Theory of Factorization

Jim Coykendall

May 26, 2005

Chapter 1

Need to Know Ring Theory

1.1 Basics and Definitions

Unless otherwise indicated we will consider all rings to be commutative with identity $1_R \neq 0$. But before we get the carried away, we consider the following definition.

Definition 1.1.1. *A ring is a set equipped with two binary operations* $(+, \cdot)$ *such that for all* $r, s, t \in R$ *we have the following.*

a) $r+(s+t)=(r+s)+t$.

b) $r+s=s+r$.

c) There exists an element $0 \in R$ *such that* $0 + r = r$ *for all* $r \in R$.

d) For all $r \in R$ *there exists an element* $s \in R$ *such that* $s + r = 0$.

e) $r(st)=(rs)t$.

f) $r(s+t)=rs+rt$.

Additionally if

g) $rs=sr$ *for all* $r, s \in R$

we say that R *is commutative. And if we have the following condition.*

h) There exists $1_R \in R$ *such that* $1_R r = r = r1_R$ *for all* $r \in R$.

Then we say that R *has an identity.*

Example 1.1.2. $\mathbb{Z}$ *is a ring with identity and* $2\mathbb{Z}$ *is a ring without identity.* $M_2(\mathbb{Z})$ *is a noncommutative ring. For commutative examples, consider* $\oplus\mathbb{Z}$, $\prod \mathbb{Z}$, $\mathfrak{C}(0,1)$ *(continuous functions on* $(0,1)$*),* $\mathbb{R}, \mathbb{Q}, \mathbb{C}$, *and* $\mathbb{Z}_n$.

Very loosely speaking, a ring is a mathematical structure where one can add and multiply. Still loosely, but a bit more precisely, a ring is an abelian group under addition with an extra multiplicative structure (that is compatible with the multiplicative structure via the distributive property).

From one point of view here is a "best case scenario" (or perhaps a worst case scenario).

Definition 1.1.3. *A ring, R, is a division ring if every nonzero element of R has a multiplicative inverse (if $x \neq 0$ then there exists $y \in R$ such that $xy = yx = 1_R$).*

We remark here that if $xy = yx = 1$ we often write x^{-1} instead of y. We also point out that a commutative division ring is referred to as a field.

A number of the examples previously listed (e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) are fields. The study of factorization is the study of the multiplicative structure of a ring. The "more interesting" rings from a factorization point of view are the rings which are not fields.

This course will be devoted to the theory of factorization, that is, we will be studying rings via their the multiplicative structure. We will begin by covering some basic concepts; we close this section with a final definition.

Definition 1.1.4. *Let R be a commutative ring with identity. An element $a \in R$ is said to be a zero-divisor if there is a nonzero $b \in R$ such that $ab = 0$. R is said to be an integral domain if 0 is the only zero-divisor in R.*

Most of this course will concentrate on factorization in integral domains.

1.2 Ideals and Their Flavors

Ideals are central in the study of the structure of rings. Ideals are the analog of the "normal subgroup" concept in group theory.

Definition 1.2.1. *Let R be a ring. A nonempty subset $I \subseteq R$ is said to be an ideal if for all $x, y \in I$ and $r \in R$*

a) $x - y \in I$, and

b) $rx \in I$.

Example 1.2.2. *Prove that in $\mathbb{Z}$, every ideal is generated by a single element (that is, any ideal is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.*

Definition 1.2.3. *Let $I \subseteq R$ be an ideal. If $I = \langle S \rangle = \{\sum_{i=0}^{n} r_i s_i | r_i \in R, s_i \in S\}$, we say that I is generated by S.*

We remark here that

$$\langle S \rangle = \bigcap_{I \supseteq S} S$$

that is, the ideal generated by S is the intersection of all ideals that contain the set S.

Definition 1.2.4. *Let $I \subseteq R$ be an ideal and $I = \langle S \rangle$.*

a) If $ab \in I \Longrightarrow a \in I$ or $b \in I$ then we say that I is prime.

b) If I is a proper ideal and $I \subseteq J \subseteq R \Longrightarrow I = J$ or $I = R$ then we say that I is maximal.

c) If $a^n \in I \Longrightarrow a \in I$ then we say that I is a radical ideal.

d) If $ab \in I$ and $a \notin I \Longrightarrow b^n \in I$ then we say that I is primary.

e) If $|S| = 1$ we say that I is principal.

Example 1.2.5. *Characterize the prime, primary, radical, and maximal ideals in $\mathbb{Z}$. Attempt the same for $\mathbb{Q}[x]$ and $\mathbb{Q}[x, y]$. Give examples that show these concepts are distinct.*

We recall the quotient ring structure. The next theorem is given without proof, but the reader should go through the straightforward proof.

Theorem 1.2.6. *If $I \subseteq R$ is an ideal, then the abelian group R/I is a ring with multiplication given by*

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I.$$

Here is a useful result showing the interplay between ideal structure and the structure of the resulting quotient ring.

Theorem 1.2.7. *Let $I \subseteq R$ be an ideal.*

a) I is maximal if and only if R/I is a field.

b) I is prime if and only if R/I is an integral domain.

c) I is radical if and only if R/I is a reduced (that is, R possesses no non-trivial nilpotents).

d) I is primary if and only if every zero divisor in R/I is nilpotent.

Proof. For a) Suppose that I is maximal and consider a nonzero element of $r + I \in R/I$. Since $r \notin I$, we have that $(I, r) = R$ and hence there is an $x \in R$ and $\alpha \in I$ such that $rx + \alpha = 1$. This means that in R/I the cosets $r + I$ and $x + I$ are inverses. For the converse, suppose that R/I is a field and suppose that $I \subsetneq J$. Select $x \in J \setminus I$ Since R/I is a field, $x + I$ has an inverse (say $y + I$). Since $xy + I = 1 + I$ we have that $(I, x) = R$. Since $(I, x) \subseteq J$, we must have that $J = R$ and this establishes part a).

For b) Suppose that I is prime and consider nonzero elements of $r+I, s+I \in R/I$. We suppose that $(r+I)(s+I) = 0+I$. Equivalently, we have that $rs \in I$, and since I is prime, we have that $r \in I$ without loss of generality. Hence the coset $r + I = 0 + I$ and R/I is an integral domain. For the converse, suppose that R/I is an integral domain and suppose $ab \in I$. Hence in R/I we have that

$(a+I)(b+I) = 0+I$; since R/I is a domain, it is immediate that $a \in I$ or $b \in I$. This establishes part b).

For c) Suppose that I is radical and suppose that $r+I \in R/I$ is nilpotent. Since $r^n + I = 0 + I$, we have that $r^n \in I$. Because I is radical, we have that $r \in I$ and hence $r + I = 0 + I$. For the converse, suppose that R/I is reduced and that $r^n \in I$. In R/I we have that $r^n + I = 0 + I$. Since R/I is reduced, $r + I = 0 + I$ implying that $r \in I$. This establishes part c).

For d) Suppose that I is primary and suppose that $r + I \in R/I$ is a zero divisor. Let $x + I$ be a nonzero coset such that $rx + I = 0 + I$. Since $x \notin I$ it must be the case that $r^n \in I$ and so $r + I$ is nilpotent. For the converse, suppose that in R/I every zero divisor is nilpotent. Let $ab \in I$ and assume that $a \notin I$. In the quotient ring this means that $b + I$ is a zero divisor. Since $b + I$ is nilpotent, we have that $b^n \in I$. This establishes part d).

□

Here is a useful corollary.

Corollary 1.2.8. *Let $I \subseteq R$ be an ideal. If I is maximal, then I is prime. If I is prime, then I is radical. If I is both radical and primary, then I is prime.*

Proof. Any field is an integral domain; any integral domain is reduced. Additionally, a reduced ring where every zero-divisor is nilpotent is a domain. □

For the next result (and a number of others) we will need the following formulation of the axiom of choice known as Zorn's Lemma.

Zorn's Lemma: Let S be a partially ordered set with the property that every chain in S has an upper bound in S. Then S has a maximal element.

Proof. Don't even try. □

Theorem 1.2.9. *If R is commutative with identity, and I is a proper ideal of R, then there is a maximal ideal of R containing I. In particular, every commutative ring with identity has a maximal ideal.*

Proof. Let $I \subsetneq R$ be a proper ideal. We consider the set

$$S = \{J | I \subseteq J \subsetneq R\}$$

of proper ideals containing I. The set S is partially ordered by inclusion. To apply Zorn's Lemma, we need to show that any chain in S has an upper bound. Let $\mathfrak{C}$ be a chain (linearly ordered subset) in S. Note that for all $I_\alpha, I_\beta \in \mathfrak{C}$ either $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$.

Consider the ideal

$$L = \bigcup_{I \in \mathfrak{C}} I.$$

Since the chain is linearly ordered, L is an ideal. Additionally L is clearly an upper bound for the chain if it remains proper. But if L is not proper, then

$1 \in L$ and hence $1 \in I$ for some $I \in \mathfrak{C}$. But this contradicts the fact that each $I \in \mathfrak{C} \subseteq S$ is proper.

Our upper bound is established; we apply Zorn's Lemma and the proof is complete. □

1.3 Irreducible and prime elements

Irreducible elements (or atoms) are the basic building blocks of factorization theory. The notion of prime is a specialization of irreducible (for integral domains). In the familiar case of of UFDs (e.g. the rational integers, $\mathbb{Z}$) the notions of prime and irreducible coincide.

Definition 1.3.1. *Let R be an integral domain. An element $x \in R$ is said to be*

a) a unit if $x|1$ (that is, $xy = 1$ for some $y \in R$),

b) irreducible (or an atom) if $x = ab$ implies that a or b is a unit in R,

c) prime if $x|ab$ implies that $x|a$ or $x|b$.

We remark here that in the general setting, 0 is a prime if and only if R is an integral domain. Additionally note that 0 is not an irreducible. Below we give an ideal theoretic characterization of the above.

Proposition 1.3.2. *Let R be an integral domain and $x \in R$.*

a) x is a unit $\iff (x) = R$.

b) x is a prime $\iff (x)$ is a prime ideal.

c) x is an irreducible $\iff (x)$ is maximal among the set of principal ideals of R.

Proof. Exercise. □

Theorem 1.3.3. *Let R be a domain. If $x \in R$ is a nonzero prime element, then x is irreducible.*

Proof. Suppose that $x = ab$ with $a, b \in R$. Since $x|ab$ we must have that $x|a$ (without loss of generality). Write $a = xr$ and substitute to obtain $x = xrb$. Hence we have that $1 = rb$ and b is a unit. This establishes thte irreducibility of x. □

Example 1.3.4. *In the ring $\mathbb{Q}[x^2, x^3] = \{\sum_{i=0}^{n} \alpha_i x^i | \alpha_i \in \mathbb{Q}, \alpha_1 = 0\}$, the elements x^2 and x^3 are nonprime irreducibles. The same is true of the element $x \in \mathbb{R} + x\mathbb{C}[x]$ and $2 \in \mathbb{Z}[\sqrt{-5}]$.*

Example 1.3.5. *Note in the ring $\overline{\mathbb{Z}} = \{z \in \mathbb{C} | p(z) = 0$ for some $p(x) \in \mathbb{Z}[x]\}$ there are no irredcubles. To see this, just note that if $z \in \overline{\mathbb{Z}}$ then $\sqrt{z} \in \overline{\mathbb{Z}}$ and hence we have the factorization $z = \sqrt{z}\sqrt{z}$ and hence z is not irreducible.*

1.4 Multiplicatively closed sets and localizations

The multiplicative subsets of an integral domain, R, reveal much about its multiplicative (factorization) structure. Additionally the multiplicative sets of a domain determine the various rings of fractions of the domain, where the factorization structure is often "easier." These rings of fractions often give insights into the factorization behavior of the original domain.

We will record a brief review of localizations in this section. Of course this may be done in a much more general setting.

Definition 1.4.1. *Let R be a domain. A nonempty subset $S \subseteq R$ (not containing 0) is said to be multiplicatively closed if $s, t \in S \Longrightarrow st \in S$. A multiplicatively closed set S is said to be saturated if $st \in S \Longrightarrow s \in S$.*

Examples of multiplicatively closed sets abound (even in the relatively tame playground of the integers). As an exercise for the reader, see if you can show that the saturated, multiplicatively closed sets in R correspond to the complements of set theoretic unions of prime ideals.

We introduce a theorem that we will use later a number of times. The theorem itself is rather central in commutative algebra. As an interesting motivation, note that applying the following theorem with $S = U(R)$ gives, as a corollary, the old chestnut that any commutative ring with identity has a maximal ideal.

Theorem 1.4.2. *Let R be commutative with identity and $I \subseteq R$ and ideal. If S is a multiplicatively closed set in R such that $S \bigcap I = \emptyset$, then there is a prime ideal $\mathfrak{P} \supseteq I$ such that $\mathfrak{P} \bigcap S = \emptyset$.*

Proof. We first assume that there is an ideal $\mathfrak{P} \subseteq R$ such that $\mathfrak{P}$ is maximal with respect to the exclusion of S (that is, $\mathfrak{P} \bigcap S = \emptyset$ and $\mathfrak{P}$ is maximal with respect to this property). We claim that such an ideal $\mathfrak{P}$ is necessarily prime. To see this, assume that we have $ab \in \mathfrak{P}$ with neither a nor b in $\mathfrak{P}$.

Since $a \notin \mathfrak{P}$, we must have that $(a, \mathfrak{P}) \supseteq \mathfrak{P}$ and hence $(a, \mathfrak{P}) \bigcap S \neq \emptyset$. So there exist $r_1 \in R$ and $p_1 \in \mathfrak{P}$ such that

$$r_1 a + p_1 = s_1 \in S.$$

In a similar fashion, we can find $r_2 \in R$ and $p_2 \in \mathfrak{P}$ such that

$$r_2 b + p_2 = s_2 \in S.$$

Multiplying the two equations above gives

$$r_1 r_2 ab + r_1 a p_2 + r_2 b p_1 + p_1 p_2 = s_1 s_2 \in S.$$

But note that since $ab \in \mathfrak{P}$, the left side of the equation is also in $\mathfrak{P}$ and hence $s_1 s_2 \in \mathfrak{P} \bigcap S = \emptyset$ which is a contradiction. This shows that $\mathfrak{P}$ is a prime ideal.

We have shown that if such an ideal exists, then it must be prime. We will now establish the existence of such an ideal. This is another application of Zorn's Lemma.

We suppose that I is an ideal and S is an multiplicatively closed set such that $I \bigcap S = \emptyset$. Consider the set of ideals

$$\Gamma := \{J | I \subseteq J \subsetneq R \text{ and } J \bigcap S = \emptyset\}.$$

It is easy to see that since Γ is nonempty (since, in particular, it contains I). Let $\mathfrak{C} = \{J_\alpha\}$ be a chain in Γ. We let $\overline{J} = \bigcup_\alpha J_\alpha$. Clearly, if $\overline{J}$ is an element of Γ then it will function as an upper bound.

To see that $\overline{J}$ is an element of Γ, we note first that $\overline{J}$ is an ideal (since $\mathfrak{C}$ is a chain).

Finally, to see that $\overline{J} \bigcap S = \emptyset$, note that if $s \in \overline{J} \bigcap S$ then $s \in J_\alpha$ for some α and hence $s \in J_\alpha \bigcap S$, which is a contradiction.

Since $\mathfrak{C}$ has an upper bound, we apply Zorn's Lemma to establish that Γ has a maximal element. This element is the ideal, maximal with respect to the exclusion of S that was claimed earlier. This completes the proof.

□

We now show the importance of multiplicatively closed sets in forming rings of fractions, or localizations. We will restrict to the case where R is an integral domain. The concept of localization (for domains) generalizes the familiar notion of quotient field (recall, the quotient field of an integral domain, R is defined to be $K = \{\frac{a}{b} | a \in R, b \in R \setminus \{0\}\}$).

Definition 1.4.3. *Let R be a domain and $S \subseteq R$ a multiplicatively closed subset of R (not containing 0). We define the localization of R at S to be*

$$R_S = \{\frac{r}{s} | r \in R, s \in S\}$$

with addition given by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

and multiplication given by

$$(\frac{r_1}{s_1})(\frac{r_2}{s_2}) = (\frac{r_1 r_2}{s_1 s_2}).$$

The fact that this rule for addition and multiplication turn R_S (actually a set of equivalence classes) into a ring is routine. Note that in the special case where $S = R \setminus \{0\}$, we have that R_S is the quotient field of R.

Example 1.4.4. *Let R be a domain and $\mathfrak{P}$ a prime ideal. It is easy to verify that the set $S := R \setminus \mathfrak{P}$ is a saturated multiplicatively closed set. The localization $R_{\mathfrak{P}} := R_S$ is called the localization of R at $\mathfrak{P}$. Verify that the ideal $\mathfrak{P}R_{\mathfrak{P}}$ is the unique maximal ideal of $R_{\mathfrak{P}}$.*

Note that, if R is a domain with quotient field K, and S is a multiplicative set, then we have the inclusions

$$R \subseteq R_S \subseteq K.$$

In other words, a localization is always an overring of R (the terminology overring refers to a ring between R and its quotient field). It is not true in general that an overring is a localization.

Example 1.4.5. *If R is a PID, show every overring is a localization.*

We finish this section by recording the correspondence theorem for localizations.

Theorem 1.4.6. *Let R be a commutative ring with identity and S a multiplicatively closed subset of R ($0 \notin S$). Then there is a one to one correspondence between prime ideals of R that exclude S and prime ideals of R_S. This correspondence is given by $\mathfrak{P} \mapsto \mathfrak{P}R_S$.*

Proof. Exercise. □

As one last new type of domain, we will define valuation domains. Valuation domains are important as they determine integral closure. It is also known that given any ideal I in the integral domain R, there is a valuation domain between R and it quotient field where I survives.

Theorem 1.4.7. *Let V be an integral domain. The following conditions are equivalent.*

1) For all nonzero $a, b \in V$ either a divides b or b divides a.

2) For all nonzero $\omega \in K$, either ω or ω^{-1} is in V.

3) V is quasi-local and any finitely generated ideal is principal.

We leave the proof as an exercise. A domain satisfying one and hence all of the above conditions is called a valuation domain.

Chapter 2

Basic Extension Rings and Homomorphisms

2.1 Homomorphisms

Definition 2.1.1. *Let R and S be rings. A function $\phi : R \longrightarrow S$ is called a homomorphism if*

a) $\phi(a+b) = \phi(a) + \phi(b)$ *and*

b) $\phi(ab) = \phi(a)\phi(b)$

As is conventional, we may apply a number of modifiers to "homomorphisms" (e.g. injective for 1-1, surjective for onto etc.).

We will always assume that in the case of rings with identity that $\phi(1_R) = 1_S$. Here is a result that demonstrates why the convention is a natural one.

Proposition 2.1.2. *If $\phi : R \longrightarrow S$ is a nonzero ring homomorphism and S is a domain, then $\phi(1_R) = 1_S$.*

Proof. Let $\phi(1_R) = a \in S$. Hence $\phi(1_R^2) = \phi(1_R)\phi(1_R) = a^2 = \phi(1_R) = a$. Hence we have that $a^2 = a$ and since S is a domain (and ϕ is nonzero) we have that $a = 1_S$. □

From here on out, if we refer to a homomorphism $\phi : R \longrightarrow S$ then we will assume that R and S are rings with 1 (if not domains) and additionally, we assume that $\phi(1_R) = 1_S$.

Definition 2.1.3. *If $\phi : R \longrightarrow S$ we say $im(\phi) = \{\phi(r) | r \in R\}$ and $ker(\phi) = \{r \in R | \phi(r) = 0\}$.*

We close this section with a familiar isomorphism theorem.

Theorem 2.1.4. *If $\phi : R \longrightarrow S$ is a ring homomorphism then $im(\phi)$ is a subring of S and $ker(\phi)$ is an ideal of R. Additionally $R/ker(\phi) \cong im(\phi)$*

Proof. The fact that $\text{im}(\phi)$ is a subring of S and $\ker(\phi)$ is an ideal of R is an easy exercise. We will establish the last statement.

Define

$$\Psi : R/\ker(\phi) \longrightarrow \text{im}(\phi)$$

by $\Psi(r + \ker(\phi)) = \phi(r)$.

If $r + \ker(\phi) = s + \ker(\phi)$ then $r = s + y$ for some $y \in \ker(\phi)$ and hence $\Psi(r + \ker(\phi)) = \phi(r) = \phi(s) = \Psi(s + \ker(\phi))$ and so Ψ is well-defined.

Note that $\Psi(r+\ker(\phi)+s+\ker(\phi)) = \Psi(r+s+\ker(\phi)) = \phi(r+s) = \phi(r)+\phi(s) = \Psi(r+\ker(\phi))+\Psi(s+\ker(\phi))$. Additionally $\Psi((r+\ker(\phi))(s+\ker(\phi))) = \Psi(rs + \ker(\phi)) = \phi(rs) = \phi(r)\phi(s) = \Psi(r + \ker(\phi))\Psi(s + \ker(\phi))$. So Ψ is a homomorphism.

To see that Ψ is one to one, suppose that $r + \ker(\phi)) \in \ker(\Psi)$. This, of course, means that $\phi(r) = 0$. Therefore $r \in \ker(\phi)$ and hence $r + \ker(\phi))$ is the $0-$coset in $R/\ker(\phi)$ and Ψ is one to one.

Clearly, Ψ is onto $\ker im(\phi)$ and the proof is complete. □

2.2 Polynomial Rings

Polynomial rings and their completions, the power series rings, are structures of fundamental importance in ring theory. We begin by defining polynomial rings and power series rings.

Definition 2.2.1. *Let R be a ring. The power series ring $R[[x]]$ is the set$\{\sum_{k=0}^{\infty} r_k x^k | r_k \in R\}$ with addition given by*

$$(\sum_{k=0}^{\infty} r_k x^k) + (\sum_{k=0}^{\infty} s_k x^k) = \sum_{k=0}^{\infty} (r_k + s_k) x^k$$

and multiplication given by

$$(\sum_{k=0}^{\infty} r_k x^k)(\sum_{k=0}^{\infty} s_k x^k) = \sum_{k=0}^{\infty} (c_k) x^k$$

with $c_k = \sum_{i=0}^{k} r_i s_{k-i}$.

The polynomial ring, $R[x]$ is the subring of $R[[x]]$ consisting of all finite sums of the form $\sum_{k=0}^{n} r_k x^k$.

We observe that we have the containments $R \subseteq R[x] \subseteq R[[x]]$. Additionally, we note that if R is commutative or has an identity, then so does $R[x]$ (resp. $R[[x]]$).

A natural question to ask is if a given property of R extends to $R[x]$ (resp. $R[[x]]$). We record a "biggie" (after recalling that a ring is called Noetherian if every ideal of R is finitely generated).

Theorem 2.2.2. *If R is a commutative Noetherian ring with identity, then so is $R[x]$.*

It is interesting to note that if $R[x]$ is Noetherian, then R must have an identity. We also note that the analogous result is true for power series ring.

Theorem 2.2.3. *Let R be an integral domain. In $R[x]$, the ideal generated by x is prime.*

Proof. Consider the ring homomorphism $\phi : R[x] \longrightarrow R$ given by $\phi(f(x)) = f(0)$. It is easy to see that this is a sirjective homomophism and hence $R \cong R[x]/\ker(\phi)$. Since R is a domain, and $\ker(\phi) = (x)$ we see that (x) is prime. □

Here are a couple of other tools needed to study factorization in $R[x]$ (among other things).

Definition 2.2.4. *Let R be a domain and $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ with $a_n \neq 0$. We say that $deg(f(x)) = n$.*

By convention, we will say that $\deg(0) = \infty$.

Proposition 2.2.5. *Let R be a domain and $f, g \in R[x]$.*

a) $deg(f + g) \leq max(deg(f), deg(g))$.

b) $deg(fg) = deg(f) + deg(g)$.

Proof. Exercise. □

Corollary 2.2.6. *If R is a domain, then $R[x]$ is a domain.*

Proof. Suppose that $fg = 0$ in $R[x]$ and that neither f nor g is 0. If $\deg(f) = n > 0$ then $\deg(fg) > 0$ which is a contradiction. Hence the degrees of both f and g are 0 and hence in R. Hence $fg = 0$ for two nonzero elements of R which is a contradiction. □

Corollary 2.2.7. *Let R be a domain and $U(R)$ be the units of R. Then $U(R) = U(R[x])$.*

Proof. It suffices to show that $U(R[x]) \subseteq U(R)$. Suppose that $f \in U(R[x])$. This means that there is a $g \in R[x]$ such that $fg = 1$. Taking the degree of both sides and applying the above, we obtain that $\deg(f) = \deg(g) = 0$. Hence $f, g \in R$ and hence $f \in U(R)$. □

2.3 power series

Many of the theorems for polynomials "go through" for power series, but, of course, many do not.

Theorem 2.3.1. *If R is a domain, then (x) is a prime ideal of $R[[x]]$.*

Proof. Same. □

Theorem 2.3.2. *If R is a domain then so is $R[[x]]$.*

Proof. Boring. □

Here is an interesting "factorization theorem" for $R[[x]]$. This should be constrasted with the case of $R[x]$.

Theorem 2.3.3. $U(R[[x]]) = \{f \in R[[x]] | f(0) \in U(R)\}$.

Proof. High school division. □

Corollary 2.3.4. *If F is a field, then every nonzero element of $F[[x]]$ is of the form $x^n u(x)$ with $n \geq 0$ and $u(x) \in U(R[[x]])$.*

Example 2.3.5. *Contrast this with $R[x]$ (even when R is a field).*

Proposition 2.3.6. *If $a \in R$ is an irreducible element then any power series of the form, $a + xf(x)$ is irreducible in $R[[x]]$.*

Proof. If $a + xf(x) = (b + xg(x))(c + xh(x))$ then $a = bc \in R$. Since a is irreducible, then we can say without loss of generality that b is a unit in R. By the previous, $b + xg(x)$ is a unit in $R[[x]]$ and we are done. □

Example 2.3.7. *The converse of the previous is not true (consider for example, $4 + x \in \mathbb{Z}[[x]]$). It should also be noted that the analog of this result is not true for $R[x]$ (this is one of the rare cases where $R[[x]]$ may be construed as more well-behaved than $R[[x]]$).*

As far as ring extensions are concerned, we have considered a number of types: $R_S, R[x]$, and $R[[x]]$. At the present, we will investigate one more type in the section (integral extension). Later we will often attempt to discern how factorization properties behave in these (and other) types of extensions.

2.4 integral extensions

In this section many proofs are omitted or abbreviated for now.

In this section R will be a domain with quotient field K and T will be a ring containing R.

Definition 2.4.1. *Let $R \subseteq T$ be an extension of rings. An element $t \in T$ is said to be integral over R if t is a root of a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$.*

Example 2.4.2. *i is integral over the ring $\mathbb{R}$ (and $\mathbb{R} + x\mathbb{C}[x]$). Any Gaussian integer (complex number of the form $a + bi$ with $a, b \in \mathbb{Z}$ is integral over $\mathbb{Z}$ (it is a root of $x^2 - 2ax + (a^2 + b^2) \in \mathbb{Z}[x]$). The element x is integral over the ring $R[x^2, x^3]$ and it should be noted that any element of R is integral over R.*

Theorem 2.4.3. *Let $R \subseteq T$ be an extension of rings and $s, t \in T$. If s and t are integral over R then so are st and $s + t$.*

Proof. Here we only sketch the idea. An equivalent way to look at the integrality concept is to note that t is integral over R if and only if $R[t]$ is a finite R module. Note that $R[t]$ is a finite R module and $R[t,s]$ is a finite $R[t]$ module and hence a finite R module. Note that both ts and $t+s$ are elements of $R[t,s]$. □

Corollary 2.4.4. *Let $R \subseteq T$ be an extension of rings. Then the set*

$$\overline{R} = \{t \in T | t \text{ is integral over } R\}$$

is a ring containing R.

Definition 2.4.5. *If $R \subseteq T$ are rings, the ring $\overline{R}_T = \{t \in T | t$ is integral over $R\}$ is called the integral closure of R in T. If $T = K$ then $\overline{R} := \overline{R}_K$ is called the integral closure of R. If $R = \overline{R}$, we say that R is integrally closed. If every element of T is integral over R then T is called an integral extension of R.*

Example 2.4.6. *The ring of algebraic integers $\overline{\mathbb{Z}}$ is the set $\overline{\mathbb{Z}} = \{z \in \mathbb{C} | p(z) = 0$ for some monic $p(x) \in \mathbb{Z}[x]\}$. The ring $\mathbb{Z}$ (in fact any UFD) is integrally closed. The extension $\mathbb{Z} \subseteq \mathbb{Z}[i]$ is an integral extension.*

Here is an important "factorization theorem" for integral extensions.

Theorem 2.4.7. *Let $R \subseteq T$ be an extension of rings. If T is integral over R and $r \in R$ is a nonunit, then r is a nonunit of T.*

Proof. Note that in any case (integral or not) that $U(R) \subseteq U(T)$. Suppose that $r \in R$ is a nonunit in R, but there is a $t \in T$ such that $rt = 1$. Since T is integral over R, there exist $r_{n-1}, r_{n-2}, \cdots, r_1, r_0 \in R$ such that

$$t^n + r_{n-1}t^{n-1} + \cdots + r_1 t + r_0 = 0.$$

Multiplying the above by r^n, we obtain

$$(rt)^n + r_{n-1}r(rt)^{n-1} + r_{n-2}r^2(rt)^{n-2} + \cdots + r_1 r^{n-1}(rt) + r_0 r^n = 0$$

which gives

$$1 = r[-r_{n-1} - r_{n-2}r - \cdots - r_1 r^{n-2} - r_0 r^{n-1}].$$

Since both factors on the right side of the above are in R, we obtain that $r \in U(R)$ and the proof is complete. □

Example 2.4.8. *It is fairly easy to see that the "integrality" assumption is needed. To see this concretely, consider the extension $R \subseteq R_S$.*

Chapter 3

Basic Domains of Factorization Theory

3.1 Euclidean domains, PIDs, and UFDs

In this chapter we will explore some of the most important domains in the theory of factorization. We begin in this section with a look at some of the classical domains where the factorization is nicest. One discovers in beginning algebra classes that Euclidean domains are PIDs and PIDs are in turn UFDs (and none of these implications can be reversed). From a factorization point of view, the factorization in these domains are the nicest (every nonzero nonunit can be factored uniquely into primes). From one point of view, these domains may seem "boring", but knowledge of the structure of these domains is essential, since many factorization properties of more general domains can be gleaned if the more general domain sits inside a UFD.

Definition 3.1.1. *A domain R is said to be Euclidean if there exists a function $\phi : (R \setminus \{0\}) \longrightarrow \mathbb{N} \bigcup \{0\}$ satisfying the following.*

1) For all nonzero $x, y \in R$, $\phi(xy) \geq \phi(x)$.

2) If $x, y \in R$ and $x \neq 0$ then there exists $q, r \in R$ such that

$$y = qx + r$$

with either $r = 0$ or $\phi(r) < \phi(x)$.

Example 3.1.2. *$\mathbb{Z}$ is Euclidean with $\phi(n) = |n|$. If K is a field, then $K[x]$ is Euclidean with $\phi(f(x)) = deg(f(x))$. Additionally, $K[[x]]$ is Euclidean with $\phi(f(x)) = n$, where $f(x) = x^n g(x)$ with $g(0) \neq 0$ (if $f(x)$ is a nonzero power series, then ew can always represent $f(x)$ uniquely in this form). The value n is often referred to as the order of $f(x)$.*

Example 3.1.3. *Can we extend the above example to the case $K[x, y]$ or $K[[x, y]]$?*

Definition 3.1.4. *A domain R is a principal ideal domain (PID) if every ideal of R is principally generated.*

Definition 3.1.5. *A domain R is a unique factorization domain (UFD) if every nonzero nonunit of R is a product of primes.*

Example 3.1.6. *Show that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. Show that this ring is a PID, but not Euclidean.*

Classically, the more familiar definition of UFD is a three-parter (the first part being that every nonero nonunit is a product of irreducibles, the second and third parts say that any two equal irreducible factorization have the same length and the irreducibles pair off up to units). We will see presently why the more compact definition above is equivalent to the more long-winded classical definition.

Lemma 3.1.7. *Let R be a domain and let $x \in R$ be a finite product of primes, say*

$$x = p_1 p_2 \cdots p_t.$$

Then this factorization is the only irreducible factorization of x (up to order and multiplication by units).

Proof. Suppose that $a_1 \cdots a_k = x$ is another irreducible factorization. We have

$$a_1 a_2 \cdots a_k = p_1 p_2 \cdots p_t.$$

Since p_1 is prime, we will assume that p_1 divides a_1 without loss of generality. Since a_1 is irreducible we have that $a_1 = u_1 p_1$ with $u_1 \in U(R)$. Cancelling p from the above equation, we get that

$$u_1 a_2 \cdots a_k = p_2 p_3 \cdots p_t.$$

Inductively, we obtain that $t = k$ and that each $a_i = u_i p_i$ (again without loss of generality). This establishes the lemma. □

Definition 3.1.8. *A domain R is said to be atomic if every nonzero nonunit of R is a product of atoms (irreducibles).*

Proposition 3.1.9. *Let R be a domain. The following conditions are equivalent.*

1) *R is atomic and any factorization into irreducibles in R is unique up to ordering and units.*

2) *Every nonzero nonunit of R is a product of primes.*

Proof. For 2) implies 1), we need only consult the previous lemma. For the other direction, since we know that every nonzero nonunit if a product of irreducibles, it will suffices to show that each irreducible is prime. To this end, let $a \in R$ be an irreducible and suppose that a divides xy in R. We suppose that x, y are nonzero nonunits and factor then in R. We write the irreducible factorizations $x = x_1x_2 \cdots x_k$ and $y = y_1y_2 \cdots y_m$. Since a divides xy we can write

$$ra = (x_1x_2 \cdots x_k)(y_1y_2 \cdots y_m)$$

for some $r \in R$.

By uniqueness of factorizations, since a is a factor that appears on the left, it must appear on the right. But since each x_i, y_j is irreducible, we must have that there is a unit $u \in R$ such that either $a = ux_i$ or $a = uy_j$. In the former case, a divides x and in the latter a divides y. Hence we have that a is prime and this concludes the proof. □

We will now explore the pecking order of these types of domains.

Theorem 3.1.10. *If R is a Euclidean domain then R is a PID.*

Proof. Let $I \subseteq R$ be a nonzero ideal. Consider the set $S = \{\phi(x) | x \in I \setminus \{0\}$. Note that S is a subset of $\mathbb{N} \bigcup \{0\}$ and must therefore have a least element. We select $x \in I$ such that $\phi(x)$ is minimal (that is $\phi(x) \leq \phi(y)$ for all nonzero $y \in I$). We claim that $I = (x)$.

Since $x \in I$ it is certainly the case that $(x) \subseteq I$. For the other containment, we will let $z \in I$. Since R is Euclidean we can find $q, r \in R$ such that $z = qx + r$ with either $r = 0$ or $\phi(r) < \phi(x)$. But note that since $z, x \in I$ we must have that $r \in I$. By the minimality of $\phi(x)$, we must have that $r = 0$ and hence x divides z. So $z \in (x)$ and we conclude that $I = (x)$ □

The next result is a very nice and often useful characterization of UFDs

Proposition 3.1.11. *An integral domain R is a UFD if and only if every nonzero prime ideal of R contains a nonzero principal prime ideal.*

Proof. Suppose first that R is a UFD. Let $P \subseteq R$ be a nonzero prime ideal in R. Let x be a nonzero element of P. Factor $x = x_1x_2 \cdots x_k \in P$ into primes. Since P is a prime ideal one of the factors (say x_i) must be in P. Hence $(x_i) \subseteq P$ and this direction is complete.

For the other direction we will assume that R is not a UFD. Consider the set $S = \{up_1p_2 \cdots p_n | u \in U(R), p_i$ nonzero primes$\}$. (Note that S contains the units of R and if R has no nonzero primes, then $S = U(R)$.) S is a multiplicative set and since R is not a UFD, we can find a nonzero $a \in R$ such that $a \in R \setminus S$.

We now claim that $(a) \bigcap S = \emptyset$. To verify this we assume that there is an $r \in R$ such that $ra = up_1p_2 \cdots p_t \in S$. If $t = 1$ then we obtain that $ra = up_1$. Since p_1 is prime, it must divide either a or r. If p_1 divides a then r is a unit and hence $a = r^{-1}up_1$ is prime. If p_1 divides r, then a is a unit. Either case is a contradiction.

We proceed by induction. Inductively, we assume that if r, a (with a a nonzero nonunit) and $ra = up_1p_2 \cdots p_t$ then a has a prime factorization. Now assume that we have

$$ra = up_1p_2 \cdots p_tp_{t+1} \in S.$$

If p_{t+1} divides r then $(\frac{r}{p_{t+1}})a = up_1p_2 \cdots p_t$ and we are done by induction. If p_{t+1} divides a and $\frac{a}{p_{t+1}}$ is a nonunit then $r(\frac{a}{p_{t+1}}) = up_1p_2 \cdots p_t$ and by induction, $\frac{a}{p_{t+1}} = p_{1_1}p_{i_2} \cdots p_{i_m}$ and hence $a = p_{t+1}p_{i_1}p_{i_2} \cdots p_{i_m}$. Finally, if $fracap_{t+1}$ is a unit, then $a = vp_{t+1}$ with $v \in U(R)$. This establishes the claim (note that this claim basically shows that the set S is saturated).

To finish the proof, we appeal to Theorem 1.4.2. Since $(a) \bigcap S = \emptyset$, Theorem 1.4.2. gives that there is a prime ideal $\mathfrak{P} \supseteq (a)$ such that $\mathfrak{P} \bigcap S = \emptyset$. Hence $\mathfrak{P}$ contains no prime element and the proposition is established.

□

Corollary 3.1.12. *Any PID is a UFD.*

Proof. Suppose that R is a PID. If R has no nonzero prime ideals, then R is a field, which is clearly a UFD. We therefores select a nonzero prime ideal $\mathfrak{P}$ in R. Since R is a PID, $\mathfrak{P} = (p)$ and p is a prime element. By the previous proposition, R is a UFD. □

Example 3.1.13. *It is now easy to see that if F is a field, then $F[x], F[[x]]$ and the ring $\mathbb{Z}$ are all UFDs (since they are all Euclidean. It is also easy to see that $F[x, y], F[[x, y]], \mathbb{Z}[x]$, and mathbbZ$[[x]]$ are not Euclidean (since they are not PIDs). We remark that $R[x], R[[x]]$ are Euclidean if and only if R is a field.*

We now show that the property "PID" is determined by prime ideals. That is, if R is not a PID then there must be a prime ideal that is nonprincipal. This property is useful since it reduces the determination of a global property of the domain to inspection of the behavior of the prime ideals. Many other properties (e.g. Noetherian) can be determined by looking only at the prime ideals.

Proposition 3.1.14. *R is a PID if and only if every prime ideal of R is principal.*

Proof. If R is a PID, it is clear that every prime ideal is principal. We will show the other direction.

Assume that R is not a PID. We select an ideal $I \subseteq R$ that is not principally generated. Our first claim is that there is an ideal $\mathfrak{P} \subseteq R$ that is maximal with respect to the property of not being principally generated. This is a straightforward application of Zorn's Lemma. Indeed, we set

$$\Gamma = \{J_\beta | J_\beta \supseteq I, J_\beta \text{ is nonprincipal}\}.$$

And we note that Γ is nonempty since $I \in \Gamma$. Let $\mathfrak{C} = \{J_\alpha\}_{\alpha \in \Lambda}$ be a chain in Γ. Consider the ideal $J := \bigcup_{\alpha \in \Lambda} J_\alpha$. J is clearly an upper bound for this

chain if J is nonprincipal. But if $J = (x)$ then $x \in J_\alpha$ for some α and hence $J_{alpha} = J = (x)$ and this is a contradiction since each J_{alpha} is nonprincipal. We obtain that J is an upper bound for the chain $\mathfrak{C}$ and applying Zorn's Lemma, we have established the first claim.

Now we claim that any such maximal nonprincipal ideal $(\mathfrak{P})$ is necessarily prime. To this end, we assume that $ab \in \mathfrak{P}$ with neither a nor b in $\mathfrak{P}$. Since $(\mathfrak{P}, a) \supsetneq \mathfrak{P}$, this ideal must be principal and we write $(\mathfrak{P}, a) = (x)$.

We now set $J = \{r \in R | rx \in \mathfrak{P}\}$. It is clear that $\mathfrak{P} \subseteq J$, but more importantly, we will show that $b \in J$. To see this, we first note that $x \in (\mathfrak{P}, a)$. Hence there exist $p \in \mathfrak{P}$ and $r \in R$ such that

$$p + ra = x.$$

Multiplying the above by b, we get that $bp + rab = bx$. Since $ab \in \mathfrak{P}$, we have that $bx \in \mathfrak{P}$ and hence $b \in J$.

Since $b \in J$ and $\mathfrak{P} \subseteq J$, we obtain that $\mathfrak{P} \subsetneq J$, and hence J is principal (we write $J = (y)$).

To finish the proof we will now show that $\mathfrak{P} = Jx$. With this final statement established we will have that $\mathfrak{P}$ is the product of two principal ideals (and hence is principal) and this contradiction will establish the proposition.

For the first containment, we let $p \in \mathfrak{P} \subseteq (\mathfrak{P}, a) = (x)$. We can therefore write $p = rx$ for some $r \in R$, and by definition, this r must be an element of J. Hence $\mathfrak{P} \subseteq Jx$.

For the other containment, suppose that $jx \in Jx$. By the definition of J, $jx \in \mathfrak{P}$ and hence $Jx \subseteq \mathfrak{P}$ and the proof is complete. □

We record an important characterization of PID that highlights the interplay between these two important types of domains.

Theorem 3.1.15. *Let R be a domain. The following conditions are equivalent.*

1) R is a PID.

2) R is a UFD and every nonzero prime ideal is maximal.

The property that every nonzero prime ideal of R is maximal is sometimes referred to as "the dimension of R is less than or equal to 1". Dimension will not be discussed extensively here, but intuitively the dimesion of a commutative ring with identity is the supremum over the lengths of chains of prime ideals in R (so in a sense is a measure of the "size" of the ring). Zero-dimensional domains are fields. One dimensional domains are precisely the non-field domains where each nonzero prime ideal is maxmial (e.g. $\mathbb{Z}$ or more generally any Dedekind domain). The domain $F[x, y]$ where F is a field is two dimensional. The chain of primes $(0) \subset (x) \subset (x, y)$ shows that $F[x, y]$ is at least two dimensional (to show that it is precisely two dimensional is a bit afield of where we are going for now).

Proof. For the implication 1) implies 2) it suffices to show every nonzero prime ideal is maximal. If R has no nonzero primes R is a field, and we are done, so we will ignore this case.

Assume that $\mathfrak{P}$ is a proper nonzero prime ideal of R and suppose that $(0) \subsetneq \mathfrak{P} \subsetneq \mathfrak{M}$, with $\mathfrak{M}$ a maximal ideal of R. Since R is a PID, we can select (prime) generators $p \in \mathfrak{P}$ and $m \in \mathfrak{M}$. Since $\mathfrak{P}$ is contained in $\mathfrak{M}$, we have that $p = rm$ for some $r \in R$. But since p is prime, we must have that p divides r or m. If p divides r, then m is a unit, and if p divides m then $\mathfrak{P} \supseteq \mathfrak{M}$. Either case is a contradiction and we are done with the first implication.

For the other implication we assume that R is a UFD and that every nonzero prime is maximal. If R has no nonzero primes, then R is a field and is clearly a PID. So assume that $\mathfrak{P}$ is a proper nonzero prime ideal. Since R is a UFD, $\mathfrak{P}$ must contain a prime element (say p). This gives the chain of prime ideals

$$(0) \subsetneq (p) \subseteq \mathfrak{P}.$$

Since all nonzero prime ideals are maximal, we have that $\mathfrak{P} = (p)$, and hence every nonzero prime ideal of R is principal. By the previous proposition, we have that R is a PID and this concludes the proof. □

3.2 Factorization in Elementary Extensions

In this section we will begin investigation into the behavior of factorization in the "standard" ring extensions. In particular, we attempt to answer the question "if R has a certain factorization behavior, does the ring extension T have similar factorization behavior?" The special cases where T is $R[x], R[[x]], R_S$ or is the integral closure of R get special attention. In this section we will be concentrating on the case where R is a UFD. To this end we will first produce a theorem to demonstrate why integral closure is less interesting in this section (it will be much more interesting later).

Theorem 3.2.1. *Any UFD (hence PID, hence Euclidean domain) is integrally closed.*

Proof. Let R be a UFD ith quotient field K, and assume that $\omega = \frac{a}{b} \in K$ is an integral element. Since R is a UFD, we can factor a and b into primes and "cancel". The upshot is that we can assume that the greatest common divisor of a and b is 1.

Since ω is integral over R, there exist $r_0, r_1, \cdots, r_{n-1} \in R$ such that

$$\omega^n + r_{n-1}\omega^{n-1} + \cdots + r_1\omega + r_0 = 0.$$

Multiplying the above equation by b^n, we obtain

$$a^n + r_{n-1}ba^{n-1} + \cdots + r_1ab^{n-1} + r_0b^n = 0.$$

Now suppose that p is a prime of R such that b divides b. The above equation shows that p divides a^n and since p is prime, p must divide a. This contradicts

the fact that the greatest common divisor of a and b is 1. We conclude that b has no prime factors. Hence b is a unit in R and $\omega = \frac{a}{b} \in R$. This shows that R is integrally closed and the proof is complete. □

Example 3.2.2. *Since $\mathbb{Z}$, $F[x]$ and $F[[x]]$ are UFDs, they are integrally closed.*

Example 3.2.3. *Consider the rings $R := \mathbb{Z}[\sqrt{-3}]$ and $T := F[x,y]/\langle x^2 - y^3\rangle$. Neither of these rings is integrally closed. For the first one note that the element $\omega = \frac{-1+\sqrt{-3}}{2}$ is an element of the quotient field of R that is a root of the polynomial $x^2 + x + 1 \in R[x]$. Since $\omega \notin R$, R is not integrally closed. For the second ring, note that in the quotient domain we have that (abusing the notation)*

$$(\frac{x}{y})^2 = \frac{x^2}{y^2} = \frac{y^3}{y^2} = y$$

and hence $\frac{x}{y}$ is a root of the polynomial $Z^2 - y$. It is easy to see that T is not integrally closed.

The upshot is that neither of these domains are UFDs since they are not integrally closed.

An important key to understanding factorization behavior in $R[x]$ and $R[[x]]$ is getting a picture of what the prime ideals in these extensions look like. Some of them (but not all) look like prime from R.

Lemma 3.2.4. *Let $I \subseteq R$ be an ideal. Denote $I[x] = \{\sum_{n=0}^{k} \alpha_n x^n | \alpha_n \in I\}$ and $I[[x]] = \{\sum_{n=0}^{\infty} \alpha_n x^n | \alpha_n \in I\}$. We have the following isomorphisms of rings.*

1) $R[x]/I[x] \cong (R/I)[x]$.

2) $R[[x]]/I[[x]] \cong (R/I)[[x]]$.

Proof. We will only show the isomorphism for the polynomial case (the power series case being an almost exact duplicate of the polynomial proof).

Define $\phi : R[x] \longrightarrow (R/I)[x]$ by $\phi(r_0 + r_1 x + \cdots + r_n x^n) = \overline{r_0} + \overline{r_1}x + \cdots + \overline{r_n}x^n$ where each $\overline{r_i}$ denotes the coset $r_i + I \in R/I$. It is easy to see ϕ is surjective and that the kernal of ϕ is precisely $I[x]$. By Theorem 2.1.4, we have that $R[x]/I[x] \cong (R/I)[x]$. □

Proposition 3.2.5. *Let R be a domain and $p \in R$ a prime element. Then p is a prime element of $R[x]$ and $R[[x]]$.*

Proof. For the polynomial case, let $p \in R$ be prime. Hence the ideal $\mathfrak{P} := (p)$ is a prime ideal. Consider $R[x]/\mathfrak{P}[x] \cong (R/\mathfrak{P})[x]$. Since $\mathfrak{P}$ is prime, we have that $(R/\mathfrak{P})[x]$ (and hence $R[x]/\mathfrak{P}[x]$) is a domain. We conclude that $(p)[x] = (p)R[x]$ is prime, and so p is prime in $R[x]$. The proof for the case of power series is similar. □

A more direct proof of the previous can give us the famous Eisenstein's Irreducibility Criterion. We will record this important result below and sketch its proof.

Corollary 3.2.6. *Let R be a domain and $p \in R$ a nonzero prime element. Suppose that $q(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ and*

1) p does not divide a_n,

2) p divides a_i, $0 \leq i \leq n-1$,

3) p^2 does not divide a_0, and

4) $gcd(a_0, a_1, \cdots, a_n) = 1$.

Then $q(x)$ is irreducible in $R[x]$.

Proof. Note that condition 4) implies that any two nontrivial factors of $q(x)$ must each have degree at least 1. The conditions 2) and 3) give that $a_0 = pk_0$ with p not dividing k_0, and $a_i = pk_i$ for $1 \leq i \leq n-1$. Suppose that we have

$$q(x) = pk_0 + pk_1x + \cdots + pk_{n-1}x^{n-1} + a_nx^n = (b_0 + b_1x + \cdots + b_mx^m)(c_0 + c_1x + \cdots + c_tx^t).$$

Equating the constant terms, we get that $b_0c_0 = pk_0$. Hence, without loss of generality, we have that p divides b_0 and p does not divide c_0. Equating the linear terms, we get that $b_0c_1 + b_1c_0 = pk_1$ and hence p divides b_1. Continuing this process, we obtain that p divides b_i for all $0 \leq i \leq m$, since $m < n$. Hence $b_0 + b_1x + \cdots b_mx^m$ is divisible by p and so a_n is divisible by p and this contradicts condition 1). □

The following is a general utility lemma that is often useful. We will use it presently (and we will appeal to it in the future as well).

Lemma 3.2.7. *If $R \subseteq T$ are rings and $\mathfrak{P} \subseteq T$ is a prime ideal, then $\mathfrak{P} \bigcap R$ is a prime ideal of R.*

Proof. Let $ab \in \mathfrak{Q} := \mathfrak{P} \bigcap R$. Since $a, b \in R \subseteq T$ and $ab \in \mathfrak{P}$ we have that $a \in \mathfrak{P}$ without loss of generality. Hence $a \in \mathfrak{P} \bigcap R = \mathfrak{Q}$ and the proof is complete. □

Proposition 3.2.8. *Let R is a UFD with quotient field K and $f(x) \in R[x]$. If $f(x)$ is irreducible in $R[x]$ then it is also irreducible in $K[x]$. If $f(x)$ is irreducible in $K[x]$ and the greatest common divisor (in R) of the coefficients of $f(x)$ is 1, then $f(x)$ is irreducible in $R[x]$.*

Basically the content of this proposition is that irreducible polynomials in $R[x]$ (where R is a UFD) are essentially the irreducible in the PID $K[x]$. The only exception is to "cheat" by having a common divisor of the coefficients of $f(x)$ in $R[x]$. For example, the polynomial $x + 1$ irreducible in $\mathbb{Z}[x]$, but $2x + 2$ is not since we can factor out a 2. Both of these polynomials are irreducible in $\mathbb{Q}[x]$ since 2 is a unit in $\mathbb{Q}$.

Proof. Suppose that $f(x) = a_0 + a_1x + \cdots a_nx^n \in R[x]$ is irreducible in $K[x]$, and that $\gcd(a_0, a_1, \cdots, a_n) = 1$. If $f(x) = h(x)k(x) \in R[x] \subseteq K[x]$, it is immediate that the degree of one of these factors must be 0. Without loss of generality, we will say that the degree of $h(x)$ is zero. Writing $h(x) = a \in R$ we see that a must divide a_i for all $0 \leq i \leq n$ and hence is a common divisor of the coefficients of $f(x)$. So $h(x) \in U(R)$ and we are done.

On the other hand, suppose that $f(x)$ is irreducible in $R[x]$ and assume that $f(x) = g(x)k(x) \in K[x]$ with each factor of degree at least 1. We "clear the denominators" by selecting $a, b \in R$ such that $ag(x) = g_1(x) \in R[x]$ and $bk(x) = k_1(x) \in R[x]$. We can now write

$$abf(x) = g_1(x)k_1(x) \in R[x]$$

and

$$ab = p_1p_2 \cdots p_t$$

as a prime factorization in R. But since primes in R remain prime in $R[x]$ we must have that each p_i divides either $g_1(x)$ or $k_1(x)$ in $R[x]$. Reindexing if necessary, we will say that $\frac{g_1(x)}{p_1 \cdots p_k} := g_2(x) \in R[x]$ and $\frac{k_1(x)}{p_{k+1} \cdots p_t} := k_2(x) \in R[x]$. Dividing the above equation by $p_1p_2 \cdots p_t$ we obtain

$$f(x) = g_2(x)k_2(x) \in R[x]$$

with each factor of degree at least one and this is the desired contradiction.

□

The curious reader may wonder why this result is stated for the polynomial case (as opposed to the power series case). The step in the proof where we clear the denominators is not possible with a general power series.

Example 3.2.9. *Show that the polynomial* $6+4x+x^2$ *is irreducible in* $\mathbb{Z}[x]$ *but not in* $\mathbb{Z}[[x]]$.

Example 3.2.10. *Over the ring* $\mathbb{Z}[\sqrt{-3}]$ *the polynomial* x^2+x+1 *is irreducible. But over the ring* $\mathbb{Z}[\omega]$ *where omega* $= \frac{-1+\sqrt{-3}}{2}$*, the polynomial* x^2+x+1 *factors into the product* $(x-\omega)(x-\overline{\omega})$*. This example shows that the condition that* R *is a UFD (or at least integrally closed) is important.*

The next result shows that unique factorization is stable under passage to polynomial rings.

Theorem 3.2.11. *If* R *is a UFD, then so is* $R[x]$.

Proof. We will show that any nonzero prime ideal contains a prime element. Let $\mathfrak{P}$ be a prime ideal of $R[x]$. We know that $\mathfrak{P} \bigcap R := \mathfrak{Q}$ is a prime ideal of R. If $\mathfrak{Q}$ is nonzero, then there is a prime element $p \in \mathfrak{Q}$ since R is a UFD. Since prime elements of R are also prime in $R[x]$ we are done in this case.

If $\mathfrak{Q} = 0$ we select a nonzero $f(x) \in \mathfrak{P}$ of minimal degree. Since $\mathfrak{P} \bigcap R = 0$ we can assume that the greatest common divisor of the coefficients of $f(x)$ is 1. Now consider $f(x)$ as an element of $K[x]$ where K is the quotient field of R. If $f(x)$ is reducible in $K[x]$ then it is reducible in $R[x]$ by our previous result. But then we have $f(x) = g(x)h(x) \in \mathfrak{P}$ and the degree of each factor is at least 1 (and hence less than the degree of $f(x)$). We conclude that either $g(x)$ or $h(x)$ is an element of $\mathfrak{P}$ and this contradicts the minimality of the degree of $f(x)$ in $\mathfrak{P}$. So $f(x)$ is an irreducible element of $K[x]$ (and hence prime since $K[x]$ is a UFD).

To finish the proof, it suffices to show that $f(x)$ generates $\mathfrak{P}$ in $R[x]$. Let $g(x) \in \mathfrak{P}$ be arbitrary. Since $K[x]$ is Euclidean, we can write

$$g(x) = k(x)f(x) + r(x)$$

where $r(x) = 0$ or $textdeg(r(x)) < \deg(f(x)$.

We again clear the denominators be selecting a nonzero $a \in R$ such that $ar(x), ak(x) \in R[x]$:

$$ag(x) = (ak(x))f(x) + ar(x).$$

And so $ar(x) \in \mathfrak{P}$. If $ar(x) \neq 0$ then $\deg(ar(x)) < \deg(f(x))$ which again contradicts the minimality of the degree of $f(x)$ in $\mathfrak{P}$. We must therefore conclude that $r(x) = 0$ and hence we have that $f(x)$ divides $ag(x)$ in $R[x]$. We write the equation

$$ag(x) = h(x)f(x)$$

and recall that any prime element of R is prime in $R[x]$. If $p \in R$ is an arbitrary prime divisor of a then we see that p must divide $h(x)$ (since it must divide $h(x)$ or $f(x)$ but the greatest common divisor of the coefficients of $f(x)$ is 1). Inducting on the number of prime divisors of a, we obtain that $f(x)$ must divide $g(x)$ and hence $f(x)$ is a prime element (and, in fact, the generator) of $\mathfrak{P}$. This concludes the proof.

□

This result is true for polynomials but not for power series in general. The following is an example of a UFD whose power series ring does not have unique factorization. What is true for power series is that if R is a PID, then $R[[x_1, x_2, \cdots, x_n]]$ is a UFD.

Example 3.2.12. *Let K be a field and w, x, y, z be indeterminates. Let $\mathfrak{P} = (x^2 + y^3 + wz^6) \subseteq K(w)[[x, y, z]]$. The quotient ring $R := K(w)[[x, y, z]]/\mathfrak{P}$ is an example of a (two dimensional, Noetherian) UFD such that $R[[t]]$ is not a UFD.*

Corollary 3.2.13. *If R is a UFD, then $R[\{x_\alpha\}_{\alpha\in\Lambda}]$ is a UFD for any set of indeterminates $\{x_\alpha\}_{\alpha\in\Lambda}$.*

Proof. For a finite set of indeterminates, the proof is an easy induction. For the more general case, any polynomial in $R[\{x_\alpha\}_{\alpha\in\Lambda}]$ involves only a finite subset of the indeterminates $\{x_\alpha\}_{\alpha\in\Lambda}$. Because of this, it can be shown that an arbitrary element has unique factorization into irreducibles. □

In the spirit of this section, we remark that if R is not a field, then $R[x]$ and $R[[x]]$ are never PIDs. It is an easy exercise to see that if a is a nonzero nonunit, then the ideal (a, x) is never principal in $R[x]$ (respectively $R[[x]]$).

We now produce a theorem that we alluded to earlier. We will only show the one variable case.

Theorem 3.2.14. *If R is a PID then $R[[x]]$ is a UFD.*

Proof. As was before, we will show that every prime ideal of $R[[x]]$ contains a prime element. Let $\Gamma \subseteq R[[x]]$ be a prime ideal. In the first case, we will assume that $x \in \Gamma$. In this case Γ contains the prime element x.

The more interesting case is when $x \notin \Gamma$. In this case we consider the ring homomorphism $\phi : R[[x]] \longrightarrow R$ defined by $\phi(f(x)) = f(0)$. We associate with this homomorphism, the ideal

$$I := \{f(0)|f(x) \in \Gamma\},$$

and note that since R is a PID, then I is principally generated (say by $z \in I$). Choose $f(x) \in \Gamma$ such that $f(0) = z$ (i.e. $f(x) = z + a_1x + a_2x^2 + \cdots$) and let $g(x) \in \Gamma$ be arbitrary. We claim that $f(x)$ must divide $g(x)$ and this will finish the proof as it will show that $\Gamma = (f(x))$ and hence $f(x)$ is prime.

To establish the claim (and playing a bit fast and loose) we note that if $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ then $b_0 \in I$. Hence there is an $r_0 \in R$ such that $r_0z = b_0$. We obtain

$$r_0f(x) = r_0z + r_0a_1x + r_0a_2x^2 + \cdots$$

and hence

$$r_0f(x) - g(x) = x[(r_0a_1 - b_1) + x(r_0a_2 - b_2) + x^2(r_0a_3 - b_3) + \cdots] = xg_1(x) \in \Gamma.$$

Since $x \notin \Gamma$ we must have that $g_1(x) = r_1z + c_1x + c_2x^2 + \cdots \in \Gamma$. As was the case before we now have

$$r_1f(x) - g_1(x) = xg_2(x)$$

with $g_2(x) \in \Gamma$. Continuing this process we obtain

$$r_0f(x) - xg_1(x) = g(x),$$

$$r_0f(x) - x(r_1f(x) - g_2(x)) = g(x),$$

$\vdots$

$$r_0 f(x) - x r_1 f(x) + x^2 r_2 f(x) - x^3 r_3 f(x) + \cdots = g(x).$$

We conclude that $f(x)(r_0 - r_1 x + r_2 x^2 + \cdots) = g(x)$ and hence $f(x)$ divides $g(x)$. So $\Gamma = (f(x))$ and therefore contains a prime element. □

We finish off this section by recording the nice behavior of localization with respect to PIDs and UFDs.

Theorem 3.2.15. *Let R be a domain and S a multiplicatively closed subset of R ($0 \notin S$). If R is a UFD (respectively PID) then R_S is a UFD (respectively PID).*

Proof. We will first establish the statement for the case where R is a UFD. Again, we will show that an arbitrary prime ideal of R_S contains a prime element. Let $\mathfrak{P} \subseteq R_S$ be a prime ideal. Note that $\mathfrak{P} \bigcap R$ is a nonzero prime ideal of R (indeed, if $\frac{p}{s} \in \mathfrak{P}$ then $p \in \mathfrak{P} \bigcap R$. Since R is a UFD, $\mathfrak{P} \bigcap R$ must contain a nonzero prime element (say x). It suffices to show that x is a prime element in R_S.

Assume that x divides $\alpha\beta \in R_S$. Write $\alpha = \frac{a}{s_1}$ and $\beta = \frac{b}{s_2}$ with $a, b \in R$ and $s_1, s_2 \in S$. Then there is a $\gamma = \frac{c}{s_3} \in R_S$ ($c \in R$ and $s_3 \in S$) such that $x\gamma = \alpha\beta$ or

$$x\frac{c}{s_3} = \frac{a}{s_1}\frac{b}{s_2}.$$

Clearing the denominators we obtain

$$xcs_1s_2 = abs_3 \in R.$$

Note that x cannot divide s_3 (if so, then $x \in S$ hence $1 \in \mathfrak{P}$). So x must divide ab and we will say that x divides a without loss of generality. Hence $a = xk$ for some $k \in R$ and so $\frac{a}{s_1} = x(\frac{k}{s_1})$. This gives that x divides $\frac{a}{s_1}$ in R_S and we have established the result for the UFD statement.

For the statement concerning the PIDs, one could prove this directly (it is easy to show, for example, that every prime ideal in R_S is principal). But we will appeal to the localization correspondence theorem. Indeed it has been shown that if R is a PID (UFD) then R_S is a UFD. It remains to see that in R_S, every nonzero prime ideal is maximal. But the correspondence theorem shows that since every nonzero prime of R is maximal, then every nonzero prime ideal of R_S is maximal. □

3.3 Dedekind Domains and Invertible Ideals

Definition 3.3.1. *Let R be a domain with quotient field K. An $R-$submodule of $I \subseteq K$ is said to be a fractional ideal if there exists a nonzero $a \in R$ such that $aI \subseteq R$.*

Definition 3.3.2. *If I, J are fractional ideals of R then $IJ = \{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J\}$.*

Example 3.3.3. *Let $R = \mathbb{Z}$. The $R-$module $\frac{2}{3}\mathbb{Z}$ is a fractional ideal, but the $R-$module $\mathbb{Q}$ is not. The set $x\mathbb{Q}[x]$ is a fractional ideal of the domain $\mathbb{Q}[x^2, x^3]$.*

Definition 3.3.4. *If I is a fractional ideal of R, we define $I^{-1} := \{x \in K | xI \subseteq R\}$ (I^{-1} is referred to as the inverse of I).*

Note that it is always the case that $II^{-1} \subseteq R$. If we get lucky and $II^{-1} = R$ then we say that I is invertible.

Example 3.3.5. *If R is a domain and $x \neq 0$ is an element of the quotient field, then it is easy to see that $I = (x)$ is a fractional invertible ideal ($I^{-1} = (x^{-1})$).*

The following result shows that, in a certain sense, invertible ideals are rare (they must be finitely generated). More specifically, invertible ideals must be rank 1 projective $R-$modules, but we will not be taking that path at this time.

Theorem 3.3.6. *Let R be a domain. If I is an invertible ideal, then I is finitely generated.*

Note that for general domains the converse of this theorem is almost never true (once the realm of principal ideals are left behind). For a concrete example, consider the ideal $I = (x, y) \subseteq \mathbb{Q}[x, y]$. It is an easy computation to show that $I^{-1} = \mathbb{Q}[x, y]$ and hence $II^{-1} = I \subsetneq \mathbb{Q}[x, y]$.

Proof. Since $II^{-1} = R$ we can find $x_1, x_2, \cdots, x_n \in I$ and $y_1, y_2, \cdots, y_n \in I^{-1}$ such that

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = 1.$$

We claim that $I = (x_1, x_2, \cdots, x_n)$. Clearly $I \supseteq (x_1, x_2, \cdots, x_n)$. Now suppose that $a \in I$. Multiplying the above equation by a, we get

$$(ay_1)x_1 + (ay_2)x_2 + \cdots + (ay_n)x_n = a.$$

Since $a \in I$ and each $y_i \in I^{-1}$, we have that each $(ay_i) \in R$ and hence $a \in (x_1, x_2, \cdots, x_n)$. This concludes the proof. □

Theorem 3.3.7. *Suppose that $I \subseteq R$ is invertible. Then there is an ideal $J \subseteq R$ such that IJ is principal.*

Proof. Suppose first that $IJ = aR$ is principal. This gives that $I(Ja^1) = R$ and hence I is invertible (with inverse Ja^{-1}).

On the other hand, if I is invertible, then $II^{-1} = R$. Let a be a nonzero element of R and note that $aI^{-1} \subseteq R$. Hence $I(aI^{-1}) = aR$ is principal. □

The next result characterizes the so-called Dedekind domains. These domains are, in a certain sense, the next best thing to UFDs. It is not true in general that the elements in a Dedekind domain factor into primes, but the ideals factor uniquely into prime ideals. A large important class of Dedekind domains are the rings of algebraic integers from number theory. Additionally, all PIDs are Dedekind (but not all UFDs, in fact a UFD is Dedekind if and only if it is a PID).

Theorem 3.3.8. *Let R be an integral domain. The following conditions are equivalent.*

1) Every nonzero ideal $I \subseteq R$ is invertible.

2) Every nonzero fractional ideal is invertible.

3) Every nonzero proper ideal of R is uniquely a product of prime ideals.

4) R is Noetherian, integrally closed, and $dim(R) \leq 1$.

Any domain satisfying one (hence all) of the above condition is called a Dedekind domain.

Proof. We outline the proof here. The fact that 1) and 2) are equivalent is straightforward and is left as an exercise. For 2) implies 3) we let I be a proper nonzero ideal of R. If I is prime then we are done. If not then select a prime ideal P_1 containing I and consider IP_1^{-1}. Since $P \supseteq I$ we have that $P^{-1} \subseteq I^{-1}$ and hence IP^{-1} is a proper ideal of R. By the same token, IP_1^{-1} is contained in a prime ideal P_2 of R. If $IP_1^{-1} = P_2$ then we have $I = P_1P_2$, and if not we continue the process. We obtain the increasing chain of ideals

$$I \subseteq IP_1^{-1} \subseteq IP_1^{-1}P_2^{-1} \subseteq \cdots .$$

Since R is Noetherian (all ideals are invertible and hence finitely generated), this process must terminate. Hence at some point, we must have

$$IP_1^{-1}P_2^{-1} \cdots P_{n-1}^{-1} = P_n$$

and hence $I = P_1P_2 \cdots P_n$.

For 3) implies 2) it suffices to show that every prime ideal is invertible. Let $P \subseteq R$ be a nonzero prime ideal and let $x \in P$ be nonzero. Since (x) is a nonzero ideal, we can write $(x) = P_1P_2 \cdots P_n$. Note that since $P \supseteq (x)$ this implies that $P \supseteq P_1P_2 \cdots P_n$ and hence P must contain one of the factors (say $P \supseteq P_1$). If $P = P_1$ then we are done, since there is an ideal (namely $P_2P_2 \cdots P_n$) such that $(P)(P_2P_3 \cdots P_n)$ is principal. We leave it as an exercise to show that $P = P_1$ (hint: consider an element $y \in P \setminus P_1$.

We leave the equivalence of 4) to 1), 2), and 3) as an exercise. □

Example 3.3.9. *The ring $\mathbb{Z}[\sqrt{-5}]$ is Dedekind. This ring is not a UFD as we have the elemental factorization $(2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$. It is easy to see that this is a nonunique factorization by applying the standard norm map. To see the reconciliation of factorization with respect to ideals, consider the ideals $\mathfrak{R} = (2, 1+\sqrt{-5})$, $\mathfrak{P} = (3, 1+\sqrt{-5})$, and $\mathfrak{Q} = (3, 1-\sqrt{-5})$. A simple computation shows that $\mathfrak{R}^2 = (2)$, $\mathfrak{PQ} = (3)$, $\mathfrak{PR} = (1+\sqrt{-5})$, and $\mathfrak{QR} = (1-\sqrt{-5})$. The elemental factorization come from rearranging the factors in the ideal factorization*

$$\mathfrak{PQRR} = (6).$$

We also note that since any principal ideal is invertible, it is immediate that every PID is Dedekind.

Definition 3.3.10. *Let R be a domain, $Inv(R) = \{I | I$ is an invertible ideal of $R\}$, and $Prin(R) = \{xR | x \in K \setminus \{0\}\}$. The quotient group $Cl(R) := Inv(R)/Prin(R)$ is called the class group of R. If $|Cl(R)| = n < \infty$ then n is called the class number of R.*

The set of invertible ideals forms a group under ideal multiplication (with identity R). The set of principal ideals forms a subgroup. Since the group of invertible ideals is often "too big" we consider the quotient group formed by taking the invertible ideals modulo the principal ideals. We shall soon see that this class group is often a good measure of how far a domain is from being a UFD. In many important cases, (e.g. rings of algebraic integers) the class group is finite. The problem of determining class numbers for rings of integers is still wide open in many cases (in fact, it is still unknown as to whether there are an infinite number of real quadratic rings of integers with class number 1). It should also be noted that in the case of Dedekind domains, the class group is an especially effective tool since every ideal is invertible.

This theorem records some useful facts concerning Dedekind domains.

Theorem 3.3.11. *Let R be a Dedekind domain.*

1) R is a UFD if and only if R is a PID.

2) If R has only finitely many maximal ideals, then R is a PID.

3) Every ideal of R can be generated by less than or equal to two elements.

Proof. 2) and 3) are left as exercises. For 1) the interesting implication is that if R is a UFD then it is a PID. But since R is Dedekind it is one dimensional. Coupling this with the UFD assumption, we obtain that R is a PID. □

Example 3.3.12. *In the previous example ($\mathbb{Z}[\sqrt{-5}]$) it turns out that the class number is two (that is, $Cl(R) \cong \mathbb{Z}_2$. We shall see later that this condition implies that although there are factorizations that are nonunique, all factorizations of the same element have the same length.*

Example 3.3.13. *For a more interesting example along these lines consider the ring* $\mathbb{Z}[\sqrt{-14}]$ *(note in this ring we have the irreducible factorization* $(3)(3)(3)(3) = (5+2\sqrt{-14})(5-2\sqrt{-14})$*. This ring has class number 4 (so the class group is isomorphic to either* $\mathbb{Z}_4$ *or* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$*). We give ideals in each of the four classes:*

$$(1), (3, 1-\sqrt{-14}), (3, 1-\sqrt{-14}), (2, \sqrt{-14}).$$

Determine the structure of the class group given this information.

We close this section with a theorem that demonstrates the fact that the class group measures loss of unique factorization.

Theorem 3.3.14. *Let* R *be a Dedekind domain. Then* R *is a UFD if and only if the class group of* R *is trivial.*

Proof. Suppose that R is a UFD and Dedekind. We have already established that R is a PID and hence any (invertible) ideal is principal. Hence $\text{Inv}(R)$ and $\text{Prin}(R)$ coincide and the class group is trivial.

On the other hand, if the class group of R is trivial, this implies that every invertible ideal is principal. But since R is Dedekind (and every ideal is invertible) we have that R is a PID (and hence a UFD). □

Chapter 4

More on Dedekind Domains, Half-Factorial Domains, and Orders

4.1 Rings of Integers

We begin this chapter with a large and important class of Dedekind domains. The proof of this theorem is lengthy and we will only sketch it.

Theorem 4.1.1. *Let F be a finite field extension of $\mathbb{Q}$ and let R be the integral closure of $\mathbb{Z}$ in F. Then R is a Dedekind domain.*

Such a Dedekind domain is called a ring of (algebraic) integers.

Proof. The idea of the proof is to show that R is one-dimensional (which follows from the fact that R is an integral extension of the one-dimensional domains $\mathbb{Z}$), Noetherian (which follows from the fact that F is a finite-dimensional extension of $\mathbb{Q}$) and integrally closed (which follows from the fact that integral closures are integrally closed). We leave it to the ambitious reader to fill in the wide gaps. □

Example 4.1.2. *It is a good computational exercise to compute the ring of integers of a quadratic extension of $\mathbb{Q}$. Let d be a square-free integer; we consider the (quadratic) extension $F := \mathbb{Q}(\sqrt{d})$. Show that the ring of integers of F is given by*

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \ mod(4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \ mod(4) \end{cases}$$

See if you can determine the ring of integers for the field $\mathbb{Q}\sqrt[3]{2}$.

We record the following useful theorem concerning rings of algebraic integers. The proof of this theorem can be found in many standard texts on number theory.

Theorem 4.1.3. *Let R be a ring of algebraic integers. Then R enjoys the following properties.*

1) $Cl(R)$ is finite.

2) Every ideal class in $Cl(R)$ contains infinitely many prime ideals.

The second statement is a generalization of the well known result in elementary number theory that if m and n are relatively prime integers then there are infinitely many primes of the form $m + an$. In fact, prime ideals tend to be distributed more or less "evenly" in the ideal classes of a ring of algebraic integers.

4.2 Half-Factorial Domains, A First Look

The class of half-factorial domains first appeared implicitly in 1960 in a paper by Carlitz. The terminology was coined by Zaks in two papers that appeared in 1976 and 1980. In his papers, Zaks abstracted the initial work of Carlitz and did a rather thorough study of half-factorial domains (it is worth mentioning that the original definition of half-factorial domain is not the same as the "accepted" one of today).

In the 1980's there was an explosion of work in the field of factorization, and the class of half-factorial domains was explored further and is still an area of rich mathematics.

Basically half-factorial domains have "half the properties" of UFDs. That is we do not require that a half-factorial domain to have unique factorization. But we do require that any two equal irreducible factorizations have the same length. We make this more precise below.

Definition 4.2.1. *An atomic domain, R, is said to be a half-factorial domain if given any factorization*

$$\alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m$$

with each α_i, β_j irreducible, then $n = m$.

The orginal definition from Zaks' paper did not make the assumption that R is atomic (so by the original definition, any domain with no irreducible elements is a half-factorial domain). The modern convention is for half-factorial domains (HFDs) to be atomic and we will follow this convention.

Example 4.2.2. *Of course any UFD is an HFD. There are amny examples of HFDs which are not UFDs. By Carlitz' 1960 paper, any ring of integers that has class number 2 is an HFD that is not a UFD (we will see this later).*

Additionally the ring $\mathbb{Z}[\sqrt{-3}]$ is an HFD, but cannot be a UFD since it is not integrally closed. An example that is easier to visualize at this stage is the ring

$$R := \mathbb{R} + x\mathbb{C}[[x]].$$

It is easy to see that this ring is not a UFD directly or by noting that it is not integrally closed. To see that this ring is an HFD, we first note that the nonzero nonunits of R are precisely the elements of the form $x^n f(x)$ where $f(x) \in \mathbb{C}[[x]]$ and $n \geq 1$ (if $n = 0$ it is easy to see that $f(0)$ is a nonzero real number and $f(x)$ is a unit). Fom this we can conclude that the irreducibles of R is precisely the subset of the nonzero nonunits consisting of elements of the form $xf(x)$ with $f(0) \neq 0$. This allows us to count the number of irreducible factors in a general nonzero nonunit. Namely the nonzero nonunit $x^n f(x)$ may have multiple factorizations, but the number of irreducible factors in a given factorization is always n.

For rings of algebraic integers, there is an extremely nice characterization of the HFD property. This beautiful result is due to Carlitz.

Theorem 4.2.3. *Let R be a ring of algebraic integers. Then R is an HFD if and only if $|Cl(R)| \leq 2$.*

More is true, in fact. This characterization neatly partitions rings of integers that are HFDs into two classes. Class number 1 rings of integers are UFDs and class number 2 rings of integers are non-UFD HFDs.

Proof. We assume first that the class number of R does not exceed 2. If the class number of R is 1 then R is a UFD and so is trivially an HFD. We will therefore suppose that the class number of R is 2.

We now claim that if $x \in R$ is irreducible and not prime, then as an ideal (x) factors into precisely two (nonprincipal) prime ideals of R. To see this suppose that

$$(x) = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_n.$$

If one of the prime ideals on the right is principal (say $\mathfrak{P}_1$) this would imply that $\mathfrak{P}_2 \cdots \mathfrak{P}_n = R$ since x is irreducible. Hence all of the prime ideals on the right must be nonprincipal. But since the class number of R is 2 and each ideal is nonprincipal, this implies that the product of any two of them is principal. Hence $\mathfrak{P}_1\mathfrak{P}_2$ is principal. Again by the irreducibility of x, we must have that $\mathfrak{P}_3 \cdots \mathfrak{P}_n = R$. Hence $n = 2$.

With this claim in hand we consider the irreducible factorization

$$\alpha_1\alpha_2 \cdots \alpha_n = \beta_1\beta_2 \cdots \beta_m.$$

Since any prime factor above must appear on both sides (and can therefore be cancelled) we can assume without loss of generality that each irreducible above is nonprime. By the claim each $(\alpha_i) = \mathfrak{P}_{i,1}\mathfrak{P}_{i,2}$ and each $(\beta_j) = \mathfrak{Q}_{j,1}\mathfrak{Q}_{j,2}$. We

now consider the elemental factorization as an ideal factorization and replace each irreducible with its prime factors to obtain:

$$\mathfrak{P}_{1,1}\mathfrak{P}_{1,2}\cdots\mathfrak{P}_{n,1}\mathfrak{P}_{n,2} = \mathfrak{Q}_{1,1}\mathfrak{Q}_{1,2}\cdots\mathfrak{Q}_{m,1}\mathfrak{Q}_{m,2}.$$

Since this factorization into prime ideals is unique, we get that $2n = 2m$ and hence $n = m$.

For the other direction, we will that the class number of R is greater than 2 and show that R cannot be an HFD.

The first case to consider is the case where there is an element in $[I] \in \mathrm{Cl}(R)$ of order $n > 2$. Let $\mathfrak{P}$ be a prime in this class and select a prime ideal $\mathfrak{Q}$ in $[I]^{-1}$. We can make this choice as there are (infinitely many) prime ideals in every ideal class of a ring of integers.

We now claim that the ideals $\mathfrak{P}^n, \mathfrak{Q}^n$, and $\mathfrak{P}\mathfrak{Q}$ are all principal and generated by irreducible elements. The fact that these ideals are principal follows easily from the choices that we made (the ideal classes where they are contained). To see that $\mathfrak{P}^n$ is generated by an irreducible, note first that $\mathfrak{P}^n = (x)$ for some $x \in R$. If $x = ab \in R$, then

$$(x) = (a)(b) = \mathfrak{P}^n.$$

In particular, since prime ideal factorizations are unique, the ideal factorization of (a) must be $\mathfrak{P}^m$ for some $m \leq n$. But since the order of $\mathfrak{P}$ is n, and (a) is principal, this forces m to be either 0 or n. Of course this means that a or b must be a unit. The proof that $\mathfrak{P}\mathfrak{Q}$ is irreducible is similar, but easier.

We now consider the ideal factorization

$$(\mathfrak{P}^n)(\mathfrak{Q}^n) = (\mathfrak{P}\mathfrak{Q})^n.$$

We now let α an irreducible generator for $\mathfrak{P}^n$, β an irreducible generator for $\mathfrak{Q}^n$, and γ an irreducible generator for $\mathfrak{P}\mathfrak{Q}$. The above equation yields

$$(\alpha)(\beta) = (\gamma)^n,$$

and this implies that there is a unit $u \in U(R)$ such that

$$\alpha\beta = u\gamma^n.$$

Since $n > 2$ we have that R is not an HFD.

The final case is the situation where every nonidentity element of the class group has order 2. Since the class number is at least 3, and every nonidentity element of the class group has order 2, we can conclude that the class group must contain a subgroup isomorphic to the Klein 4-group ($\mathbb{Z}_2 \oplus \mathbb{Z}_2$). Writing this subgroup additively, we select prime ideals $\mathfrak{P}$ in the class corresponding to the element $(0, 1)$, $\mathfrak{Q}$ in the class corresponding the element $(1, 0)$, and $\mathfrak{R}$ in the class corresponding to $(1, 1)$. In a similar fashion to the previous argument $\mathfrak{P}^2$ is principal and generated by the irreducible α, $\mathfrak{Q}^2$ is principal and generated by the irreducible β, $\mathfrak{R}^2$ is principal and is generated by the irreducible γ, and

$\mathfrak{PQR}$ is principal and generated by the irreducible δ. We consider the ideal factorization

$$(\mathfrak{P}^2)(\mathfrak{Q}^2)(\mathfrak{R}^2) = (\mathfrak{PQR})^2$$

or equivalently

$$(\alpha)(\beta)(\gamma) = (\delta)^2.$$

We now have that there is a unit $u \in U(R)$ such that $\alpha\beta\gamma = u\delta^2$ and hence R is not an HFD. This completes the proof. □

4.3 Imaginary Quadratic Fields

We begin by considering rings of algebraic integers in imaginary quadratic fields. That is $F = \mathbb{Q}[\sqrt{d}]$ with d a square-free integers and $d < 0$. R is the integral closure of $\mathbb{Z}$ in F. We have seen (more generally) that

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod(4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod(4). \end{cases}$$

There is a nice result for UFDs in imaginary quadratic fields. We use the notation for d above instead of the discriminant notation more frequently used in number theory.

Theorem 4.3.1. *If R is an imaginary quadratic ring of integers, then R is a UFD if and only $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.*

Here is an open conjecture (the fact that it has been open since the time of Gauss shows that the real case is quite a bit more problematic that the imaginary case).

Conjecture 4.3.2. *There are infinitely many real quadratic UFDs.*

Another result from number theory, coupled with Carlitz' Theorem, shows that the search for imaginary quadratic HFDs is a finite one.

Proposition 4.3.3. *There are only finitely many totally complex abelian extensions of $\mathbb{Q}$ with a given degree and class number.*

The proof of this is beyond the scope of this book, but what the result means for us is that given degree 2 complex extensions of $\mathbb{Q}$ with class number 2 is finite. In fact, all imaginary quadratic fields of class number 2 have been found (and hence all imaginary quadratic HFDs). Using the notation from above, the imaginary quadratic HFDs correspond to $d = -5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123, -187, -235, -267, -403, -427$.

It is now natural to consider subrings of quadratic rings of integers. For the quadratic case, one can explicitly write down the orders in a quadratic ring of

integers (an order is a subring with the same quotient field as the original ring of integers). The quadratic order of index (or conductor) $n \in \mathbb{N}$ is the ring

$$R_n = \begin{cases} \mathbb{Z}[n\sqrt{d}] & \text{if } d \equiv 2, 3 \mathrm{mod}(4) \\ \mathbb{Z}[n(\frac{1+\sqrt{d}}{2})] & \text{if } d \equiv 1 \mathrm{mod}(4). \end{cases}$$

We observe that the order R_n is integrally closed if and only if $n = 1$. So the only chance for UFDs occur when $n = 1$. HFDs, however, do not suffer from the restriction "integrally closed". There is an example of an HFD that is not integrally closed in this class of domains. Namely $\mathbb{Z}[\sqrt{-3}]$ (this corresponds to $d = -3$ and $n = 2$). To see that this domain is an HFD, we will use the fact that $\mathbb{Z}[\omega]$, with $\omega = \frac{1+\sqrt{-3}}{2}$, is a UFD. We will take as given that $\mathbb{Z}[\omega]$ is a UFD and we will outline the details that $\mathbb{Z}[\sqrt{-3}]$ is an HFD below.

Example 4.3.4. *In this example, we outline the proof that $\mathbb{Z}[\sqrt{-3}]$ is an HFD. We use the fact that $R := \mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega] := T$, with $\omega = \frac{-1+\sqrt{-3}}{2}$ (we have adjusted ω, making it a primitive cube root of unity, for computational ease), and that the larger domain is a UFD. We first claim that every element $t \in T$ there is a natural number $0 \leq n \leq 2$ such that $\omega^n t \in R$. Additionally if two distinct powers in this range have the property that $\omega^n t \in R$, then $\omega^m t \in R$ for all n.*

To see this let $t = x + y\omega \in T$. Note that $\omega t = x\omega + y\omega^2 = -y + (x - y)\omega$ (using the fact that $\omega^2 = -1 - \omega$) and $\omega^2 t = (y - x) - x\omega$. So if x and y are both even then $\omega^m t \in R$ for all m. If x is even and y is odd then only $\omega^2 t$ is in R, if x is odd and y is even then $t \in R$ but neither ωt nor $\omega^2 t$ is in R. Finally, if x and y are both odd, then only omegat is in R. This established the claim.

We now claim that any irreducible of R remains irreducible in T. To see this we assume that the irreducible $r \in R$ factors nontrivially $r = xy \in T$. By the claim, there are powers of ω, each between 0 and 2, such that $\omega^a x \in R$ and $\omega^b y \in R$. Hence we have the factorization

$$(\omega^a x)(\omega^b y) = r\omega^{a+b}.$$

If $a + b \equiv 0 mod(3)$ then we have contradicted the irreducibility of $r \in R$. But if $a + b$ is not a multiple of 3, then by our previous claim, any power of ω times r is an element of R and hence $r = u + v\omega$ with both u and v even. Since $xy = r$ as straightforward computation shows that either $x = x_1 + x_2\omega$ with x_1, x_2 both even or $y = y_1 + y_2\omega$ with both y_1, y_2 even. We will assume without loss of generality that x has this property. Hence any power of ω times x is an element of R and we have

$$(\omega^{-b} x)(\omega^b y) = r$$

and we have our desired contradiction. Hence every irreducible in R is irreducible in T.

To finish this example, we take an irreducible factorization

$$\alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m$$

in R. Since each of these factors remains irreducible in T, we can think of this as an irreducible factorization in the UFD T. Hence $n = m$.

One may wonder how it is that we know that the ring $T = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a UFD (which was central in the above approach). It is known that the class number of T is 1, and this can be determined (for example) by the Minkowski bound. It turns out that every ideal class contains an ideal of norm bounded by the a constant depending on certain invariants of the field. The proof is geometric in nature and can be found in a number of texts. We state the theorem more precisely for the interested reader.

Theorem 4.3.5. *Let R be a ring of integers with quotient field K. Suppose the $[K : \mathbb{Q}] = n = r_1 + 2r_2$ with r_1 the number of real embeddings of K in $\mathbb{C}$ and $2r_2$ the number of complex embeddings. In any ideal class of R there is an ideal I such that*

$$N(I) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}$$

where d_K denotes the field discriminant and $N(I)$ is the norm of I.

This bound allows one to compute the class number of a field by looking for ideals below the Minkowski bound and (if nothing else) doing a long computation to find the class structure. For the example that we just did, the relevant numbers are $d_K = -3, n = 2$, and $r_2 = 1$. The Minkowski bound for this field turns out to be $\frac{2\sqrt{3}}{\pi}$ which is approximately 1.103. Hence there is an ideal of norm less than 1.103 in every ideal class. But the norm is an integer and the only ideal with norm 1 is the unit ideal, hence T has class number 1 and is a UFD.

One may ask what are the imaginary quadratic HFDs that are nontrivial orders. We have the one example $\mathbb{Z}[\sqrt{-3}]$, but are there others? As we have seen, the orders with $n > 1$, are not integrally closed so one might think of the HFD property as a best possible outcome from a factorization point of view. But as it turns out, the example given above is unique.

Proposition 4.3.6. *The domain $\mathbb{Z}[\sqrt{-3}]$ is the unique imaginary quadratic HFD that is not integrally closed.*

Proof. We have already shown that $\mathbb{Z}[\sqrt{-3}]$ is an HFD, we will concentrate on uniqueness here. We briefly recall that the imaginary quadratic orders take on the form:

$$R_n = \begin{cases} \mathbb{Z}[n\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod(4) \\ \mathbb{Z}[n(\frac{1+\sqrt{d}}{2})] & \text{if } d \equiv 1 \bmod(4) \end{cases}$$

with $d < 0$.

We tackle this problem in a couple of cases. The first case will be the case where $d \equiv 2, 3 \mathrm{mod}(4)$. In this case we write $R = \mathbb{Z}[n\sqrt{d}]$.

We consider the element $n\sqrt{d} \in R$ and claim that this element is irreducible. To see this we consider the norm

$$N(n\sqrt{d}) = -dn^2$$

and recall that the norm of a general element is given by

$$N(x + yn\sqrt{d}) = x^2 - dn^2y^2.$$

It is easy to see that $x^2 - dn^2y^2 \geq -dn^2$ if $y \neq 0$. We conclude that if $x + yn\sqrt{d}$ is a proper divisor of $n\sqrt{d}$ then $x + yn\sqrt{d} = x \in \mathbb{Z}$. But clearly $n\sqrt{d}$ is not divisible by any integer in R.

Since we have the $n\sqrt{d}$ is irreducible, we consider the factorization

$$(n\sqrt{d})(n\sqrt{d}) = (d)(n)(n).$$

Since the left has two irreducible factors and $n > 1$, we see that for R to be an HFD it is necessary that n must be prime (in $\mathbb{Z}$) and $d = -1$. So at this point we have deduced that the only possible HFDs are the ones of prime index in the Gaussian integers.

Suppose that we have an HFD of index p (prime) in the Gaussian integers. We write $\mathbb{Z}[pi] \subseteq \mathbb{Z}[i]$. We now consider the element $p + pi \in \mathbb{Z}[pi]$. Note the the norm is given by

$$N(p + pi) = 2p^2$$

and so any proper divisor of $p + pi$ must have norm $2, p, 2p$, or p^2. Additionally if one divisor has norm k then the other divisor must have norm $\frac{2p^2}{k}$ and hence we can assume that our divisor has norm either 2 or p. It is easy to see that there is no element of $\mathbb{Z}[pi]$ of norm 2 or p. This completes the first case.

We will now assume that $d \equiv 1 \mathrm{mod}(4)$. In this case we write $R = \mathbb{Z}[n(\frac{1+\sqrt{d}}{2})]$. In an analogous fashion, we consider the element $n(\frac{1+\sqrt{d}}{2}) \in R$. Computing the norm, we obtain

$$N(n(\frac{1+\sqrt{d}}{2})) = n^2(\frac{1-d}{2})$$

and we again claim that this element is irreducible.

If $x + yn(\frac{1+\sqrt{d}}{2})$ divides $n(\frac{1+\sqrt{d}}{2})$ then its norm must divide $n(\frac{1-d}{2})$. We compute the norm of our general element:

$$N(x + yn(\frac{1+\sqrt{d}}{2})) = x^2 + xy + n^2y^2(\frac{1-d}{2}) = (x + \frac{n}{2}y)^2 - \frac{d}{4}n^2y^2.$$

For convenience we will also assume that the the norm of our divisor is bounded above by $n^2(\frac{1-d}{8})$ since the norm of a proper divisor of an element must be no

more than one half of the norm of the original element (since the quotient must be an integer).

For a fixed value of y a quick application of calculus shows that the norm form is minimized when $x = -\frac{n}{2}y$ and the minimum value at this point is $-\frac{d}{4}n^2y^2$. From this we obtain

$$-\frac{d}{4}n^2y^2 \leq n^2(\frac{1-d}{8})$$

noindent which gives

$$y^2 \leq \frac{d-1}{2d} < 1.$$

It is immediate that $y = 0$ and hence the element $n(\frac{1+\sqrt{d}}{2})$ is divisible by an integer which is a contradiction. Hence $n(\frac{1+\sqrt{d}}{2})$ is irreducible.

As before we consider the factorization

$$n(\frac{1+\sqrt{d}}{2})n(\frac{1-\sqrt{d}}{2}) = n^2(\frac{1-d}{4}) = (n)(n)(\frac{1-d}{4})$$

and since the factors on the left are irreducible, it is necessary for n to be prime and $d = -3$ for R to be an HFD. So the only possibilities are the orders of prime index in the ring $\mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-3}}{2}$. In this case we already know that the case $p = 2$ works (since it is $\mathbb{Z}[\sqrt{-3}]$). We will therefore assume that $p > 2$.

In the ring $\mathbb{Z}[p\omega]$ we consider the element $p + p\omega$. The norm of this element is

$$N(p + p\omega) = 3p^2$$

and so, as before, if $p + p\omega$ has a proper divisor, it must have a divisor of norm 3 or p. It is easy modular arithmetic to see that $\mathbb{Z}[p\omega]$ has no element of norm p. To eliminate the norm 3 possibility consider

$$N(a + pb\omega) = a^2 + pab + p^2b^2 = (a + \frac{1}{2}pb)^2 + \frac{3}{4}p^2b^2.$$

If it were possible to produce an element of norm 3, we would have $(a + frac12pb)^2 + \frac{3}{4}p^2b^2 = 3$ or

$$(2a + pb)^2 + 3p^2b^2 = 12.$$

It is clear that b cannot be 0. Hence we get $3p^2b^2 \leq 12$ and so $p \leq 2$ which is a contradiction.

To finish this off, we consider the factorization

$$(p + p\omega)(p + \overline{\omega}) = (p)(p)(p)$$

and since $p + p\omega$ is irreducible, we have that R is not an HFD. This concludes the proof.

□

As an ending note to this section, the search for HFDs as orders in real quadratic rings of integers is more fruitful. In fact inside the ring of integers $\mathbb{Z}[\sqrt{2}]$ the orders $\mathbb{Z}[n\sqrt{2}]$ produce HFDs for the values $n = 59, 179, 227, 251, 379, 419, 443, 643, 683, 827,$ and 1187. This list is almost certainly not exhaustive, and it has been conjectured that there are infinitely many HFDs that exist as orders in $\mathbb{Z}[\sqrt{2}]$.

4.4 Some Generalizations

We begin this section by looking at a fairly rich variety of elemental factorizations that can be given even in a ring with relatively small class number.

Example 4.4.1. *We consider the ring $\mathbb{Z}[\sqrt{-14}]$. It turns out that the class group of this domain is isomorphic to $\mathbb{Z}_4$. For convenience of notation we will say that each prime P_i comes from the class that corresponds to $\overline{1} \in \mathbb{Z}_4$, each prime M_i comes from the class corresponding to $\overline{2} \in \mathbb{Z}_4$ and each prime Q_i comes from the class corresponding to $\overline{3} \in \mathbb{Z}_4$. Since we want interesting factorizations we will ignore primes coming from the principal class (prime elements). Note that since we are dealing with rings of integers, we have infinitely many primes in every class.*

We consider the following principal ideals

1) $(x_1) = P_1^8$

2) $(x_2) = P_1^4 P_2^4$

3) $(x_3) = P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8$

4) $(x_4) = P_1^4 Q_1^4$

5) $(x_5) = P_1 P_2 P_3 P_4 Q_1 Q_2 Q_3 Q_4$

6) $(x_6) = M_1^2$

We make some observations about the factorizations of the elements $x_1, x_2, x_3, x_4, x_5, x_6$. When we speak of factorizations being "distinct" or "the same" we will be ignoring silly fiddling with units.

1) The element x_1 factors uniquely into its product of irreducible elements. If we let α be a generator of the principal ideal P_1^4, we find that $x_1 = u\alpha^2$ for some $u \in U(R)$. Since (x_1) is a power of a single prime ideal, this forces uniqueness of the generator of P_1^4 (up to a unit) and hence the factorization of x_1.

2) The element x_2 has three distinct factorizations all of length 2. To see this, consider the principal ideals $(\alpha_i) = P_1^i P_2^{4-i}$ for $0 \leq i \leq 4$. The ideal $(x_2) = (\alpha_i)(\alpha_{4-i})$ and so we have (up to units)

$$x_2 = \alpha_0\alpha_4 = \alpha_1\alpha_3 = \alpha_2^2.$$

3) The element x_3 has 35 factorizations, each of length 2. Since all of the ideals are in the same class, combining these to make principal ideals (irreducibles) is no different. But choosing the 4 primes in an arbitrary manner from 8 to "build" irreducibles makes for much variety. There are $\frac{1}{2}\binom{8}{4} = 35$ different pairs of irreducibles that can be created in a factorization of x_3.

4) The element x_4 has but two distinct factorizations, but one is of length 2 and the other is of length 4. We let $(\alpha) = P_1^4$, $(\beta) = Q_1^4$, and $(\gamma) = P_1Q_1$. Up to units our factorizations are

$$x_4 = \alpha\beta = \gamma^4.$$

5) The element x_5 has 24 factorizations of length 4 and 1 factorization of length 2. The factorization of length 2 is fairly easy to see. If we let $\alpha = P_1P_2P_3P_4$ and $\beta = Q_1Q_2Q_3Q_4$, we have up to units that $x_5 = \alpha\beta$. The 24 factorizations of length 4 come from creating irreducibles as generators of the ideals P_iQ_j. There are $4! = 24$ ways to do this.

6) The element x_6 is actually irreducible, but computationally, it can be a bit deceptive as its norm is a square.

We now introduce some definitions that extend the notion of HFDs in some natural directions that may be inspired by the previous example.

Definition 4.4.2. *Let $r > 1$ be an integer. We say that the atomic domain D is a congruence half-factorial domain of order r (CHFD−r) if*

$$\alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m$$

with each α_i, β_j irreducible implies that $n \equiv m mod(r)$.

And here is another generalization.

Definition 4.4.3. *Let k be a natural number. We say that the atomic domain D is a $k-$HFD if*

$$\alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m$$

with each α_i, β_j irreducible and $n \leq k$ implies that $n = m$.

We pause here to make a couple of simple observations. Of course, any atomic domain is 1−HFD. If D is not $t-$HFD then it is not $k-$HFD for any $k \geq t$. Also note that D is an HFD if and only if D is $k-$HFD for all k.

The following theorem shows that at least a little exoticness is needed for these classes of domains.

Theorem 4.4.4. *Let D be a Dedekind domain with torsion class group such that every ideal class contains a prime ideal. The following conditions are equivalent.*

1) $|Cl(R)| \leq 2$.

2) D *is an HFD.*

3) D *is a* $k-$*HFD for some* $k > 1$.

4) D *is a CHFD*$-r$ *for some* $r > 1$.

We now produce a result in line of our first example from this section.

Theorem 4.4.5. *Let* R *be a Dedekind domain and* $x \in R$ *a nonzero nonunit. Then up to units,* x *has finitely many irreducible factorizations in* R.

Proof. We write the ideal (x) as

$$(x) = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_n.$$

Any irreducible factorization for x can be formed by subproducts of the above prime ideal factorization that form principal ideals (if any). Clearly the number of such possible subproducts if finite (it can be coarsely counted by counting partitions and rearrangements for every partition...this number grows extremely fast, but is finite).

□

We remark that the theorem above is still correct if "Dedekind" is replaced by "Noetherian".

We cannot resist the following corollary which is standard in number theory.

Corollary 4.4.6. *If* R *is a ring of integers and* $n \in \mathbb{N}$ *then there exists only finitely many elements* $\alpha \in R$ *(up to units) such that* $|N(\alpha)| \leq n$.

Chapter 5

Elasticity and the Davenport Constant

5.1 The Davenport Constant

We momentarily sidestep into the theory of finite abelian groups. The Davenport constant is an invariant of a finite abelian group that has been studied from a purely group theoretic point of view. We will introduce the Davenport constant in this section and will soon see how it is tied to the theory of factorization.

Definition 5.1.1. *Let G be a finite abelian group. We say that the ($G-$)sequence $\{g_1, g_2, \cdots, g_n\}$ of (not necessarily distinct) elements of G is a zero sequence if $g_1 + g_2 + \cdots + g_n = 0$. Additionally we say that the sequence has a zero subsequence if there is a subsequence that sums to 0 (more precisely there exist $1 \leq i_1 \leq 2 \leq \cdots \leq i_k \leq n$ such that $g_{i_1} + g_{i_2} + \cdots + g_{i_k} = 0$).*

Example 5.1.2. *If $G = \mathbb{Z}_4$ then the sequence $\{1, 1, 1, 1\}$ is a zero sequence. The sequence $\{1, 2, 3\}$ is not a zero sequence but does have a zero subsequence. Neither $\{1, 2\}$ nor $\{1, 1, 1\}$ have zero subsequences.*

Definition 5.1.3. *Let G be a finite abelian group. We define the Davenport constant of G to be*

$$D(G) = min\{n| \text{ every } G-\text{sequence of length } n \text{ has a zero subsequence}\}.$$

Some authors define $D(G)$ to be the maximum length of a zero sequence that contains no proper zero subsequence. The reader should show that these two definitions are equivalent.

Example 5.1.4. *Show that $D(\mathbb{Z}_4) = 4$, $D(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 3$ $D(\mathbb{Z}_6) = 6$, $D(\mathbb{Z}_2 \oplus \mathbb{Z}_4) = 5$, and $D(\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2) = 4$.*

Proposition 5.1.5. *If G be a finite abelain group, then $D(G) \leq |G|$.*

Proof. Consider the sum $g_1 + g_2 + \cdots + g_n + g_{n+1} + \cdots + g_{n+r}$. We claim that if $r > 0$ then there exists a zero subsequence. To see this consider the equations below.

$$\begin{cases} g_1 & := x_1 \\ g_1 + g_2 & := x_2 \\ g_1 + g_2 + g_3 & := x_3 \\ \vdots & \vdots \\ g_1 + g_2 + g_3 + \cdots + g_{n-1} & := x_{n-1} \\ g_1 + g_2 + g_3 + \cdots + g_{n-1} + g_n & := x_n \end{cases}$$

If none of the x_i, $1 \leq i \leq n$ are 0 then all of the x_i's are distinct (if not then $x_r = x_s$ for some $r > s$ and $g_{s+1} + \cdots + g_r = 0$). Hence the elements $x_1, x_2, \cdots, x_n$ are all distinct and this contradicts the fact that $|G| = n$, and the proof is complete. □

Corollary 5.1.6. *If G is cyclic of order n then $D(G) = |G| = n$.*

Proof. We already know that $D(G) \leq n$, to show equality consider the generator α of G. The sequence of α repeated n times is a zero sequence with no proper zero subsequence, since α generates G. □

We now give a couple of results that almost get us to the frontier of closed form respresentations of the Davenport constant. Despite what would seem to be a quite simple and seductive problem is actually quite difficult and aloof. We supply this knowledge without proof and encourage the reader to go farther (but perhaps after tenure).

Theorem 5.1.7. *Let p be a (nonzero) prime integer and $G \cong \mathbb{Z}_{p^{a_1}} \oplus \mathbb{Z}_{p^{a_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{a_n}}$ then $D(G) = 1 + \sum_{i=1}^{n}(p^{a_i} - 1)$.*

Theorem 5.1.8. *Let m and n be integers with m dividing n. If $G \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ then $D(G) = m + n - 1$.*

We now begin our exploration of the connection between this group-theoretic invariant and the theory of factorization.

Theorem 5.1.9. *Let R be a Dedekind domain and let $|C(R)| = n < \infty$. If $\alpha \in R$ is irreducible and $(\alpha) = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_m$ then $m \leq D(G)$. Equality is attained for some irreducible in R if there are infinitely many prime ideals in every class.*

We remark that in a worst case scenario, we only need n prime ideals in every class (and this is usually too sloppy as well) as the proof should illustrate.

Proof. Suppose thaat $(\alpha) = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_m$. We write this equation additively in the class group as

$$[\mathfrak{P}_1] + [\mathfrak{P}_2] + \cdots + [\mathfrak{P}_m] = 0.$$

Since α is irreducible, no proper subsequence can be a zero subsequence (if so we can construct two proper principal divisors of α). It is now immediate that $m \leq D(G)$.

For the next statement, we will assume that there is a prime in every class and we choose a zero sequence of length $k = D(G)$:

$$[I_1] + [I_2] + \cdots + [I_k] = 0.$$

Now choose a prime $\mathfrak{P}_i$ in the class $[I_i]$ and notice that $(\beta) = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_k$ is principal and β is irreducible since so subproduct of the primes is principal. In this case we see that $D(G)$ is the length of the longest possible prime factorization of an irreducible.

□

5.2 The Elasticity of a Domain

In this section we will assume that R is atomic. We first define the elasticity of a domain.

Definition 5.2.1. *Let R be an atomic domain. We define the elasticity of a nonzero nonunit $r \in R$ to be*

$$\rho(r) = sup\{\frac{n}{m} | r = \alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m\}$$

where the α's and β's are irreducible.

We define the elasticity of the domain R to be

$$\rho(R) = sup\{\frac{n}{m} | \alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m\}$$

where the α's and β's are irreducible.

We note here that our convention will be the the elasticity of a field is 1. Also it is clear that the elasticity of any HFD (UFD) is 1 as well. In a certain sense, the elasticity of a domain is a measure of how "wildly" factorization lengths of an element can be.

Example 5.2.2. *Consider the domain*

$$R := \mathbb{Z}[x, y_{1,1}, y_{1,2}, y_{2,1}, y_{2,2}, y_{2,3}, \cdots, y_{n,1}, y_{n,2}, \cdots, y_{n,n+1}, \cdots]$$

and the ideal

$$\mathfrak{P} = (x - y_{1,1}y_{1,2}, x - y_{2,1}y_{2,2}y_{2,3}, \cdots, x - y_{n,1}y_{n,2}\cdots y_{n,n+1}, \cdots).$$

In the domain $R/\mathfrak{P}$, the element x has infinite elasticity.

Example 5.2.3. *Show that the domains $\mathbb{Z}[\sqrt{-14}]$ and $\mathbb{Z}[\sqrt{-89}]$ have elasticity 2 and 6 respectively. In both cases, produce elements of the domain that attain this maximum elasticity.*

This next example is from a paper by Gonzalez.

Example 5.2.4. *Let $d \equiv 1 mod(4)$ be a square free integer and $\omega = \frac{1+\sqrt{d}}{2}$. Define $A = \mathbb{Z}[2\omega]$, $B = \mathbb{Z}[\omega]$ and consider the domain $R := A + xB[x]$. Show that if $d \equiv 1 mod(8)$ then $\rho(R) = \infty$ and if $d \equiv 5 mod(8)$ then $1 \leq \rho(R) \leq 3max\{\frac{|Cl(R)|}{2}, 1\}$. (Hint: for the case $d \equiv 1 mod(8)$ consider the elements $f = x(x+\omega)^n$ and $\overline{f} = x(x+\overline{\omega})^n$.)*

We now produce a result that shows a connection between elasticity and the Davenport constant.

Theorem 5.2.5. *Let R be a ring of algebraic integers with class group G. Then*

$$\rho(R) = \begin{cases} \frac{D(G)}{2} \leq \frac{|G|}{2} & \text{if } |G| \neq 1, \\ 1 & \text{if } |G| = 1. \end{cases}$$

Proof. If G is trivial then the result is clear, so we will suppose that $|G| = n > 1$ and $r = D(G)$.

Let $[I_1] + [I_2] + \cdots + [I_r] = 0$ be a zero sequence (with no proper zero subsequence) of maximal length. It is easy to see that $-[I_1] - [I_2] - \cdots - [I_r] = 0$ is also a maximal zero sequence with no proper zero subsequences. Choose prime ideals $\mathfrak{P}_i \in [I_i]$ and $\mathfrak{Q}_i \in -[I_i]$. Note that

$$\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_r = (\alpha)$$

is principal, as is

$$\mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_r = (\beta),$$

and

$$\mathfrak{P}_i\mathfrak{Q}_i = (\gamma_i).$$

Additionally, as we have seen before, α, β, and each γ_i are irreducible in R.

Manipulating ideal factorizations as before, we obtain the elemental factorization

$$\alpha\beta = u\gamma_1\gamma_2\cdots\gamma_r.$$

for some unit $u \in U(R)$.

Counting the factors above, we have that $\rho(R) \geq \frac{r}{2} = \frac{D(G)}{2}$.

On the other hand suppose that we have the irreducible factorization

$$\alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m.$$

We will assume that each α_i, β_j is nonprime (we can cancel primes in pairs and having the "extra" primes on both games gives smaller elasticity data).

We write each

$$(\alpha_i) = P_{i,1}P_{i,2}\cdots P_{i,t_i}$$

with each $t_i \leq r = D(G)$ since we have seen that $D(G)$ is the longest possible length of a prime ideal factorization of an irreducible.

We now have the ideal factorization

$$(\alpha_1)(\alpha_2)\cdots(\alpha_n) = (P_{1,1}\cdots P_{1,t_1})(P_{2,1}\cdots P_{2,t_2})\cdots(P_{n,1}\cdots P_{n,t_n}).$$

To "refactor" in terms of the β_j's we must shuffle the ideal factorization above to obtain a (possibly) different arrangement consisting of a collection of subproducts that are each principal and generated by an irreducible. Note that the longest possible factorization theoretically possible (that is, the largest value for m) occurs if we can pair off the primes above (for each $P_{i,j}$ we can find $P_{i',j'}$ such that $P_{i,j}P_{i',j'}$ is principal). This observation gives that $m \leq \frac{t_1+t_2+\cdots+t_n}{2}$. Hence we have

$$\frac{m}{n} \leq \frac{t_1+t_2+\cdots+t_n}{2n} \leq nr2n = \frac{r}{2} = \frac{D(G)}{2}.$$

We conclude that $\rho(R) \leq \frac{D(G)}{2}$, and hence we have equality from the first part of the proof. Since we have already observed that $D(G) \leq |G|$, we now have

$$\rho(R) = \frac{D(G)}{2} \leq \frac{|G|}{2}$$

if $|G| > 1$ and the proof is complete. □

It is interesting to observe that for a ring of integers that the elasticity is always of the form $\frac{n}{2}$ and that the elasticity is attained by an element in R.

Example 5.2.6. *For the rings* $\mathbb{Z}[\sqrt{-17}]$,$\mathbb{Z}[\sqrt{-21}]$, $\mathbb{Z}[\sqrt{-26}]$, $\mathbb{Z}[\sqrt{-41}]$, $\mathbb{Z}[\sqrt{-65}]$, *and* $\mathbb{Z}[\frac{1+\sqrt{-83}}{2}]$ *compute the class group, elasticity, and find an element that attains the maximal elasticity.*

Example 5.2.7. *Show that if* $A = \mathbb{Z}[\sqrt{5}] \subseteq B = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ *and* $C = \mathbb{Z}[\sqrt{85}] \subseteq D = \mathbb{Z}[\frac{1+\sqrt{85}}{2}]$ *then the domains* $A + xB[x]$ *and* $C + xD[x]$ *are both HFDs.*

5.3 The Length and Boundary Functions

Definition 5.3.1. *Let* R *be an atomic domain and* $R^* = R \setminus \{0\}$. *A function* $\phi : R^* \longrightarrow \mathbb{N}$ *is called a length function on* R *if the following conditions hold.*

1) $\phi(xy) = \phi(x) + \phi(y)$.

2) $\phi(x) = 0$ *if and only if* $x \in U(R)$.

We remark here that D. D. Anderson (et. al.) showed that $1 \leq \rho(R) \leq \frac{M}{m}$ where $M = \sup\{\phi(x)|x \text{ is nonprime and irreducible}\}$ and $minf\{\phi(x)|x \text{ is nonprime and irreducible}\}$.

Proposition 5.3.2. *R is an HFD if and only if R admits a length function ϕ such that $im(\phi) = \mathbb{N}$ and $\phi(x) = 1$ if and only if x is irreducible.*

Here is a useful generalization of the length function. This map is defined on the quotient field of an HFD, and is referred to the boundary map, ∂_R.

Definition 5.3.3. *Suppose that R is an HFD with quotient field K. We define a function $\partial_R : K^* \longrightarrow \mathbb{Z}$ by*

$$\partial_R(\alpha) = \partial_R(\frac{r}{s}) = \partial_R(\frac{\pi_1\pi_2\cdots\pi_n}{\xi_1\xi_2\cdots\xi_m}) = n - m$$

where $\alpha = \frac{r}{s}$ with $r, s \in R$ and $\pi_1\pi_2\cdots\pi_n = r$ and $\xi_1\xi_2\cdots\xi_m = s$ are irreducible factorizations.

Our convention will be if $R = K$ then $\partial_R(\alpha) = 0$ for all $\alpha \in K^*$.

Note that if we restrict ∂_R to the nonzero elements of R, we get a length function for our HFD R that has value 1 on all of the irreducibles of R.

At the outset, it is not clear that such a function is well-defined. We shall see that ∂_R is well-defined (and the proof will depend on the fact that R is an HFD).

Proposition 5.3.4. *If R is an HFD than ∂_R is a well-defined function. Additionally, for all $\alpha, \beta \in K^*$, $\partial_R(\alpha\beta) = \partial_R(\alpha) + \partial_R(\beta)$ and so ∂_R is a homomorphism from K^* into the integers.*

Proof. To show that ∂_R is well defined, suppose that $\alpha = \beta \in K^*$. We write $\alpha = \frac{\pi_1\pi_2\cdots\pi_n}{\xi_1\xi_2\cdots\xi_m}$ and $\beta = \frac{a_1a_2\cdots a_k}{b_1b_2\cdots b_t}$ with each α_i, β_i, a_i and b_i irreducible. It suffices to show that $n - m = k - t$.

Since $\alpha = \beta$ we must have that

$$\pi_1\pi_2\cdots\pi_n b_1b_2\cdots b_t = \xi_1\xi_2\cdots\xi_m a_1a_2\cdots a_k.$$

As R is an HFD, we obtain $n+t = m+k$ or $n-m = k-t$ as desired. Hence $\partial_R(\alpha) = \partial_R(\beta)$ and ∂_R is well-defined.

Using the above notation, we have $\partial_R(\alpha) = n - m$ and $\partial_R(\beta) = k - t$. Note that since

$$\alpha\beta = \frac{\pi_1\pi_2\cdots\pi_n a_1a_2\cdots a_k}{\xi_1\xi_2\cdots\xi_m b_1b_2\cdots b_t}$$

we have $\partial_R(\alpha\beta) = n + k - (m + t) = n - m + k - t = \partial_R(\alpha) + \partial_R(\beta)$, and the proof is complete. □

Definition 5.3.5. *Let R be an integral domain with quotient field K. A domain T such that $R \subseteq T \subseteq K$ is called an overring of R.*

Of course, any localization of R is an overring. For an example of an overring that is not a localization consider the overring of $\mathbb{Q}[x,y]$ given by $\mathbb{Q}[x,y,\frac{y}{x},\frac{y}{x^2},\frac{y}{x^3},\cdots]$.

Definition 5.3.6. *Let R be a domain with quotient field K. An element $\alpha \in K$ is said to be almost integral over R if there is a nonzero $r \in R$ such that $r\alpha^n \in R$ for all $n \geq 0$.*

The next result will show that the modifier "almost" is being used properly.

Proposition 5.3.7. *Let R be an integral domain with quotient field K. If $\alpha \in K$ is integral over R, then α is almost integral.*

Proof. We sketch the proof and encourage the reader to fill in the details. Suppose $\alpha = \frac{r}{s}$ is integral over R, then α is a root of the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$. Note first that that $s^{n-1}(\alpha)^k = s^{n-1}(\frac{r^k}{s^k})$ and so for all $k \leq n-1$, $s^{n-1}\alpha^k \in R$. To deal with the situation where $k \geq n$ note first that by the integrality of α, we have

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0.$$

Since α^n is a linear combination of the lower powers of α, we see that $s^{n-1}\alpha^n \in R$. Continue by induction since all of the higher powers of α can be expressed as an $R-$linear combination of $\{1,\alpha,\cdots,\alpha^{n-1}\}$. □

It should be noted that the notions of integrality and almost integrality coincide in the realm of Noetherian rings. For an example of an element that is almost integral but not integral consider the element $\frac{1}{x}$ over the ring $\mathbb{Q}[x,y,\frac{y}{x},\frac{y}{x^2},\frac{y}{x^3},\cdots]$.

Here is the reason for this diversion into almost integrality. The boundary map is very good at detecting almost integral elements.

Theorem 5.3.8. *Let R be an HFD with quotient field K. If $\alpha \in K$ is almost integral over R, then $\partial_R(\alpha) \geq 0$.*

Proof. Suppose that for some nonzero $r \in R$ we have $r\alpha^n \in R$ for all $n \geq 0$. Using the fact that ∂_R is a homomorphism, we obtain

$$\partial_R(r) + n\partial_R(\alpha) \geq 0$$

for all $n \geq 0$. This is ridiculous if $\partial_R(\alpha) < 0$, and this proof is complete. □

One purpose that the boundary can help us with is in determination of which overrings of HFDs are still HFDs.

Example 5.3.9. *We have seen that $\mathbb{Z}[\sqrt{-3}]$ is an HFD and its integral closure $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a UFD. More generally it has been shown that any R is a quadratic order (contained in the field $\mathbb{Q}(\sqrt{d})$) that is an HFD then, in the case that $d \equiv 2,3 mod(4)$, R must be of the form $\mathbb{Z}[n\sqrt{d}]$ and n must be either 1 or an*

inert prime integer. If $d \equiv 1 mod(4)$ *then* R *must be of the form* $\mathbb{Z}[n(\frac{1+\sqrt{d}}{2})]$ *with* n *equal to 1,* p *or* $2p$ *where* p *is an inert prime integer (the terminology "inert" in this context means that* p *remains prime in the full ring of integers).*

Additionally, it has also been shown that if an order is an HFD, then its integral closure is also an HFD. SLightly more generally, any domain between the HFD order and its integral closure is also an HFD (note that this can only apply to the "$2p$*" case above). Also note that the real interest of this example is in the real case, since the only nontrivial quadratic order that is an HFD is the imaginary case is the ring* $\mathbb{Z}[\sqrt{-3}]$.

It has been shown for rings of integers, that the integral closure of an HFD is always an HFD. This statement is not true in general.

Chapter 6

Integral Closures of HFDs

6.1 More Results on the Boundary

We begin with a useful note on the behavior of HFD overrings and ∂_R. Unless otherwise noted in this chapter, R will be an HFD with quotient field K and $\overline{R}$ will be the integral closure of R.

We begin by recalling that if R is a UFD, then $R = \overline{R}$ is integrally closed. HFDs do not have to be integrally closed and it is natural to ask if the integral closure of an HFD is still an HFD. This short chapter will focus on this question.

Lemma 6.1.1. *Let R be an HFD and S an overring of R such that no nonunit of S has boundary 0. The following conditions hold.*

1) $\partial_R(\alpha) \geq 0$ for all $\alpha \in S^*$.

2) $s \in S$ is a unit if and only if $\partial_R(s) = 0$.

3) No nonunit of R becomes a unit in S.

4) Every irreducible element of R remains irreducible in S.

Proof. For condition 1), assume that there is an $\alpha \in S^*$ such that $\partial_R(\alpha) = -n < 0$. We now choose an irreducible $r \in R$ that is not a unit a unit in S (such a choice is possible, for otherwise, S is a field). Since r is irreducible in R, we have that $\partial_R(r) = 1$. Now we consider the element $r^n\alpha \in S$. Since r is a nonunit in S, so is $r^n\alpha$. Note that $\partial_R(r^n\alpha) = 0$ and this contradicts the assumption that S has no nonunits of boundary 0. This establishes the first property.

For the second statement, the fact that S contains no nonunits of boundary 0 also shows that if s is a unit in S then $\partial_R(s) = 0$ (since $\partial_R(ss^{-1}) = 0$ and neither $\partial_R(s)$ nor $\partial_R(s^{-1})$ can be negative).

For the third statement, assume that r is a nonunit such that $r^{-1} \in S$. But since $\partial_R(1) = 0 = \partial_R(r) + \partial_R(r^{-1})$ and since the boundary of r is positive, this forces the boundary of r^{-1} to be negative, which contradicts property 1).

Finally, we will assume that r is an irreducible in R that reduces in S. Let us write $r = \alpha\beta$ with α and β nonunit factors of r in S. Note that this implies that $\partial_R(\alpha) + \partial_R(\beta) = 1$ since r is irreducible in R. This forces the boundary of either α or β to be 0, and by condition 2) the one of boundary 0 is a unit. This concludes the proof of the lemma. □

Theorem 6.1.2. *Let R be an HFD and S an overring of R such that no nonunit of S has boundary 0. Then S is an HFD if and only if $\partial_R(\alpha) = 1$ for all irreducible $\alpha \in S$.*

Proof. Since the result trivially holds if $S = K$ we will ignore this possibility.

For the first direction we will assume that S is an HFD and that there exists an irreducible $\alpha \in S$ such that $\partial_R(\alpha) = n > 1$. We write

$$\alpha = \frac{\pi_1\pi_2\cdots\pi_{k+n}}{\xi_1\xi_2\cdots\xi_k}$$

with each π_i, ξ_j irreducible in R (and hence in S by the previous lemma). This gives rise to the irreducible factorization (in S)

$$\alpha\xi_1\xi_2\cdots\xi_k = \pi_1\pi_2\cdots\pi_{k+n}.$$

Since $n > 1$ and α, ξ_i, π_j are all irreducible in S, we have that S is not an HFD, which is our desired contradiction.

For the other direction, we suppose that $\partial_R(\alpha) = 1$ for all irreducible $\alpha \in S$. First note that since every nonunit of S^* has positive boundary, S must be atomic. So we consider the irreducible factorizations in S

$$\alpha_1\alpha_2\cdots\alpha_n = \beta_1\beta_2\cdots\beta_m.$$

Applying the boundary map, we get

$$\sum_{i=1}^{n} \partial_R(\alpha_i) = \sum_{i=1}^{m} \partial_R(\beta_i)$$

but since each α_i and β_i has boundary 1, we immediately get $n = m$. □

The conditions of the theorem may seem a bit esoteric, but a major important motivation is the case where $R \subseteq S$ is integral. Although in an integral extension, there is no guarantee that every nonunit of S has boundary 0, it is a good place to start (since every element in an integral extension of R must have non-negative boundary). Here is a question alomg these lines. If R is an HFD and S is an integral extension such that S has no nonunit of boundary 0, then S is atomc. Is the converse true?

The big question that we would like to address (at least partially) is "If R is an HFD, is $\overline{R}$ an HFD?" The answer is yes for orders in rings of algebraic integers and we will tackle this case first.

For the rest of this discussion, our situation will be R will be an order that is an HFD, and $\overline{R}$ (the integral closure of R) will be the full ring of integers.

Definition 6.1.3. *Let $R \subseteq \overline{R}$ and let*

$$I = \{x \in \overline{R} | x\overline{r} \in R, \forall \overline{r} \in \overline{R}\}.$$

I is called the conductor ideal for the order R.

The conductor ideal is the largest ideal common to both R and $\overline{R}$. We remark that for orders in rings of integers, the conductor is always nonzero. Additionally we recall from number theory that for any ring of integers (and hence any order), if $J \subseteq R$ is an ideal, then R/J is a finite ring.

Example 6.1.4. *Let*

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 mod(4), \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 mod(4). \end{cases}$$

The conductor ideal for the extension $\mathbb{Z}[n\omega] \subseteq \mathbb{Z}[\omega]$ is the ideal $n\mathbb{Z}[\omega]$. The conductors ideal for the extension $\mathbb{Z} \subseteq \mathbb{Z}[x]$ is 0.

Lemma 6.1.5. *If $x \in \overline{R}$ is such that x is not contained in any prime ideal of $\overline{R}$ containing the conductor I, then there exists $n \in \mathbb{N}$ such that $x^n \in R$.*

Proof. Consider the finite ring $\overline{R}/I$. The coset $x + I$ must be a unit in $\overline{R}/I$. Since $\overline{R}/I$ is finite, the coset $x + I$ must be a root of unity. Hence there is a natural number n such that $x^n + I = 1 + I$. Hence $x^n - 1 \in I \subseteq R$ and the proof is complete. □

Lemma 6.1.6. *Let R be an HFD and $\mathfrak{P}$ be a nonzero prime ideal of $\overline{R}$ of order d in $Cl(\overline{R})$. If $\mathfrak{P}$ does not contain the conductor I, then $\mathfrak{P}^d$ can be generated by an irreducible element of R.*

Proof. Certainly $\mathfrak{P}^d = \overline{R}\alpha$ for some irreducible $\alpha \in \overline{R}$. By our earlier lemma, there is a natural number n such that $\alpha^n \in R$. We let k be minimal such that $\overline{R}\alpha^k$ is generated by an element $r \in R$. This gives that $\overline{R}\alpha^k = \overline{R}r$ and hence

$$\mathfrak{P}^{dk} = \overline{R}\alpha^k = \overline{R}r.$$

We now claim that r is irreducible in R. If not, then since r is only contained in the prime $\mathfrak{P}$, the factorization $r = ab$ (with a and b nonunits) implies that the ideal factorization of b in $\overline{R}$ is a power of $\mathfrak{P}$. Hence we obtain that $\overline{R}b = \mathfrak{P}^{dm} = \overline{R}\alpha^m$ which implies that $m \leq k$ by minimality, and hence r is irreducible. What is more, there exists $u \in U(\overline{R})$ such that $ur = \alpha^k$. Applying the boundary we get

$$\partial_R(ub) = k\partial_R(\alpha) = 1.$$

Therefore, $k = 1$ and $\alpha = ur$. Therefore $\mathfrak{P}^d = \overline{R}r$ with b irreducible in R and the proof is complete. □

Theorem 6.1.7. *If R is an order and R is an HFD, then $\overline{R}$ is an HFD.*

Proof. We will suppose that $\overline{R}$ is not an HFD and derive contradictions. Since $\overline{R}$ is not an HFD, we know that the class number of $\overline{R}$ is greater than 2. We consider two cases.

In the first case, we suppose that there is a class in $\mathrm{Cl}(\overline{R})$ of order $n > 2$. We now select a prime, $\mathfrak{P}$, in this class of order n and a prime $\mathfrak{Q}$ in the class of $\mathfrak{P}^{-1}$. Both of these primes are selected as to not contain the conductor ideal (this can be accomplished since every ideal class contains infinitely many primes and the conductor is contained in only finitely many primes).

We write $\mathfrak{P}^n = \overline{R}a$, $\mathfrak{Q}^n = \overline{R}b$ and $\mathfrak{P}\mathfrak{Q} = \overline{R}\gamma$. Of course, γ is irreducible in $\overline{R}$ and by the previous lemma, we can assume that a and b are irreducibles in R. These ideal factorization give the existence of a unit $u \in \overline{R}$ such that $u\gamma^n = ab$. We apply the boundary to get

$$n\partial_R(\gamma) = \partial_R(a) + \partial_R(b) = 2.$$

Since $n > 2$ we have that $\partial_R(\gamma) = \frac{2}{n} < 1$ and so $\partial_R(\gamma) = 0$. Recall that since γ is not in any prime containing the conductor, there is a k such that $\gamma^k \in R$. Hence γ^k is an element of R of boundary 0 and hence a unit. This is our desired contradiction.

In the second case, we assume that every ideal class in $\overline{R}$ is of order 2. As we have seen, this means that the class group of $\overline{R}$ must contain a subgroup isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. We choose primes (none of which contain the conductor) $\mathfrak{P}$ in the class corresponding to (0,1), $\mathfrak{Q}$ in the class corresponding to (1,0), and $\mathfrak{R}$ in the class corresponding to (1,1). As before, we write $\mathfrak{P}^2 = \overline{R}a$, $\mathfrak{Q}^2 = \overline{R}b$, $\mathfrak{R}^2 = \overline{R}c$, and $\mathfrak{P}\mathfrak{Q}\mathfrak{R} = \overline{R}\gamma$. Similar to the previous case, we have that a, b, c, γ are irreducibles in $\overline{R}$ and we can assume that $a, b, c \in R$. So we can find a unit $u \in U(\overline{R})$ such that $abc = u\gamma^2$. Applying the boundary, we have

$$\partial_R(abc) = 3 = 2\partial_R(\gamma)$$

and hence $\partial_R(\gamma) = \frac{3}{2}$, which is a contradiction. This completes the proof. □

6.2 Pathology for Integral Closures

For many of the nice known cases the integral closure of an HFD is an HFD (see the previous section). But it is not true in general that the integral closure of an HFD is again an HFD. The known counterexample is rather strange in the sense that the example is an HFD whose integral closure fails to be an HFD because it fails to be atomic. Careful inspection of the example will reveal that for this example, the inegral closure is not an HFD (but is an HFD in the original sense of Zaks' definition).

A refined question that remains open is "If the integral closure of an HFD is atomic, is it an HFD?"

This section is devoted to a presentation of the example of an HFD with non-HFD integral closure. The example is rather delicate and consists of a number of steps which we will briefly outline here.

1. We begin with the ring $\mathbb{Z}_2[\{x^\alpha\}]_{\alpha\in\mathbb{Q}^+}$ and we localize this ring at the maximal ideal generated by positive rational powers of x. This is a one-dimensional nondiscrete valuation domain with value group $\mathbb{Q}$ and residue field $\mathbb{Z}_2$.

2. Letting $\mathfrak{M}$ be the maximal ideal from the domain in the first step, we form the domain $\mathbb{Z}_2 + t\mathfrak{M}[t]$.

3. We then localize to form the domain $T := (\mathbb{Z}_2 + t\mathfrak{M}[t])_{(t\mathfrak{M}[t])}$. This domain is an HFD and the proof is fairly straightforward.

4. We now construct the domain $T[x+t]$. This domain is also an HFD, but the proof is more intricate.

5. We take two particular prime ideals of $T[x+t]$ (intuitively one of them is generated by $x+t$ and the other is the prime containing all elements involving t).

6. Finally we localize the previous domain at the set complement of the union of the two primes from the previous step. It is then shown that this domain is an HFD, but its integral closure is not atomic (and hence not an HFD).

The details of this process comprise the remainder of this section.

The Construction

We begin be letting V be a one-dimensional valuation domain with value group $\mathbb{Q}$ and with residue field being the field of two elements ($\mathbb{F}_2$). We will denote the quotient field of V by K. For the of sake convenient computations, we write

$$V = (\mathbb{F}_2[x^\alpha])_{\mathfrak{N}}$$

where the notation $\mathbb{F}_2[x^\alpha]$ denotes "polynomials" over the field $\mathbb{F}_2$ in the indeterminate x where the exponents (α) are in the positive rationals. $\mathfrak{N}$ denotes the maximal ideal of $\mathbb{F}_2[x^\alpha]$ consisting of all "polynomials" with zero constant coefficient, and if p is an element of V, we denote its value by $v(p)$. Considering the polynomial ring $V[t]$, we form the ring T via the following $D+M$ construction:

$$T = \mathbb{F}_2 + t\mathfrak{M}[t]$$

where $\mathfrak{M} = \mathfrak{N}\mathbb{F}_2[x^\alpha]_{\mathfrak{N}}$ is the maximal ideal of V.

For convenience, we pass to the localization:

$$T_1 = T_{t\mathfrak{M}[t]} = (\mathbb{F}_2 + t\mathfrak{M}[t])_{t\mathfrak{M}[t]}.$$

At this point we make a couple of useful observations about the ring T_1.

Lemma 6.2.1. *An element of* $T_1 = (\mathbb{F}_2 + t\mathfrak{M}[t])_{t\mathfrak{M}[t]}$ *is irreducible if and only if it can be written in the form*

$$u(x^{\alpha_1}t + \epsilon_1 x^{\alpha_2}t^2 + \cdots + \epsilon_n x^{\alpha_n}t^n)$$

for u *a unit in* T_1*, each* ϵ_i *either 0 or a unit in* T_1*, and* $\alpha_i \in \mathbb{Q}, \alpha_i > 0$*.*

Proof. Let $\beta \in T_1$ be an irreducible; in particular, β is a nonunit. Hence β can be written in the form

$$\beta = \frac{x^{\alpha_k}t^k + \epsilon_{k+1}x^{\alpha_{k+1}}t^{k+1} + \cdots + \epsilon_{k+m}x^{\alpha_{k+m}}t^{k+m}}{f(t)} \tag{6.1}$$

where $f(t)$ is in the complement of the maximal ideal and each ϵ_i is either 0 or a unit of $T_1 \subseteq V$. For convenience we write $u = \frac{1}{f(t)}$. Assume that $k > 1$ and let the integer i be chosen $k \leq i \leq k+m$ such that $\alpha_i \leq \alpha_j$ for all $k \leq j \leq k+m$. Consider the following factorization of β:

$$\beta = ux^{\frac{\alpha_i}{2}}t(x^{(\alpha_k - \frac{\alpha_i}{2})}t^{k-1} + \epsilon_{k+1}x^{(\alpha_{k+1}-\frac{\alpha_i}{2})}t^k + \cdots + \epsilon_{k+m}x^{(\alpha_{k+m}-\frac{\alpha_i}{2})}t^{k+m-1}).$$

Hence if $k > 1$ then β is reducible. This shows the first direction.

For the other implication, we assume that β takes the form

$$\beta = u(x^{\alpha_1}t + \epsilon_1 x^{\alpha_2}t^2 + \cdots + \epsilon_n x^{\alpha_n}t^n).$$

Assume that we can factor $\beta = ab$ with both a and b nonunits. Using the form of a general nonunit element from the proof of the first implication (and grouping units), we obtain

$$\beta = u_1(x^{a_k}t^k + \sum_{i=1}^{m}\bar{\epsilon}_{k+i}x^{a_{k+i}}t^{k+i})u_2(x^{b_r}t^r + \sum_{j=1}^{s}\tilde{\epsilon}_{r+j}x^{b_{r+j}}t^{r+j}) = ab.$$

with u_1, u_2, units in T_1 and the $\bar{\epsilon}$'s and the $\tilde{\epsilon}$'s either units of T_1 or 0. So we can assume without loss of generality that $k = 0$, and this in turn implies that that $a_k = 0$ which is a contradiction. This establishes the lemma. □

In the representation of a general nonunit β given above (**??**), we call the integer k the *least degree* of β, and we use the notation $\sigma(\beta) = k$ (we note here that the least degree of β is independent of the representation of the form (**??**) chosen).

With the previous lemma in hand, we note the following corollary.

Corollary 6.2.2. *The ring* $T_1 = (\mathbb{F}_2 + t\mathfrak{M}[t])_{t\mathfrak{M}[t]}$ *is a quasi-local, half-factorial domain whose quotient field is isomorphic to* $K(t)$ *where* K *is the quotient field of* V*.*

Proof. The statement "quasi-local" is obvious and the fact that the quotient field of T_1 is isomorphic to $K(t)$ is straightforward as well. We shall show that T_1 is a half-factorial domain. Using the above notation for the least degree of an element $f(t) \in T_1$, we observe that $f(t)$ is a unit in T_1 if and only if $\sigma(f(t)) = 0$. We also note that for $f(t), g(t) \in T_1$, $\sigma(f(t)g(t)) = \sigma(f(t)) + \sigma(g(t))$. Hence the atomicity of the ring T_1 follows immediately from these facts since given any nonzero element of T_1, its least degree is finite.

We now consider two irreducible factorizations of an element in T_1,

$$f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m.$$

Applying σ to both sides, we obtain

$$\sigma(f_1) + \sigma(f_2) + \cdots + \sigma(f_n) = \sigma(g_1) + \sigma(g_2) + \cdots + \sigma(g_m).$$

Since f_i, $1 \leq i \leq n$ and g_j, $1 \leq j \leq m$ are all assumed irreducible, the previous lemma gives that $\sigma(f_i) = 1 = \sigma(g_j)$. Hence $n = m$. □

We now proceed with our construction. In the next stage we want to consider a particular overring of the ring T_1. Indeed, consider the element $x + t \in K(t)$, the quotient field of T_1. We wish to consider first the ring

$$T_2 = T_1[x + t] = (\mathbb{F}_2 + t\mathfrak{M}[t])_{t\mathfrak{M}[t]}[x + t].$$

We have to make one more step in our construction, but again we pause to collect some information about the ring T_2.

Lemma 6.2.3. *Any element of T_2 can be written in the form:*

$$\sum_{i=0}^{n} f_i(x + t)^i$$

with each $f_i \in T_1$ (this expression is not necessarily unique). What is more the following two sets form prime ideals in T_2:

$$(x + t)T_2 \tag{6.2}$$

$$\{\sum_{i=0}^{n} g_i(x + t)^i | g_i \in t\mathfrak{M}[t]_{t\mathfrak{M}[t]}\}. \tag{6.3}$$

Put more simply, the element $x + t$ is a prime element of T_2 and the extension of the prime ideal $t\mathfrak{M}[t]_{t\mathfrak{M}[t]}$ is a prime ideal in T_2. (We also remark here that the "nonuniqueness" parenthetical remark can be seen by considering that the element $xt(x + t)^2$ can be rewritten in the form $(x^2t + xt^2)(x + t)$.)

Proof. We will first show that the element $x + t$ is a prime element of T_2. Certainly, $x + t$ is a prime element of $K[t]$ as $x + t$ is irreducible and $K[t]$ is a unique factorization domain. We now argue that $x + t$ is a prime element of $V[t]$.

Assume that $(x + t)|\nu_1(t)\nu_2(t)$ where $\nu_1(t), \nu_2(t) \in V[t] \subseteq K[t]$. As $x + t$ is prime in $K[t]$, we can say without loss of generality that $x + t$ divides $\nu_1(t)$ (in $K[t]$); it suffices to show that the quotient is in $V[t]$.

Assume that we have

$$(x + t)(k_0 + k_1t + \cdots + k_nt^n) = (w_0 + w_1t + \cdots + w_{n+1}t^{n+1})$$

with $k_i \in K$ and $w_i \in V$. It is easy to see (by multiplying out the left side of the above equation and equating coefficients) that $k_0 + k_1t + \cdots + k_nt^n$ must be an element of $V[t]$. This shows that $x + t$ is a prime element of $V[t]$.

Since $x + t \in V[t]$ is prime, it follows that $x + t \in V[t]_{\mathfrak{A}}$ is prime (where $\mathfrak{A}$ is the set of elements of $V[t]$ of the form $1 + tx^\alpha f(t)$ with $f(t) \in V[t]$ and $\alpha \in \mathbb{Q}^+$, the positive rationals). Noting that $V[t]_{\mathfrak{A}}$ is an overring of T_2 we now show that $x + t$ is a prime element of T_2.

As above, if $\alpha_1, \alpha_2 \in T_2$ are such that $(x + t)|\alpha_1\alpha_2$ then without loss of generality, $x + t$ divides α_1 (in $V[t]_{\mathfrak{A}}$) and we are left with the task of showing that the quotient is in T_2. Since $x+t$ divides $\alpha_1 = t_0+t_1(x+t)+\cdots+t_m(x+t)^m$ ($t_i \in T_1$ for $0 \leq i \leq m$), we write the quotient as $\frac{w_0+w_1t+\cdots+w_nt^n}{1+tx^\alpha f(t)} \in V[t]_{\mathfrak{A}}$. We have the equation

$$(x + t)(\frac{w_0 + w_1t + \cdots + w_nt^n}{1 + tx^\alpha f(t)}) = t_0 + t_1(x + t) + \cdots + t_m(x + t)^m.$$

As we wish to show that $\frac{w_0+w_1t+\cdots+w_nt^n}{1+tx^\alpha f(t)}$ is an element of T_2, we can assume without loss of generality that for all $1 \leq i \leq m$, $t_i = 0$ (indeed, if any element t_i for $1 \leq i \leq m$ is nonzero, then one needs merely to transfer these elements to the left side of the displayed equation above and factor out an "$(x + t)$").

Additionally, we note that the element $1 + tx^\alpha f(t)$ is a unit in $T_1 \subseteq T_2$ so, in fact, it suffices to show that the element $w_0 + w_1t + \cdots + w_nt^n$ is an element of T_2. We have the equation

$$(x + t)(w_0 + w_1t + \cdots + w_nt^n) = \overline{t_0}$$

where $\overline{t_0} \in T_1 \subseteq T_2$. Viewing $\overline{t_0}$ up to a unit as a polynomial in $V[t]$, a simple inductive argument shows that the values of the elements w_i for $0 \leq i \leq n$ are all positive (and, in fact, $w_0 = 0$ since $\overline{t_0} \in T_1$) hence the element $w_0 + w_1t + \cdots + w_nt^n \in T_1 \subseteq T_2$. This establishes that $x + t$ is a prime element of T_2.

To see that the set

$$\wp = \{\sum_{i=0}^{n} g_i(x + t)^i | g_i \in t\mathfrak{M}[t]_{t\mathfrak{M}[t]}\}$$

forms a prime ideal of T_2, we shall realize $\wp$ as an intersection. In particular, we claim that

$$\wp = tV[t]_{tV[t]} \bigcap T_2.$$

The inclusion $\wp \subseteq tV[t] \bigcap T_2$ is clear. For the other inclusion, we consider an element, β of $tV[t] \bigcap T_2$. We first consider β as an element of T_2 and write it as

$$\beta = \alpha_0 + \alpha_1(x+t) + \cdots + \alpha_n(x+t)^n$$

with each $\alpha_i \in T_1$. For the moment, we make the further assumption that each $\alpha_i \in \mathbb{F}_2 + t\mathfrak{M}[t]$. If each $\alpha_i \in t\mathfrak{M}[t]$ then we have our desired inclusion, so let k be the maximal integer such that $\alpha_k \in \mathbb{F}_2 + t\mathfrak{M}[t] \setminus t\mathfrak{M}[t]$. Multiplying out $\alpha_k(x+t)^k$ gives an extraneous "x^k" term, contradicting the containment of β in $tV[t]$ (hence $\beta \in \wp$ in this case). In the general case, we multiply β by the appropriate factor $u \in U(\mathbb{F}_2 + t\mathfrak{M}[t]_{t\mathfrak{M}[t]})$ so that each coefficient of $(x+t)^i$ is in $\mathbb{F}_2 + t\mathfrak{M}[t]$. As above, $u\beta \in \wp$. Since u is a unit of T_2, $\beta \in \wp$. This concludes the proof. □

For the sake of clarity, we take a last step in our construction. Letting the set S denote the complement of the set-theoretic union of the prime ideals $\wp$ and $(x+t)T_2$, we define

$$R = (T_2)_S.$$

Theorem 6.2.4. *The ring R is a half-factorial domain whose integral closure, $\overline{R}$, does not possess the half-factorial property (in fact, $\overline{R}$ is not even atomic).*

Proof. First we demonstrate that R is a half-factorial domain. If $g \in R$ is a nonzero nonunit, then by construction g is an element of either (the extension of) the prime ideal $\wp$ or the prime ideal $(x+t)$. Without loss of generality (by adjusting g by an appropriate unit), we assume g to be an element of T_2.

As $g \in T_2$, it is clear that there is a maximal $n \geq 0$ and an $h \in T_2$ such that $g = (x+t)^n h$. As $x+t$ is a prime element of T_2 (and hence of the localization R) by the previous lemma, any factorization of g must contain precisely n copies of $x+t$ (up to a unit) as factors. It suffices, therefore, to show that h has the half-factorial property in R.

So we assume that $h \in T_2 \subseteq R$ is a nonunit with no factor of $x+t$. But as $h \in \wp$, this implies that (up to a unit) h may be considered to be an element of T_1. Corollary 2.2 shows that we can always factor h into m factors of least degree 1 (where m is the least degree of h) and these factors are irreducible since $h \notin (x+t)$. This completes the first part of the proof.

We now demonstrate that the integral closure of the domain R is not atomic. Indeed, consider the family of elements in the quotient field of R:

$$x^{\frac{1}{n}} = \frac{x^{1+\frac{1}{n}}t}{xt}.$$

To see that these elements are in $\overline{R}$, note that each such element satisfies the following polynomial over R:

$$Y^{2n} - (x+t)Y^n + xt.$$

It is easy to see that this family of elements consists of nonunits. Also note that the element $x \in \overline{R}$ cannot be factored into irreducible elements. Indeed, the existence of the elements $x^{\frac{1}{n}} \in \overline{R}$ show that no positive rational power of x can possibly be irreducible since for all positive rationals q, $x^q = (x^{\frac{q}{2}})^2$. What is more, it is easy to see that up to units in $\overline{R}$, the only nonunits dividing x are of the form x^q with q a positive rational number. Hence, we see that the ring $\overline{R}$ is not atomic. This completes the proof. □

Chapter 7

More General Factorization Types

Most of this chapter is derived from the papers "Factorization in Integral Domains" and "Factorization in Integral Domains, II". These two very important paper by D. D. Anderson, D. F. Anderson, and M. Zafrullah played a very large role in the recent explosion of work in the field of factorization. They are both classics and are highly recommended reading.

7.1 The Definitions

For completeness, we reiterate if necessary.

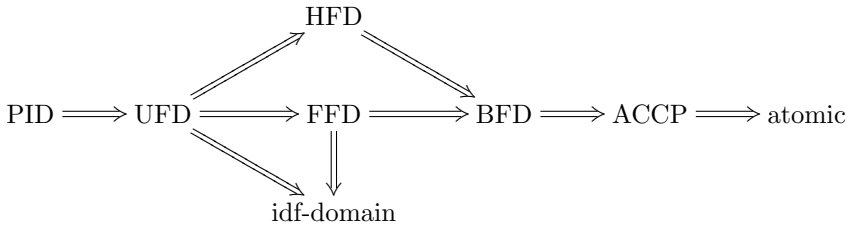
Definition 7.1.1. *Let R be an integral domain. We say that R is*

1. *atomic if every nonzero nonunit of R is a product of atoms.*
2. *ACCP (satisfies the ascending chain condition on principal ideals) if there is no strictly ascending chain of principal ideals.*
3. *BFD (bounded factorization domain) if R is atomic and for every nonzero nonunit $r \in R$ there is a bound on the lengths of factorizations of r into irreducibles.*
4. *HFD (half-factorial domain) if R is atomic and each factorization of a given nonzero nonunit has the same length.*
5. *UFD (unique factorization domain) if every nonzero nonunit of R has a (unique) factorization into prime elements.*
6. *idf-domain (irreducible-divisor-finite) if each nonzero element has at most a finite number of nonassociate irreducible divisors.*

7. *FFD (finite factorization domain) if R is atomic and every nonzero nonunit has only finitely many nonassociate irreducible divisors (hence a finite number of factorizations up to units).*

7.2 The Relationships and Some Examples

We first diagram the implications. We will sketch all of the implications in this section.



We are already familiar with the fact that PID implies UFD and UFD implies HFD so we will ignore these.

Theorem 7.2.1. *Any domain that satisfies ACCP is atomic.*

Proof. We first note that any nonzero nonunit of R is divisible by an irreducible. To see this, suppose that x is a nonzero nonuunit in R. If the ideal (x) is maximal with respect to being principal then x is irreducible. If (x) is not contained in an ideal that is maximal with respect to being principal, this means that for all (y) containing (x), there exists $(y_1) \supsetneq (y) \supsetneq (x)$. Since the same is true for (y_1), we can construct an infinite increasing chain of principal ideals

$$(x) \subsetneq (y) \subsetneq (y_1) \subsetneq (y_2) \subsetneq \cdots$$

and this contradicts ACCP.

Now let x be a nonzero nonunit of R. By the above, we know that x is divisible by an irreducible π_1. If $\frac{x}{\pi_1}$ is a unit then x is associated to the irreducible π_1. If not, then $\frac{x}{\pi_1}$ is divisible by an irreducible, π_2. Continuing this process gives rise to the increasing chain of principal ideals

$$(x) \subsetneq (\frac{x}{\pi_1}) \subsetneq (\frac{x}{\pi_1\pi_2}) \subsetneq \cdots$$

Since R is ACCP this sequence must terminate. So (using the notation above) we can find a unit $u \in R$ such that $u = \frac{x}{\pi_1\pi_2\cdots\pi_n}$ and hence $ux = \pi_1\pi_2\cdots\pi_n$ and hence R is atomic. □

Corollary 7.2.2. *Any Noetherian ring is ACCP and hence atomic.*

Proof. Noetherian rings satisfy the ascending chain condition on ideals and hence ACCP. □

Proposition 7.2.3. *Any BFD is ACCP.*

Proof. Assume that R is a BFD that is not ACCP. We select an infinite ascending chain of principal ideals

$$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots \subsetneq (x_n) \subsetneq (x_{n+1}) \subsetneq \cdots$$

Since R is atomic (since R is a BFD), x can be factored into irreducibles and there must be a maximal length of factorizations (say n).

We write $x = r_1x_1$ with r_1 a nonunit. But since x_2 properly divides x_1 there is a nonunit r_2 such that $x_1 = r_2x_2$ and hence we have

$$x = r_1x_1 = r_1r_2x_2,$$

and continuing this process we obtain

$$x = r_1r_2 \cdots r_nx_n$$

with x_n and each r_i a nonunit. Hence this last factorization of x must have at least $n + 1$ irreducible factors and this is the desired contradiction. □

We remark that the implications HFD, FFD $\Longrightarrow$ BFD, FFD $\Longrightarrow$ idf-domain, and UFD$\Longrightarrow$ idf-domain, FFD, HFD are more straightforward and are left to the reader.

None of the implications diagrammed at the beginning of this section are reversible. We will look at a couple of illuminating examples.

Example 7.2.4. *This rather famous example, due to Grams, shows that atomic domains are not always ACCP. We merely sketch the approach. Such a domain should have the property of atomicity without ACCP...in other words there should be elements that when factored "correctly" have an irreducible factorization, but if factored another way, one might, if not careful, find an infinite ascending chain of factors.*

For the relevant example, we let F be a field and S the subset of the natural numbers generated additively by the set $\{\frac{1}{3}, \frac{1}{(2)(5)}, \frac{1}{(2^2)(7)}, \cdots, \frac{1}{2^kp_k}, \cdots\}$ where p_k denotes the k^{th} odd prime. Let $F[x;S]$ be the group ring $\{\sum \alpha_i x^{s_i} | \alpha_i \in F, s_i \in S\}$. If $\mathfrak{M}$ is the ideal generated by all monomials with positive exponents, then the domain $F[x;S]_{\mathfrak{M}}$ is atomic but not ACCP.

The ideals

$$(x^{\frac{1}{2}}) \subsetneq (x^{\frac{1}{4}}) \subsetneq (x^{\frac{1}{8}}) \subsetneq \cdots$$

form an infinite ascending chain, so this domain is not ACCP.

The fact that this domain is atomic is more delicate. As a nudge in the right direction, show that the elements of the form x^a where $a = \frac{1}{2^kp_k}$ are atoms in this domain.

Example 7.2.5. *In a similar spirit to the previous example, we again consider the construction $F[x;S]_{\mathfrak{M}}$ with the only change from the previous example is that we will let $S = \langle \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \cdots, \frac{1}{p_k}, \cdots \rangle$.*

The key to this example is the observation that every element of S can be written uniquely in the form

$$n_0 + \frac{n_1}{2} + \frac{n_2}{3} + \cdots + \frac{n_k}{p_k}$$

with each $0 \leq n_i \leq p_i - 1$. Since for a given $s \in S$ the largest prime in the denominator is bounded, this puts an upper limit on the size of a proper chain of principal ideals ascending from x^s.

The fact that this domain is not a BFD is lucid since for all primes p we have $x = (x^{\frac{1}{p}})^p$.

We remark here that any Noetherian domain is BFD.

Example 7.2.6. *Let R be a ring of integers with class number greater than 2. As we have seen, rings of algebraic integers are always FFD (since any element has only finitely many distinct factorizations). Since the class number exceeds 2, this cannot be an HFD. Hence neither FFD nor BFD can imply HFD.*

Example 7.2.7. *Consider the ring $R := \mathbb{Q} + x\mathbb{R}[x]$. This is similar to the example $\mathbb{R} + x\mathbb{C}[x]$ done earlier. The same argument as before shows that R is an HFD. But this ring is not an FFD. To see this, note that x^2 is divisible by the irreducible λx (for any $\lambda \in \mathbb{R}$). Clearly there are uncountably many of these and since $\mathbb{Q}$ is countable, it is easy to see that R is not an FFD.*

Example 7.2.8. *An easy example of a non-atomic idf domain is any discrete valaution domain of dimension at least 2. This is trivially an idf domain since this ring possesses a unique irreducible (which is, in fact, prime). Since the dimension is greater than 1, the domain is non-atomic.*

7.3 Polynomial Extensions

Proposition 7.3.1. *Let R be an atomic domain. The following conditions are equivalent.*

1) *For each $n \geq 2$ and $a_1, a_2, \cdots, a_n \in R^*$ there exists $c_1, \cdots, c_n \in R$ with no common factors and irreducible $b_1, \cdots, b_m \in R$ such that $a_i = b_1 b_2 \cdots b_m c_i$ for all $1 \leq i \leq n$.*

2) *$R[\{x_\alpha\}]$ is atomic for any family of indeterminates.*

3) *$R[x, y]$ is atomic.*

Proof. For 1) implies 2) select $f \in R[\{x_\alpha\}]$. Factor f as a product $f = f_1 f_2 \cdots f_k$ such that the only factors of each f_i of smaller degree than f_i are constants (and we can certainly accomplish this using a degree argument). To continue this factorization, write each

$$f_i = a_0 + a_1\overline{X} + \cdots + a_n\overline{X}^n = b_0 b_1 \cdots b_n(c_0 + c_1\overline{X} + \cdots + c_n\overline{X}^n)$$

using the assumption from 1). Hence we have an algorithm for factoring f into irreducibles.

2) implies 3) is trivial.

For 3) implies 1) we will let F be the quotient field of R. Consider the polynomial $a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_ny \in F[x, y]$. Since $a_n \neq 0$, this polynomial must be irreducible (as an element of $F[x, y]$).

In $R[x, y]$ we can only factor this by "pulling out constants" and since $R[x, y]$ we can complete this process by writing

$$a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+a_ny = b_1b_2\cdots b_m(c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+c_ny)$$

with each b_i irreducible and the c_i having no factor in common. This completes the proof.

□

We remark here that there are atomic domains, R for which $R[x]$ is not atomic.

Proposition 7.3.2. *R is ACCP if and only if $R[x]$ is ACCP.*

Proof. We observe immediately that if R is not ACCP, the same infinitely ascending chain of principal ideals can be used for $R[x]$. So one direction is clear.

For the other direction, we will assume that R is ACCP but $R[x]$ is not and come to a contradiction. If $R[x]$ is not ACCP, we have an infinite ascending chain of principal ideals given by

$$(f_1) \subsetneq (f_2) \subsetneq (f_3) \subsetneq \cdots$$

The sequence of the degrees associated with the generators f_i is non-ascending. If the degree of any f_i is 0, then $f_j \in R$ for all $j \geq i$ and we are done since R satisfies ACCP. We will assume that the sequence of dgrees stabilizes at some $k > 0$. But from this point in the sequence look at the sequence of ideals in R generated by the leading coefficients of the f_i's. This chain must stabilize at some point as well. Hence we can find two polynomial generators in the chain f_i and f_j such that $(f_i) \subsetneq (f_j)$. So we have that the degrees of f_i and f_j coincide, as do the leading coefficients. Since f_i is in (f_j), $f_i - f_j$ is in (f_j) and has smaller degree. Hence $f_i = f_j$ and so $(f_i) = (f_j)$. This completes the proof. □

Proposition 7.3.3. *Let R be a domain. The following conditions are equivalent.*

1) R is a BFD.

2) $R[x]$ is a BFD.

3) $R[[x]]$ is a BFD.

We merely outline the proof of this.

Proof. The fact that 2) and 3) imply 1) is easy. For the implication 1) implies 2) bound the factors of $f(x)$ by using its degree and the number of irreducibles that one can "pull out". For the implication 1) implies 3) write $f(x) = x^n g(x)$ and note that the number of factors is bounded by n and the number of factors of $g(0) \in R$. □

Proposition 7.3.4. *R is an FFD if and only if $R[x]$ is an FFD.*

Proof. Of course the first implication is the more interesting one. Let $f \in R[x]$ and K be the quotient field of R. As an element of the PID, $K[x]$, f has only finitely many nonassociate factors. If f has infinitely many in $R[x]$ then there is an infinite collection $\{f_n\}$ of nonassociate factors of f such that $f_1 K[x] = f_n K[x]$ for all $n \geq 1$.

Now write $f = f_n g_n \in R[x]$. This gives factorizations of the leading coefficient and since R is an FFD there must only be finitely many of these. Hence infinitely many of the f_n have associate leading coefficients. But $f_1 K[x] = f_n K[x]$ and leading coefficients are the same. Hence $f_1 = f_n$ and we have a contradiction. The other direction is easy. □

Chapter 8

Polynomials and Power Series over HFDs

To get going in this section we some background.

8.1 Krull Domains

Definition 8.1.1. *Let R be a domain satisfying the following conditions.*

1) R_P is a Noetherian valuation domain for all minimal (nonzero) primes.

2) $R = \bigcap_{P:minimal} R_P$.

3) Every nonzero $r \in R$ is contained in only finitely many minimal primes.

Such a domain is called a Krull domain.

Noetherian Krull domains are characterized in a familiar fashion.

Theorem 8.1.2. *Let R be a Noetherian integral domain. The following conditions are equivalent.*

1) R is a Krull domain.

2) R is an integrally closed domain.

Krull domains are effective generalizations of Dedekind domains that behave nearly as well.

Proposition 8.1.3. *Let R be a domain. The following conditions are equivalent.*

1) R is a one dimensional Krull domain.

2) R is a Dedekind domain.

The behavior of Krull domains is "better" than Dedekind domains, in a certain sense, in the next result.

Proposition 8.1.4. *If R is a Krull domain, then $R[x]$ and $R[[x]]$ are Krull domains.*

Here is an extremly important result that will allow us to generalize Carlitz' result to a more general setting.

Proposition 8.1.5. *If R is Krull then $R[x]$ is Krull and $Cl(R) \cong Cl(R[x])$. What is more in $Cl(R[x])$ there is a prime in every ideal class.*

The beauty of this result is that even is R does not have a prime in every class, $R[x]$ does. This allows for the application of some of our earlier techniques.

Theorem 8.1.6. *Suppose that R is a Krull domain. The following conditions are equivalent.*

1) $R[x]$ is an HFD.

2) $|Cl(R)| \leq 2$

The proof of this theorem is very similar to the proof of Carlitz' result. The reader is encouraged to try it.

As a closing remark we note that there exist Dedekind HFDs such that $R[x]$ is not an HFD.

8.2 Polynomials Over HFDs

Unlike ACCP, BFD, FFD, UFD, the HFD property is not preserved in polynomial extensions. In this section we find a necessary condition for preservation of the HFD property in $R[x]$ and we will classify all Noetherian polynomial HFDs.

In this section, R is an integral domain with quotient field K. We first record a useful lemma.

Lemma 8.2.1. *Let $p(x)$ be irreducible in $R[x]$, and let $0 \neq r \in R$. If $rp(x) = r_1 r_2 ... r_t f_1 f_2 ... f_k$ with $r_i \in R$ for $1 \leq i \leq t$ and $f_i \in R[x]$ with $0 < deg(f_i) < deg(p)$ for $1 \leq i \leq k$, then no f_i is monic.*

Proof. Suppose that $rp(x) = r(q_{n+m}x^{n+m} + q_{n+m-1}x^{n+m-1} + ... + q_1 x + q_0) = (r_n x^n + ... + r_0)(x^m + s_{m-1}x^{m-1} + ... + s_0) = g_1(x)g_2(x)$ with $n \geq 1$.

From this we obtain the following system of equations:

$$\begin{aligned} r_n &= rq_{n+m} \\ r_{n-1} + r_n s_{m-1} &= rq_{n+m-1} \\ &\vdots \\ r_0 + r_1 s_{m-1} + ... + r_m s_0 &= rq_m \end{aligned}$$

Inductively from these equations, we get that $r|r_i$ for every i. Therefore, $g_1(x) = rg(x)$ with $g(x) \in R[x]$. This shows that $p(x) = g(x)g_2(x)$, which is a contradiction. □

With this lemma in hand, we can now prove a result that gives a necessary condition for $R[x]$ to be an HFD.

Theorem 8.2.2. *Let R be an integral domain. If $R[x]$ is an HFD, then R is integrally closed.*

Proof. Assume that R is not integrally closed. We shall show that $R[x]$ is not an HFD. We note that we can also assume that R is an HFD, for if not, then $R[x]$ is certainly not an HFD.

Let K be the quotient field of R, and let $\omega \in K \setminus R$ such that ω satisfies the monic irreducible polynomial $p(x) = x^n + p_{n-1}x^{n-1} + ... + p_1x + p_0 \in R[x]$. Also assume that $\omega = \frac{r}{s}$ with $r, s \in R$ such that r and s have no factor in common (which is possible since R is an HFD). Consider the following element of $R[x]$:

$$s^n p(x) = s^n x^n + p_{n-1}s^n x^{n-1} + ... + p_1 s^n x + p_0 s^n = (sx - r)q(x)$$

with $q(x) \in R[x]$.

By assumption we have the following facts.

1. The number of factors of one irreducible factorization of the left hand side is $mn + 1$, where m is the number of irreducible factors of s.

2. The polynomial $(sx - r)$ is irreducible.

So we will investigate the number of factors of $q(x)$.

Notice that the leading coefficient of $q(x)$ is s^{n-1}. Assume that $q(x) = f_1(x)...f_k(x)r_1...r_t$ where each $f_i \in R[x]$ is irreducible of positive degree and each r_i is irreducible in R. As $p(x)$ is irreducible in $R[x]$, the previous lemma shows that none of the f_i's is monic, and so we obtain the equation

$$s^{n-1} = L_1...L_k r_1...r_t$$

where L_i is the leading coefficient of $f_i(x)$ and is a nonunit.

As R is an HFD, we have that $k + t \leq m(n - 1)$. We conclude that the number of irreducible factors of $s^n p(x)$ (from this point of view) is $k + t + 1 \leq m(n-1) + 1 \leq mn + 1$. For $R[x]$ to be an HFD, the last inequality must be an equality, and hence m=0. This contradicts the fact that $\omega \in K \setminus R$. □

We now give a corollary to this theorem which completely classifies all Noetherian HFDs that have "polynomial stability".

Corollary 8.2.3. *Let R be a Noetherian ring. Then the following conditions are equivalent.*

1) R is a Krull domain with $|Cl(R)| \leq 2$.

2) $R[x]$ is an HFD.

3) $R[x_1, ..., x_n]$ is an HFD for all $n \geq 1$.

4) $R[x_1, ..., x_n]$ is an HFD for some $n \geq 1$.

Proof. We first observe that the implications 3) implies 4) and 4) implies 2) are obvious. We will show that 1) implies 3) and 2) implies 1).

For the implication 1) implies 3), since R is a Krull domain with $|\mathrm{Cl}(R)| \leq 2$, then $R[x_1, ..., x_n]$ is also a Krull domain with $|\mathrm{Cl}(R[x_1, ..., x_n])| = |\mathrm{Cl}(R)|$. Since if R is a Krull domain, then $R[x]$ is an HFD if and only if $|\mathrm{Cl}(R)| \leq 2$, we obtain the result inductively.

For 2) implies 1), we assume that $R[x]$ is an HFD. The previous theorem shows that R is integrally closed and hence a Krull domain (as R is Noetherian). Once again applying a result of Zaks, we obtain that R must have $|\mathrm{Cl}(R)| \leq 2$, and this concludes the proof. □

8.3 Power series extensions

Power series extensions are oftentimes more problematic than polynomial extensions. Many classical results that hold (in general commutative algebra) sometimes fail wildly in the setting of power series. Passing to a completion (even an $x-$adic one) is sometimes a bit tricky and some nice properties may be lost.

For the sake of perspective, a striking example of this phenomenon is in dimension theory. A classical result for polynomials is that if the (Krull) dimension of a ring ($\dim(R)$) is finite (say $\dim(R) = n$), then so is the dimension of $R[x]$ (in particular, if $\dim(R) = n$ then $n + 1 \leq \dim(R[x]) \leq 2n + 1$). This is wildly untrue (and in fact, from the non-Noetherian point of view, usually untrue) in the case of power series rings. In fact, there are $0-$dimensional rings whose power series extensions are infinite dimensional. Of course, it should be noted that there are instances in which the behavior of formal power series is at least as nice as the analog behavior in polynomials. One example where this occurs is in the case of the passage of the unit group of a ring to polynomials and power series. It is well-known that $U(R) = U(R[x])$ and that the set of units in $R[[x]]$ is the set of power series $f(x) \in R[[x]]$ such that $f(0) \in U(R)$.

An even more striking example of good power series behavior involves (semi-)quasi-local rings. It is a central result that R is quasi-local (resp., semi-quasi-local) if and only if $R[[x]]$ is quasi-local (resp. semi-quasi-local). The analogous result for polynomials is not true, since the ring $R[x]$ is *never* semi-quasi-local. But such nice behavior of power series rings relative to the polynomial case is the exception and not the rule in practice.

From a factorization point of view we can find bad behavior as well. For example, there are UFDs which have non-UFD power series extensions [**?**].

As has been pointed out earlier, if $R[x]$ is an HFD, then R is integrally closed. Since for the polynomial case, the coefficient ring being integrally closed is necessary for $R[x]$ to have a chance at the half-factorial property, intuitively one would (perhaps) expect that $R[[x]]$ being an HFD would demand at least this much. In light of this "intuition" let us revisit an earlier example.

Example 8.3.1. *Consider the order $R := \mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\sqrt{\omega}]$ where $\omega = \frac{1+\sqrt{-3}}{2}$. As noted before, R is an HFD with $R[x]$ failing to be an HFD. We again look at the factorization in $\mathbb{Z}[x]$ that demonstrated the loss of the half-factorial property:*

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

A close inspection of this factorization shows that, in contrast to the $\mathbb{Z}[x]$ case, this does not deny the half-factorial property in $\mathbb{Z}[[x]]$. The reason for this is that the element x^2+x+1, although an irreducible in $\mathbb{Z}[x]$, is a unit in $\mathbb{Z}[[x]]$. Hence up to units, the factorizations on both sides of the above equation are of length 2.

In fact, in the example above, $R[[x]]$ is, in fact, an HFD. Much more general situations are considered in [**?**]. We will outline a proof that the above example is a (non-integrally closed) example of an HFD such that $R[[x]]$ is an HFD. A more thorough treatment of this phenomenon can be found in [**?**].

Theorem 8.3.2. *Let R be a $1-$dimensional domain with integral closure $\overline{R}$ and conductor I. Also suppose that every nonzero coset of $\overline{R}/I$ can be written in the form $u + I$ with $u \in U(\overline{R})$. Then $\overline{R}$ is a UFD implies that $R[[x]]$ is an HFD.*

Before beginning this proof, we note that, in particular, the hypotheses apply to the ring $\mathbb{Z}[\sqrt{-3}]$. Indeed, the integral closure of this ring is (the UFD) $\mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-3}}{2}$ and the conductor of $\mathbb{Z}[\omega]$ to $\mathbb{Z}[\sqrt{-3}]$ is the ideal $2\mathbb{Z}[\omega] = \mathfrak{P}$. Since this conductor ideal is prime, the quotient ring $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$ is isomorphic to $\mathbb{F}_4$, the field of 4 elements. It is easy to see that the nonzero cosets can be written in the form $1 + \mathfrak{P}, \omega + \mathfrak{P}$, and $\omega^2 + \mathfrak{P}$.

We will now give an outline of the proof of the theorem.

Proof. We claim that every irreducible element of $R[[x]]$ is again irreducible in $\overline{R}[[x]]$. If not, then we factor an irreducible $f \in R[[x]]$ as gh with $g, h \in \overline{R}[[x]]$. First note that if both h and g are in $I[[x]]$, then this is a direct contradiction. We begin by assuming that *neither* g nor h is an element of $I[[x]]$; we write

$$g(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k(b_k + b_{k+1}x + \cdots)$$

where b_k is the first term not in the conductor I. We write $b_k = u_1 + I_g$ with u_1 a unit of $\overline{R}$ and $I_g \in I$. Collapsing notation we write

$$g = \overline{g} + x^k(u_g + I_g)$$

where u_g is a unit power series with constant coefficient $u_1 \in U(\overline{R})$ and $\overline{g} \in I[[x]]$.

In a similar fashion, we write

$$h = \overline{h} + x^m(u_h + I_h)$$

with u_h a unit power series with constant coefficient $v_1 \in U(\overline{R})$, $\overline{h} \in I[[x]]$, and $I_h \in I$.

Note that

$$\begin{aligned} gh =& \overline{g}\overline{h} + \overline{g}x^m(u_h + I_h) + \overline{h}x^k(u_g + I_g) + \\ &+ x^{k+m}(u_g u_h + u_g I_h + u_h I_g + I_g I_h). \end{aligned}$$

Since $\overline{h}, \overline{g}, I_g$, and I_h are in $I[[x]]$ and g and h are in $R[[x]]$, we obtain that $u_g u_h$ is an element of $R[[x]]$. As a consequence we note that since

$$g = \overline{g} + x^k(u_g + I_g)$$

we have that

$$u_h g = u_h \overline{g} + x^k(u_h u_g + u_h I_g)$$

and so $u_h g \in R[[x]]$. Similarly, we obtain that $u_g h \in R[[x]]$.

We now note that

$$f = gh = (u_h g)(u_g h)(u_h u_g)^{-1}$$

and we have a contradiction. The final case to consider is the case when precisely one of the factors, g or h, is an element of $I[[x]]$. We will assume without loss of generality that $g = \overline{g}$ is the factor in $I[[x]]$. In this case, $u_h g \in R[[x]]$ and we have

$$f = gh = (u_h g)(u_h^{-1} h)$$

which is again a contradiction.

Now that we have established that every irreducible in $R[[x]]$ is irreducible in $\overline{R}[[x]]$, we observe that if we have two irreducible factorizations in $R[[x]]$

$$f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m$$

then each f_i, g_j is irreducible in $\overline{R}[[x]]$ which is a UFD (since $\overline{R}$ is a 1 dimensional UFD and hence a PID). Hence $n = m$. □

We cannot resist highlighting what we believe to be an interesting implication of this example.

Corollary 8.3.3. *There exist HFDs R such that the half-factorial property is lost in $R[x]$ and regained in $R[[x]]$.*

Proof. If one considers the ring $R := \mathbb{Z}[\sqrt{-3}]$, then this is an HFD such that $R[x]$ is not an HFD, since R is not integrally closed. Nonetheless, the above result shows that $R[[x]]$ is indeed an HFD. □

Here is a final observation along these lines.

Corollary 8.3.4. *If $R[[x]]$ is a UFD, then R and $R[x]$ are UFDs. If $R[[x]]$ is an HFD, then R is an HFD, but $R[x]$ is not necessarily an HFD.*

Proof. First we note that any irreducible element of R remains irreducible in $R[[x]]$. Indeed, if $\pi \in Irr(R)$ and $\pi = f(x)g(x)$ with $f(x), g(x) \in R[[x]]$ then we write $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i$ and factor

$$\pi = (\sum_{i=0}^{\infty} a_i x^i)(\sum_{i=0}^{\infty} b_i x^i).$$

It is immediate that we get the factorization

$$\pi = a_0 b_0$$

and since $\pi \in Irr(R)$, either a_0 or b_0 is a unit in R, forcing either $f(x)$ or $g(x)$ to be a unit in $R[[x]]$. This establishes our claim.

Given this claim, we consider the following factorization in R

$$\pi_1 \pi_2 \cdots \pi_n = \xi_1 \xi_2 \cdots \xi_m$$

with each $\pi_i, \xi_j \in Irr(R)$.

If $R[[x]]$ is an HFD, then all of the above irreducible elements remain irreducible in $R[[x]]$ and since $R[[x]]$ is an HFD, we must have $n = m$ and R is an HFD.

Additionally, if $R[[x]]$ is a UFD, then every irreducible element of $R[[x]]$ is prime, and hence each π_i and ξ_j is a prime element of $R[[x]]$ (and it is easy to see that the elements are therefore prime as elements of R). Hence R is a UFD.

We now have that if $R[[x]]$ is a UFD (respectively HFD) then R is a UFD (respectively HFD). The fact that if $R[[x]]$ is a UFD implies that $R[x]$ is a UFD follows from the previously mentioned result of Gauss, and the absence of the analogous result for HFDs is demonstrated by the above example. □

We remark here that one might notice that there is a similar result for the case of (semi)quasi-local rings. That is, if $R[[x]]$ is (semi)quasi-local then R is (semi)quasi-local, but $R[x]$ is not. One thing to contrast, however, is that $R[x]$ is *never* (semi)quasi-local.

Bibliography