoid. The following claims are equivalent.

(a) *The monoid algebra $R[M]$ is a D-domain.*

(b) *The pair (R, M) has the FC-property and M is a valuation monoid.*

Acknowledgments

The authors would like to thank:

- Dr. Felix Gotti for mentoring this research project.
- the MIT PRIMES-USA research program for making this research opportunity possible.

End of presentation

Thank you for listening!

References


D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Factorization in integral domains*, J. Pure Appl. Algebra **69** (1990) 1–19.


G. Blitz, F. Gotti, D. Han, and H. Liang, *Maximal common divisors in monoid algebras*. Preprint on arXiv: `https://arxiv.org/abs/2609.18947`.


R. Gilmer, *Commutative Semigroup Rings*, Chicago Lectures in Mathematics, University of Chicago Press, 1984.


A. Grams, *Atomic rings and the ascending chain condition for principal ideals*, Math. Proc. Cambridge Philos. Soc. **75** (1974) 321–329.


F. Gotti, *Increasing positive monoids of ordered fields are FF-monoids*, J. Algebra **518** (2019) 40–56.


M. Zafrullah, *On a property of pre-Schreier domains*, Comm. Algebra **15** (1987) 1895–1920.


M. Cen, F. Gotti, E. Guo, and P. Ragnarsson, *The D-property in domains and monoids*, 2026.