PRIME ELEMENT STABILITY IN RING EXTENSIONS OF INTEGRAL DOMAINS

BOFAN LIU, SEABERT MAO, AND MICHAEL ZHAO

Abstract. The behavior of prime elements under ring extensions of integral domains is a fundamental topic in commutative algebra. Given an extension of integral domains $R \subseteq T$ and a prime element p of R, we identify conditions under which p remains prime in intermediate rings. Assuming that p is prime in T, we prove that p remains prime in every intermediate ring whenever T is an integral overring of a 1-dimensional domain R. Furthermore, we show that if p is coprime to the conductor of the extension $R \subseteq T$, then p remains prime in T and all intermediate rings. Next, with the help of a result on prime behavior in minimal extensions, we prove that this prime stability holds for any extension satisfying the FCP condition, i.e., every chain of distinct intermediate rings between R and T is finite. Finally, we determine that if an extension $R \subset T$ satisfies prime stability for a given prime element p and $v_p(r)$ is finite for all nonzero $r \in R$, then T must be an overring of R.

Contents

1. Introduction

In the field of commutative ring theory, the behavior of prime ideals in extensions of commutative rings has been studied extensively. Some of the most notable contributions have been made by Anderson and Dobbs in [**?**] and Robson in [**?**]. They have determined when commutative rings $R \subset T$ share the same prime ideals. In addition, they were able to expand this question to intermediate rings by determining when all three commutative rings $R \subset S \subset T$ share the same prime ideals.

Date: January 22, 2026.

Key words and phrases. integral domain, prime element, prime stability, intermediate ring, ring extension, integral overring, finite chain property (FCP), order.

Although in domains prime elements correspond to principal prime ideals, treating them directly highlights arithmetic phenomena not visible at the ideal level. More recently, prime elements have been considered in a few papers, such as [**?**] and [**?**, Lemma 4.7]. These include criteria for primality in orders of quadratic number fields and the stability of prime elements in the integral closure of a Noetherian domain.

Consider the ring extensions $\mathbb{Z} \subset \mathbb{Z}[3i] \subset \mathbb{Z}[i]$. The rational prime 3 is prime in $\mathbb{Z}$ and remains prime in $\mathbb{Z}[i]$, but it fails to be prime in the intermediate ring $\mathbb{Z}[3i]$ (indeed $(3i)^2 = -9 = 3 \cdot (-3)$ in $\mathbb{Z}[3i]$, yet $i \notin \mathbb{Z}[3i]$ so $3 \nmid 3i$ in $\mathbb{Z}[3i]$). Motivated by this example and the conjectures in [**?**], we investigate conditions ensuring that such instability cannot arise. We refer to this phenomenon as prime stability. Concretely, given an extension of domains $R \subset T$, we study when an element $p \in R$ that is prime in R (and possibly prime in T) remains prime in every intermediate ring S with $R \subseteq S \subseteq T$. We also determine various types of extensions that exhibit this form of stability. Throughout this paper, all rings are assumed to be integral domains.

The main results of this paper are as follows. In Section 3, we prove Conjecture 1.2.5 from [**?**]. This asserts that in 1-dimensional domains $R \subseteq T$ where T is an integral overring of R, if p is prime in R and T, then p is prime in all intermediate rings. In Section 4, we generalize a result inspired by Proposition 1.1.36 in [**?**]: if a prime element $p \in R$ is coprime to the conductor $(R : T)$, i.e. $pR + (R : T) = R$, then p remains prime in T and all intermediate rings. As an application, we show that if p is prime in an order of a number field, then p remains prime in the ring of integers and in all intermediate orders. This classical fact (see [**?**]) appears here as a special case of our theorem, thereby linking these commutative algebra inquiries with the field of algebraic number theory. In Section 5, we develop a tool for minimal extensions and show that the finite chain property (FCP), which asserts that every chain of intermediate rings is finite, provides an alternative sufficient condition for prime stability. We also combine several criteria characterizing FCP from [**?**] with our results. Finally, in Section 6, we consider the converse problem and determine that if an extension $R \subset T$ satisfies prime stability for a fixed p and $v_p(r)$ is finite for all nonzero $r \in R$, then T is necessarily an overring of R, showing that prime stability for a fixed element imposes strong structural constraints on the extension.

2. Preliminaries

To study how prime elements behave across ring extensions, we begin by recalling some basic notions from ring theory and dimension theory. These notions will serve as tools for formulating sufficient conditions with minimal restrictions. We start with the definition of the Krull dimension.

Definition 2.1. The *Krull dimension* or *dimension* of a ring R, denoted as $\dim R$, is the supremum of the numbers n for which there exists a chain of prime ideals

$$P_0 \subset P_1 \subset \cdots \subset P_n.$$

Consider a 1-dimensional ring R. From the definition, all nonzero prime ideals in R are maximal. This direct observation becomes crucial in Section 3.

Next, we define a couple of terms related to integrality.

Definition 2.2. Let $R \subseteq T$ be domains, and let t be any element of T. We say that t is *integral over* R if t is the root of some monic polynomial with coefficients in R. In addition, we say T is an *integral extension* of R if every element of T is integral over R.

The reason why integrality is crucial, specifically integral extensions, is because it preserves many ideal-theoretic properties. We can see this happen in [**?**].

Proposition 2.3 ([**?**])**.** *If $R \subseteq T$ is an integral ring extension, then* $\dim R = \dim T$.

Next, we define overrings, which also play a central role in our setup.

Definition 2.4. A ring extension T of a domain R is an *overring* of R if T is a subring of the quotient field of R.

Consider $R \subseteq T$, where T is an overring of R. The reason why overrings are important is that they allow us to assume that all the elements of intermediate rings are of the form $\frac{a}{b}$ where $a, b \in R$.

Finally, the conductor ideal measures how much structure the two rings share.

Definition 2.5. Let $R \subseteq T$ be an extension. The conductor ideal $I = (R : T) :- \{r \in R \mid rT \subseteq R\}$.

We can easily verify that $0 \in I$ since $0 \cdot T = 0 \in R$.

Thus, in a domain, we can rewrite

$$I :- \{0\} \cup \left\{ r \in R \setminus \{0\} \mid T \subseteq \frac{1}{r}R \right\}.$$

Notice that if conductor I is nonzero, then there exists an $r \in R \setminus \{0\}$ such that for all $t \in T$, we can write $t = \frac{s}{r}$ where $s \in R$. Therefore, we have the following.

Proposition 2.6. *Consider the extension $R \subseteq T$. If the conductor is nonzero, then T is an overring of R.*

When analyzing the structure of extensions, in Section 5, we consider the finiteness condition FCP, which limits the number or depth of intermediate rings.

Definition 2.7. A ring extension $R \subseteq T$ satisfies *FCP* if all chains of intermediate rings are finite.

In Section 6, the valuation $v_p(r)$ will play an important role as a key condition for our converse problem.

Definition 2.8. Let R be an integral domain, $p \in R$ a prime element, and $r \in R \backslash \{0\}$. We define the *p-valuation* of r, denoted $v_p(r)$, as

$$v_p(r) := \max\{n \in \mathbb{Z}_{\geq 0} \mid p^n \mid r \text{ in } R\}.$$

That is, $v_p(r)$ is the largest power of p dividing r in R.

3. Prime Element Stability in 1-dimensional Integral Overrings

Recall Conjecture 1.2.5 in [**?**].

Conjecture 3.1. *Suppose that T is an integral overring of a 1-dimensional domain R. If p is prime in both R and T, then p remains prime in every intermediate ring S with $R \subseteq S \subseteq T$.*

With the notation as in Conjecture 3.1, let $\frac{a}{b} \in T$ for some $a, b \in R$. We would like to be able to assume that one of a and b is not a multiple of p, as motivated by the following.

Remark 3.2. Let $a, b \in T$. Suppose that we have $\frac{a}{b}$ a multiple of p in T, so that $\frac{a}{b} = p \cdot \frac{c}{d}$ for some $c, d \in T$. We would like to simplify the equation to $ad = pbc$. From this we find that ad is a multiple of p in R, so a or d is a multiple of p in R. However, this information is not useful, as for example if a and b are both multiples of p so that $a = pa'$ and $b = pb'$ then

$$\frac{a}{b} = \frac{pa'}{pb'} = \frac{a'}{b'}$$

and then we have the same situation but with a and b replaced by a' and b', so no information is gained.

To avoid situations like this, we attempt to divide both a and b by p whenever a and b are multiples of p. For this process to always terminate, every element of R would need to have only finitely many factors of p. However, this condition does not hold for a general ring R.

Example 3.3. Consider the ring $R = \mathbb{Z} + x\mathbb{Q}[x]$. Then, the quotient $R/(2)$ is isomorphic to $\mathbb{Z}/(2)$, which is an integral domain since 2 is prime in $\mathbb{Z}$, so 2 is prime in R. However, we see that we can factor out infinitely many factors of 2 from x, as $x = 2^k \cdot \frac{x}{2^k}$ for all integers k. However, this does not satisfy the condition that R must be 1-dimensional, because in the ring $R = \mathbb{Z} + x\mathbb{Q}[x]$, we see that $(x)\mathbb{Q}[x]$ is a prime ideal of R contained in the prime ideal (2).

We now present the class of rings for which the undesirable situation in Example 3.3 does not occur.

Definition 3.4. A ring R is *Archimedean* if every element a has only finitely many powers of b dividing it for all $a, b \in R$, meaning that $\frac{a}{b^k} \notin R$ for some integer k.

Motivated by Example 3.3, we will show that if a ring is 1-dimensional, then it is Archimedean. The following can be found in [**?**] without proof, thus we will also provide a proof of the theorem.

Lemma 3.5. [**?**] *Any* 1*-dimensional ring* R *is Archimedean.*

Proof. Assume for the sake of contradiction that there exist $a, b \in R$ such that $\frac{a}{b^d} \in R$ for all integers d and b is not a unit. Let B be any maximal ideal of R containing (b), so that B is prime.

Now, consider the ideal

$$I = (a)R\left[\frac{1}{b}\right]$$

which is in R by the assumption. We see that $bI \subsetneq bR$, so as $bI = I$ we see that $I \subsetneq (b) \subseteq B$.

Let S be the multiplicatively closed set

$$\left\{1, b, b^2, b^3, \cdots\right\} \cdot (R \setminus B).$$

We claim that I avoids S. Assume for the sake of contradiction that I contains cb^k for some $c \in R \setminus B$ and some nonnegative integer k, so that $cb^k = ar$ for some $r \in R\left[\frac{1}{b}\right]$. Then, we see that $a\left(\frac{r}{b^k}\right) = c$ is in I, so it is in B, a contradiction, proving the claim.

Now, since there exists an ideal of R avoiding S, there exists an ideal J of R which is maximal with respect to avoiding S by Zorn's lemma on the nonempty partially ordered set under inclusion of ideals in R avoiding S. We see that J must be prime, as S is multiplicatively closed. Now, since J avoids S, which contains $R \setminus B$, we see that J is in B, but J also cannot contain b since $b \in S$, so B strictly contains J, a contradiction since both are prime. □

Remark 3.6. The set S naturally falls out of considering elements which are not in I, and it is "minimal" in some sense, as in this proof we cannot replace S with any smaller multiplicatively closed set.

Next, we provide a lemma which will be a central part of our ultimate proof in this section but is also interesting in its own right.

Lemma 3.7. *Let* $R \subseteq T$ *be an extension of* 1*-dimensional domains and* $p \in R$ *prime in* T*. Then, the following are equivalent:*

(1) p *is prime in* R*.*
(2) $pT \cap R = pR$*.*

Proof. We will show that (2) $\implies$ (1) directly and (1) $\implies$ (2) by contraposition.

First, assume that the second condition is true. This implies that for all $r \in R$ we have

$$p \mid_T r \implies p \mid_R r$$

Now, let $a, b \in R$ be such that $p \mid_R ab$. We would like to show that $p \mid_R a$ or $p \mid_R b$. Then, we see that $p \mid_T ab$, so $p \mid_T a$ or $p \mid_T b$. This implies that $p \mid_R a$ or $p \mid_R b$, implying that p is prime in R.

Now, assume that the second condition is not true. This implies that

$$pT \cap R \neq pR.$$

Since $pR \subseteq pT \cap R$, this implies that

$$pR \subsetneq pT \cap R.$$

Because R is 1-dimensional and $pT \cap R$ is a prime ideal in R, we see that pR cannot be prime, so p is not prime in R, so we are done. □

We now provide an example of the lemma.

Example 3.8. When $R = \mathbb{Z}[pi]$ and $T = \mathbb{Z}[i]$ where $p \in \mathbb{Z}$ is a prime in T, we see that p is not prime in R since $pi \cdot pi = -p^2$ is a multiple of p in R but $p \nmid_R pi$. Furthermore, we see that $pi \in R$ but $i \notin R$, in agreement with the theorem.

Lemma 3.7 allows us to quickly determine when p is prime in a smaller ring, a strong tool when it comes to proving that p is prime in an intermediate ring. We now prove Conjecture 1.2.5 from [**?**].

Theorem 3.9. *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.*

Proof. We see that $R \subseteq S$ and $S \subseteq T$ are integral extensions. From Proposition 2.3, we know that $\dim S = \dim R = 1$. Thus, we can apply Lemma 3.7 to the extension $S \subseteq T$, so that it suffices to show the following.

(*) If $t \in T$ satisfies $pt \in S$, then $t \in S$.

Write

$$t = \frac{b}{c}$$

for $b, c \in R$ with $c \neq 0$. Since R is 1-dimensional, by Lemma 3.5, it is Archimedean, so only finitely many powers of p divide b or c. Thus we can factor

$$b = p^r b', \quad c = p^s c',$$

where $p \nmid_R b', c'$. Therefore if $r \leq s$ we may divide a factor of p^r from both b and c and if $r \geq s$ then we may divide a factor of p^s from both b and c, so that we may assume p divides at most one of b and c.

We want to prove $p \nmid_R c$. For the sake of contradiction, assume that $p \mid_R c$. Then $c = pc_1$ with $c_1 \in R$. Thus

$$\frac{b}{p} = c_1 \cdot \frac{b}{c} \in T,$$

so

$$p \cdot \frac{b}{p} = b \in R.$$

Applying Lemma 3.7 to $R \subseteq T$ implies that $\frac{b}{p} \in R$, contradicting $p \nmid_R b$. Thus $p \nmid_R c$.

Notice that if there exist $d, e \in S$ such that $ptd + e = t$, then $t \in S$ since we know $pt \in S$. This is equivalent to

$$\frac{b}{c}(pd - 1) = -e \in S.$$

Thus, it suffices to show that there exists $d \in S$ such that $c \mid_S (pd - 1)$. Since $R \subseteq S$, it is sufficient that there exists $d \in R$ such that $c \mid_R (pd - 1)$.

Then, since pR is maximal in the 1-dimensional domain R and $c \notin pR$, we see that $pR + cR = R$, so there exist $k, d \in R$ with $ck + pd = 1$, or $pd - 1 = -ck$, implying that

$$c \mid_R (pd - 1).$$

Hence $t \in S$, establishing $(*)$.

By Lemma 3.7 for $S \subseteq T$, condition $(*)$ implies p is prime in S. Since S was arbitrary, p is prime in every intermediate ring. □

Notice that we only use the integrality of T over R to make sure that S is 1-dimensional. Thus, we have the following corollary.

Corollary 3.10. Let $R \subseteq T$ be 1-dimensional domains and T be an overring of R. If p is prime in R and T, then p is prime in every 1-dimensional intermediate ring S.

We now provide an example of Theorem 3.9.

Example 3.11. Let $F_0 \subset F_1 \subset F_2 \subset F_3 \subset \dots$ be algebraic field extensions. Now, consider the ring extension $R = F_0 + xF_1[x] + x^2F_2[x] + x^3F_3[x] + \cdots \subset L[x] = \bar{R}$. Note that $\bar{R}$ is a 1-dimensional integral overring of R. We can see that $1 + x$ is prime in R and $\bar{R}$, so $1 + x$ must be prime in all intermediate rings between R and $\bar{R}$.

The restriction to 1-dimensional domains in Theorem 3.9 is essential. If we drop the dimension condition while retaining the assumption that T is an integral overring of R, prime stability may fail. The following example illustrates this phenomenon.

Example 3.12. Let F be a field and set

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

Here T is an integral overring of R, since y is integral over R (satisfying $t^2 - y^2 \in R[t]$), and hence both S and T are integral over R. Note also that $\dim R = \dim T = 2$, so R is not 1-dimensional.

Consider $p := x \in R$. In R we have

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

which is an integral domain, so x is prime in R. Similarly, in $T = F[x, y]$ the ideal (x) is prime, since

$$T/(x) \cong F[y]$$

is a domain. However, in the intermediate ring S we have the factorization

$$xy^3 = (xy) \cdot y^2,$$

and x divides neither factor in S. Thus x is not a prime element of S.

4. Prime Element Stability via Conductor Coprimality

In light of Theorem 3.9, it is natural to ask under what other conditions would a prime p remain "stable". In this section, we focus on the role of the conductor in the behavior of prime elements under extensions of domains. Specifically, we show that when a prime element is "coprime" to the conductor of an extension, it remains prime not only in the extension itself but also in all intermediate rings. We begin with a motivating example that illustrates this phenomenon.

Example 4.1. Let $K = \mathbb{Q}(\sqrt{5})$ and $\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Set

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

and for each divisor $d \mid 6$ define

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

Then the only intermediate rings are S_2 and S_3. Let $p = 7$. Since $\gcd(7, 6) = 1$, we have $7R + I = R$, and one can check that 7 remains prime in R, S_2, S_3, and $\mathscr{O}_K$.

This example suggests that coprimality governs the stability of primality across intermediate rings. This phenomenon is not isolated; a related result appears in the arithmetic of rings of integers.

Proposition 4.2 ([?, Proposition 1.1.36])**.** *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 $\gcd(n, p) = 1$.*

Both Example 4.1 and Proposition 4.2 highlight the same underlying principle: a suitable coprimality condition can guarantee that a prime element remains prime in all intermediate rings. At the same time, they arise in different contexts. Proposition 4.2 treats towers of rings of integers and provides a precise equivalence, while Example 4.1 illustrates one direction of this behavior in a more general construction.

Motivated by these parallels, we abstract the coprimality condition into the language of conductors. This leads to the following general result.

Theorem 4.3. *Let $R \subseteq T$ be domains, $p \in R$ prime, and $I := (R : T) \neq 0$ such that $pR + I = R$. Then p remains prime in T and in every intermediate ring S with $R \subseteq S \subseteq T$.*

Proof. Since $pR + I = R$, there exist $v \in R$ and $u \in I$ such that

$$pv + u = 1.$$

Now suppose p divides ab in T, i.e., there exists $c \in T$ such that

$$pc = ab, \quad a, b, c \in T.$$

Multiplying both sides by u^2, we get

$$pcu^2 = (au)(bu).$$

Without loss of generality, assume p divides au (since p is prime in R). Then there exists $r \in R$ such that

$$pr = ua.$$

Now we have

$$pr + pva = ua + pva = a,$$

so

$$p(r + va) = a.$$

Thus p divides a in T, and therefore p is prime in T.

Let S satisfy $R \subseteq S \subseteq T$. Since the conductor grows with the ring, we have

$$I = (R : T) \subseteq (R : S) =: I_S.$$

Hence the same element $u \in I \subseteq I_S$ satisfies the same coprimality condition, so the argument of the above steps applies verbatim. It follows that p is prime in every intermediate ring S. □

The preceding theorem shows that if a prime element is coprime to the conductor, its primality is preserved across all intermediate rings. This theorem generalizes the phenomenon observed in Example 4.1 and Proposition 4.2, showing that the conductor plays a central role in controlling the stability of primes across intermediate rings. To illustrate the necessity of the coprimality condition with the conductor, we conclude with two counterexamples in which the condition fails and prime stability does not hold, even though T is an integral overring of R.

Example 4.4. 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

$$p = 2x \in R.$$

In R, element p is prime because

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

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

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

so p is no longer prime in T.

The preceding example shows that prime stability may fail when the conductor vanishes. For a second counterexample, we turn to a situation where the conductor is nonzero but the prime element is not coprime to it. Specifically, we return to the same extension

$$F[x, y^2, y^3] \subset F[x, xy, y^2, y^3] \subset F[x, y],$$

already considered in Example 3.12. In this instance, however, our emphasis is on the conductor and the failure of coprimality.

Example 4.5. 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 (indeed $R \subset T \subset F[x, y]$).

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 an integral 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.

This demonstrates that even with a nonzero conductor in an integral overring extension, the coprimeness requirement is still essential for prime stability.

We now illustrate how Theorem 4.3 applies in the classical setting of orders in algebraic number theory. We first recall the standard notion of an order in that context.

Definition 4.6. An order of an algebraic number field K is a subring $\mathscr{O} \subseteq \mathscr{O}_K$ which is also a $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

First we record the standard criterion from order theory that we will use as a hypothesis.

Theorem 4.7. [?, Theorem 6.1] *Let K be a number field, $\mathscr{O}$ an order in K, and $\mathfrak{f} = (\mathscr{O} : \mathscr{O}_K)$ the conductor. A nonzero prime ideal $\mathfrak{p}$ of $\mathscr{O}$ is invertible if and only if $\mathfrak{p} + \mathfrak{f} = \mathscr{O}$.*

Using this fact we immediately obtain the desired statement about prime elements.

Corollary 4.8. Let $\mathscr{O}$ be an order in a number field K with conductor $\mathfrak{f} = (\mathscr{O} : \mathscr{O}_K)$. If $p \in \mathscr{O}$ is a prime element then p remains prime in $\mathscr{O}_K$ and in every intermediate order $\mathscr{O} \subseteq S \subseteq \mathscr{O}_K$.

We give two complementary proofs. The first relies directly on Theorem 4.3, while the second combines the 1-dimensional result from the previous section with a lemma from the literature. In this way, we see two distinct applications of our stability criteria converging to the same corollary.

Proof A: Any principal fractional ideal is invertible, hence $p\mathscr{O}$ is invertible. Since p is a prime element, $p\mathscr{O}$ is a prime ideal of $\mathscr{O}$. And so by Theorem 4.7, $p\mathscr{O}$ is coprime to the conductor $\mathfrak{f}$. Applying Theorem 4.3, p is prime in $\mathscr{O}_K$ and every intermediate order S.

Proof B: Invoke the standard lemma ([?, Lemma 4.7]) that: if R is a Noetherian domain and T is the integral closure of R, then any prime element of R remains prime in T. In our situation $\mathscr{O}$ is an order (hence Noetherian), $\mathscr{O}_K$ is the integral closure of $\mathscr{O}$ (hence an integral overring), and both are 1-dimensional. Thus, any prime element $p \in \mathscr{O}$ remains prime in $\mathscr{O}_K$. Combining this with Theorem 3.9 shows that p remains prime in every intermediate order S.

This corollary is not new: it also follows from the classical theory of orders (see [?]). It shows that Theorem 4.3 together with the Theorem 3.9 generalize parts of that theory, illustrating the broad applicability of our stability criteria to phenomena in algebraic number theory.

5. Prime Element Stability under FCP

In this section, we will explore the finite property FCP, which states that the length of each chain of intermediate rings is finite.

The FCP property allows us to look at finite chains, specifically the minimal ring extensions that build them. In order to do this, we present the following lemma.

Lemma 5.1. *Let R be a domain with $p \in R$ prime. Then, if $R[a]$ is a simple extension of R satisfying*

$$R[pa] = R[a],$$

and for all $r \in R$ with $p \mid_{R[a]} r$ we have that $p \mid_R r$, then p is prime in $R[a]$.

Proof. If $s = \sum_{k=0}^{d} r_k(pa)^k$ is some element of $R[pa]$ for $r_0, r_1, \ldots, r_d \in R$, then we note that

$$s - r_0 = p\left(\sum_{k=1}^{d} r_k p^{k-1} a^k\right).$$

This is a multiple of p in $R[pa]$, as $\sum_{k=1}^{d} r_k p^{k-1} a^k \in R[a]$ and $R[a] = R[pa]$. Therefore, whenever $r_0, r_1, \ldots, r_d \in R$ are such that $s = \sum_{k=0}^{d} r_k(pa)^k$, we see that s is a multiple of p in $R[pa]$ if and only if r_0 is a multiple of p in $R[pa]$, which occurs if and only if r_0 is a multiple of p in R by assumption.

Now if $b = \sum_{k=0}^{d} b_k(pa)^k$ and $c = \sum_{k=0}^{d} c_k(pa)^k$ are some elements of $R[pa]$, then $bc = \sum_{k=0}^{2d} x_k(pa)^k$, where $x_k = \sum_{j=0}^{k} b_j c_{k-j}$ where $b_j = c_j = 0$ for all $j \geq d$. Now bc is a multiple of p in $R[pa]$ if and only if $x_0 = b_0 c_0$ is a multiple of p in R. Since p is prime in R we see that b_0 or c_0 is a multiple of p in R, implying that b or c is a multiple of p in $R[pa]$. This means that p is prime in $R[pa]$, proving the lemma. □

Utilizing this lemma, we now get the following result on minimal ring extensions.

Theorem 5.2. *Let $R \subset T$ be a minimal extension of domains, and let p be a prime element in R. Then p is prime or a unit in T.*

Proof. Since T is a minimal extension of R, we see that $T = R[a]$ for some element $a \in T$. Then consider the ring

$$R[pa],$$

which satisfies $R \subseteq R[pa] \subseteq R[a]$. If $R[pa] = R[a]$, then by Lemma 5.1 we see that p is prime in T or there exists $r \in R$ such that $\frac{r}{p} \in T$ but $\frac{r}{p} \notin R$. Otherwise, we see that $R[pa] = R$, in which case if we let $r = pa \in R$ then $\frac{r}{p} \in T$ but $\frac{r}{p} \notin R$. In either case we get that p is prime in T or there exists $r \in R$ which is not a multiple of p in R such that $T = R\left[\frac{r}{p}\right]$. We will prove that in this case, we must have that p is a unit.

Now, consider the ring

$$R\left[\frac{r^2}{p}\right].$$

Since p is prime in R and r is not a multiple of p in R, it follows that r^2 is not a multiple of p in R. Therefore $R \subsetneq R\left[\frac{r^2}{p}\right] \subseteq T$, so we must have that $R\left[\frac{r^2}{p}\right] = R\left[\frac{r}{p}\right]$, meaning that $\frac{r}{p}$ is in $R\left[\frac{r^2}{p}\right]$. Hence, there exist $a_0, a_1, \ldots, a_d \in R$ such that

$$\sum_{k=0}^{d} a_k \left(\frac{r^2}{p}\right)^k = \frac{r}{p}.$$

Dividing by r gives that

$$\frac{a_0}{r} + \left(\sum_{k=1}^{d} a_k r^{k-1} \left(\frac{r}{p} \right)^k \right) = \frac{1}{p}.$$

Therefore, it suffices to prove that $\frac{a_0}{r} \in R$, as then we have that $\frac{1}{p} \in T$ and so p is a unit in T.

Assume for the sake of contradiction that $\frac{a_0}{r}$ is not in R. Rearranging the equation gives that

$$\frac{a_0}{r} = \frac{1}{p} - \left(\sum_{k=1}^{d} a_k r^{2k-1} \left(\frac{1}{p} \right)^k \right),$$

implying that $\frac{a_0}{r} \in R\left[\frac{1}{p}\right]$. Then, we see that as $\frac{a_0}{r}$ is in $R\left[\frac{1}{p}\right]$ but not in R, it is equal to $\frac{b}{p^d}$ for some $b \in R$ which is not a multiple of p and some positive integer d. Then, we see that $\frac{a_0}{r} = \frac{b}{p^d}$ gives that $a_0 p^d = br$. The left hand side is a multiple of p in R but the right hand side is not, a contradiction, so $\frac{a_0}{r} \in R$, proving the theorem. □

Notice that this result is especially strong because it makes few assumptions about the nature of R and T. A natural application can be seen in the proof of the following theorem, which presents alternate conditions that imply prime stability in all intermediate rings.

Theorem 5.3. *If an extension $R \subset T$ satisfies FCP and p is prime in R and not a unit in T, then p is prime for all intermediate rings.*

Proof. Consider any intermediate ring S satisfying $R \subseteq S \subseteq T$. We first prove that there exists a chain $R = S_0 \subset S_1 \subset \cdots \subset S_n = T$ such that S_k and S_{k+1} are adjacent for $k = 0, 1, \ldots, n-1$. Consider the partially ordered set of all chains of rings which start at R, include S, and end at T ordered under inclusion. Notice that every chain of chains has an upper bound given by the union of all chains in the chain. Therefore, by Zorn's lemma, we see that there exists a maximal element of this partially ordered set. We claim that if this maximal element is the chain $R = S_0 \subset S_1 \subset \cdots \subset S_n = T$, then S_k and S_{k+1} are adjacent for $k = 0, 1, \ldots, n-1$. Indeed, if there exists a ring $S_k \subset S' \subset S_{k+1}$, then

$$S_0 \subset S_1 \subset \cdots \subset S_k \subset S' \subset S_{k+1} \subset S_{k+2} \subset \cdots \subset S_n$$

is a greater chain in the partially ordered set, a contradiction, so S_k and S_{k+1} must be adjacent.

Now, we claim that p must be prime in S_k for all $k = 0, 1, \ldots, n$, implying in particular that p is prime in S. Assume for the sake of contradiction that this is not true, and consider k minimal for which p is not prime in S_k. Note that $k \neq 0$ by assumption, and so S_{k-1} must exist and p must be prime in S_{k-1}. Now, by Theorem

5.2 we see that p must be either prime or a unit in S_k, so p is a unit in S_k. Therefore $p^{-1} \in S_k \subseteq T$, but p is not a unit in T, a contradiction, proving the theorem. □

Building on the existing FCP literature and Theorem 5.3, we obtain a criterion that ensures prime stability in certain rings. In particular, Theorem 4.2 in [**?**] characterizes FCP, which allows us to deduce a corollary regarding prime stability under these conditions.

Corollary 5.4. Let $R \subset T$ be an extension with p prime in R and $C := (R : T)$. If T is a finitely generated R-module and R/C is an Artinian ring, then p remains prime in every intermediate ring extension $R \subset S \subset T$.

6. A Necessary Condition for Prime Stability

Now that we have three sets of conditions that imply prime stability, a natural follow-up to our previous sections is to find a necessary condition for prime stability. Specifically, in this section, we want to answer the following question.

Question 6.1. *Given an extension $R \subseteq T$, if $p \in R$ is a fixed prime element in both R and T and remains prime in every intermediate ring S with $R \subseteq S \subseteq T$, then what can we say about the extension?*

Notice that all three sets of sufficient conditions either require or imply the larger ring is an overring. In Section 3, our conditions were 1-dimension, integral, and overring. In Section 4, our condition was conductor coprimality which will only occur for a nonzero conductor, so from Proposition 2.6, overring is implied. In Section 5, we used the FCP to prove prime stability. However, from [**?**], in a minimal extension $R \subset R'$ where R' is a domain, either both R and R' are fields or R' is an overring of R. Since R and R' are not fields or else all elements would be a unit, we have R' must be an overring of R. Under the FCP condition, there exists a finite chain from R to T formed by minimal extensions, each being an overring, which implies that T is an overring of R.

This observation motivates us to ask whether overring is implied from prime stability. From this question, we have the following theorem.

Theorem 6.2. *Let $R \subseteq T$ be an extension of domains, and let $p \in R$ be a fixed prime element in both rings. If p remains prime in every intermediate ring S with $R \subseteq S \subseteq T$, and $v_p(r)$ is finite for all nonzero $r \in R$, then T must be an* overring *of R.*

To prove this theorem, we first establish a few useful lemmas.

Lemma 6.3. *Let $R \subseteq T$ be domains, and let $p \in R$ be prime in all intermediate rings between R and T, including R and T. If t is an element of T but not of R, then t is the root of some polynomial*

$$x = c_0 + c_1 px + px^2 Q(x)$$

for some $c_0, c_1 \in R$ and $Q \in R[x]$.

Proof. Consider the ring $R[pt, pt^2]$, which contains R but is contained in T. By assumption we have that p is prime in this ring, and furthermore note that

$$(pt)^2 = p \cdot pt^2$$

is a multiple of p, so pt is a multiple of p in this ring. This implies that $t \in R[pt, pt^2]$, so that t is equal to some polynomial in $R[x, y]$ evaluated at $x = pt$ and $y = pt^2$. This implies

$$t = c_0 + c_1 pt + pt^2 Q(t)$$

for some $c_0, c_1 \in R$ and $Q \in R[x]$, proving the lemma. □

Lemma 6.4. *Let R be a domain with fraction field K, and let $p \in R$ be a prime such that $v_p(r)$ is finite for all $r \in R$. Let $R' = R_{(p)}$. Then for any nonzero polynomial $P(x) \in K[x]$, there exists a unique minimal integer n, not necessarily nonnegative, such that*

$$P^*(x) := p^n P(x) \in R'[x].$$

Furthermore $P^*(x)$ is nonzero modulo p. Also, we let $P^*(x) = 0$ if $P(x) = 0$.

Proof. If $P(x) = 0$ then $P^*(x) = 0$ is unique. Otherwise, define $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$ for $a, b \in R$. Then the minimal n for which $p^n P(x) \in R'(x)$ is the negative of the minimal $v_p(c)$ over all nonzero coefficients c of P. Then $p^n P(x) \in R'[x]$ is nonzero modulo p because otherwise we could decrease n by 1 and still have $p^n P(x) \in R'[x]$. Uniqueness of n follows from the minimality condition. □

Lemma 6.5. *Let R be a domain with fraction field K, and let p be a prime in R such that $v_p(r)$ is finite for all $r \in R$. Also, let $R' = R_{(p)}$. Then for all $A, B, C \in K[x]$ such that $A(x)B(x) = C(x)$, we have that $A^*(x)B^*(x) = C^*(x)$. In other words, we have that*

$$A^* B^* = (AB)^*.$$

Proof. First, if $A(x) = 0$ or $B(x) = 0$ then $C(x) = A(x)B(x) = 0$, and so $C^*(x) = 0 = A^*(x)B^*(x)$. Otherwise, let $A^*(x) = p^a A(x)$ and $B^*(x) = p^b B(x)$. Now, note that p is prime in R and therefore prime in R' from the correspondence between prime ideals in R avoiding (p) and prime ideals in R', so that it is prime in $R'[x]$ as well. Therefore, we see that $R'[x]/pR'[x]$ is a domain. This means that since A^* and B^* are nonzero modulo p, we must have that

$$A^*(x)B^*(x) = p^{a+b} A(x)B(x)$$

must be nonzero modulo p, which by Lemma 6.4 implies that in fact

$$A^*(x)B^*(x) = p^{a+b} A(x)B(x) = C^*(x),$$

proving the lemma. □

Now, we will prove the theorem.

Proof. We argue by contradiction. Assume there exists

$$t \in T \setminus K.$$

First, we notice that by Lemma 6.3 we have that t is algebraic over R, and therefore there exist $c_0, c_1, \ldots, c_d \in R$ such that

$$c_0 + c_1 t + c_2 t^2 + \cdots + c_d t^d = 0.$$

Multiplying this by c_d^{d-1}, we see that

$$c_0 c_d^{d-1} + c_1 c_d^{d-2} (c_d t) + c_2 c_d^{d-3} (c_d t)^2 + \cdots + (c_d t)^d = 0.$$

In particular, we see that if

$$a = c_d t$$

then a is integral over R, but a is not in K. This implies that a is algebraic over K and has a nonlinear minimal polynomial

$$Q(x) \in K[x].$$

Consider $R' := R_{(p)}$. All the conditions of Lemma 6.4 are satisfied, so we can define

$$Q^*(x) \in R'[x].$$

Because $Q(x)$ is the minimal polynomial of a over K, any other polynomial in $K[x]$ that vanishes at a is divisible by $Q(x)$ in $K[x]$. In particular, since a is integral over R there exists a monic polynomial $B(x) \in R[x] \subseteq R'[x]$ with a as a root. Then there exists some $S(x) \in K[x]$ with

$$Q(x)S(x) = B(x),$$

and so by Lemma 6.5 we have that

$$Q^*(x)S^*(x) = B^*(x).$$

Since $B(x) \in R'[x]$ is monic, it is nonzero modulo p, so by Lemma 6.4 we get that

$$B^*(x) = B(x),$$

and therefore

$$Q^*(x)S^*(x) = B(x).$$

In particular, in R', the leading coefficient of $Q^*(x)$ divides the leading coefficient of $B(x)$, which is 1, so the leading coefficient of $Q^*(x)$ is a unit of R'.

Now, again by Lemma 6.3, we see that a satisfies

$$a = a_0 + a_1 pa + pa^2 P(a)$$

for some $a_0, a_1 \in R'$ and $P \in R'[x]$, and so a is the root of some polynomial

$$A(x) = a_0 + (a_1 p - 1)x + px^2 P(x) \in R'[x],$$

where $P(x) \in R'[x]$ is nonzero. Then since $Q(x)$ is the minimal polynomial of a in $K[x]$, we see that there exists $U(x) \in K[x]$ such that

$$Q(x)U(x) = A(x),$$

so that by 6.5 we have that

$$Q^*(x)U^*(x) = A^*(x).$$

Now $A(x) \in R'[x]$ has x coefficient equivalent to $-1 \pmod p$, and therefore $A(x)$ is nonzero modulo p. Then by Lemma 6.4 we must have that

$$A^*(x) = A(x),$$

and so

$$Q^*(x)S^*(x) = A(x).$$

Now reduce this equality modulo p. The right-hand side becomes

$$\overline{A}(x) \equiv a_0 - x \pmod p,$$

and thus $\overline{A}(x)$ is a degree 1 polynomial in $(R'/(p))[x]$.

On the other hand, $Q^*(x)$ has a leading coefficient which is a unit and therefore nonzero modulo p, so the degree of the reduction $\overline{Q^*}(x)$ modulo p is the same as the degree of Q^*, which is at least 2 because otherwise t would be in K. Now the reduction $\overline{U^*}(x)$ of $U^*(x)$ modulo p is nonzero by Lemma 6.4. Then

$$\overline{Q^*}(x) \cdot \overline{U^*}(x)$$

has degree at least 2, contradicting the fact that $\overline{A}(x) = a_0 - x$ has degree 1. Therefore no such t exists, so T is an overring of R. □

Notice that Archimedean implies finite $v_p(r)$ by definition. Additionally, from Lemma 3.5, we know that all 1-dimensional rings are Archimedean. Combining with Theorem 3.9, we obtain the following corollary.

Corollary 6.6. Let $R \subseteq T$ be 1-dimensional integral domains, and let $p \in R$ be prime in both R and T. Then p remains prime in all intermediate rings if and only if T is an *overring* of R.

The contrapositive of Theorem 6.2 can also be useful to show prime stability does not hold in an extension, as shown in the following example.

Example 6.7. Let $K \subset L$ be fields. Notice that $L[x]$ is not an overring of $K[x]$, since the coefficients of elements in $L[x]$ may not lie in $Frac(K) = K$.

Let p be a prime element in $K[x]$, equivalently an irreducible polynomial in $K[x]$. Similarly, a prime element in $L[x]$ is just an irreducible polynomial in $L[x]$. Observe that $\deg(p) \geq 1$, so for any $r \in K[x]$, the p-adic valuation $v_p(r)$ is finite. Hence, by the contrapositive of Theorem 6.2, there does not exist an element p that is simultaneously prime in $K[x]$, $L[x]$, and all intermediate rings $K[x] \subseteq S \subseteq L[x]$.

Acknowledgements

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 report, 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.

Bofan Liu: Seven Lakes High School, Katy, TX 77494
Email address: liubofan@live.com

Seabert Mao: Saratoga High School, Saratoga, CA 95070
Email address: seabertmao@gmail.com

Michael Zhao: Westwood High School, Austin, TX 78750
Email address: zhaom901@gmail.com