Arithmetic Rings and Integrality

Jim Coykendall

July 15, 2010

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 nontrivial 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 $\Longleftrightarrow$ $(x) = R$.

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

c) x is an irreducible $\Longleftrightarrow$ (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 $(a, \mathfrak{P}) \supsetneq \mathfrak{P}$ 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 $\mathrm{im}(\phi)$ is a subring of S and $\ker(\phi)$ is an ideal of R is an easy exercise. We will establish the last statement.

Define

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

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. As an exercise in linear algebra, it can be shown (for domains) that this is equivalent to the existence of a finitely generated $R-$module, A, such that $tA \subseteq A$. Suppose that A is the module for t and B is the module for s (and arrange it so that 1 is in A and B). Hence $(u+v)AB \subseteq AB$ and $uvAB \subseteq AB$. □

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

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

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 $R \subseteq R_S$.*

Proposition 2.4.9. *If R_i is a collection of integrally closed domains, all contained inside some large domain T, then $\bigcap R_i$ is integrally closed.*

Proof. Exercise. □

Theorem 2.4.10. *Let R be an integral domain. Then $R = \bigcap_{\mathfrak{M}} R_{\mathfrak{M}}$ where $\mathfrak{M}$ ranges over the maximal ideals of R.*

Proof. Certainly the containment $R \subseteq \bigcap_{\mathfrak{M}} R_{\mathfrak{M}}$ is clear. For the other containment, we suppose that $\frac{a}{b} \in \bigcap_{\mathfrak{M}} R_{\mathfrak{M}}$. Let $I = \{x \in R | xa \in (b)\}$ and note that if $I = R$, then we are done (as then $\frac{a}{b} \in R$). If, on the other hand, I is a proper ideal of R, we expand I to a maximal ideal (say $I \subseteq \mathfrak{N}$). Since $\frac{a}{b} \in R_{\mathfrak{N}}$, we have that $fracab = \frac{c}{s}$ with $s \notin \mathfrak{N}$. Hence $as = bc$ which implies $s \in I \subseteq \mathfrak{N}$. This completes the proof. □

Proposition 2.4.11. *If R is integrally closed and S is a multiplicative subset of R, then R_S is integrally closed.*

Proof. Suppose that $\frac{a}{b} \in K$ and we have the equation

$$(\frac{a}{b})^n + \frac{r_{n-1}}{s_{n-1}}(\frac{a}{b})^{n-1} + \cdots + \frac{r_1}{s_1}(\frac{a}{b}) + \frac{r_0}{s_0} = 0.$$

Multiplying through by the appropriate denominator we obtain the auxilary equation

$$t_n(\frac{a}{b})^n + t_{n-1}r_{n-1}(\frac{a}{b})^{n-1} + \cdots + t_1r_1(\frac{a}{b}) + t_0r_0 = 0$$

with each $t_i \in S$. Note that this equation implies that the element $t_n\frac{a}{b}$ is integral over R. Since R is integrally closed, we have that

$$t_n\frac{a}{b} = r$$

and hence

$$\frac{a}{b} = \frac{r}{t_n}$$

and this completes the proof.

□

Corollary 2.4.12. *R is integrally closed if and only if $R_{\mathfrak{M}}$ is integrally closed for all $\mathfrak{M} \in MaxSpec(R)$.*

Proof. Exercise. □

Here is a last (for now) lemma on integrality that we will utilize in the next chapter.

Lemma 2.4.13. *Let R be a commutative ring and u an invertible element of a ring containing R. Then u^{-1} is integral over R if and only if $u^{-1} \in R[u]$.*

Proof. Exercise. □

Chapter 3

Valuations and valuation domains

3.1 Basics

Definition 3.1.1. *Let R be an integral domain, we say that R is a valuation domain if given any two nonzero $a, b \in R$, we have that either $a|b$ or $b|a$.*

Equivalently, R is a valuation domain if for any ω in the quotient field of R, we have that either ω or ω^{-1} is an element of R.

The following result gives a number of nice properties of valuation domains.

Theorem 3.1.2. *Let R be a valuation domain. Then R has the following properties.*

1. *R is quasi-local.*
2. *R is integrally closed.*
3. *Every overring of R is a valuation domain.*
4. *Every overring of R is a localization of R.*
5. *R every finitely generated ideal of R is principal.*
6. *R all (prime) ideals of R are linearly ordered.*
7. *If I is any ideal in R, then $\sqrt{I}$ is prime.*

Example 3.1.3. *Noetherian valuation domains (e.g. $\mathbb{Z}_{(p)}$ and $\mathbb{F}[[x]]$). Many other example exist with some strange properties (e.g. no height on prime, principal maximal ideal contrasted with maximal ideal that is a union of the primes contained in it).*

The following is quite useful.

Theorem 3.1.4. *Let $R \subseteq T$ be rings, $u \in U(T)$, and I a proper ideal in R. Then I survives in $R[u]$ or in $R[u^{-1}]$.*

Proof. If not, then we obtain two equations:

$$a_0 + a_1 u + \cdots + a_n u^n = 1$$

and

$$b_0 + b_1 u^{-1} + \cdots + b_m u^{-m} = 1$$

with each $a_i, b_j \in I$. We assume that $n \geq m$ and further has been chosen as small as possible. First we multiply the second equation by u^n to get

$$(1 - b_0)u^n = b_1 u^{n-1} + \cdots + b_m u^{n-m}.$$

Now merely multiply the first equation by $1 - b_0$ and substitute to find a similar equation for u with smaller n. □

This give rise to an important theorem.

Theorem 3.1.5. *Let K be a field and $R \subseteq K$ and I a proper ideal of R. Then there exists a valuation domain V ($R \subseteq V \subseteq K$) such that K is the quotient field of V and I survives in V.*

Proof. Consider all pairs, R_j, I_j where R_j is a ring between R and K and I_j is a proper ideal of R_j. We partially order this set by declaring that $\geq$ means both that $R_j \supseteq R_i$ and that $I_j \supseteq I_i$. Zornify to get maximal pair (V, J). It will suffice to show that V is a valuation domain. To this end, suppose that $u \in K$ (quotient field of V), we merely need to show that either u or u^{-1} is an element of V. But by the previous result, we have that J (and hence I) survives in either $V[u]$ or $V[u^{-1}]$. By the maximality of V, this implies that either $V[u]$ or $V[u^{-1}]$ is V and hence either u or u^{-1} is an element of V.

□

The following theorem illustrates the importance of valuation domains in the realm of integrality.

Theorem 3.1.6. *Let R be an integral domain with quotient field K, then*

$$\overline{R} = \bigcap_{R \subseteq V \subseteq K} V$$

where V ranges over the valuation overrings of R.

Proof. One containment is clear. For the other, assume that x is an element of every valuation overring of R. It suffices to show that x is integral over R. Recall that x is integral over R if and only if $x \in R[x^{-1}]$. We suppose that x is not in $R[x^{-1}]$. So there is a valuation overring of $R[x^{-1}]$ (and hence of R) such that (x^{-1}) survives. Necessarily, this is a valuation ring not containing x. □

Here is a result that is easy to show, but interesting in its content. It is "rare" for overrings of certain types of domains persist in this property:

Proposition 3.1.7. *Every overring of a valuation domain is again a valuation domain.*

Definition 3.1.8. *We say that the domain R is a Bezout domain if every finitely generated ideal is principal.*

The following is an ideal theoretic characterization of valuation domains.

Theorem 3.1.9. *Let R be an integral domain. R is a valuation domain if and only if R is a quasilocal Baezout domain.*

Proof. It is known that if R is a valuation domain, then it is quasilocal and it is also easy to see (by induction) that any finitely generated ideal must be principal.

For the more interesting direction, we suppose that R is a quasilocal domain with the property that every finitely generated ideal of R is principal. Suppose that $a, b \in R$ are both nonzero. We consider the ideal (a, b). By assuption, this mean that $(a, b) = (x)$, and hence $x|a$ and $x|b$ and what is more, we can find $r, s \in R$ such that

$$ra + sb = x.$$

Writing $\frac{a}{x} = a'$ and $\frac{b}{x} = b'$, we obtain the equation

$$ra' + sb' = 1.$$

Recalling that R is quasilocal, we note that at least one of r', sb' is not in the maximal ideal $\mathfrak{M}$, and hence a unit of R. Without loss of generality, we say that ra' (and hence a') is a unit of R. Hence a and x are associates and since x divides b, we must have that $a|b$. This concludes the proof.

□

Another way to look at valuation domains is via the concept of a valuation.

Definition 3.1.10. *Let K be a field. A valuation on K is a map $v : K \setminus \{0\} \longrightarrow \mathbb{Z}$ satisfying for all $a, b \in K^*$*

1. *$v(ab) = v(a) + v(b)$,*
2. *$v(a + b) \geq min(v(a), v(b))$.*

Example 3.1.11. *$\mathbb{Q}$, quotient field of a power series ring, more complicated valuations.*

Theorem 3.1.12. *Let K be a field with valuation v. The set of elements $R := \{x \in K | v(x) \geq 0\} \bigcup \{0\}$ is a (the) valuation domain associated to v.*

Proof. Since $v(x + y) \geq \min(v(x), v(y))$ we see that R is closed under addition. Also note that R is closed under multiplication. To see that R is a valuation domain, note that if $\omega \in K$ then either $v(\omega)$ or $v(\omega^{-1})$ is positive. □

Example 3.1.13. *The $p-$adics. Inverse limits and completions.*

3.2 Invertible ideals

In this section we introduce and develop the concept of invertibility. One might consider the concept of invertibility a generalization of (and somewhat akin to) principality. In a certain sense, invertible ideals are similar to principal ideals.

Definition 3.2.1. *Let R be an integral domain with quotient field K. An $R-$submodule of K (say I) is called a fractional ideal of R if there is a nonzero $a \in R$ such that $aI \subseteq R$.*

The condition that $aI \subseteq R$ is a finiteness condition that guarantees that I is not "too big". For example, $\frac{1}{2}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$, but $\mathbb{Q}$ is not.

Definition 3.2.2. *Let R be a domain and I a nonzero fractional ideal. We define the inverse of I via*

$$I^{-1} = \{x \in K | xI \subseteq R\}.$$

Note that $II^{-1} \subseteq R$. If $II^{-1} = R$, we say that I is invertible.

We make a couple of observations. Firstly we note that the set of invertible ideals of R forms a group under multiplication (with R functioning as the identity). We also note that every (nonzero) principal ideal of R is invertible and the set of all nonzero principal ideals forms a subgroup of the group of all invertible ideals. Although we will explore this in a more in depth fashion later we pause to define the class group.

Definition 3.2.3. *Let R be a domain. We define the class group of R by*

$$Cl(R) := Inv(R)/Prin(R),$$

where $Inv(R)$ denotes the group of invertible ideals and $Prin(R)$ denotes the subgroup of principal ideals.

But now we will talk about invertible ideals of R. Thhis first theorem is (in my view) nonintuitive. But it certainly narrows down the field for what "can" be invertible.

Theorem 3.2.4. *Let R be a domain and I an invertible ideal. Then I is finitely generated.*

It should be made clear that the converse is very far from true.

Proof. Since $II^{-1} = R$, we can find $a_1, \cdots, a_n \in I$ and $b_1, \cdots, b_n \in I^{-1}$ such that

$$a_1b_1 + a_2b_2 + \cdots a_nb_n = 1.$$

We claim that $\{a_1, \cdots, a_n\}$ is a generating set for I. To this end note that if $x \in I$ then we have

$$(xb_1)a_1 + (xb_2)a_2 + \cdots + (xb_n)a_n = x$$

and since each $xb_i \in R$ by definition, we see that each $x \in I$ is an $R-$linear combination of the a_i's.

□

Theorem 3.2.5. *If R is quasilocal and I is an invertible ideal of R then I is principal.*

Proof. Suppose that R is quasilocal and that I is invertible (without loss of generality, we will say that $I \subseteq R$. Since I is finitely generated, say $I = \langle a_1, \cdots, a_n \rangle$ and $II^{-1} = R$, we must have that there exist $b_1, \cdots, b_n \in I^{-1}$ such that

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n = 1.$$

Since each $a_ib_i \in R$ and since R is quasilocal, we observe that not all of the terms a_ib_i can be elements of the maximal ideal. Hence, without loss of generality, we will say that $a_1b_1 = u$ is a unit in R. And since for all $2 \leq k \leq n$ we have that

$$a_k = u^{-1}ua_k = u^{-1}(b_1a_k)a_1$$

and hence each $a_k \in (a_1)$ and so I is principal.

□

One can adjust the above proof to obtain:

Corollary 3.2.6. *If R is semiquasilocal and I is invertible, then I is principal.*

Of course over a global domain, invertible need not imply principal (for example consider the ideal $(3, 1 + \sqrt{-5})$ in the domain $\mathbb{Z}[\sqrt{-5}]$).

A final theorem for the section.

Theorem 3.2.7. *Let I be a finitely generated ideal. Then I is invertible if and only if $I_{\mathfrak{M}}$ is principal for all $\mathfrak{M} \in MaxSpec(R)$.*

Proof. Exercise. □

Chapter 4

Prüfer and Dedekind Domains

The notion of Prüfer domain globalizes our aforementioned notion of valuation domain. One can think of Prüfer domains of the non-Noetherian analog of the more familiar Dedekind domains. We begin with the formal definition.

Definition 4.0.8. *We say that the integral domain R is a Prüfer domain if every finitely generated ideal of R is invertible.*

Given the definition above, a large class of Prüfer domains includes the valuation domains and, more generally, the Bezout domains.

Example 4.0.9. *For a couple of exotic example of Prüfer domains, we consider the ring of all algebraic integers $\overline{\mathbb{Z}}$ and the ring of entire functions. Both of these example turn out to be Bezout. For a non-Bezout example, consider the ring $\mathbb{Z}[\sqrt{-5}] + \mathbb{Q}(\sqrt{-5})[[x]]$.*

There are a zillion equivalent characterizations of Prüfer in the literature. For now here are three.

Theorem 4.0.10. *Let R be an integral domain. The following conditions are equivalent.*

1. *R is a Prüfer domain.*
2. *$R_{\mathfrak{P}}$ is a valuation domain for all $\mathfrak{P} \in Spec(R)$.*
3. *$R_{\mathfrak{M}}$ is a valuation domain for all $\mathfrak{M} \in MaxSpec(R)$.*

Proof. Note that 2. implies 3. is easy. We will show that 1. implies 2. and that 3. implies 1.

For the implication 1. implies 2., we assume that R is a Prüfer domain and show that $R_{\mathfrak{P}}$ is a valuation domain. Since $R_{\mathfrak{P}}$ is quasilocal, it suffices to show that every finitely generated ideal of $R_{\mathfrak{P}}$ is principal. Consider the ideal

$\langle a_1, \cdots, a_n\rangle$ of $R_{\mathfrak{P}}$ and note that this ideal is a fractional (and hence invertible) ideal of R. Hence the extension of this ideal to $R_{\mathfrak{P}}$ is invertible and hence principal.

For the implication 3. implies 1., we consider the finitely generated ideal $I = \langle a_1, \cdots, a_n\rangle$ of R. Note that $I_{\mathfrak{M}}$ is necessarily principal (for all $\mathfrak{M} \in \text{MaxSpec}(R)$) and hence I is invertible. □

Theorem 4.0.11. *Let R be a Prüfer domain with quotient field K and let V be a valuation overring of R, then $V = R_{\mathfrak{P}}$ for some $\mathfrak{P} \in Spec(R)$.*

Example 4.0.12. *Consider the valuation on the field $\mathbb{F}(x, y)$ indiced by the ord map on $\mathbb{F}[x, y]$. In the valuation overring of $\mathbb{F}[x, y]$ induced by this map, we have that x and y survive but are associates. One can see that this valuation domain is not a localization of $\mathbb{F}[x, y]$.*

Proof. Let M be the maximal ideal of V and $\mathfrak{P}$ its contraction to R. Note that if $s \in R\backslash\mathfrak{P}$ then $s^{-1} \in V$ (lest $s \in \mathfrak{M}$). Therefore it is easy to see that $R_{\mathfrak{P}} \subseteq V$.

For the other containment, we first note that $R_{\mathfrak{P}}$ is a valuation domain since R is Prüfer. Suppose that $v \in V$. If $v \notin R_{\mathfrak{P}}$ then $v^{-1} \in R_{\mathfrak{P}}$. Hence $v^{-1} = \frac{r}{s}$ with $s \notin \mathfrak{P}$. Note that $r \in \mathfrak{P}$ and hence $vr = s \in \mathfrak{M}$ which is our contradiction. □

Theorem 4.0.13. *Any overring of a Prüfer domain is again a Prüfer domain.*

Proof. Note that if T is an overring of R and $\mathfrak{Q}$ is a prime ideal of T and $\mathfrak{P} := R \bigcap \mathfrak{Q}$ then the previous makes it easy to see that $R_{\mathfrak{P}} = T_{\mathfrak{Q}}$ and hence is a valuation domain. Hence T is Prüfer. □

We tie some stuff together.

Theorem 4.0.14. *Let R be a domain. The following conditions are equivalent.*

1. *R is a Prüfer domain.*

2. *Every overring of R is a Prüfer domain.*

3. *Every overring of R is integrally closed.*

4. *Every overring is an intesection of localizations of R.*

Theorem 4.0.15. *Let K be a field and x an indeterminate. Let V be a valuation domain between K and $K(x)$ with $V \neq K(x)$ but $K(x)$ being the quotient field of V. Then V is either $K[x]]$ localized at some prime $\mathfrak{P} = (f)$ or $V = K[x^{-1}]_{(x^{-1})}$.*

Proof. Either x or x^{-1} is an element of V. If $x \in V$ then $K[x] \subseteq V$ and since $V[x]$ is Prüfer (PID) then $V = K[x]_{(f)}$. If, on the other hand, we have that $x \notin V$, then $K[x^{-1}]$ is strictly contained in V. Once again, $V = K[x^{-1}]_{\mathfrak{P}}$ and since $x \notin V$, $x^{-1} \in \mathfrak{P}$ and hence $\mathfrak{P} = (x^{-1})$. □

The following is often called the "u, u^{-1} lemma" and it is quite useful.

Theorem 4.0.16. *Let R be quasilocal and integrally closed and $u \in K$, the quotient field of R. If u is the root of a polynomial equation over R with at least one of the coefficients an element of $U(R)$, then either u or u^{-1} is an element of R.*

Proof. Suppose that the equation for u takes the form

$$au^n + bu^{n-1} + \cdots = 0.$$

Note that in any case, au is integral over R and is hence in R. If $au \in U(R)$ then note that $u^{-1} \in R$ and we are done. If au is not a unit, we consider the equation

$$(au + b)u^{n-1} + \cdots = 0.$$

If b is a unit, then $au + b$ is a unit and once again, u is integral (and therefor in) R. If b is not a unit, we proceed by induction and at some point, there must be a unit coefficient. □

Here is another useful theorem that allows us to build Prüfer domains.

Theorem 4.0.17. *Let R be a Prüfer domain with quotient field K. If F is an algebraic extension of K and T is the integral closure of R in F, then T is Prüfer.*

Proof. Let $\mathfrak{N}$ be a maximal ideal of T and let $\mathfrak{M} := \mathfrak{N} \bigcap R$. Our aim is to show that $T_{\mathfrak{N}}$ is a valuation domain. To this end, suppose that $\lambda \in F$. Note that λ is a root of a polynomial equation over $R_{\mathfrak{M}}$. Since $R_{\mathfrak{M}}$ is a valuation domain, we can adjust this equation so that (at least) one of the coefficients is a unit in $R_{\mathfrak{M}} \subseteq T_{\mathfrak{N}}$. By the u, u^{-1} lemma, either λ or λ^{-1} is in $T_{\mathfrak{N}}$. This concludes that proof. □

4.1 More on Integrality

Before we impose a tighter (Noetherian) restriction on our domains, we will look a bit closer at integral extension. This will be done in a slighty more general setting.

Theorem 4.1.1. *Let $R \subseteq T$ be rings and u an element of a ring containing T. If u is integral over T and T is integral over R, then u is integral over R.*

Proof. Suppose that u stisfies the polynomial equation

$$u^n + t_{n-1}u^{n-1} + \cdots + t_1 u + t_0 = 0$$

with each $t_i \in T$. Consider $M = R[t_0, t_1, \cdots, t_{n-1}, u]$. It is easy to see that M is a finitely generated R module and hence u is integral over R. □

Here are some properties that may be satisfied by the pair of rings $R \subseteq T$. We say that the extension $R \subseteq T$ satisfies:

1. Lying over (LO) if for any $\mathfrak{P} \in \operatorname{Spec}(R)$, there is a $\mathfrak{Q} \in \operatorname{Spec}(T)$ such that $\mathfrak{Q} \bigcap R = \mathfrak{P}$.

2. Going up (GU) if given primes $\mathfrak{P}_0 \subseteq \mathfrak{P}_1$ of R and $\mathfrak{Q}_0$ a prime in T with $\mathfrak{Q}_0 \bigcap R = \mathfrak{P}_0$, there exists a prime $\mathfrak{Q}_1 \subseteq T$ with $\mathfrak{Q}_0 \subseteq \mathfrak{Q}_1$ and $\mathfrak{Q}_1 \bigcap R = \mathfrak{P}_1$

3. Going down (GD) if given primes $\mathfrak{P}_0 \supseteq \mathfrak{P}_1$ of R and $\mathfrak{Q}_0$ a prime in T with $\mathfrak{Q}_0 \bigcap R = \mathfrak{P}_0$, there exists a prime $\mathfrak{Q}_1 \supseteq T$ with $\mathfrak{Q}_0 \supseteq \mathfrak{Q}_1$ and $\mathfrak{Q}_1 \bigcap R = \mathfrak{P}_1$

4. Incomparable (INC) If $\mathfrak{Q}_0$ and $\mathfrak{Q}_1$ are distinct primes in T such that $\mathfrak{Q}_0 \bigcap R = \mathfrak{Q}_1 \bigcap R$, then $\mathfrak{Q}_0$ and $\mathfrak{Q}_1$ are incomparable.

The key to comparing primes of R and primes of T often lie in the study of multiplicative sets.

Theorem 4.1.2. *Let $R \subseteq T$ be rings. The following are equivalent.*

1. *GU holds.*

2. *If $\mathfrak{P}$ is a prime ideal of R and S is the compliment of $\mathfrak{P}$ in R and $\mathfrak{Q}$ is an ideal of T maximal with respect to the exclusion of S, then $\mathfrak{Q} \bigcap R = \mathfrak{P}$.*

Proof. For the 2. implies 1. implication, suppose that we have $\mathfrak{P}_0 \subseteq \mathfrak{P}_1$ are primes of R and that $\mathfrak{Q}_0$ is a prime in T contracting to $\mathfrak{P}_0$ in R. Note that $Q_0 \bigcap S$ is empty (where S is the compliment of $\mathfrak{P}_1$ in R. We expand $\mathfrak{Q}_0$ to $\mathfrak{Q}_1$ that is maximal with respect to the exclusion of S. By assumption, $\mathfrak{Q}_1 \bigcap R = \mathfrak{P}_1$.

For the other direction, we let $\mathfrak{Q}$ be maximal with respect to the exclusion of S, which is the complement of $\mathfrak{P}$ in R. Assuming GU, we have to prove that $\mathfrak{Q} \bigcap R = \mathfrak{P}$. Certainly, $\mathfrak{Q}$ lies over some prime ideal and GU allows us to expand this to a prime $\mathfrak{Q}_1$ lying over $\mathfrak{P}$. The maximality of $\mathfrak{Q}$ shows that $\mathfrak{Q} = \mathfrak{Q}_1$.

□

Corollary 4.1.3. *GU implies LO.*

Proof. Immediate. □

Theorem 4.1.4. *Let $R \subseteq T$ be rings. The following are equivalent.*

1. *INC holds.*

2. *If $\mathfrak{P} \subseteq R$ is a prime ideal and $\mathfrak{Q} \subseteq T$ contracting to $\mathfrak{P}$ the Q is maximal with respect to the exclusion of S, the complement of $\mathfrak{P}$ in R.*

Proof. Exercise. □

Here is a look at what happens in the case of integral extensions.

Theorem 4.1.5. *Let $R \subseteq T$ be an extension of rings with T integral over R. Then the pair $R \subseteq T$ satisfies GU and INC.*

Proof. Using the characterization of GU from the previous (and the notation), we must show that $\mathfrak{Q} \bigcap R = \mathfrak{P}$. Certainly we have that $\mathfrak{Q} \bigcap R \subseteq \mathfrak{P}$. If we do not have equality, we choose and $x \in \mathfrak{P}$ that is not in the contraction of $\mathfrak{Q}$. Hence the ideal $(\mathfrak{Q}, x)$ properly contains $\mathfrak{Q}$, hence it must hit S, That is, we can find $q \in \mathfrak{Q}$ and $a \in T$ such that $s = q + ax$.

Write the equation of integrality for $a \in T$:

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

and then multiply by x^n to obtain an equation of integrality for ax:

$$(ax)^n + r_{n-1}x(ax)^{n-1} + \cdots + r_1 x^{n-1}(ax) + r_0 x^n = 0.$$

Recall that $ax = s - q$ and so, if we replace in the preceding equation, we obtain

$$(s)^n + r_{n-1}x(s)^{n-1} + \cdots + r_1 x^{n-1}(s) + r_0 x^n = q_1 \in \mathfrak{Q}.$$

Note that the left side of the above is in R and $\mathfrak{Q}$ and hence in $\mathfrak{P}$. Since $x \in \mathfrak{P}$ then it follows that $s \in \mathfrak{P}$.

To show that integral extensions satisfy INC, we use the previous. Assume that $\mathfrak{P} = \mathfrak{Q} \bigcap R$, we wish to show that $\mathfrak{Q}$ is maximal with respect to the exclusion of $S = R \setminus \mathfrak{P}$. SUppose on the contrary that $\mathfrak{Q}$ is properly contained in I and $I \bigcap S$ is empty. Select $u \in I \setminus \mathfrak{Q}$ and recall that u is integral over R. Among all monic polynomials in $R[x]$ such that $f(u) \in \mathfrak{Q}$ we select one of least degree (and the degree will be larger than 1). Say our polynomial is

$$u^n + r_{n-1}u^{n-1} + \cdots + r_1 u + r_0.$$

Note that the constant term is an element of I. Hence $r_0 \in I \bigcap R \subseteq \mathfrak{P} \subseteq \mathfrak{Q}$. Hence

$$u(u^{n-1} + \cdots + r_1)$$

is in $\mathfrak{Q}$. But neither factor is.

□

Definition 4.1.6. *We say that the chain of prime ideals of R*

$$\mathfrak{P}_0 \subseteq \mathfrak{P}_1 \subseteq \cdots \subseteq \mathfrak{P}_n$$

has length n.

Definition 4.1.7. *The Krull dimension of R is the supremum over the lengths of chains of primes in R.*

Example 4.1.8. *The dimension of $\mathbb{Z}$ is 1. Any field has dimension 0.*

Here are a couple of lemmas to pave the way for us.

Lemma 4.1.9. *If $R \subseteq T$ is GU then dim$(R) \leq$ dim(T).*

Proof. Suppose that we have a chain of primes of length n in R:

$$\mathfrak{P}_0 \subseteq \mathfrak{P}_1 \subseteq \cdots \subseteq \mathfrak{P}_n.$$

Repested application of GU allows to to construct the chain of primes of T:

$$\mathfrak{Q}_0 \subseteq \cdots \subseteq \mathfrak{Q}_n$$

with each $\mathfrak{Q}_i \bigcap R = \mathfrak{P}_i$.

□

Lemma 4.1.10. *If $R \subseteq T$ is INC then dim$(R) \geq$ dim(T).*

Proof. Suppose that we have the chain of primes of T:

$$\mathfrak{Q}_0 \subsetneq \mathfrak{Q}_1 \subsetneq \cdots \subsetneq \mathfrak{Q}_n$$

Since the extension $R \subseteq T$ is INC, the ideals in the corresponding chain of primes obtained by intersecting with R:

$$\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \cdots \subsetneq \mathfrak{P}_n$$

are all distinct. Hence the lemma.

□

Theorem 4.1.11. *If $R \subseteq T$ is an extension of domains satisfying GU and INC, then dim$(R) =$ dim(T).*

Proof. Immediate from the previous two lemmas. □

4.2 Dedekind Domains

Dedekind domains may be considered analogs of UFDs (from a factorization point of view) or PIDS (from an ideal-theoretic point of view). Dedekind domains enjoy many “nice” properties and although some may exhibit certain pathological behavior, most Dedekind domains are well-behaved. All rings of algebraic integers are Dedekind domains for example.

We first define Dedekind domains in terms of invertible ideals.

Definition 4.2.1. *We say that R is a Dedekind domain if every nonzero ideal is invertible.*

So Dedekind domains are the Noetherain Prüfer domains.

There are many equivalent characterizations of Dedekind domains in the literature. Here are a few.

Theorem 4.2.2. *Let R be an integral domain. The following conditions are equivalent.*

1. *R is Dedekind.*

2. *R is one-dimensional (or less), integrally closed, and Noetherian.*

3. *R is Noetherian and the localization of R at any prime is a Noetherian valuation domain.*

4. *Every nonzero ideal in R is a product of prime ideals.*

Proof. For 1 implies 2, we have that R is Dedekind (that is, all ideals are invertible). Note that Noetherian is automatic since invertible ideals are finitely generated. Now let $\mathfrak{M}$ be a maximal ideal. For all such $\mathfrak{M}$, $R_{\mathfrak{M}}$ must be a PID (since all ideals of R are invertible, they all must be locally principal). So $R_{\mathfrak{M}}$ is a PID for all $\mathfrak{M}$ and hence R is 1 dimensional. Additionally, since R is integrally closed if and only if each $R_{\mathfrak{M}}$ is integrally closed, we have that R is also integrally closed.

For the implication 2 implies 3, we note that the Noetherian is automatic. It will suffice to show that the localization at any maximal ideal is a Noetherian valuation domain. By way of contradiction, we suppose that for some maximal ideal $\mathfrak{M}$, we have that $R_{\mathfrak{M}}$ is not a Noetherian valuation domain. We do note that $R_{\mathfrak{M}}$ is Noetherian and 1 (or less) dimensional. Suppose that R is not a PID.

Abusing the notation, we now assume that R is local with maximal ideal $\mathfrak{M}$. We first claim that the maximal ideal $\mathfrak{M}$ is the annihilator of $R/(x)$ for some nonzero, nonunit $x \in R$. To this end the set of all annihilators of nonzero elements of $R/(x)$ is contained in a maximal one (via ACC) and the set of all zero divisors on $R/(x)$ is the set theoretic union of all of the maximal ones, and each of these is prime. Note that annihilators are nonzero since the maximal ideal of R is the radical of any nonzero ideal within it. Hence our maximal ideal $\mathfrak{M}$ must be the annihilator of some nonzero, nonunit $y \in R$. We have that

$$\mathfrak{M}y \subseteq (x)$$

and hence $\frac{y}{x}$ is an element of $\mathfrak{M}^{-1}$. We see that $\mathfrak{M}^{-1}$ properly contains R and hence $\mathfrak{M}\mathfrak{M}^{-1} \supseteq \mathfrak{M}$.

If $\mathfrak{M}\mathfrak{M}^{-1} = \mathfrak{M}$ then we have that (every element of) $\mathfrak{M}^{-1}$ is integral over R. Hence $\mathfrak{M}^{-1}$ is contained in R which is a contradiction. Hence $\mathfrak{M}\mathfrak{M}^{-1} = R$. Hence R is principal and we are done.

For the implication 3 implies 1, we have that each $R_{\mathfrak{M}}$ is a Noetherian valuation domain. So if $I \subseteq R$ is an ideal then I is finitely generated and locally principal for all $\mathfrak{M}$ and hence I is an invertible ideal of R.

The connection with 4 is an exercise.

□

Theorem 4.2.3. *If R is a one dimensional Noetherian domain and T is an overring of R, then T is again one dimensional and Noetherian*

We will prove this later.

Corollary 4.2.4. *If R is one dimensional and Noetherian then the integral closure of R is Dedekind.*

Theorem 4.2.5. *If R is Dedekind with quotient field K and F is a finite extension field of K, then T, the integral closure of R in K, is Dedekind.*

Proof. We already know that T is Prüfer. To see that it is Dedekind, we merely need Noetherian. Let $\{u_1, \cdots, u_n\}$ be a basis for F over K (we can, and do, demand that each $u_i \in T$). Let $T_0 = R[u_1, \cdots, u_n]$. Note that T_0 is Noetherian and 1 dimensional and T is its integral closure. Hence T is Dedekind. □

We will now take an excursion to prove an important result in commutative algebra that we needed above. We first recall that a composition series for the $R-$module M is a chain

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

with the property that each M_i/M_{i+1} is simple. It is known that if M has a composition series then one can refine any series to a composition series and that any two refined series have the same length.

We have the following theorem.

Theorem 4.2.6. *Let R be a ommutative ring. The following are equivalent.*

1. *R is Noetherian and $0-$dimensional.*
2. *Any finitely generated $R-$module has finite length.*
3. *R has finite length as an $R-$module.*
4. *R is Artinian.*

Proof. For the implication 1 implies 2, we note that if R is $0-$dimensional, then all of its primes are minimal and maximal. Since there are only finitely many primes over (0), there are only finitely many of them, say $M_1, M_2, \cdots, M_n$. Note that the product $M_1 \cdots M_n$ is in the Jacobson (and the nil) radical. Since this product is finitely generated, it must be nilpotent. We will say that $(M_1 \cdots M_n)^k = 0$.

Let N be a finitely generated $R-$module. Between) and N we can insert nk intermediate modules as follows

$$N \supset \cdots \supset B \supset M_i B \supset \cdots \supset 0$$

with B being N multiplied by some product of the M_i's (with appropriate repetition allowed). Note that B/M_iB is a finitely generated module over R/M_i and hence only finitely many more can be inserted into the gap between B and M_iB.

2 implies 3 is clear.

3 implies 1. If R has finite (fixed) length, it certainly must be ACC and hence Noetherian. To show that R is 0-dimensional, we reduce the problem. Suppose that there is a chain of primes $P \subsetneq M$ in R. Passing to the quotient R/P we merely need to show that if R is a domain of finite length, then R is a field. If R is of finite length, we find a minimal (nonzero) ideal I and choose $0 \neq x \in I$. Note that $xI = I$ and so there is an $\alpha \in I$ such that $x\alpha = x$. Since R is a domain, $\alpha = 1$, $I = R$ and hence R is a field.

Note that 3 and 4 are equivalent.

□

Corollary 4.2.7. *Let R be a domain. Then R is Noetherian and dimension ≤ 1 if and only if for any nonzero ideal I in R, R/I has finite length.*

Proof. If R is Noetherian and and of dimension ≤ 1 then for all $I \neq 0$, R/I is Noetherian and $0-$dimensional. The converse of this statement is clear. □

Proposition 4.2.8. *If R is a zero-dimensional ring, then any non-zero-divisor is a unit.*

Proof. Exercise. □

Here is a last crucial lemma.

Lemma 4.2.9. *Let R be a one dimensional integral domain and a, c nonzero elements of R. If $J = \{x \in R | xa^n \in (c)\}$, then $(J, a) = R$.*

Proof. Note that $c \in J$ so that $J \neq 0$. By the previous, every non-zero-divisor in R/J has an inverse. By abuse of notation, we consider a as an element of R/J and assert that a is not a zero-divisor. Note that if $ab = 0$ in R/J, we would have that $ab \in J$. Hence $a^n ab \in J$, hence $b \in J$. This shows that a is not a zero divisor in R/J and hence $(J, a) = 0$. □

Now for the theorem.

Theorem 4.2.10. *If R is a one dimensional Noetherian domain and T is an overring of R, then T is again one dimensional and Noetherian.*

Proof. Let $a \in R$ be arbitrary. The strategy is to show that T/aT is a finitely generated $R-$module. Since any ideal of T contains an element of R, we will be done by the previous.

To this end, we write $I_m = (a^m T \bigcap R, aR)$. Note that this is a descending chain of ideals of R all containing aR. Since this chain becomes stabilizes, we will say that it stabilizes at I_n and for this value of n we claim that

$$T \subseteq \frac{1}{a^n} R + aT.$$

To see this we take $t \in T$ and write $t = \frac{b}{c}$ with $b, c \in R$. Taking a, c as in the previous lemma, we have that $(J, a) = R$ where $J = \{x \in R | xa^n \in (c)\}$. We can write

$$1 = j + za$$

with $j \in J$ and $z \in R$. Hence $t = \frac{bj}{c} + tza$. Note that $ja^k \in (c)$ for some k so

$$\frac{bj}{c} = \frac{b}{c}\frac{ja^k}{a^k} \in \frac{1}{a^k}R.$$

And so $t \in \frac{1}{a^k}R + aT$ for some k. So if $k \leq n$ we have established what we wanted. Let us assume that k is as small as possible but $k > n$. We have

$$t\frac{u}{a^k} + at_1.$$

Hence

$$u = a^k(t - at_1)$$

and so u is in a^kT and R and hence in I_k.

Since $k > n$ we have $I_k = I_{k+1}$ and hence $u = a^{k+1}t_2 + au_1$. Substituting $t = \frac{u_1}{a^{k-1}} + a(t_1 + t_2)$ and this is a contradiction. Since we have established te veraciy of the containment, we have that T/aT is contained in a cyclic $R-$module. Hence it is finitely generated.

□

We end this section with a quick look at almost Dedekind domains

Theorem 4.2.11. *Let D be a domain with that is not a field. The following conditions are equaivalent.*

1. *D is almost Dedekind.*
2. *Cancellation holds for nonzero ideals of D.*
3. *D is a one-dimesional Prüfer domain with no idempotent maximal ideal.*
4. *D is a Prüfer domain and $\bigcap_{n=0}^{\infty} A^n = (0)$ for every proper ideal $A \subset D$.*

4.3 More on Dedekind domains and class groups

Theorem 4.3.1. *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. □

Example 4.3.2. *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 $\mathfrak{R}^2 = (2)$, $\mathfrak{P}\mathfrak{Q} = (3)$, $\mathfrak{P}\mathfrak{R} = (1+\sqrt{-5})$, and $\mathfrak{Q}\mathfrak{R} = (1-\sqrt{-5})$. The elemental factorization come from rearranging the factors in the ideal factorization*

$$\mathfrak{P}\mathfrak{Q}\mathfrak{R}\mathfrak{R} = (6).$$

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

Definition 4.3.3. *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 4.3.4. *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 4.3.5. *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 4.3.6. *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 4.3.7. *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). □

Theorem 4.3.8. *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. Done. □

Example 4.3.9. *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 4.3.10. *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.

Definition 4.3.11. *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 4.3.12. *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 4.3.13. *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 $\mathfrak{P}\mathfrak{Q}\mathfrak{R}$ is principal and generated by the irreducible δ. We consider the ideal factorization

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

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. □

We end our section on Dedekind domains now with the following catchy result.

Theorem 4.3.14. *If R is Dedekind and $I \subseteq R$ is an ideal, then I is 2-generated (actually $1\frac{1}{2}$ generated).*

Bibliography