Prime Element Stability in Ring Extensions

Bofan Liu, Seabert Mao, and Michael Zhao
Mentors: Prof. Jim Coykendall and Jared Kettinger
PRIMES-USA

Fall-Term PRIMES Conference

October 18, 2025

Table of Contents

1. Background and Introduction
2. 1-Dimensional Integral Overrings
3. Stability via Conductor Coprimality
4. FCP Extensions
5. Acknowledgments and References

Background

- We will consider only commutative rings with identity.

Background

- We will consider only commutative rings with identity.

Definition

A zero divisor in a ring is an element r such that $rt = 0$ for some nonzero t.

Background

- We will consider only commutative rings with identity.

Definition

A zero divisor in a ring is an element r such that $rt = 0$ for some nonzero t.

Definition

A domain is a ring where the only zero divisor is 0.

Background

- We will consider only commutative rings with identity.

Definition

A zero divisor in a ring is an element r such that $rt = 0$ for some nonzero t.

Definition

A domain is a ring where the only zero divisor is 0.

- Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x, y]$

Background

- We will consider only commutative rings with identity.

Definition

A zero divisor in a ring is an element r such that $rt = 0$ for some nonzero t.

Definition

A domain is a ring where the only zero divisor is 0.

- Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x, y]$

Definition

A noninvertible element p of a ring R is prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Background

- We will consider only commutative rings with identity.

Definition

A zero divisor in a ring is an element r such that $rt = 0$ for some nonzero t.

Definition

A domain is a ring where the only zero divisor is 0.

- Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x, y]$

Definition

A noninvertible element p of a ring R is prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

- Ex. $2, 3, 5, 7, \cdots \in \mathbb{Z}, x \in \mathbb{Z}[x]$

Background

- We will consider only commutative rings with identity.

Definition

A zero divisor in a ring is an element r such that $rt = 0$ for some nonzero t.

Definition

A domain is a ring where the only zero divisor is 0.

- Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x, y]$

Definition

A noninvertible element p of a ring R is prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

- Ex. $2, 3, 5, 7, \cdots \in \mathbb{Z}, x \in \mathbb{Z}[x]$

Definition

We call a ring T a ring extension of R if R is a subring of T.

Background

- We will consider only commutative rings with identity.

Definition

A zero divisor in a ring is an element r such that $rt = 0$ for some nonzero t.

Definition

A domain is a ring where the only zero divisor is 0.

- Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x, y]$

Definition

A noninvertible element p of a ring R is prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

- Ex. $2, 3, 5, 7, \cdots \in \mathbb{Z}, x \in \mathbb{Z}[x]$

Definition

We call a ring T a ring extension of R if R is a subring of T.

- Ex. $\mathbb{Z} \subseteq \mathbb{Z}[i]$

Introducing the Problem

Question

Given a ring extension $R \subseteq T$ with p prime in R, when does p remain stable, or when is p prime, in intermediate rings $R \subseteq S \subseteq T$?

Introducing the Problem

Question

Given a ring extension $R \subseteq T$ with p prime in R, when does p remain stable, or when is p prime, in intermediate rings $R \subseteq S \subseteq T$?

Example

Consider $R = \mathbb{Z}$ and $T = \mathbb{Z}[i]$ for $p = 3$. Note that p is not prime in the intermediate ring $S = \mathbb{Z}[3i]$, as $(3i)^2 = -3 \cdot 3$ but $3 \nmid_{\mathbb{Z}[3i]} 3i$, so prime stability does not hold in this case.

Introducing the Problem

Question

Given a ring extension $R \subseteq T$ with p prime in R, when does p remain stable, or when is p prime, in intermediate rings $R \subseteq S \subseteq T$?

Example

Consider $R = \mathbb{Z}$ and $T = \mathbb{Z}[i]$ for $p = 3$. Note that p is not prime in the intermediate ring $S = \mathbb{Z}[3i]$, as $(3i)^2 = -3 \cdot 3$ but $3 \nmid_{\mathbb{Z}[3i]} 3i$, so prime stability does not hold in this case.

Theorem (de Castro, 2020)

Let $\mathbb{Z}[\omega]$ be a quadratic integer ring, and consider $\mathbb{Z} \subset \mathbb{Z}[n\omega] \subset \mathbb{Z}[\omega]$. Let $p \in \mathbb{Z}$ be prime in both $\mathbb{Z}$ and $\mathbb{Z}[\omega]$. Then p is prime in $\mathbb{Z}[n\omega]$ if and only if $\gcd(n, p) = 1$.

Prime Stability in 1-Dimensional Integral Overrings

Definition

A domain R is 1-dimensional if every nonzero prime ideal in R is maximal.

Prime Stability in 1-Dimensional Integral Overrings

Definition

A domain R is 1-dimensional if every nonzero prime ideal in R is maximal.

- $\mathbb{Z}, \mathbb{Q}[x]$ are both 1-dimensional.
- Every nonzero prime ideal in $\mathbb{Z}$ is (p) for some prime number p. If $x \notin (p)$, then $(p, x) = \mathbb{Z}$ according to Bezout's theorem, so (p) is maximal in $\mathbb{Z}$.

Prime Stability in 1-Dimensional Integral Overrings

Definition

A domain R is 1-dimensional if every nonzero prime ideal in R is maximal.

- $\mathbb{Z}, \mathbb{Q}[x]$ are both 1-dimensional.
- Every nonzero prime ideal in $\mathbb{Z}$ is (p) for some prime number p. If $x \notin (p)$, then $(p, x) = \mathbb{Z}$ according to Bezout's theorem, so (p) is maximal in $\mathbb{Z}$.

Definition

Let $R \subseteq T$ be domains. We say that T is an overring of R if T is a subring of the quotient field of R.

Prime Stability in 1-Dimensional Integral Overrings

Definition

A domain R is 1-dimensional if every nonzero prime ideal in R is maximal.

- $\mathbb{Z}, \mathbb{Q}[x]$ are both 1-dimensional.
- Every nonzero prime ideal in $\mathbb{Z}$ is (p) for some prime number p. If $x \notin (p)$, then $(p, x) = \mathbb{Z}$ according to Bezout's theorem, so (p) is maximal in $\mathbb{Z}$.

Definition

Let $R \subseteq T$ be domains. We say that T is an overring of R if T is a subring of the quotient field of R.

- $\mathbb{Z}[i]$ is not an overring of $\mathbb{Z}$ because $\mathbb{Z}[i]$ is not inside $Frac(\mathbb{Z}) = \mathbb{Q}$.
- $\mathbb{Z}[i]$ is an overring of $\mathbb{Z}[2i]$ because they have the same quotient field $\mathbb{Q}(i)$.

Prime Stability in 1-Dimensional Integral Overrings

Definition

Let $R \subseteq T$ be domains. We say that this extension is integral if every element of T is a root of a monic polynomial from $R[x]$.

Prime Stability in 1-Dimensional Integral Overrings

Definition

Let $R \subseteq T$ be domains. We say that this extension is integral if every element of T is a root of a monic polynomial from $R[x]$.

Example

In $\mathbb{Z}[i]$, the element i is a root of $x^2 + 1 = 0$. More generally, the element $a + bi \in \mathbb{Z}[i]$ is a root of $x^2 - 2ax + (a^2 + b^2) = 0$. Thus, the extension $\mathbb{Z} \subset \mathbb{Z}[i]$ is integral.

Prime Stability in 1-Dimensional Integral Overrings

Definition

Let $R \subseteq T$ be domains. We say that this extension is integral if every element of T is a root of a monic polynomial from $R[x]$.

Example

In $\mathbb{Z}[i]$, the element i is a root of $x^2 + 1 = 0$. More generally, the element $a + bi \in \mathbb{Z}[i]$ is a root of $x^2 - 2ax + (a^2 + b^2) = 0$. Thus, the extension $\mathbb{Z} \subset \mathbb{Z}[i]$ is integral.

Proposition

If $R \subseteq T$ is an integral extension, then $\dim(R) = \dim(T)$. Specifically, if R is 1-dimensional, then T is also 1-dimensional.

Prime Stability in 1-Dimensional Integral Overrings

Theorem (C-K-L-M-Z, 2025)

Let R be 1-dimensional and T be an integral overring of R. If p is prime in R and T, then p is prime in every intermediate ring S.

Prime Stability in 1-Dimensional Integral Overrings

Theorem (C-K-L-M-Z, 2025)

Let R be 1-dimensional and T be an integral overring of R. If p is prime in R and T, then p is prime in every intermediate ring S.

Example

Note that 3 is prime in $\mathbb{Z}$ and $\mathbb{Z}[i]$. According to de Castro's theorem, since $\gcd(3, 10) = 1$, we see that 3 is also prime in $\mathbb{Z}[10i]$. Our theorem tells us that 3 is prime in all intermediate rings between $\mathbb{Z}[10i]$ and $\mathbb{Z}[i]$, such as $\mathbb{Z}[5i]$.

Prime Stability in 1-Dimensional Integral Overrings

Theorem (C-K-L-M-Z, 2025)

Let R be 1-dimensional and T be an integral overring of R. If p is prime in R and T, then p is prime in every intermediate ring S.

Example

Note that 3 is prime in $\mathbb{Z}$ and $\mathbb{Z}[i]$. According to de Castro's theorem, since $\gcd(3, 10) = 1$, we see that 3 is also prime in $\mathbb{Z}[10i]$. Our theorem tells us that 3 is prime in all intermediate rings between $\mathbb{Z}[10i]$ and $\mathbb{Z}[i]$, such as $\mathbb{Z}[5i]$.

Example

Let $\mathcal{O}$ be an order in a number field K. If $p \in \mathcal{O}$ is a prime element then p remains prime in $\mathcal{O}_K$ and in every intermediate order $\mathcal{O} \subseteq S \subseteq \mathcal{O}_K$.

Prime Stability via Conductor Coprimality

Definition

Let $R \subseteq T$ be an extension. The conductor ideal $(R : T) := \{r \in R \mid rT \subseteq R\}$.

Prime Stability via Conductor Coprimality

Definition

Let $R \subseteq T$ be an extension. The conductor ideal $(R : T) := \{r \in R \mid rT \subseteq R\}$.

- Intuitively, the conductor ideal can be thought of the set of elements that pulls down the extension ring to the subring.
- The conductor ideal of $R \subseteq T$ is the largest ideal shared by R and T.

Prime Stability via Conductor Coprimality

Definition

Let $R \subseteq T$ be an extension. The conductor ideal $(R : T) := \{r \in R \mid rT \subseteq R\}$.

- Intuitively, the conductor ideal can be thought of the set of elements that pulls down the extension ring to the subring.
- The conductor ideal of $R \subseteq T$ is the largest ideal shared by R and T.

Example

Consider the extension $\mathbb{Z}[x^2, x^3] \subset \mathbb{Z}[x]$. The conductor is $x^2\mathbb{Z}[x]$ since $a \cdot \mathbb{Z}[x] \in \mathbb{Z}[x^2, x^3]$ for all $a \in x^2\mathbb{Z}[x]$. Additionally, we can show it covers all elements having that property.

Prime Stability via Conductor Coprimality

Theorem (C-K-L-M-Z, 2025)

Let $R \subseteq T$ be domains, let $p \in R$ be prime, and $I := (R : T) \neq 0$ such that $pR + I = R$. Then p remains prime in T and in every intermediate ring S.

Prime Stability via Conductor Coprimality

Theorem (C-K-L-M-Z, 2025)

Let $R \subseteq T$ be domains, let $p \in R$ be prime, and $I := (R : T) \neq 0$ such that $pR + I = R$. Then p remains prime in T and in every intermediate ring S.

Example

Let $K = \mathbb{Q}(\sqrt{5})$ and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Set

$$R = \mathbb{Z} + 6\mathcal{O}_K, \quad I = (R : \mathcal{O}_K) = 6\mathcal{O}_K,$$

and for each divisor $d \mid 6$, define

$$S_d = \mathbb{Z} + d\mathcal{O}_K.$$

Then the only intermediate rings are S_2 and S_3. Let $p = 7$. Since $\gcd(7, 6) = 1$, we have $7R + I = R$. Since 7 is prime in R, it is also prime in S_2, S_3, and $\mathcal{O}_K$.

Prime Stability via Conductor Coprimality

Example (Vanishing Conductor)

Consider the extension

$$R = \mathbb{Z}[2x] \subset T = \mathbb{Z}[x],$$

where T is an integral overring of R. Here the conductor is

$$I = (R : T) = \{t \in T \mid tT \subseteq R\} = 0,$$

so the conductor vanishes.

Prime Stability via Conductor Coprimality

Example (Vanishing Conductor)

Consider the extension

$$R = \mathbb{Z}[2x] \subset T = \mathbb{Z}[x],$$

where T is an integral overring of R. Here the conductor is

$$I = (R : T) = \{t \in T \mid tT \subseteq R\} = 0,$$

so the conductor vanishes. Let

$$p = 2x \in \mathbb{Z}[2x] = R.$$

In R, element p is prime because

$$\mathbb{Z}[2x]/(2x) \cong \mathbb{Z},$$

which is a domain. However, in $T = \mathbb{Z}[x]$, we can factor

$$2x = 2 \cdot x,$$

so p is no longer prime in T.

Prime Stability via Conductor Coprimality

Example

Let F be a field and set

$$R := F[x, y^2, y^3] \subset T := F[x,\ xy,\ y^2,\ y^3] \subset F[x, y],$$

Note that T is an integral overring of R.

Prime Stability via Conductor Coprimality

Example

Let F be a field and set

$$R := F[x, y^2, y^3] \subset T := F[x,\ xy,\ y^2,\ y^3] \subset F[x, y],$$

Note that T is an integral overring of R.
Take $p := x$. The conductor $I := (R : T)$ is nonzero. In fact one can check precisely that

$$I = (R : T) = (y^2, y^3).$$

Notice that

$$R/(x, I) \cong R/(x, y^2, y^3) \cong F,$$

so (x, I) is a proper ideal of R. Hence $xR + I \neq R$, i.e. x and the conductor I are not coprime.

Prime Stability via Conductor Coprimality

Example

Let F be a field and set

$$R := F[x, y^2, y^3] \subset T := F[x,\, xy,\, y^2,\, y^3] \subset F[x, y],$$

Note that T is an integral overring of R.
Take $p := x$. The conductor $I := (R : T)$ is nonzero. In fact one can check precisely that

$$I = (R : T) = (y^2, y^3).$$

Notice that

$$R/(x, I) \cong R/(x, y^2, y^3) \cong F,$$

so (x, I) is a proper ideal of R. Hence $xR + I \neq R$, i.e. x and the conductor I are not coprime. In R, the element x is prime because

$$R/(x) \cong F[y^2, y^3]$$

is a domain. However in T we have the factorization $xy^3 = (xy) \cdot y^2$, and x divides neither factor. Hence, x is not prime in T.

Prime Stability in FCP Extensions

Definition

A chain of rings is a set C of rings such that for all $R, T \in C$, we have that $R \subseteq T$ or $T \subseteq R$.

Prime Stability in FCP Extensions

Definition

A chain *of rings is a set C of rings such that for all $R, T \in C$, we have that $R \subseteq T$ or $T \subseteq R$.*

Definition

A ring extension T of R satisfies the Finite Chain Property *(FCP) if every chain of intermediate rings is finite.*

Prime Stability in FCP Extensions

Definition

A chain *of rings is a set C of rings such that for all $R, T \in C$, we have that $R \subseteq T$ or $T \subseteq R$.*

Definition

A ring extension T of R satisfies the Finite Chain Property *(FCP) if every chain of intermediate rings is finite.*

- An example of this is $\mathbb{Z}[30i] \subseteq \mathbb{Z}[i]$.

Prime Stability in FCP Extensions

Definition

A chain *of rings is a set C of rings such that for all $R, T \in C$, we have that $R \subseteq T$ or $T \subseteq R$.*

Definition

A ring extension T of R satisfies the Finite Chain Property *(FCP) if every chain of intermediate rings is finite.*

- An example of this is $\mathbb{Z}[30i] \subseteq \mathbb{Z}[i]$.
- A ring extension $R \subsetneq T$ is minimal if there are no intermediate rings $R \subsetneq S \subsetneq T$.

Prime Stability in FCP Extensions

Definition

A chain *of rings is a set C of rings such that for all $R, T \in C$, we have that $R \subseteq T$ or $T \subseteq R$.*

Definition

A ring extension T of R satisfies the Finite Chain Property *(FCP) if every chain of intermediate rings is finite.*

- An example of this is $\mathbb{Z}[30i] \subseteq \mathbb{Z}[i]$.
- A ring extension $R \subsetneq T$ is minimal if there are no intermediate rings $R \subsetneq S \subsetneq T$.
- Equivalently, we say that R and T are adjacent.

Prime Stability in FCP Extensions

Theorem (C-K-L-M-Z, 2025)

Let $R \subset T$ be adjacent rings, and let p be a prime in R. Then p is either prime or a unit in T.

Prime Stability in FCP Extensions

Theorem (C-K-L-M-Z, 2025)

Let $R \subset T$ be adjacent rings, and let p be a prime in R. Then p is either prime or a unit in T.

Theorem (C-K-L-M-Z, 2025)

If T is a ring extension of R satisfying FCP where $p \in R$ is prime in R and p is a non-unit of T, then p is prime in all intermediate rings.

Prime Stability in FCP Extensions

Theorem (C-K-L-M-Z, 2025)

Let $R \subset T$ be adjacent rings, and let p be a prime in R. Then p is either prime or a unit in T.

Theorem (C-K-L-M-Z, 2025)

If T is a ring extension of R satisfying FCP where $p \in R$ is prime in R and p is a non-unit of T, then p is prime in all intermediate rings.

Example

Consider the ring extension $\mathbb{Z}[ni] \subseteq \mathbb{Z}[i]$ for any positive integer n. This satisfies FCP, as all intermediate rings are of the form $\mathbb{Z}[di]$ for $d \mid n$, and so every chain has finite length. Therefore, if p is prime in $\mathbb{Z}[ni]$, then it is prime in every intermediate ring.

Prime Stability in FCP Extensions

Example

Note that $\mathbb{Z} \subseteq \mathbb{Z}\left[\frac{1}{n}\right]$ also satisfies FCP for any positive integer n, as all intermediate rings are of the form $\mathbb{Z}\left[\frac{1}{d}\right]$ for $d \mid n$, and so every chain has finite length. Furthermore, a prime p in $\mathbb{Z}$ and non-unit in $\mathbb{Z}\left[\frac{1}{n}\right]$ must satisfy $\gcd(p, n) = 1$, and therefore $\gcd(p, d) = 1$, so p is prime in $\mathbb{Z}\left[\frac{1}{d}\right]$. Therefore, this example satisfies the theorem.

Prime Stability in FCP Extensions

Example

Note that $\mathbb{Z} \subseteq \mathbb{Z}\left[\frac{1}{n}\right]$ also satisfies FCP for any positive integer n, as all intermediate rings are of the form $\mathbb{Z}\left[\frac{1}{d}\right]$ for $d \mid n$, and so every chain has finite length. Furthermore, a prime p in $\mathbb{Z}$ and non-unit in $\mathbb{Z}\left[\frac{1}{n}\right]$ must satisfy $\gcd(p, n) = 1$, and therefore $\gcd(p, d) = 1$, so p is prime in $\mathbb{Z}\left[\frac{1}{d}\right]$. Therefore, this example satisfies the theorem.

Example

For any positive integer n, define

$$R = \mathbb{Z} + x\mathbb{Q}[x], T = \mathbb{Z}\left[\frac{1}{n}\right] + x\mathbb{Q}[x].$$

All intermediate rings are of the form $\mathbb{Z}\left[\frac{1}{d}\right] + x\mathbb{Q}[x]$ for some $d \mid n$. We see that T is an extension of R satisfying FCP, so every element prime in R and non-unit in T must be prime in every intermediate ring as well.

Acknowledgments

- We would like to deeply thank our mentors, Jared Kettinger and Prof. Jim Coykendall, for guiding us along our research, giving insightful feedback to our presentation, and offering us encouragement.
- We would also like to thank the PRIMES program for making this experience possible by giving us this amazing research opportunity.
- Additionally, we would like to thank the PRIMES Conference organizers for giving us this opportunity to present our research.

References

[1] Robert Gilmer and Jack Ohm. Integral domains with quotient overrings. *Mathematische Annalen*, 153(2):97–103, 1964.

[2] David E. Dobbs. On chains of overrings of an integral domain. *Trends in Commutative Rings Research*, page 173, 2004.

[3] Paolo Zanardo. Intersections of powers of a principal ideal and primality. *Journal of Pure and Applied Algebra*, 188(1):287–304, 2004.

[4] Philip J. de Castro. Prime stability in intermediate extensions of integral domains. *Master's thesis*, Clemson University, 2020.

[5] David F. Anderson and David E. Dobbs. Pairs of rings with the same prime ideals. *Canadian Journal of Mathematics*, 32(2):362–384, 1980.

[6] David E. Dobbs, Gabriel Picavet, and Martine Picavet-L'Hermitte. Characterizing the ring extensions that satisfy FIP or FCP. *Journal of Algebra*, 371:391–429, 2012.

References

[7] Frank-Olaf Schreyer. Integral ring extensions and Krull dimension. In *An Introduction to Algebraic Geometry: A Computational Approach*, pages 69–78. Springer, 2025.

[8] David E. Dobbs. On the commutative rings with at most two proper subrings. *International Journal of Mathematics & Mathematical Sciences*, 2016.

[9] J. C. Robson. Prime ideals in intermediate extensions. *Proceedings of the London Mathematical Society*, 3(2):372–384, 1982.

[10] David E. Dobbs. When the juxtaposition of two minimal ring extensions produces no new intermediate rings. *Palestine Journal of Mathematics*, 6(1):31–44, 2017.

[11] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. 3rd edition. American Mathematical Society, Providence, RI, 2022.

Thank you!