On the Ascent of Atomicity to Monoid Algebras

Felix Gotti
fgotti@mit.edu

Massachusetts Institute of Technology

Summer Workshop for the Intrepid Mathematician
SWIM 2024

August 5, 2024

Outline

Some Notation and Reminders

Some Notation Adopted Here

- $\mathbb{N} := \{1, 2, 3, \dots\}$,
- $\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, \dots\}$,
- $\mathbb{P}$ denotes the set of primes, and
- $R[x]$ denotes the ring consisting of all polynomials with coefficients in a given commutative ring R (for now, assume that $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$).

What Are Atomicity and Factorization Theory?

Fundamental Theorem of Arithmetic: Each nonzero nonunit of $\mathbb{Z}$

1. can be factored into atoms/irreducibles (here, standard primes)
2. in an essentially unique way ($6 = 2 \cdot 3$ same as $6 = (-2) \cdot (-3)$).

Another Classical Theorem: Each nonzero nonunit of $\mathbb{Z}[x]$ (or $\mathbb{R}[x]$)

1. can be factored into atoms/irreducibles (here, irreducible polynomials)
2. in an essentially unique way.

Question. What do atomicity and factorization theory mean?

Let R be a ring (not only $\mathbb{Z}$, $\mathbb{Z}[x]$, or $\mathbb{R}[x]$), and let M be a monoid.

- Factorization Theory
  - Assuming that R (resp., M) satisfies condition (1) in the theorems above, can we understand how much R (resp., M) deviates from satisfying condition (2)?
- Atomicity
  - Can we decide whether R (or M) satisfies condition (1) in the theorems above.
  - If not, can we understand how much R (or M) deviates from satisfying condition (1)?

Relevance of Atomicity and Factorization Theory

Why are atomicity and factorization theory relevant?

- Basic philosophical curiosity.
- Pragmatism: Divide and Conquer!
- Intrinsic mathematical purposes: Fermat's Last Theorem.

Example: Fermat's Last Theorem

1. Lamé had supposedly proved Fermat's Last Theorem back in 1847 using that the ring $\mathbb{Z}[\zeta_p]$ is a UFD for any primitive p-root of unity ζ_p (that is, that $\mathbb{Z}[\zeta_p]$ satisfies both conditions in the FTA).
2. However, $\mathbb{Z}[\zeta_{23}]$ is **not** a UFD as proved by Kummer later ($\mathbb{Z}[\zeta_{23}]$ does not satisfy the uniqueness conditions in the FTA).
3. Kummer developed an (ideal number) theory to understand the deviation of $\mathbb{Z}[\zeta_p]$ from being a UFD.
4. This may be considered the origin of factorization theory.
5. Kummer applied the same theory to prove Fermat's Last Theorem for infinitely many $p \in \mathbb{P}$, including all primes p such that $\mathbb{Z}[\zeta_p]$ is a UFD.

Commutative Monoids

Definition. A commutative monoid is a pair $(M, *)$, where M is a set and $*$ is a binary operation on M satisfying the following conditions.

- $*$ is associative: $b * (c * d) = (b * c) * d$ for all $b, c, d \in M$;
- $*$ is commutative: $b * c = c * b$ for all $b, c \in M$;
- there exists $e \in M$ such that $e * b = b$ for all $b \in M$.

Today's Conventions

- We call a commutative monoid $(M, *)$ simply a monoid if it is cancellative: $b * d = c * d$ implies $b = c$ for all $b, c, d \in M$.
- For a monoid $(M, *)$, we write M instead of $(M, *)$.

Remark. Any monoid M here is written additively, unless otherwise is specified: we denote the binary operation of M by $+$ instead of $*$.

Definition. Let M be a monoid.

- $\mathcal{U}(M)$ denotes the set of invertible elements of M.
- M is an (abelian) group if $\mathcal{U}(M) = M$.

Examples of Monoids

- The groups $(\mathbb{Z}, +)$ and $\mathbb{Z}/n\mathbb{Z}$ under modular addition (for every $n \in \mathbb{N}$).
- $\mathbb{N}_0$ and $\mathbb{Q}_{\ge 0}$ under the standard addition.
- $\mathbb{N}$ and $\mathbb{Q}_{\ge 1}$ under the standard multiplication.

Definition. A subset N of a monoid M is called a submonoid of M if N contains the identity element and is closed under the operation of M.

Remark. For $S \subseteq M$, the arbitrary intersection of (additive) submonoids of M containing S is also a submonoid of M and is denoted by $\langle S \rangle$.

Examples of Submonoids

- Additive submonoids of $\mathbb{N}_0$ are called numerical monoids.
  - $\mathbb{N}_0 \setminus \{1\}$ and $\{0\} \cup \mathbb{N}_{\ge n}$ (for every $n \in \mathbb{N}$).
- Additive submonoids of $\mathbb{Q}_{\ge 0}$ are called Puiseux monoids.
  - $\{0\} \cup \mathbb{Q}_{\ge 1}$ and $\left\langle \frac{1}{p} : p \in \mathbb{P} \right\rangle = \left\langle \left\{ \frac{1}{p} : p \in \mathbb{P} \right\} \right\rangle$.

Linearly Ordered Monoids

Definition. Let M be a monoid.

- M is torsion-free if for all $b, c \in M$ and $n \in \mathbb{N}$, the equality $nb = nc$ implies that $b = c$.
- The pair $(M, \preceq)$ is a linearly ordered monoid (LOM) if $\preceq$ is a total order relation on M such that for all $b, c, d \in M$, the inequality $b \prec c$ implies $b + d \prec c + d$.

Examples of LOMs

- Every Puiseux monoid under the standard order.
- Every submonoid of $(\mathbb{Z}^2, +)$ under the lexicographical order.

Theorem (Levi, 1913)

For a commutative monoid M, the following conditions are equivalent.

- *M can be turn into a LOM.*
- *M is cancellative and torsion-free.*

Difference Group and Rank

Definition. Let M be a monoid.

1. The group of formal differences of M is called its difference group and is denoted by $\mathcal{G}(M)$.
2. The rank of M is the rank of the abelian group $\mathcal{G}(M)$, which is the maximum size of an integrally independent set inside $\mathcal{G}(M)$.

Examples

- The rank-1 torsion-free monoids are precisely the submonoids of $(\mathbb{Q}, +)$.
- The rank-1 torsion-free monoids that are not groups are precisely the submonoids of $(\mathbb{Q}_{\geq 0}, +)$, i.e., the (nonzero) Puiseux monoids.

Rings, Integral Domains, and Fields

Definition. A (commutative) ring is a triple $(R, +, \cdot)$, where M is a set and $+$ and $\cdot$ are binary operation on M satisfying the following conditions.

- $(R, +)$ is an abelian group whose identity is denoted by 0.
- $(R, \cdot)$ is a monoid whose identity is denoted by 1.
- $+$ and $\cdot$ are distributive: $a(b + c) = ab + ac$ for all $a, b, c \in R$.

Examples

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are rings.
- $\mathbb{Z}[x]$ and $\mathbb{R}[x]$ are rings.

Definitions

1. An integral domain is a ring R such that for all $a, b \in R$ the equality $ab = 0$ implies that either $a = 0$ or $b = 0$, in which case, $(R \setminus \{0\}, \cdot)$ is called the multiplicative monoid of R.
2. A field is an integral domain such R that $(R \setminus \{0\}, \cdot)$ is an abelian group.

Examples

- $\mathbb{Q}$ and $\mathbb{R}$ are fields, while $\mathbb{Z}$ is an integral domain that is not a field.
- If R is an integral domain, then $R[x]$ is also an integral domain.

Monoid Algebras

Let R be a commutative ring, and let M be a commutative monoid.

Definition. The monoid algebra $R[M]$ of M over R is the commutative ring with identity consisting of all polynomial expressions in an indeterminate x with coefficients in R and exponents in M (under polynomial-like addition and multiplication).

Example. For $f := x^4 + x^{\frac{3}{2}}$ and $g := x^{\frac{3}{2}} + 1$ in the monoid algebra $\mathbb{Z}[\mathbb{Q}_{\geq 0}]$,

$$f + g = x^4 + 2x^{\frac{3}{2}} + 1 \quad \text{and} \quad f \cdot g = x^{4+\frac{3}{2}} + x^4 + x^3 + x^{\frac{3}{2}}.$$

Examples of Monoid Algebras

- The polynomial ring $R[x]$ is the monoid algebra $R[\mathbb{N}_0]$.
- The Laurent polynomial ring $R[x^{\pm 1}]$ is the monoid algebra $R[\mathbb{Z}]$.

Monoid Algebras Without Nonzero Zero-Divisors

Question. Which monoid algebras are integral domains?

Theorem (well-known)

Let R be a commutative ring, 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 turn into a LOM.*
- *R is an integral domain, and M is both cancellative and torsion-free.*

Definition. Let $R[M]$ be an integral monoid algebra, and let $(M, \preceq)$ be a LOM. Then every nonzero element $f \in R[M]$ can be written canonically as follows:

$$f = r_1 x^{m_1} + \cdots + r_k x^{m_k},$$

where $r_1 r_2 \cdots r_k \neq 0$ and $m_1 \succ m_2 \succ \cdots \succ m_k$. In this case,

- $\operatorname{supp} f := \{m_1, \dots, m_k\}$ is called the support of f, and
- $\deg f := m_1$ is called the degree of f.

Atomicity

Definition. Let M be a monoid.

1. $a \in M \setminus \mathcal{U}(M)$ is an atom (or an irreducible) if for any $b, c \in M$ the equality $a = b + c$ implies that either $b \in \mathcal{U}(M)$ or $c \in \mathcal{U}(M)$.
2. We let $\mathcal{A}(M)$ denote the set of atoms of M.
3. $b \in M$ is atomic if either b is a unit or $b = a_1 + \cdots + a_n$ for some $a_1, \dots, a_n \in \mathcal{A}(M)$.
4. M is atomic if every element of M is atomic.
5. An integral domain is atomic if its multiplicative monoid is atomic.

Examples

- Every numerical monoid N is atomic with $|\mathcal{A}(N)| < \infty$.
- The Puiseux monoid $M = \left\langle \frac{1}{p} : p \in \mathbb{P} \right\rangle$ is atomic with $\mathcal{A}(M) = \left\{ \frac{1}{p} : p \in \mathbb{P} \right\}$.
- $\mathbb{Q}_{\geq 0}$ is not atomic and $\mathcal{A}(\mathbb{Q}_{\geq 0})$ is empty ($q = \frac{q}{2} + \frac{q}{2}$ for all $q \in \mathbb{Q}_{>0}$).
- $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are atomic domains.
- $\mathbb{Z} + x\mathbb{Q}[x]$ is a non-atomic integral domain.

Ascent of Atomicity to Monoid Algebras (over $\mathbb{Q}$)

Question. Is the monoid algebra $\mathbb{Q}[M]$ atomic when M is atomic (and torsion-free)?

Remark. If M satisfies the ACCP, $\mathbb{Q}[M]$ also satisfies the ACCP, and so it is atomic.

Example. For $q \in (0,1) \cap \mathbb{Q}$ with $q^{-1} \notin \mathbb{N}$, the Puiseux monoid $M_q := \langle q^n : n \in \mathbb{N}_0 \rangle$ is atomic (but does not satisfy the ACCP).

Theorem (Bu-G.-Li-Zhao, PRIMES 2022)

The monoid algebra $\mathbb{Q}[M_{3/4}]$ is atomic.

Problem (Open Questions)

Let $(p_n)_{n \ge 0}$ be the strictly increasing sequence of odd primes, and let $q \in (0,1) \cap \mathbb{Q}$ with $q^{-1} \notin \mathbb{N}$.

1. *Is $\mathbb{Q}[M]$ atomic when $M = \left\langle \frac{1}{2^n p_n} : n \in \mathbb{N} \right\rangle$?*
2. *Is $\mathbb{Q}[M]$ atomic when $M = \left\langle \frac{1}{p_n p_{n+2}} : n \in \mathbb{N} \right\rangle$?*
3. *Is $\mathbb{Q}[M_q]$ atomic when $M_q := \langle q^n : n \in \mathbb{N}_0 \rangle$?*

Ascent of Atomicity to Monoid Algebras (over Finite Fields)

Question. For a finite field F, is the monoid algebra $F[M]$ atomic when M is atomic (and torsion-free)?

Theorem (Coykendall-G., 2019)

For every $p \in \mathbb{P}$, there exists an atomic torsion-free monoid M of rank at most 2 such that the monoid algebra $\mathbb{F}_p[M]$ is not atomic.

Problem (Open Questions)

Let $(p_n)_{n \geq 0}$ be the strictly increasing sequence of odd primes, and let $q \in (0, 1) \cap \mathbb{Q}$ with $q^{-1} \notin \mathbb{N}$.

1. *Is $\mathbb{F}_2[M]$ atomic when $M = \left\langle \frac{1}{2^n p_n} : n \in \mathbb{N} \right\rangle$?*
2. *Is $\mathbb{F}_2[M]$ atomic when $M = \left\langle \frac{1}{p_n p_{n+2}} : n \in \mathbb{N} \right\rangle$?*
3. *Is $\mathbb{F}_2[M_q]$ atomic when $M_q := \langle q^n : n \in \mathbb{N}_0 \rangle$?*

Ascent of Atomicity to Monoid Algebras (over Integral Domains)

Theorem (Coykendall-G., 2019)

There exists an atomic torsion-free monoid M with rank $\aleph_0$ such that the monoid algebra $R[M]$ is not atomic for any integral domain R.

Observations

- Pro 1: This theorem works not only for fields, but also for integral domains.
- Pro 2: The monoid M is somehow "universal": it does not depend on the choice of the integral domain R.
- Con: The monoid M is too big: it has infinite rank.

Here is a more recent result resolving the last con.

Theorem (G.-Rabinovitz, PRIMES 2023)

There exists an atomic rank-1 torsion-free monoid M such that the monoid algebra $R[M]$ is not atomic for any integral domain R.

A Weaker Notions of Atomicity: Almost Atomicity

Definition. Let M be a monoid.

- $b \in M$ is almost atomic if there exists an atomic element $c \in M$ such that $b + c$ is atomic.
- M is almost atomic if every element of M is almost atomic.
- An integral domain is almost atomic if its multiplicative monoid is almost atomic.

Remark. Every atomic monoid/domain is almost atomic.

Examples

- If $M := \langle \frac{1}{p} : p \in \mathbb{P} \rangle$, then the monoid $M \cup \mathcal{G}(M)_{\geq 1}$ is almost atomic but not atomic.
- $\mathbb{Z} + \mathbb{Z}x + x^2\mathbb{Q}[x]$ is an almost atomic integral domain that is not atomic.

Theorem (CrowdMath, 2024)

There exists an almost atomic rank-1 torsion-free monoid M such that the monoid algebra $\mathbb{F}_2[M]$ is not almost atomic.

A Weaker Notions of Atomicity: Quasi-Atomicity

Definition. Let M be a monoid.

- $b \in M$ is quasi-atomic if there exists $c \in M$ such that $b + c$ is atomic.
- M is quasi-atomic if every element of M is quasi-atomic.
- An integral domain is quasi-atomic if its multiplicative monoid is quasi-atomic.

Remark. Every almost atomic monoid/domain is quasi-atomic.

Examples

1. $\langle \mathbb{Z}[\frac{1}{2}]_{\ge 0} \cup \mathbb{Z}[\frac{1}{3}]_{\ge 4/3} \rangle$ is quasi-atomic but not almost atomic.
2. $\mathbb{Z} + \mathbb{Z}x + x^2\mathbb{R}[x]$ is quasi-atomic but not almost atomic.

Theorem (CrowdMath, 2024)

There exists a quasi-atomic rank-1 torsion-free monoid M such that the monoid algebra $\mathbb{F}_2[M]$ is not quasi-atomic.

References

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

J. G. Boynton and J. Coykendall, *On the graph divisibility of an integral domain*, Canad. Math. Bull. **58** (2015) 449–458.

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

CrowdMath 2024, *Generalizations of the Notion of Primes*, https://artofproblemsolving.com/polymath/mitprimes2024

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

F. Gotti, *On semigroup algebras with rational exponents*, Comm. Algebra **50** (2022) 3–18.

References

F. Gotti and H. Rabinovitz, *On the ascent of atomicity to one-dimensional monoid algebras*. Submitted. Preprint on arXiv: https://arxiv.org/abs/2310.18712.

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

N. Lebowitz-Lockard, *On domains with properties weaker than atomicity*, Comm. Algebra **47** (2019) 1862–1868.

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

J. Okninński, *Commutative monoid rings with krull dimension*. In: Semigroups Theory and Applications (Eds. H. Jürgensen, G. Lallement, and H. J. Weinert), pp. 251–259. Lecture Notes in Mathematics, vol. 1320. Springer, Berlin, Heidelberg, 1988.

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

End of Presentation

THANK YOU!