What are discrete valuation rings? What are Dedekind domains?

A mathematical essay by Wayne Aitken*

Fall 2019†

This essay introduces discrete valuation rings (DVRs), and shows that they have several possible definitions that are equivalent (we call these "characterizations"). We will use discrete valuations and other ideas to see that Dedekind domains have several interesting equivalent characterizations as well. Along the way we will study properties of Dedekind domains and their fractional ideals. For example, we will classify the discrete valuations of a Dedekind domain in terms of its nonzero prime ideals, and use these valuations to gain a better understanding of fractional ideals. This essay also introduces local methods to the study of Dedekind domains and integral domains more generally. We will often work in integral domains, generally or with some constraints, rather than always assuming we are working in a Dedekind domain. A purpose of this approach is to open the way to the study of rings that are not quite Dedekind; for example, Appendix B considers integral domains, such as orders in algebraic number fields, that are like Dedekind domains except fail to be integrally closed. Appendix E considers integral domains that a like Dedekind domains except they fail to be Noetherian.

An intended audience includes readers studying number theory who are familiar with the ring of integers in an algebraic number field, and who have proved that such rings are Dedekind domains.[1] For such a reader, results about Dedekind domains are mainly applicable in the context of algebraic number fields. Such a reader is likely to have proved that every PID is a Dedekind domain (in particular that PIDs, even UFDs, are integrally closed), and perhaps the theorem on the unique factorization of ideals into prime ideals in a Dedekind domain. For this audience, this essay is not an introduction to Dedekind domains but is, in a sense, a part two in the study of Dedekind domains. Even so, I try to make this essay as self-contained as possible. For example, we will include independent proofs, along the way, that every PID is a Dedekind domain and that every fractional ideal factors uniquely as the product of powers of prime ideals. Because it is self-contained in this way, another possible audience consists of readers interested in the general

†Version of December 3, 2019.

[1]For example, I envision readers who have studied the relevant chapters of an introductory textbook at the level of P. Samuel, *Algebraic Theory of Numbers*, I. Steward and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, or D. Marcus, *Number Fields*.

subject of commutative algebra and who want to explore Dedekind domains and related rings. Such a reader could likely get by with no prior exposure to Dedekind domains as long as they have enough background to understand the concepts used in the definitions, and is likely not to need extra motivation to pursue the abstract approach followed here.

As the name suggests, the theory of Dedekind domains owes much to Dedekind's work in the 19th century on ideals in the context of algebraic number fields. The modern version is largely due to Emmy Noether who in the 1920s studied and characterized Dedekind domains as a general type of ring for which unique factorization of ideals and other results, including some traditionally associated to integers in an algebraic number field, could be proved. In a sense, by doing so she invented the field of commutative algebra. Similarly, this essay does not deal with integers in a number field specifically, but with general integral domains that satisfy various axiomatic properties. So this essay is very much in the spirit of Noether's abstract and axiomatic approach. Of course this essay draws on the work of several other mathematicians in commutative algebra who pioneered the local approach starting with Wolfgang Krull in the 1930s. I have also drawn inspiration and ideas from several other expository accounts by various authors. This material is a cornerstone of modern commutative algebra, number theory, and algebraic geometry, and so is pretty standard, but I have tried to give my own twist on the subject and I hope I have provides some novel viewpoints here and there.

I have attempted to give full and clear statements of the definitions and results, with motivations provided where possible, and give indications of any proof that is not straightforward. However, my philosophy is that, at this level of mathematics, straightforward proofs are best worked out by the reader. So although this is a leisurely account of the subject, some of the proofs may be quite terse or missing altogether. Whenever a proof is not given, this signals to the reader that they should work out the proof, and that the proof is straightforward. Supplied proofs are sometimes just sketches, but I have attempted to be detailed enough that the reader can supply the details without too much trouble. Even when a proof is provided, I encourage the reader to attempt a proof first before looking at the provided proof. Often the reader's proof will make more sense because it reflects their own viewpoint, and may even be more elegant. In addition to this challenge to work out proofs, itself a very good exercise for the reader, I have provided around 60 labeled exercises so a reader can deepen their knowledge – these are usually less essential to the main narrative, so can be skipped in a first reading.

1 Required background

This document is written for readers with some basic familiarity with introductory abstract algebra including some basic facts about groups and their homomorphisms, rings (at least commutative rings), integral domains, fields, polynomial rings (in one variable), ideals, and at least some exposure to modules. In this document all rings will be commutative with a unity element. I assume familiarity with principal, prime and maximal ideals, and with the basics concerning PIDs (principal ideal domains: integral domains whose ideals are all principal). For example, readers should be familiar with the fact that every maximal ideal $\mathfrak{m}$ in a commutative

ring R is a prime ideal, and that $R/\mathfrak{m}$ is a field. In Exercise 3, I also assume familiarity with Euclidean domains, but this exercise is optional. For us, a *proper ideal* is any ideal that is not the whole ring. I assume the result that every proper ideal is contained in a maximal ideal (we often work in Noetherian domains where this follows from the ascending chain condition; for general commutative rings, we would have to use Zorn's lemma). I assume familiarity with the result that an ideal is the whole ring if and only if it contains a unit. For us, a *local ring* is a commutative ring with exactly one maximal ideal. I assume the reader knows, or can verify, that in a local ring R the unit group $R^\times$ is just $R \setminus \mathfrak{m}$ where $\mathfrak{m}$ is the maximal ideal, and conversely if the units $R^\times$ of R are such that $R \setminus R^\times$ is an ideal then R is a local ring with maximal ideal $\mathfrak{m} = R \setminus R^\times$. The reader should also be familiar with the multiplication of ideals (which we review and extend in Sections 3 and 4).

I assume that the reader is familiar with Noetherian rings.[2] One definition is that a Noetherian ring is a commutative ring such that every ideal is finitely generated. So the reader should be familiar with the concept of finitely generated ideals and modules. We really only need the Noetherian concept for integral domains, and we use the term *Noetherian domain* for an integral domain that is Noetherian. In Section 4 we will make use of the following result.

Proposition. *Suppose R is a Noetherian ring. If M is a finitely generated R-module then all R-submodules of M are also finitely generated R-modules.*

We also use the ascending chain condition for Noetherian rings, and the following:

Proposition. *Let $\mathcal{I}$ be a collection of ideals of a Noetherian ring R. If $\mathcal{I}$ is nonempty, then there is a maximal element $I \in \mathcal{I}$ in the sense that there is no $I' \in \mathcal{I}$ with $I \subsetneq I'$.*

Some authors regard fields as Dedekind domains, some do not. We will regard fields as Dedekind domains, and will give the following traditional definition:

Definition 1. A *Dedekind domain* is an integral domain R such that

1. R is Noetherian,
2. R is integrally closed (in the fraction field of R), and
3. every nonzero prime ideal of R is maximal.

As mentioned above, I expect many readers to already have some basic familiarity with Dedekind domains, including the definition and the following results:

1. The ring of integers in an algebraic number field satisfies the above definition of Dedekind domain.
2. Sometimes unique factorization of elements fails in such Dedekind domains.
3. But still Dedekind domains generalize PIDs. In particular, every PID is integrally closed and is in fact a Dedekind domain.

[2] See, for example, my short expository essay *Noetherian modules and rings*.

4. Unique factorization is restored at the level of ideals: every ideal in a Dedekind domain factors essentially uniquely as the product of prime ideals.

We don't really use (1) and (2) in this document, but they provide a primary motivation for considering Dedekind domains at all, at least for number theorists. We will use (3) and (4) in our study of DVRs, but will end up giving independent proofs as we move on to Dedekind domains. So they are not strictly necessary as background from a logical point of view. In fact we will prove (4) twice, once using local methods in the main body, and then a second time in Appendix A, where we consider a standard non-local proof likely similar to proofs that the reader may have seen. This appendix is provided for the convenience of the reader, and to help the reader compare the two approaches.

Since the notion of integrally closed appears in the definition of Dedekind domain, we expect that the reader is familiar with the idea of integral elements over a ring (in terms of roots of monic polynomials with coefficients in a given ring), and the notion of integral closure.

Every integral domain R is a subfield of its field of fractions K. In essence, K is the smallest field containing R. We assume the reader is familiar with such *fields of fractions*, which we also call *fraction fields*. This is a simple example of a localization $S^{-1}R$ of R. Starting with Section 6, I will assume the reader is familiar with the basics of localization, at least in the setting of an integral domain.[3] Since we localize only in an integral domain R, any localization $S^{-1}R$ can be regarded as an intermediate ring

$$R \subseteq S^{-1}R \subseteq K.$$

Here S is a multiplicative system of R. For us, a multiplicative system of R is a subset closed under multiplication, containing 1 but not 0. We assume the reader is also familiar with the localization of ideals of an integral domain. This includes the relationship between ideals of R and ideals of the localization, which is especially simple in the case of prime ideals. We assume the reader is also familiar with the localization of modules, at least for R-submodules of the field of fractions K. For such a module I, the localization $S^{-1}I$ will also be an R-submodules of the field of fractions K. We also assume familiarity with the following:

Proposition. *Suppose R is an integral closed integral domain and that S is a multiplicative system. Then the localization $S^{-1}R$ is integrally closed.*

Suppose R is a Dedekind domain and that S is a multiplicative system. Then the localization $S^{-1}R$ is a Dedekind domain.

Actually, we really only require the first claim as background (which is a good exercise if a reader has not seen it), since we supply arguments for the rest.

Suppose R is an integral domain, and $x \in K$ where K is the field of fractions. Then we can form the ring extension of R generated by x. We write this as $R[x]$, and since $x \in K$ this will be a subring of K. We use this construction in Section 5. On the other hand $R[X]$ with a upper-case X will denote the ring of polynomials with coefficients in R. The rings $R[x]$ and $R[X]$ are related: $y \in R[x]$ if and only if there is a polynomial $f \in R[X]$ such that $y = f(x)$. A key result is that x is integral over R if and only if $R[x]$ is a finitely generated R-module. We will

[3] See my previous expository essay on localization in integral domains.

supply an argument when needed that finitely-generated here implies integral. The other direction is more straightforward: the reader should be able to show that if x is integral and satisfies a monic polynomial of degree d then $R[x]$ is generated by $1, x, \ldots, x^{d-1}$ (one way is to show by induction that $1R + xR + \ldots + x^{d-1}R$ contains the power x^{d+k} for all $k \geq 0$).

When we get to the Chinese remainder theorem in Section 10 we will need to work with Cartesian products of rings $R_1 \times R_2$. The reader should know that the product of rings is a ring under componentwise operations. (Although for our application we will only need to know that it is a group under addition).

If I is an ideal in an integral domain R (or more generally, a commutative ring) then there is natural surjective ring homomorphism $R[X] \to (R/I)[X]$ between polynomial rings that sends X to X. It essentially acts by replacing each coefficient with its equivalence class mod I. We use this homomorphism in Section 11 to help prove Gauss's lemma in Dedekind domains.

2 Discrete valuation rings

In this section we will consider several equivalent characterization of discrete valuation rings. We start by thinking of such rings as rings arising from discrete valuations.

Definition 2. A *discrete valuation* of a field K is a surjective homomorphism

$$v \colon K^\times \to \mathbb{Z}$$

between the multiplicative group $K^\times$ of the field and the additive group $\mathbb{Z}$ such that the following law holds for sums: for all $x, y \in K^\times$, if $x + y \neq 0$ then

$$v(x + y) \geq \min\{v(x), v(y)\}.$$

Remark. Observe that valuations satisfy a multiplicative law $v(xy) = v(x) + v(y)$ and an additive law $v(x + y) \geq \min\{v(x), v(y)\}$. We can extend these laws to all elements $x, y \in K$ by defining $v(0) = \infty$ and then extending addition and the order relation to $\mathbb{Z} \cup \{\infty\}$ in the obvious way. In particular, we can then remove the restriction $x + y \neq 0$ in the above definition.

Exercise 1. Suppose $w \colon K^\times \to \mathbb{Z}$ satisfies the above, except for the assumption of surjectivity. Assume instead that w has nontrivial image. Show that $v \stackrel{\text{def}}{=} \frac{1}{e}w$ is a discrete valuation where e is the smallest positive number in the image of w. Such a w is called a *unnormalized discrete valuation*, and sometimes for emphasis what we call a discrete valuation is called a *normalized discrete valution.*

Exercise 2. Let $F[X]$ be the ring of polynomials over a field F. Can the degree map be extended into a valuation of the field of fractions $F(X)$ of $F[X]$? What about (-1) times the degree map?

Lemma 1. *If v is a discrete valuation then $v(1) = 0$, $v(-1) = 0$, and $v(-x) = v(x)$ for all $x \in K^\times$.*

In the following we use the convention $v(0) = \infty$ mentioned above. (We can easily rephrase the definitions and statements to avoid this though, but it is a convenient convention).

Proposition 2. *Let $v\colon K^\times \to \mathbb{Z}$ be a discrete valuation. Then*

$$\mathcal{O}_v \stackrel{\text{def}}{=} \{x \in K \mid v(x) \geq 0\}$$

is a local integral domain, with maximal ideal

$$\mathfrak{p}_v \stackrel{\text{def}}{=} \{x \in K \mid v(x) \geq 1\}$$

and unit group

$$\mathcal{O}_v^\times = \{x \in K \mid v(x) = 0\}.$$

Also $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$ for all $x \in K^\times$, so K is the fraction field of $\mathcal{O}_v$.

If $v(x) \neq v(y)$ then the inequality $v(x+y) \geq \min(v(x), v(y))$ becomes an equality:

Proposition 3. *Let $v\colon K^\times \to \mathbb{Z}$ be a discrete valuation which we extend to $0 \in K$ using the convention $v(0) = \infty$. If $x, y \in K$ are such that $v(x) \neq v(y)$ then*

$$v(x+y) = \min\{v(x), v(y)\}.$$

Proof. Suppose, say, that $v(y) > v(x)$. We outline two arguments for the result.

In the first argument, observe that x cannot be zero. By dividing x and y by x, we reduce to the case $x_1 = x/x = 1$ and $y_1 = y/x$. Since $v(y_1) > v(x_1) = 0$, we have $y_1 \in \mathfrak{p}_v$. Thus $1 + y_1$ is a unit in $\mathcal{O}_v$, so $v(1 + y_1) = 0 = v(1)$.

For the second argument, suppose that $v(x+y) \neq v(x)$. Thus $v(x+y) > v(x)$. Then

$$v(x) = v((x+y) - y) \geq \min\{v(x+y), v(y)\} > v(x),$$

a contradiction. □

Corollary 4. *Let $v\colon K^\times \to \mathbb{Z}$ be a discrete valuation which we extend to $0 \in K$ using the convention $v(0) = \infty$. Suppose $x_1, \ldots, x_k \in K$ are such that $v(x_1)$ is strictly less than $v(x_i)$ for all $i \neq 1$. Then*

$$v(x_1 + \ldots + x_k) = v(x_1).$$

In particular, $x_1 + \ldots + x_k$ is nonzero.

Proof. Let $x = x_1$ and $y = x_2 + \ldots + x_k$. Use the above proposition. □

Definition 3. A *discrete valuation ring* (DVR) is any ring of the form

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$$

where K is a field and where $v\colon K^\times \to \mathbb{Z}$ is a discrete valuation.

Definition 4. Let $v\colon K^\times \to \mathbb{Z}$ be a discrete valuation. If $\pi \in K^\times$ is such that

$$v(\pi) = 1$$

then we call π a *uniformizer* of v. Since discrete valuations are surjective, such uniformizers exist.

The following shows the usefulness of a uniformizer in terms of unique factorization.

Proposition 5. *Let $v\colon K^\times \to \mathbb{Z}$ be a discrete valuation with uniformizer π. Then every element x of $K^\times$ can be written uniquely as*

$$x = u\pi^k$$

where $k \in \mathbb{Z}$ and where u is a unit in $\mathcal{O}_v$. When x is written in this form, $v(x) = k$.

Remark. This shows that every DVR is a simple type of UFD.

Given a nonzero ideal I of $\mathcal{O}_v$ we must have a smallest value $v(x)$ among elements $x \in I$. This can be used to show the following:

Proposition 6. *Let $v\colon K^\times \to \mathbb{Z}$ be a discrete valuation with uniformizer π. The nonzero ideals of the ring $\mathcal{O}_v$ are $\pi^k\mathcal{O}_v$ where $k \geq 0$. These ideals are distinct and*

$$\pi^k\mathcal{O}_v = \{x \in K \mid v(x) \geq k\}.$$

An element of K is a uniformizer if and only if it generates $\mathfrak{p}_v$ as an ideal.

Corollary 7. *Every DVR is a PID with a unique nonzero prime ideal.*

Exercise 3. Show that every DVR is a Euclidean domain.

Recall that an integral domain R is integrally closed if, for any monic polynomial $f \in R[X]$, every root of f in the field of fractions of R is actually in R.

Proposition 8. *Every DVR is integrally closed.*

Proof. We can appeal to the theorem that every PID or even every UFD is integrally closed. However, there is a nice proof that uses properties of valuations. Let $\mathcal{O}_v$ be a DVR with valuation $v : K^\times \to \mathbb{Z}$ where K is the fraction field of $\mathcal{O}_v$. Let f be a monic polynomial in $\mathcal{O}_v[X]$ with root $x \in K$. We wish to show $x \in \mathcal{O}_v$, so we assume otherwise: suppose that $x \notin \mathcal{O}_v$, so $v(x) = -k < 0$. We can express the equation $f(x) = 0$ as follows:

$$x^d = a_{d-1}x^{d-1} + \ldots + a_1x + a_0$$

where each $a_i \in \mathcal{O}_v$. The valuation of the left hand side is $-dk$, and the valuation of each term on the right is greater than or equal to $-(d-1)k$. So the right hand side must have strictly greater valuation than the left hand side, a contradiction. Thus $v(x) \geq 0$, and $x \in \mathcal{O}_v$. □

Exercise 4. Suppose $v_1, v_2 \colon K^\times \to \mathbb{Z}$ are two valuations. Show that if $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$ then $v_1 = v_2$. Conclude that $v \mapsto \mathcal{O}_v$ is a bijection between the set of discrete valuations of a given field K and the set of discrete valuation rings with field of fractions K.

We have established various properties of discrete valuation rings. Some of these properties are actually sufficient for an integral domain to be a discrete valuation ring. We start with one such property:

Proposition 9. *Suppose that R is an integral domain and suppose π is a nonzero element of R that is not a unit. Suppose that every nonzero element of R can be written as $u\pi^k$ with $k \geq 0$ and with $u \in R^\times$. Then the fraction field K of R has the property that every nonzero element can be written uniquely as $u\pi^k$ with $k \in \mathbb{Z}$ and with $u \in R^\times$. The function $u\pi^k \mapsto k$ defines a discrete valuation $K^\times \to \mathbb{Z}$, and R is the associated discrete valuation ring with uniformizer π.*

Corollary 10. *Suppose that R is an integral domain. Then R is a DVR if and only if there is a non-unit, nonzero $\pi \in R$ such that every nonzero element of R can be written as $u\pi^k$ for some unit $u \in R^\times$ and some $k \in \mathbb{N}$.*

Building on the above results, we can prove a deeper theorem:

Theorem 11. *Suppose that R is a local Noetherian domain whose maximal ideal $\mathfrak{m}$ is nonzero and principal. Then R is a DVR. Conversely, every DVR is a local Noetherian domain with a nonzero principal maximal ideal.*

Proof. Write $\mathfrak{m}$ as πR. Observe that if $x \in R$ is not a unit then x can be written as $x_1\pi$ for some $x_1 \in R$. If x_1 is not a unit then we can write $x = x_1\pi = x_2\pi^2$ for some $x_2 \in R$. And so on. There are two possible types of elements in R: (1) those for which this process stops and so can be written as $u\pi^k$ for some unit u and $k \geq 0$, and (2) those for which the process does not stop, and so we can write such an element x as $x_k\pi^k$ for all $k \in \mathbb{N}$. Call the second type of element "exceptional". Of course 0 is exceptional. We wish to show that 0 is the only exceptional element.

First we show that if $x = x_1\pi \neq 0$ then $xR \subsetneq x_1R$. Of course $xR \subseteq x_1R$ holds, but suppose $xR = x_1R$. Then $x_1 = xy$ for some $y \in R$. In other words, $x = xy\pi$. We write this as $x(1 - y\pi) = 0$. However, $1 - \pi y$ is a unit. Thus $x = 0$, a contradiction.

So, let x be exceptional and nonzero, and write

$$x = x_1\pi = x_2\pi^2 = x_3\pi^3 = \dots$$

with $x_i = x_{i+1}\pi$. By the above claim,

$$xR \subsetneq x_1R \subsetneq x_2R \subsetneq x_3R \subsetneq \dots.$$

This contradicts the Noetherian assumption. Thus the only exceptional element is 0. By Corollary 10 this means that R is a DVR. (The converse is straightforward). □

Remark. Serre points out in his *Local Fields* (Chapter I, §2) that we do not need to assume in advance that R is an integral domain: we can replace that assumption with the assumption that R is a commutative ring (with unity) such that π is not a nilpotent element ($\pi^k \neq 0$ for all k). He goes on to say that the proof is much simpler if R is assumed to be an integral domain. However, if one uses the proof given here, the general case is not much harder: just add the observation (after showing that 0 is the only exceptional element) that $(u\pi^k)(v\pi^l) \neq 0$ if u, v are units, so R is an integral domain.

Exercise 5. Check that the above proof can be modified, as mentioned in the remark, to prove the following: *Let R be a local Noetherian ring whose maximal ideal is πR where π is not a nilpotent element ($\pi^k \neq 0$ for all $k \in \mathbb{N}$). Then R is a discrete valuation ring.*

We can use Theorem 11 to strengthen Corollary 7.

Corollary 12. *Let R be an integral domain. Then the following are equivalent:*

1. *R is a DVR.*
2. *R is a PID with a unique nonzero prime ideal.*
3. *R is a PID with a unique nonzero maximal ideal.*

Recall that every PID is a Dedekind domain (but not every Dedekind domain is a PID). The above corollary actually can be generalized to all Dedekind domains with a unique nonzero prime ideal. If we are willing to accept the unique factorization of ideals result, the proof is simple. Later in the document we will pursue another approach that leads to a proof that does not rely on the unique factorization of ideals.

Theorem 13. *Let R be an integral domain. Then R is a discrete valuation ring if and only if R is a Dedekind domain with a unique nonzero prime ideal.*

Proof. Let R be a DVR. We can appeal to the theorem that every PID is a Dedekind domain. However, we can give a direct proof that uses Proposition 8 to show that R is integrally closed. The ring R has only one nonzero prime ideal, and it is maximal. Finally, R is Noetherian since R is a PID. Thus R is a Dedekind domain.

For the other direction, suppose R is a Dedekind domain with unique nonzero prime ideal $\mathfrak{p}$. By the unique factorization theorem for ideals in a Dedekind domain, we have that the nonzero ideals of R are all uniquely of the form $\mathfrak{p}^k$. If $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ then πR cannot be $\mathfrak{p}^k$ with $k \geq 2$, so $\pi R = \mathfrak{p}$. By definition of Dedekind domain, R is a Noetherian domain. So we apply Theorem 11.

(Another approach, once we admit fractional ideals, is to define the valuation of the fractional ideal $\mathfrak{p}^k$ to be k, where $k \in \mathbb{Z}$. Next define the valuation of $\alpha \neq 0$ in the field of fractions K to be the valuation of the fractional ideal αR.) □

The proof of the above result suggests another charactarization. Call a ring *strongly local* (to coin a new term) if it is local and if there is a largest proper nonmaximal ideal $\mathfrak{n}$ in the sense that all proper nonmaximal ideals are contained in $\mathfrak{n}$. For example, a DVR is strongly local whose largest proper nonprime ideal is $\mathfrak{n} = \mathfrak{p}^2$. A DVR is also Noetherian. These two properties characterize DVRs:

Proposition 14. *Suppose R is an integral domain. Then R is a discrete valuation ring if and only if R is a strongly local Noetherian domain.*

Proof. We discussed already one implication. For the other implication, let $\mathfrak{m}$ be the maximal ideal, and let $\mathfrak{n}$ be the largest proper nonmaximal ideal. Let $\pi \in \mathfrak{m} \setminus \mathfrak{n}$. Then $\mathfrak{m} = \pi R$. Now apply Theorem 11. □

Next we consider a fairly simple characterization of DVRs among Noetherian domains:

Proposition 15. *Let R be a Noetherian domain with fraction field K. Assume R is not a field. Then R is a DVR if and only if x or x^{-1} is in R for each $x \in K^\times$.*

Proof. One direction is straightforward, so assume x or x^{-1} is in R for each $x \in K^\times$. We restate this assumption as follows: if $a, b \in R$ are nonzero then either a/b or b/a is in R. In other words, $a \in bR$ or $b \in aR$. So $aR \subseteq bR$ or $bR \subseteq aR$. Thus the set of principal ideals in R are totally ordered by inclusion.

Since R is Noetherian, there is a maximal element πR among the set of proper nonzero principal ideals of R. Since the set of principal ideals in R are totally ordered, πR is the maximum proper principal ideal. So for each non-unit $a \in R$ we have $aR \subseteq \pi R$. Thus $a \in \pi R$. We conclude that πR is the set of non-units. Thus πR is the unique maximal ideal. Now apply Theorem 11. □

Exercise 6. A *valuation ring* is an integral domain R such that for all $x \neq 0$ in the field of fractions K either x or x^{-1} is in R. The above proposition shows that a Noetherian valuation ring is a DVR. Let us consider valuation rings that are not necessarily Noetherian. (1) Show that the collection of principal ideals in such a valuation ring R is totally ordered by inclusion. (Hint: see the proof of the above proposition). (2) Show that any finitely generated ideal in such a valuation ring R is principal. (3) Show that every valuation ring is local.

Exercise 7. Suppose R is a commutative ring such that the collection of principal ideals is totally ordered by inclusion. Show that the collection of *all* ideals is also totally ordered by inclusion. Based on the previous exercise, conclude that the collection of ideals of a valuation ring are totally ordered by inclusion.

Exercise 8. Suppose R is an integral domain such that the collection of principal ideals is totally ordered by inclusion. Show that R is a valuation ring.

Exercise 9. Let R be a valuation ring with nonzero maximal ideal $\mathfrak{m}$. Show that either $\mathfrak{m} = \mathfrak{m}^2$ or $\mathfrak{m}$ is principal. Hint: let $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$ (if such exists), and use Exercise 6 to argue that $aR \subseteq \pi R$ for all non-units $a \in R$.

Now we assume the reader is comfortable with the concept of the product of ideals. (If not the reader can skip ahead to the next section where this concept is reviewed in some generality.) This concept leads naturally to the notion of divisibility:

Definition 5. Let I and J be two ideals of an integral domain. We say that I *divides* J if there is an ideal I' such that $II' = J$. In this case we write $I \mid J$.

Proposition 16. *Let I and J be ideals of an integral domain. If $I \mid J$ then $J \subseteq I$.*

Throughout this document, we will be interested in the situation where $J \subseteq I$ guarantees that $I \mid J$. Clearly this happens in DVRs given the explicit description of ideals. We now consider two results related to divisibility in the case of principal ideals in local integral domains.

Lemma 17. *Let R be a local integral domain with maximal ideal $\mathfrak{m}$. Suppose I and J are ideals with $IJ = aR$ where $a \in R$. Then there are elements $b \in I$ and $c \in J$ such that $bc = a$.*

Proof. We jump to the case $a \neq 0$, and we write a as a finite sum: $a = \sum b_i c_i$ with each $b_i \in I$ and $c_i \in J$. Since each $b_i c_i \in aR$, we can write $b_i c_i = a u_i$ with $u_i \in R$. Observe that $1 = \sum u_i$, so is not possible for each u_i to be in $\mathfrak{m}$. Thus u_i is a unit for at least one value of i. For such i we have $(u_i^{-1} b_i) c_i = a$ as desired. □

Proposition 18. *Suppose I is an ideal in a local integral domain. If I divides a nonzero principal ideal then I is itself principal.*

Proof. We have $IJ = aR$ for some ideal I and some nonzero $a \in R$. By the previous lemma we also have $bc = a$ where $b \in I$ and $c \in J$. Clearly $bR \subseteq I$. We claim that in fact $I = bR$.

Let $d \in I$. Observe that $dc \in aR$, so $dc = ar$ for some $r \in R$. Thus

$$ad = (bc)d = (dc)b = arb.$$

Since a is nonzero, $d = rb \in bR$ as desired. □

Theorem 19. *Suppose that R is an integral domain. Then R is a DVR if and only if R has a unique nonzero maximal ideal and has the property that $I \mid J$ for all ideals I and J with $J \subseteq I$.*

Proof. One direction is straightforward given our description of ideals of a DVR. So suppose R has a unique maximal ideal, and that $I \mid J$ for all ideals I and J with $J \subseteq I$. Let I be a nonzero ideal, and let $a \in I$ be nonzero. Since $aR \subseteq I$ we have that I divides aR. So by the previous proposition we have that I is principal. Thus I is a PID, which means it is a DVR by Theorem 11. □

In summary, we have shown that we can characterize DVRs in myriad ways. Let R is an integral domain with fraction field K. Then any of the following provides a necessary and sufficient condition for R to be a DVR.

1. R is $\mathcal{O}_v$ for a discrete valuation $v \colon K^\times \to \mathbb{Z}$. (Definition 3)
2. There is a non-unit, nonzero $\pi \in R$ such that every nonzero element of R can be written as $u\pi^k$ for some unit $u \in R^\times$ and some $k \in \mathbb{N}$. (Corollary 10)
3. R is local and Noetherian, with a principal, nonzero maximal ideal. (Theorem 11)
4. R is a PID with a unique nonzero prime ideal. (Corollary 12)

5. R is a PID with a unique nonzero maximal ideal. (Corollary 12)
6. R is a Dedekind domain with a unique nonzero prime ideal. (Theorem 13)
7. R is a strongly local Noetherian domain. (Proposition 14)
8. R is Noetherian, not a field, and x or x^{-1} in R for all x in the field of fractions of R. (Proposition 15)
9. R has a unique nonzero maximal ideal and has the property that $I \mid J$ for all ideals I and J with $J \subseteq I$. (Theorem 19)
10. R is local and Noetherian with invertible maximal ideal. (Definitions and proof below, see especially Theorem 22 or the remarks after Proposition 35)

The first nine summarize the previous material. The last of these will be proved after we review the theory of fractional ideals.[4]

If we begin with a Noetherian domain R with a unique nonzero prime ideal $\mathfrak{p}$, then R is a DVR if and only if one, and hence all, of the following hold:

1. $\mathfrak{p}$ is principal (Theorem 11)
2. R is a PID. (Corollary 12)
3. R is a Dedekind domain (i.e., R is integrally closed). (Theorem 13)
4. R is a strongly local. (Proposition 14)
5. x or x^{-1} in R for all x in the field of fractions of R. (Proposition 15)
6. R has the property that $I \mid J$ for all ideals I and J with $J \subseteq I$. (Theorem 19)
7. $\mathfrak{p}$ is invertible. (Definitions and proof below, see especially Theorem 22)

(Exercise 21 adds a eighth condition: $\mathfrak{p}/\mathfrak{p}^2$ is a vector space of dimension 1 over the field $R/\mathfrak{p}$.)

Finally, we observe that DVRs are maximal proper subrings of their fraction fields.

Proposition 20. *Suppose R is a DVR with field of fractions K. If $R \subsetneq R' \subseteq K$ and if R' is a subring of K, then $R' = K$.*

3 Submodules of the fraction field

Our next goals are to (1) make good on the promise to show that any local Noetherian domain with invertible maximal ideal is a DVR which includes explaining the ideal of invertible, and (2) give another proof of Theorem 13 that does not rely on the pre-acceptance of the unique factorization theorem for Dedekind domains.

[4] There is also an 11th characterization. Exercise 21 gives the following necessary and sufficient condition: R is local and Noetherian with maximal ideal $\mathfrak{m}$ having the property that $\mathfrak{m}/\mathfrak{m}^2$ is a vector space of dimension 1 over the field $R/\mathfrak{m}$. This exercise can be skipped in a first reading.

We start by explaining the concept inverse for ideals. This concept will help us meet these two immediate goals, but will also be useful for better understanding Dedekind domains and similar rings. (Much of this section is likely review, but the reader should verify for themselves any unfamiliar result.)

Let R be an integral domain with fraction field K. The collection of nonzero ideals of R forms a commutative monoid under the product operation with $I = R$ providing the identity element. When R is a Dedekind domain this monoid can be expanded into a group by adding fractional ideals to the monoid. Such fractional ideals will provide (multiplicative) inverses for nonzero ideals. We will define fractional ideals in the next section, but for now we mention that they are a kind of R-submodule of K. So in order to prepare the way for fractional ideals, we will first discuss R-submodules of K in general.

We assume the reader has at least a basic familiarity with modules in general, but we will focus on R-submodules of K. Recall that K is an R-module. In fact, any ring containing R is an R-module. Every ideal of R is an R-submodule of K, and an R-submodule I of K is an ideal of R if and only I is contained in R. (Note we will use letters such as I and J for R-submodules of K since we are thinking of such submodules as a straightforward generalization of ideals.)

Recall that if I_1 and I_2 are R-submodules of K (or submodules of any fixed module) then we can define the sum

$$I_1 + I_2 \stackrel{\text{def}}{=} \{x_1 + x_2 \mid x_1 \in I_1, x_2 \in I_2\}.$$

The sum is an R-submodule of K. This sum is commutative and associative. The zero submodule is the identity. So we get an additive monoid of R-submodules of K.

The intersection $I_1 \cap I_2$ of two R-submodules of K is itself an R-submodule. This operation is commutative and associative, and K is the identity. So we get a commutative monoid of R-submodules of K under intersection.

The operations of addition and intersection are meaningful for the collection of submodules of any fixed R-module M, and do not make special use of our case where $M = K$. However we will be especially concerned with an operation, the product of submodules, that uses the fact that $M = K$ has a product. The product of R-submodules I_1, I_2 of K is defined as follows:

$$I_1 I_2 \stackrel{\text{def}}{=} \left\{ \sum_i x_i y_i \;\middle|\; \text{where each } x_i \in I_1 \text{ and where each } y_i \in I_2 \right\}.$$

Here the sums are finite sums, and a sum with zero terms is defined here to be 0. This operation results in an R-submodule of K. This operation is commutative and associative, and the ideal $I = R$ is the identity. Thus we get a commutative monoid. Note also that $I_1 I_2$ is the minimum R-submodule of K (under inclusion) containing all products xy where $x \in I_1$ and $y \in I_2$. So we can think of it as the submodule generated by such products. (Of course, we can similarly think of $I_1 + I_2$ as the submodule generated by sums of the form $x + y$ with $x \in I_1, y \in I_2$.)

The operations of sum, intersection, and product are monotonic in the sense that if $I_1 \subseteq I_1'$ then

$$I_1 + I_2 \subseteq I_1' + I_2, \qquad I_1 \cap I_2 \subseteq I_1' \cap I_2, \qquad I_1 I_2 \subseteq I_1' I_2.$$

We also have a distributive law

$$I(J_1 + J_2) = IJ_1 + IJ_2.$$

Given $x \in K$ then

$$xR \stackrel{\text{def}}{=} \{xr \mid r \in R\}.$$

We sometimes write Rx for xR (since R is an integral domain, it is commutative). Observe that xR is an R-submodule of K; it is called a *principal submodule*. It is the minimum among submodules of K (under inclusion) containing x, and so is sometimes called the *R-submodule of K generated by x*. We extend this notation a bit: given $x \in K$ and an R-submodule I of K then

$$xI \stackrel{\text{def}}{=} \{xy \mid y \in I\}.$$

This results in an R-submodule of K. We have identities and properties such as

$$x(yI) = (xy)I, \quad xI = (xR)I, \quad (xR)(yR) = (xy)R \quad \text{and} \quad (I \subseteq J \implies xI \subseteq xJ).$$

The identity $(xR)(yR) = (xy)R$ implies that the collection of principal submodules is closed under multiplication. Obviously $R = 1R$ is principal, so the collection of principal submodules forms a submonoid of the collection of all R-submodules of K. The collection of nonzero principal submodules also forms a submonoid of the collection of all R-submodules of K.

Given $x_1, \ldots, x_k \in K$, there is a minimum R-submodule of K containing these elements. It is

$$x_1R + \ldots + x_kR.$$

(Here minimum is with respect to inclusion). Given an infinite subset U of K, we can also form a minimum R-submodule of K containing U: just take the intersection of all R-submodules that contain U. Its elements are all the finite R-linear combinations of elements of U. We will not need the infinite case in this document.

Definition 6. Suppose I is an R-submodule of K. We say that I is *invertible* if there is an R-submodule J of K such that

$$IJ = R.$$

In this case J is called the *inverse* of I.

Proposition 21. *Let R be an integral domain with field of fractions K. If $x \in K^\times$ then xR is invertible with inverse $x^{-1}R$. So if R is a PID them every nonzero ideal is invertible.*

If I and J are R-submodules of K such that $IJ = xR$ for some $x \in K^\times$, then I and J are invertible. More generally, I and J are both invertible if and only if IJ is invertible.

Since a DVR is a PID, its maximal ideal $\mathfrak{m}$ is invertible (along with all nonzero ideals). This is one direction of our promised result. We are also ready to prove the more substantial converse that a local Noetherian domain with invertible maximal ideal is a DVR. All we need here is (1) the notion of invertibility, and (2) our previous result on strongly local Noetherian domains.

Theorem 22. *Let R be an integral domain. Then R is a discrete valuation ring if and only if R is a local Noetherian domain whose maximal ideal is invertible.*

Proof. If R is a DVR, then it is a PID, and all nonzero principal ideals are invertible.

Now suppose R is a local Noetherian domain with maximal ideal $\mathfrak{m}$ and suppose there is an R-submodule $\mathfrak{m}^{-1}$ of K with $\mathfrak{m}\mathfrak{m}^{-1} = R$. To show that R is a DVR, it is enough, by Proposition 14, to show that R is strongly local. Let I be a proper nonmaximal ideal. From $I \subseteq \mathfrak{m}$ we have $\mathfrak{m}^{-1}I \subseteq R$. However, $\mathfrak{m}^{-1}I = R$ cannot hold since $I \neq \mathfrak{m}$. So $\mathfrak{m}^{-1}I \subseteq \mathfrak{m}$. Hence $I \subseteq \mathfrak{m}^2$. We conclude that R is strongly local since every proper nonmaximal ideal is contained in $\mathfrak{m}^2$. □

Remark. See the remark after Proposition 35 for another short argument.

If an R-submodule of R is invertible, then its inverse has the following explicit description:

Proposition 23. *Suppose $IJ = R$ where I and J are R-submodules of K. In other words, suppose I and J are inverses. Then*

$$J = \{x \in K \mid xI \subseteq R\}.$$

Proof. The direction $J \subseteq \{x \in K \mid xI \subseteq R\}$ is straightforward.

Suppose that $xI \subseteq R$. In other words, $(xR)I \subseteq R$. So $(xR)IJ \subseteq RJ$. Thus $xR \subseteq J$, and so $x \in J$. □

Proposition 23 implies that $\{x \in K \mid xI \subseteq R\}$ is the unique candidate for the inverse of I. It also suggests a necessary criterion for invertibility. Observe that in the above proposition neither I nor J can be the zero module. This forces J to contain some nonzero x. In other words, there is an $x \in K^\times$ such that $xI \subseteq R$.

Example 1. As long as R is not all of K, the module $I = K$ is not invertible. Otherwise, there is an $x \in K^\times$ with $xK \subseteq R$. But clearly $xK = K$, a contradiction.

In spite of the fact that I may not be invertible, we will still label $\{x \in K \mid xI \subseteq R\}$ as I^{-1} with the caveat that although it is the only possible inverse, it may fail to be the inverse simply because no inverse of I exists.

Definition 7. Let R be an integral domain and let K be its fraction field. If I is an R-submodule of K then

$$I^{-1} \stackrel{\text{def}}{=} \{x \in K \mid xI \subseteq R\}.$$

Proposition 24. *Let R be an integral domain, and let K be its fraction field. If $x \in K^\times$ then*

$$(xR)^{-1} = x^{-1}R.$$

Proof. Recall that $(xR)^{-1}$ is the inverse of xR if an inverse exists. But xR is in fact invertible with inverse $x^{-1}R$. □

Proposition 25. *Let R be an integral domain and let K be its fraction field. If I is an R-submodule of K then the following hold:*

- *I^{-1} is an R-submodule of K.*

- *II^{-1} is an ideal of R.*
- *In fact, II^{-1} is the maximum (for inclusion) among ideals of R of the form IJ where J is an R-submodule of K.*

If I and J are R-submodules of K then the following holds:

- *$IJ \subseteq R$ then $J \subseteq I^{-1}$*
- *If $I \subseteq J$ then $J^{-1} \subseteq I^{-1}$.*

Proof. These are straightforward. (It is efficient to prove the fourth claim before the third claim, since the fourth claim implies the third.) □

4 Fractional ideals

Let R be an integral domain with fraction field K. The collection of nonzero ideals of R forms a commutative monoid under the product operation. A fundamental discovery in algebraic number theory and commutative algebra is that for a certain class of widely used integral domains (namely Dedekind domains) this monoid can be expanded to include some nonzero R-submodules of K such that the result is an Abelian group. However, we want to be careful about what to add. For example, we do not want to add $I = K$ to the monoid since, as we have seen, $I = K$ is not invertible (except for the trivial situation where $R = K$). In the last section we introduced the definition

$$I^{-1} \stackrel{\text{def}}{=} \{x \in K \mid xI \subseteq R\}$$

where I^{-1} will be the inverse, if it exists, of a given R-submodule I of K. If, however, $I^{-1} = \{0\}$ then, of course, I^{-1} cannot be the inverse of I. So the existence of a nonzero $x \in K$ with $xI \subseteq R$ is a necessary condition for invertibility.

So in order to allow invertibility, we will restrict our attention to nonzero I which satisfy this condition. This motivates the definition of *fractional ideal*:

Definition 8. Let R be an integral domain with fraction field K. A *fractional ideal* of R is a nonzero R-submodule I of K such that $xI \subseteq R$ for some $x \in K^\times$. In other words, xI is an ideal of R for some nonzero $x \in K$. In this context, a regular ideal I of R is sometimes called an *integral ideal*.

Here are a few useful equivalent characterizations of fractional ideals:

Proposition 26. *Let I be a nonzero R-submodule of K. Then the following are equivalent:*

- *I^{-1} is not $\{0\}$.*
- *I is a fractional ideal: there is a nonzero $x \in K$ such that $xI \subseteq R$.*
- *There is a nonzero $d \in R$ such that $dI \subseteq R$.*
- *There is a nonzero $d \in R$ such that $I \subseteq d^{-1}R$.*

- *There is a nonzero $x \in K$ such that $I \subseteq xR$.*

Remark. Let I be a fractional ideal. Then any nonzero $d \in R$ such that $I \subseteq d^{-1}R$ can be called a "common denominator". So a fractional ideal is just an R-submodule of K with a common denominator.

Proposition 27. *Every nonzero ideal of an integral domain is a fractional ideal. If $x \in K^\times$ then xR is a fractional ideal. Every nonzero R-submodule of a fractional ideal is a fractional ideal.*

Remark. If $x \in K^\times$ then we call xR a *principal fractional ideal*.

Exercise 10. Let R be a PID. Show that every fractional ideal is principal.

Proposition 28. *If I_1 and I_2 are fractional ideals then so are the sum $I_1 + I_2$, the product $I_1 I_2$, and the intersection $I_1 \cap I_2$. If I is a fractional ideal, then I^{-1} is a fractional ideal.*

Proof. Let $a_1, a_2 \in R$ be nonzero elements such that $a_1 I_1$ and $a_2 I_2$ are ideals of R. Then $a_1 a_2 (I_1 + I_2)$ is an ideal, as is $a_1 a_2 (I_1 I_2)$. Note $I_1 \cap I_2$ is nonzero: multiply a nonzero element of $I_1 \cap R$ with a nonzero element of $I_2 \cap R$. Since $I_1 \cap I_2$ is an R-submodule of a fractional ideal, it must be a fractional ideal.

For the last claim, note that I and I^{-1} are both nonzero since I is a fractional ideal. If $y \in I$ is nonzero, then $yI^{-1} \subseteq R$. (One can also argue that $yR \subseteq I$ so $I^{-1} \subseteq y^{-1}R$). □

Corollary 29. *The collection of fractional ideals of an integral domain R forms a commmutative monoid under the product operation. This monoid contains, as submonoids, (1) the monoid of nonzero ideals, (2) the monoid of principal fractional ideals.*

If R is a DVR, then the monoid of fractional ideals is easily described.

Proposition 30. *Let R be a DVR with uniformizer π. Then the fractional ideals of R are all principal of the form $\pi^k R$ with $k \in \mathbb{Z}$. These are distinct, and form a group under multiplication. The map $k \to \pi^k R$ is an isomorphism between the additive group $\mathbb{Z}$ and the multiplicative group of fractional ideals of R.*

Exercise 11. Let R be a DVR. Show that the only nonzero R-submodule of K that is not a fractional ideal is K itself.

We will see that for Dedekind domains every fractional ideal is invertible, so, as in the special case of a DVR, this monoid is actually a group. However, for general integral domains the question of invertibility is trickier. In fact, we have another necessary condition for invertibility.

Proposition 31. *If I is an invertible R-submodule of K then I is finitely generated.*

Proof. If $IJ = R$ then there are finite sequences $x_1, \ldots, x_k \in I$ and $y_1, \ldots, y_k \in J$ of elements such that

$$1 = \sum x_i y_i.$$

If $x \in I$ then

$$x = \sum x_i(xy_i)$$

which is in $x_1R + \ldots + x_nR$. Thus $I = x_1R + \ldots + x_nR$. □

We now have two necessary conditions for invertibility of nonzero R-submodules I of K: (1) $xI \subseteq R$ for some $x \in K^\times$, and (2) I is finitely generated. However, the second clearly implies the first.

Proposition 32. *Suppose I is a finitely generated R-submodule of K. Then I is a fractional ideal.*

The proceeding two propositions suggests that, for the purposes of invertibility, we focus on finitely generated fractional ideals. However, if R is not Noetherian, this excludes even some nonzero integral ideals. So if we want all nonzero integral ideals to be invertible, we should focus on Noetherian domains.[5]

The collection of finitely generated fractional ideals has closure properties. This is summarized by the next proposition (to see this, express any finitely generated fractional ideal as $x_1R_1 + \ldots + x_2R_2$ and use distributive laws in the case of I_1I_2):

Proposition 33. *Let I_1 and I_2 be finitely generated fractional ideals of R. Then $I_1 + I_2$ and I_1I_2 are also finitely generated fractional ideals. In particular, the collection of finitely generated fractional ideals forms a commutative monoid under products (with identity R).*

As mentioned above, if we want every nonzero integral ideal to have a chance of being invertible, we should work in a Noetherian domain. In this case all fractional ideals are automatically finitely generated:

Proposition 34. *If R is a Noetherian domain then all fractional ideals are finitely generated. In fact, a nonzero R-submodule I of the fraction field K is finitely generated if and only if I is a fractional ideal.*

Proof. Recall that if M is a finitely generated module over a Noetherian ring then all its submodules are finitely generated. In the case of R-submodules I of K, we have already established that (1) if I is a fractional ideal then it is a submodule of a principal fractional ideal, and (2) that if I is finitely generated and nonzero then it is a fractional ideal. □

5 Invertibility criteria and results

In this section we will begin in earnest our study of invertible fractional ideals, and see how invertibility is connected with the integrally closed condition. Recall that if I is a fractional ideal then I^{-1} is defined as the fractional ideal $\{x \in K \mid xI \subseteq R\}$, with the caveat that I^{-1} might not be an actual inverse. In general we can only expect $II^{-1} \subseteq R$. But if I is invertible, then I^{-1} will be the true inverse in the

[5] In a non-Noetherian ring the best you can do is for all finitely generated fractional ideals to be invertible. Integral domains where every finitely generated fractional ideal is invertible are called *Prüfer domains*. See Appendix E for more information.

sense that $II^{-1} = R$. In this section we will be interested in determining when I^{-1} is the true inverse of I.

We have established an important case where we have invertibility: every principal fractional ideal is invertible. For local integral domains we have the following tidy result:

Proposition 35. *Let R be a local integral domain. Then a fractional ideal I of R is invertible if and only if I is principal.*

Proof. One direction is clear, so suppose I is invertible: $II^{-1} = R$. Let $a \in R$ be nonzero such that $J_1 = aI$ and $J_2 = aI^{-1}$ are ideals. Since $J_1 J_2 = a^2 R$, we can apply Proposition 18 to conclude that J_1 and J_2 are principal. Thus I is principal. □

Remark. This can be used to give another proof of Theorem 22 since we have established that a local Noetherian domain with a principal nonzero maximal ideal is a DVR.

Now we will see how the integrally closed condition can give us necessary conditions for invertibility. Recall that R is integrally closed if, for each monic $f \in R[X]$, every root of f in K is actually in R. To relate this to invertibility of fractional ideals, we begin with what seems like an unrelated question: Given a fractional ideal I for R, can we find a larger subring of K such that I is a module for that ring as well (with scalar multiplication coming from the multiplication of K)? This would require that for every x in the larger ring, $xI \subseteq I$ still holds. This motivate the following definition:

Definition 9. Let R be an integral domain and let K be its fraction field. If I is a fractional ideal, then

$$\mathcal{R}(I) \stackrel{\text{def}}{=} \{x \in K \mid xI \subseteq I\}.$$

This set $\mathcal{R}(I)$ turns out to be the sort of ring we want:

Proposition 36. *Let R be an integral domain and let K be its fraction field. If I is a fractional ideal of R, then the following hold:*

- *$\mathcal{R}(I)$ is a subring of K containg R: so $R \subseteq \mathcal{R}(I) \subseteq K$.*
- *I is a fractional ideal of $\mathcal{R}(I)$, where scalar multiplication is induced by the product of K. In fact, $\mathcal{R}(I)$ is the maximum subring R' of K (under inclusion) such that I is a fractional ideal of R'.*
- *$\mathcal{R}(I) \subseteq (II^{-1})^{-1}$.*
- *$\mathcal{R}(I)$ is a fractional ideal of R.*

Proof. Verifying these properties are mostly straightforward. For example, to show $\mathcal{R}(I) \subseteq (II^{-1})^{-1}$, observe that $xI \subseteq I$ implies $xII^{-1} \subseteq II^{-1} \subseteq R$. Note that $(II^{-1})^{-1}$ is a fractional ideal of R, and recall that any nonzero R-submodule of a fractional ideal is a fractional ideal. □

When R is Noetherian we see a connection between $\mathcal{R}(I)$ and integral elements.

Proposition 37. *Let R be a Noetherian domain. Then every element of $\mathcal{R}(I)$ is integral over R.*

Proof. Let $x \in \mathcal{R}(I)$. Since $\mathcal{R}(I)$ is a ring, the ring $R[x]$ is a subring of $\mathcal{R}(I)$. Also observe that $R[x]$ is an R-submodule of $\mathcal{R}(I)$, so $R[x]$ is also a fractional ideal. In particular it is finitely generated as an R-module since R is Noetherian. Fix a finite generating set of $R[x]$. Each generator is of the form $f(x)$ for some polynomial $f \in R[X]$. Fix such a polynomial for each generator, and let d be the largest degree among these polynomials. Observe that since x^{d+1} can be written as an R-linear combination of the generators, we can find a monic polynomial g of $R[X]$ of degree $d+1$ such that $g(x) = 0$. Thus x is integral over R. □

Corollary 38. *Let R be a Noetherian domain that is integrally closed (in its field of fractions). If I is a fractional ideal of R then*

$$\mathcal{R}(I) = R.$$

This leads to the following consequence in the case that R is an integrally closed Noetherian domain.

Proposition 39. *Let R be an integrally closed Noetherian domain. If I and J are fractional ideals such that $IJ \subseteq I$ in R, then J is an ideal of R.*

We can use these ideas to come up with criteria for invertibility, at least in the case of maximal ideals. The first criterion is useful for general integral domain R.

Proposition 40. *Let R be an integral domain and let $\mathfrak{m}$ be a nonzero maximal ideal of R. Then $\mathfrak{m}$ is invertible if and only if $\mathfrak{m}^{-1}$ is not contained in $\mathcal{R}(\mathfrak{m})$.*

Proof. Since $R \subseteq \mathfrak{m}^{-1}$, we have that $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}^{-1} \subseteq R$. Since $\mathfrak{m}$ is maximal, either $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ or $\mathfrak{m}\mathfrak{m}^{-1} = R$.

We now prove the contrapositive version of the claim. Suppose $\mathfrak{m}$ is not invertible. Then $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$. Thus $\mathfrak{m}^{-1} \subseteq \mathcal{R}(\mathfrak{m})$. Conversely, if $\mathfrak{m}^{-1} \subseteq \mathcal{R}(\mathfrak{m})$ then $\mathfrak{m}\mathfrak{m}^{-1} \subseteq \mathfrak{m}$, so $\mathfrak{m}$ is not invertible. □

The next criterion is useful for integrally closed Noetherian domains. It follows from the previous proposition using the equality $\mathcal{R}(\mathfrak{m}) = R$. (We do not need to exclude the trivial case where $\mathfrak{m} = \{0\}$, since in this case $\mathfrak{m}^{-1} = K = R$ and the result holds.)

Proposition 41. *Let R be an integrally closed Noetherian domain and let $\mathfrak{m}$ be a maximal ideal of R. Then $\mathfrak{m}$ is invertible if and only if $\mathfrak{m}^{-1}$ is not an integral ideal.*

Remark. Since $R \subseteq \mathfrak{m}^{-1}$, we can rephrase the above criterion as giving a condition for $\mathfrak{m}^{-1}$ to be R. This condition is $\mathfrak{m}^{-1} = R$ if and only if $\mathfrak{m}$ is not invertible.

In practice, we sometimes use the following criterion that follows immediately from the above.

Corollary 42. *Let R be an integrally closed Noetherian domain and let $\mathfrak{m}$ be a maximal ideal of R. If there is a fractional ideal I of R that is not an integral ideal and if $I\mathfrak{m} \subseteq R$, then $\mathfrak{m}$ is invertible.*

Proof. From $I\mathfrak{m} \subseteq R$ we have $I \subseteq \mathfrak{m}^{-1}$. So $\mathfrak{m}^{-1}$ cannot be an integral ideal of R (it cannot be contained in R). Now use the above proposition. □

We will use this criterion to show that a Dedekind domain that is not a field must have at least one invertible maximal ideal. But first we need a lemma.

Lemma 43. *Let R be a Noetherian domain with fraction field K. If R is not a field then there is a nonzero prime ideal $\mathfrak{p}$ of R and an $x \in K^\times \setminus R$ such that $x\mathfrak{p} \subseteq R$.*

Proof. Let $\mathcal{S}$ be the collection of all nonzero ideals I for which there is an $x \in K^\times \setminus R$ such that $xI \subseteq R$. Any nonzero proper principal ideal is in $\mathcal{S}$, so $\mathcal{S}$ is not empty. By the Noetherian property there is a maximal element $\mathfrak{p}$ in $\mathcal{S}$. Observe that $\mathfrak{p}$ is a proper ideal since the identity ideal R is not in $\mathcal{S}$. Fix $x \in K^\times \setminus R$ where $x\mathfrak{p} \subseteq R$

Suppose $ab \in \mathfrak{p}$ but $b \notin \mathfrak{p}$ where $a, b \in R$. Since $x\mathfrak{p} \subseteq R$, we have $ax(\mathfrak{p}+bR) \subseteq R$. By maximality of $\mathfrak{p}$, we have $ax \in R$. Thus $x(\mathfrak{p} + aR) \subseteq R$. By maximality of $\mathfrak{p}$ again we have $\mathfrak{p} + aR = \mathfrak{p}$. Thus $a \in \mathfrak{p}$. Hence $\mathfrak{p}$ is prime. □

Theorem 44. *Let R be a Dedekind domain that is not a field. Then R has an invertible prime ideal.*

Proof. By Lemma 43, there is a nonzero prime ideal $\mathfrak{p}$ and a fractional principal ideal xR that is not an integral ideal such that $(xR)\mathfrak{p} \subseteq R$. Since R is a Dedekind domain, the prime ideal $\mathfrak{p}$ is maximal. By Corollary 42, $\mathfrak{p}$ is invertible. □

As promised, we now prove Theorem 13 without using the unique factorization theorem for ideals. We need to reprove the following:

Theorem 45. *A Dedekind domain R with a unique nonzero prime ideal is a DVR.*

Proof. Let $\mathfrak{p}$ be the nonzero prime ideal of R. By Theorem 44, $\mathfrak{p}$ is invertible. Thus by Theorem 22 (or Proposition 35 plus Theorem 11) R is a DVR. □

Exercise 12. Let R be a Dedekind domain with a unique prime ideal $\mathfrak{p}$. Let x be as in Lemma 43. Show that $x^{-1} \in R$ and that $\mathfrak{p} = x^{-1}R$. Use this to give another proof of Theorem 45 by using Theorem 11 to conclude that R is a DVR.

Hint: if $x\mathfrak{p} \subseteq \mathfrak{p}$ then $x \in \mathcal{R}(\mathfrak{p})$, which cannot happen. So what is $x\mathfrak{p}$?

The next two exercises concern the rings $\mathcal{R}(I)$.

Exercise 13. Show that if $\mathcal{R}(I) = R$ for all fractional ideals of an integral domain R then R is integrally closed.

Hint: suppose $x \in K \setminus R$ is integral over R. Show that $I = R[x]$ is an R-submodule of K. Show that I is a finitely generated R-module, hence is a fractional ideal. Show that since I is a ring we have $I^2 \subseteq I$. Conclude that

$$R \subsetneq I \subseteq \mathcal{R}(I).$$

Note: an integral domain R such that $\mathcal{R}(I) = R$ for all fractional ideals I is said to be *completely integrally closed*. This exercise shows that a completely integrally closed domain is indeed integrally closed. Corollary 38 shows that for Noetherian domains integrally closed implies completely integrally closed.

Exercise 14. The *normalization* of an integral domain R is defined to be the set of all elements of its fraction field K that are integral over R. Suppose R is a Noetherian domain. Show that $x \in K$ is in the normalization of R if and only if $x \in \mathcal{R}(I)$ for some fractional ideal I (Hint: see previous exercise). Conclude that the normalization is the union of the rings $\mathcal{R}(I)$.

If I, J are fractional ideals, show that $\mathcal{R}(I)$ is contained in $\mathcal{R}(IJ)$. Show then that if $x, y \in K$ are in the normalization of R then $x, y \in \mathcal{R}(I)$ for some fractional ideal I. Conclude that the normalization is a subring of K.

The next three exercises concern cancellation in special cases. Inverses are very handy for cancellation, but unfortunately we cannot hope to have invertibility for a general fractional ideal except in Dedekind domains. There are situations where we, nevertheless, have cancellation even for non-invertible fractional ideals. The next two exercises illustrate some special cases. (See Appendix E for other situations where we have cancellation.)

Exercise 15. Let R be a local integral domain, and suppose

$$IJ = J = RJ$$

where I is a nonzero ideal and where J is a finitely generated fractional ideal. Show that we can cancel J to get $I = R$.

Hint: otherwise, note that $\mathfrak{m}J = J$ where $\mathfrak{m}$ is the maximal ideal. Take a minimal generating set of J as an R-module, and get a contradiction by making it smaller. (Recall that $1 - a$ is a unit if $a \in \mathfrak{m}$). (This is related to Nakayama's lemma in commutative algebra. See Exercise 18.)

Exercise 16. Extend the above to any integral domain R. In other words, suppose

$$IJ = J$$

where I is a nonzero ideal and where and J is a finitely generated fractional ideal. Show that $I = R$.

Hint (using localization, see Section 6 below): Suppose otherwise that I is contained in a maximal ideal $\mathfrak{m}$, so that $\mathfrak{m}J = J$. Now localize, and use the previous exercise to derive a contradiction.

Hint (using linear algebra over the fraction field of R): Set up a system of equations, and identify a singular matrix. From the resulting determinant, show that $1 \in I$.

Exercise 17. Use Proposition 39 and the previous exercise to prove the following cancellation law when R is an integrally closed Noetherian domain. If I and J are fractional ideals such that $IJ = J$, then $I = R$.

Conclude further that if $I_1 J = I_2 J$ where I_1, I_2, and J are fractional ideals one of which is invertible, then $I_1 = I_2$.

The following four exercises build on each other to culminate in another condition that characterizes discrete valuation rings.

Exercise 18. Let R be a local commutative ring, let I be a ideal of R, and let M be a finitely generated R-module. Generalize Exercise 15 and prove the following version of Nakayama's lemma: if $IM = M$ then $M = 0$ or $I = R$. (Here IM is defined as the submodule of M given by finite sums of elements of the form am where $a \in I$ and $m \in M$).

Exercise 19. Let R be a local commutative ring and let I be a proper ideal of R. Let M be an R-module and let N be a submodule of M. Assume that either (1) M is finitely generated as an R-module, or at least that (2) the quotient M/N is finitely generated as an R-module. Use the previous exercise to prove the following version of Nakayama's lemma: If $M = N + IM$ then $M = N$. (Hint: consider the quotient module M/N).

Exercise 20. Let R be a local commutative ring with maximal ideal $\mathfrak{m}$. Let k be the field $R/\mathfrak{m}$, called the *residue field*.

(1) Show that the scalar multiplication law

$$R/\mathfrak{m} \times \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2, \qquad [a] \cdot [b] \stackrel{\text{def}}{=} [ab] \quad \text{with } a \in R \text{ and } b \in \mathfrak{m}$$

is well-defined and makes the Abelian group $\mathfrak{m}/\mathfrak{m}^2$ into a k-vector space.

(2) Suppose $\mathfrak{m}$ is finitely generated. Use the previous exercise to show that if $[a_1], \ldots, [a_n] \in \mathfrak{m}/\mathfrak{m}^2$ spans the k-vector space $\mathfrak{m}/\mathfrak{m}^2$ where $a_1, \ldots, a_n \in \mathfrak{m}$, then $a_1, \ldots, a_n$ generate the ideal $\mathfrak{m}$. Hint: use the previous exercise with

$$M = I = \mathfrak{m}, \qquad N = a_1 R + \ldots + a_n R.$$

Exercise 21. Let R be a local Noetherian domain with maximal ideal $\mathfrak{m}$, and residue field $k = R/\mathfrak{m}$. Show that R is a DVR if and only if the k-vector space $\mathfrak{m}/\mathfrak{m}^2$ has dimension 1.

Exercise 22. Define an *irreducible* ideal in an integral domain to be a nonzero proper ideal that is not equal to IJ for nonzero proper ideals I and J. Show that in a Noetherian domain every nonzero proper ideal of R factors as the product of irreducible ideals.

Hint: use ascending chains and use Exercise 16 to show that if $I = J_1 J_2$ for nonzero proper ideals J_1, J_2 then $I \subsetneq J_1$ and $I \subsetneq J_2$.

6 Localizing fractional ideals

In this section, and the remaining sections, we assume the reader is familiar with localization, at least in the context of integral domains.[6] In this section we review this theory and expand the theory to include fractional ideals. (Although much of this section is likely review, the reader should verify for themselves any unfamiliar result.)

Localization is a process of forming a new ring $S^{-1}R$ from a given commutative ring and multiplicative system S. Although this can be done for any commutative ring, the prototypical setting and the most accessible situation is when we localize

[6] See, for example, my expository essay on localization in integral domains.

with integral domains. In this document, when we localize we will always assume R is an integral domain, and that S is a subset of R closed under multiplication that contains 1 but does not contain 0. In other words, S is a multiplicative submonoid of $R \setminus \{0\}$. The nice thing about this situation is that the ring $S^{-1}R$ can be identified with the subring of the fraction field K of R consisting of elements of the form r/s where $r \in R$ and $s \in S$. An important example is where $S = R \setminus \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal of R. In this case $S^{-1}R$ is written $R_{\mathfrak{p}}$. In this case $R_{\mathfrak{p}}$ is a local ring.

We can localize modules as well. Given an R-module M, localization produces an $S^{-1}R$-module called $S^{-1}M$. We will limit ourselves to the nice case where I is an R-submodule of K. If I is an R-submodule of K, then $S^{-1}I$ can be identified with the set elements of the form x/s with $x \in I$ and $s \in S$. Here x/s is just notation for xs^{-1}. The nice thing about this case is that $S^{-1}I$ is again a subset of K. Note that the localization of ideals is a special case of this type of localization. We assume the reader is familiar with localizing such modules (if not, it is a reasonable exercise to check the details). For example, we take it as established from earlier work (or leave it to the reader to check) that $S^{-1}I$ is an $S^{-1}R$ submodule of K. Note that $y \in S^{-1}I$ if and only if it is of the form $x(r/s)$ where $x \in I, r \in R, s \in S$. So we sometimes write $I(S^{-1}R)$ for $S^{-1}I$. This is especially common when $S^{-1}R$ is $R_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$. In this case we often write $IR_{\mathfrak{p}}$ for $S^{-1}I$.

Proposition 46. *If I is a fractional ideal of R, then $S^{-1}I$ is a fractional ideal of $S^{-1}R$.*

Proof. We have $xI \subseteq R$ for some $x \in K^{\times}$. Observe $x(S^{-1}I) \subseteq S^{-1}R$. □

We take the next two propositions as established from previous work (or we leave the proofs to the reader):

Proposition 47. *Let I_1, I_2 be R-submodule of K. Then, as $S^{-1}R$-modules,*

$$S^{-1}(I_1 + I_2) = (S^{-1}I_1) + (S^{-1}I_2),$$

$$S^{-1}(I_1 I_2) = (S^{-1}I_1)(S^{-1}I_2),$$

and

$$S^{-1}(I_1 \cap I_2) = (S^{-1}I_1) \cap (S^{-1}I_2).$$

The correspondence is also well-behaved with respect to principle ideals:

Proposition 48. *If $x \in K$ then*

$$S^{-1}(xR) = x(S^{-1}R).$$

More generally, if U is a set of elements of K, and if I is the R-submodule generated by U then $S^{-1}I$ is the R-submodule generated by U in $S^{-1}R$.

Remark. The module generated by a $x_1, \ldots, x_k \in K$ is just $x_1R + \ldots + x_kR$. We have also mentioned the R-submodule generated by an infinite set U, and the above proposition does apply to this case. However, we do not need the case of infinite U in this document.

Corollary 49. *Suppose I is a principal fractional ideal of R, then $S^{-1}I$ is a principal fractional ideal of $S^{-1}R$. Suppose I is a finitely generated fractional ideal of R, then $S^{-1}I$ is a finitely generated fractional ideal of $S^{-1}R$.*

We can also derive results about inverses. Warning: we assume I is finitely generated here.

Proposition 50. *Suppose I is a finitely generated fractional ideal of R. Consider I^{-1} as a fractional ideal of R and consider $(S^{-1}I)^{-1}$ as a fractional ideal of $S^{-1}R$. Then*

$$(S^{-1}I)^{-1} = S^{-1}I^{-1}.$$

Proof. The inclusion $S^{-1}I^{-1} \subseteq (S^{-1}I)^{-1}$ is straightforward. For the other inclusion, let $x_1, \ldots, x_k$ be generators of I as an R-module. Suppose $x \in (S^{-1}I)^{-1}$. Then $xx_i = r_i/s_i$ for some $r_i \in R$ and $s_i \in S$. So $(s_1 \cdots s_k)x \in I^{-1}$. □

We take is as established from earlier work that every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R.[7] We can extend this to fractional ideals.

Proposition 51. *If J is a fractional ideal of $S^{-1}R$, then there is a fractional ideal I of R such that $J = S^{-1}I$.*

Proof. Recall that xJ is an ideal of $S^{-1}R$ for some $x \in K^\times$. Let I' be an ideal of R with $S^{-1}I' = xJ$. Now consider $I = x^{-1}I'$. □

Corollary 52. *Suppose R is an integral domain with multiplicative system S. If R is a PID then so is $S^{-1}R$. If R is Noetherian, then so is $S^{-1}R$.*

Proof. This follows from the above proposition and Corollary 49. □

Corollary 53. *Suppose R is an integral domain with multiplicative system S. If every fractional ideal of R is invertible, then every fractional ideal of $S^{-1}R$ is invertible.*

In a similar vein, we have the following:

Proposition 54. *Let R be an integral domain with field of fractions K. Let S be a multiplicative system of R. If R is integrally closed in K, then $S^{-1}R$ is integrally closed in K.*

Remark. The usual proof involves manipulating polynomials, and I assume the reader has seen it. (If not, it is a good exercise; See for example, Exercise 41). We sketch another argument that highlights the techniques given in this document. It requires the extra assumption that R is Noetherian, which holds in the situations we are most interested in.

Start by showing, for any finitely generated fractional ideal I, the identity (where the right-hand side is in $S^{-1}R$):

$$S^{-1}\mathcal{R}(I) = \mathcal{R}(S^{-1}I).$$

[7] In fact, given an ideal J of $S^{-1}R$, the ideal $I = (J \cap R)$ will work, and will be the maximum such I.

We have $\mathcal{R}(I) = R$ (Corollary 38), so $S^{-1}R = \mathcal{R}(S^{-1}I)$. This holds for all fractional ideals I (assuming R is Noetherian), and all fractional ideals of $S^{-1}R$ are of the form $S^{-1}I$. By Exercise 13, the integral domain $S^{-1}R$ is integrally closed.

We can express some of the above results in terms of homomorphisms of monoids.

Proposition 55. *Let R be an integral domain and let S be a multiplicative system. The map*

$$I \mapsto S^{-1}I$$

is a monoid homomorphism from the multiplicative monoid of nonzero R-submodules of K to the multiplicative monoid of nonzero $S^{-1}R$-submodules of K.

This map restricts to a surjective monoid homomorphism from the multiplicative monoid of fractional ideals of R to the multiplicative monoid of fractional ideals of $S^{-1}R$. If the domain of this map is a group, then so is the image, and the map is a group homomorphism.

This map further restricts to a surjective monoid homomorphism from the multiplicative monoid of nonzero integral ideals of R to the multiplicative monoid of nonzero integral ideals of $S^{-1}R$.

We can say something about the kernel:

Proposition 56. *Let R be an integral domain with fraction field K and let S be a multiplicative system. Suppose I is an R-submodule of K that maps to the identity under the above described homomorphism: in other words, suppose $S^{-1}I = S^{-1}R$. Then I must intersect S. Conversely, if I is an integral ideal that intersects S, then it maps to the identity: $S^{-1}I = S^{-1}R$.*

Proof. If $S^{-1}I = S^{-1}R$ then $1 = x/s$ for some $x \in I$ and $s \in S$. □

Finally, we remind the reader of the correspondence of prime ideals. We take this as established from earlier work:

Proposition 57. *Let R be an integral domain, and let S be a multiplicative system of R. The rule $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ defines an inclusion preserving bijection*

$$\{\textit{Prime ideals of } R \textit{ disjoint from } S\} \;\to\; \left\{\textit{Prime ideals of } S^{-1}R\right\}.$$

The inverse sends a prime ideal $\mathfrak{p}$ of $S^{-1}R$ to $\mathfrak{p} \cap R$, and is also inclusion preserving.

This correspondence, together with earlier results, leads to the following theorem:

Theorem 58. *Let R be an integral domain, and let S be a multiplicative system of R. If R is a Dedekind domain, then so is $S^{-1}R$.*

Proof. We know that $S^{-1}R$ must be an integrally closed Noetherian domain by Proposition 54 (and the remark following it) and Corollary 52. So we just need to show that every nonzero prime ideal $\mathfrak{q}$ of $S^{-1}R$ is maximal.

Suppose that $\mathfrak{q}$ is a nonzero prime ideal of $S^{-1}R$, and let $\mathfrak{m}$ be a maximal ideal of $S^{-1}R$ containing it. By the above proposition, there are prime ideal $\mathfrak{p}_1, \mathfrak{p}_2$

of R such that $\mathfrak{q} = S^{-1}\mathfrak{p}_1$ and $\mathfrak{m} = S^{-1}\mathfrak{p}_2$. Since the correspondence is inclusion perserving in both directions, $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$. Obviously $\mathfrak{p}_1, \mathfrak{p}_2$ are not zero, so they must be equal since every nonzero prime ideal of R is maximal. Thus their images $\mathfrak{q}, \mathfrak{m}$ are equal, and so $\mathfrak{q}$ is maximal. □

7 Some local to global results

Now we investigate the relationship between properties of an integral domain R and the corresponding properties of the localizations $R_\mathfrak{m}$. This will allow us to prove results about various types of integral domains, including Dedekind domains, in a unified and elegant manner by reducing to the easier local situation.

Proposition 59. *Let R be an integral domain with field of fractions K. If I is an R-submodule of K then*

$$I = \bigcap_{\mathfrak{m} \in \mathcal{M}} IR_\mathfrak{m}$$

where $\mathcal{M}$ is the set of maximal ideals of R.

Proof. One direction is straightforward.

Suppose $x \in \bigcap IR_\mathfrak{m}$. Let J_x be defined as follows:

$$J_x \stackrel{\text{def}}{=} \{y \in R \mid yx \in I\}.$$

Observe that J_x is an ideal of R. If $J_x \neq R$ then let $\mathfrak{m}$ be a maximal ideal containing J_x. However, $x \in IR_\mathfrak{m}$ so is of the form a/s with $a \in I$ and $s \notin \mathfrak{m}$. Thus $s \in J_x$, a contradiction. So J_x contains 1. □

Corollary 60. *If R is an integral domain then*

$$R = \bigcap_{\mathfrak{m} \in \mathcal{M}} R_\mathfrak{m}$$

where $\mathcal{M}$ is the set of maximal ideals of R.

The above proposition yields a very useful test for inclusion and equality:

Corollary 61. *Let R be an integral domain and let I and J be R-submodules of the fraction field of R. Then $I \subseteq J$ if and only if $IR_\mathfrak{m} \subseteq JR_\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$. Similarly, $I = J$ if and only if $IR_\mathfrak{m} = JR_\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$.*

Now we illustrate the power of the local approach by investigating various properties of integral domains and their fractional ideals:

Proposition 62. *Suppose that R is an integral domain with fraction field K. Then R is integrally closed in K if and only if $R_\mathfrak{m}$ is integrally closed in K for all maximal ideals $\mathfrak{m}$.*

Proof. Proposition 54 yields one direction. Suppose that $R_\mathfrak{m}$ is integrally closed for each maximal $\mathfrak{m}$. Let $f \in R[X]$ be a monic polynomial, and let $x \in K$ be a root. In particular, $x \in R_\mathfrak{m}$ for each $\mathfrak{m}$ since $R_\mathfrak{m}$ is integrally closed. So $x \in \cap R_\mathfrak{m}$. Thus $x \in R$ by Corollary 60. □

Proposition 63. *Let R be an integral domain. Then R has the property that every nonzero prime ideal is maximal if and only if $R_{\mathfrak{m}}$ has that property for all maximal ideals $\mathfrak{m}$.*

Proof. Suppose R has the property in question. By the correspondence of primes (Proposition 57), $R_{\mathfrak{m}}$ must have the property in question as well. Conversely, suppose $R_{\mathfrak{m}}$ has the property in question for all maximal ideals $\mathfrak{m}$. Let $\mathfrak{p}$ be any nonzero prime ideal of R and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. By assumption and the prime correspondence $\mathfrak{p}R_{\mathfrak{m}} = \mathfrak{m}R_{\mathfrak{m}}$, so by the prime correspondence (Proposition 57) $\mathfrak{p} = \mathfrak{m}$. □

Now we are ready to prove one of the most important characterizations of Dedekind domains:

Theorem 64. *Let R be a Noetherian domain. Then R is a Dedekind domain if and only if $R_{\mathfrak{m}}$ is a discrete valuation ring for all nonzero maximal ideals $\mathfrak{m}$ of R.*

Proof. If the zero ideal is maximal, then R is a field, which is considered a Dedekind domain. So the claim is trivially true in this case. We now assume that the zero ideal is not maximal.

Suppose R is a Dedekind domain. Then $R_{\mathfrak{m}}$ is a Dedekind domain for each nonzero maximal ideal $\mathfrak{m}$ by Theorem 58. Observe that each such $R_{\mathfrak{m}}$ has a unique nonzero prime ideal, namely $\mathfrak{m}R_{\mathfrak{m}}$. So each such $\mathfrak{m}R_{\mathfrak{m}}$ is a DVR by Theorem 13.

Suppose that $R_{\mathfrak{m}}$ is a DVR for each nonzero maximal ideal $\mathfrak{m}$. Then R is Noetherian by assumption, every nonzero prime ideal of R is maximal by Proposition 63, and R is integrally closed by Proposition 62 □

Remark. An *almost Dedekind domain* is defined to be an integral domain R such that $R_{\mathfrak{m}}$ is a DVR for all nonzero maximal ideals $\mathfrak{m}$. The above theorem implies that every Noetherian almost Dedekind domain is a true Dedekind domain. However, there exists non-Noetherian almost Dedekind domains. See Appendix E for more information.

Every PID is a Dedekind domain, a fact we have taken to be established background knowledge. In a sense, we do not need to take it as established since it follows as an easy corollary to the above theorem.

Corollary 65. *Every PID is a Dedekind domain.*

Proof. Let R be a PID and let $\mathfrak{m}$ be a nonzero maximal ideal of R. Then $R_{\mathfrak{m}}$ is a PID by Corollary 52. In fact, $R_{\mathfrak{m}}$ is a DVR by Theorem 11. So R is a Dedekind domain by the above theorem. □

Theorem 66. *Let I be a finitely generated fractional ideal of an integral domain R. Then I is invertible as a fractional ideal of R if and only if $IR_{\mathfrak{m}}$ is invertible as a fractional ideal of $R_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R.*

Proof. One direction is straightforward. For the other direction, apply Corollary 61 to show $II^{-1} = R$. □

Corollary 67. *If R is a Dedekind domain, then every fractional ideal is invertible, and so the monoid of fractional ideals under products forms an Abelian group. This group is generated by the nonzero ideals of R.*

Proof. Use Theorem 64 and the fact that every fractional ideal of a DVR is invertible. Finally, note that every fractional ideal J in R has the property that aJ is an ideal for some nonzero $a \in R$. Thus $(aR)J = I$ for some nonzero ideal I. Hence $J = I(aR)^{-1}$. □

Remark. Later we will see that this group is generated by the nonzero prime ideals of R.

Exercise 23. Show that every finitely generated ideal in an almost Dedekind domain is invertible. (See the remarks after Theorem 64 for the definition of almost Dedekind domain.)

Corollary 68. *Let I be a finitely generated fractional ideal of an integral domain R. Then I is invertible if and only if $IR_{\mathfrak{m}}$ is a principal fractional ideal of $R_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R.*

Proof. Use Proposition 35. □

We can strengthen Corollary 67, giving us one of the major results about Dedekind domains. (A result of Emmy Noether).

Theorem 69. *Let R be an integral domain. Then R is a Dedekind domain if and only if every nonzero ideal of R is invertible.*

Proof. Corollary 67 gives one direction, so suppose that every nonzero ideal of R is invertible. By Proposition 31, every nonzero ideal of R is finitely generated, so R must be a Noetherian domain. By Theorem 64 it is now enough to show $R_{\mathfrak{m}}$ is a DVR for any nonzero maximal ideals $\mathfrak{m}$ of R. Let $\mathfrak{m}$ be a nonzero maximal ideal of R. Since $\mathfrak{m}$ is invertible in R, the maximal ideal $\mathfrak{m}R_{\mathfrak{m}}$ is invertible in $R_{\mathfrak{m}}$. By Theorem 22, this implies that $R_{\mathfrak{m}}$ is a DVR. □

Exercise 24. Let R be an integral domain and let u be in fraction field of R. Show that u is a unit in R if and only if it is a unit in $R_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m}$ of R.

8 Discrete valuations of Dedekind domains

Suppose R is a Dedekind domain with fraction field K and let $\mathfrak{p}$ be a nonzero prime ideal of R. Then $R_{\mathfrak{p}}$ is a DVR. Let $v_{\mathfrak{p}} \colon K^{\times} \to \mathbb{Z}$ be the discrete valuation associated with $R_{\mathfrak{p}}$. We consider this valuation for elements of R:

Proposition 70. *Suppose R is a Dedekind domain with discrete valuation $v_{\mathfrak{p}}$ where $\mathfrak{p}$ is a nonzero prime ideal. (As usual, let $v_{\mathfrak{p}}(0) = \infty$). If $a \in R$ then (1) $v_{\mathfrak{p}}(a) \geq 0$, and (2) $v_{\mathfrak{p}}(a) > 0$ if and only if $a \in \mathfrak{p}$.*

Proof. Observe that $R \subseteq R_{\mathfrak{p}}$, and that $(\mathfrak{p}R_{\mathfrak{p}}) \cap R = \mathfrak{p}$. □

Corollary 71. *Suppose R is a Dedekind domain with fraction field K. Then the map $\mathfrak{p} \mapsto v_{\mathfrak{p}}$ is an injective map from the set of nonzero prime ideals of R to the set of discrete valuations of K.*

Our next goal is to strengthen this corollary by identifying the image of the map $\mathfrak{p} \mapsto v_{\mathfrak{p}}$. In other words, we want to identify which valuations are of the form $v_{\mathfrak{p}}$. By the above proposition, only valuations that are nonnegative on R can be of the form $v_{\mathfrak{p}}$, so we have at least this restriction on the image.

Lemma 72. *Let R be an integral domain with fraction field K. If $v\colon K^\times \to \mathbb{Z}$ is a valuation with $v(r) \geq 0$ for all $r \in R$ then*

$$\mathfrak{p} = \{a \in R \mid v(a) > 0\}$$

is a nonzero prime ideal of R.

Proof. The properties of v imply that $\mathfrak{p}$ is a prime ideal of R. If $\mathfrak{p}$ is the zero ideal, then v would be identically zero on $K^\times$ since K is the field of fractions of R. This contradicts the surjectivity of $v\colon K^\times \to \mathbb{Z}$. □

Lemma 73. *Suppose R is a Dedekind domain with fraction field K. Suppose that $v\colon K^\times \to \mathbb{Z}$ is a valuation with $v(r) \geq 0$ for all $r \in R$. Let $\mathfrak{p}$ be the associated nonzero prime ideal $\{a \in R \mid v(a) > 0\}$. Then*

$$v = v_{\mathfrak{p}}.$$

Proof. Observe that $v(r/s) \geq 0$ for all $r/s \in R_{\mathfrak{p}}$ where $r \in R$ and $s \in R \smallsetminus \mathfrak{p}$. In particular, $R_{\mathfrak{p}} \subseteq \mathcal{O}_v$. By Proposition 20 we have $R_{\mathfrak{p}} = \mathcal{O}_v$ since $R_{\mathfrak{p}}$ is a DVR. Now use Exercise 4. □

This lemma allows us to conclude the following:

Theorem 74. *Suppose R is a Dedekind domain with fraction field K. Then the map $\mathfrak{p} \mapsto v_{\mathfrak{p}}$ is a bijection from the set of nonzero prime ideals of R to the set of discrete valuations of K that are nonnegative on R.*

For any prime p in $\mathbb{Z}$, write v_p for $v_{\mathfrak{p}}$ with $\mathfrak{p} = p\mathbb{Z}$.

Corollary 75. *The map $p \mapsto v_p$ is a bijection from the set of (positive) primes of $\mathbb{Z}$ to the set of discrete valuations of $\mathbb{Q}$.*

Proof. Observe that every discrete valuation must be nonnegative on $\mathbb{Z}$. □

One of the main theorems for Dedekind domains, perhaps the main theorem, is that ideals factor uniquely into prime ideals. I felt free to assumed this result as background for the proof of Theorem 13 in Section 2, since this document is in some sense a part two in the theory of Dedekind domains. We later saw an alternate proof of Theorem 13 (see Theorem 45) which did not use the unique factorization theorem. So from a logical perspective the results we have proved up to now do not depend on this unique factorization theorem. Now that we know that the fractional ideals of a Dedekind domains form a group, we can give a brief proof of at least the existence of a prime factorization, with uniqueness coming later. This will be important in showing that, for example, $v_{\mathfrak{p}}(a) = 0$ for all but a finite number of valuations of a Dedekind domain.

Theorem 76. *Let R be a Dedekind domain. Every nonzero ideal can be written as the product of nonzero prime ideals. (We adopt the convention that the empty product is the identity ideal R).*

Proof. The following proof is based on the fact that the set of fractional ideals of R forms a groups under the product operation. So we freely use properties of groups.

Suppose otherwise that there is a nonzero ideal that is not such a product. By the Noetherian property there is a maximal such ideal I. Note that I must be a proper ideal. Let $\mathfrak{p}$ be a maximal ideal containing I. Then $I \neq I\mathfrak{p}^{-1}$ since $\mathfrak{p} \neq R$, and

$$I \subsetneq I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R.$$

So

$$I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$$

for some $k \geq 0$ and nonzero prime ideals $\mathfrak{p}_i$. Thus

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{p}.$$

□

Exercise 25. Use properties of prime ideals to show that the decomposition of the above theorem is unique up to order of the prime factors. (We will see another justification for uniqueness later using valuations).

Exercise 26. Prove Theorem 76 using the following chain argument. Start with any nonzero ideal I. Show that if $\mathfrak{p}$ is a prime ideal containing I then $I = \mathfrak{p}I'$ for some ideal I'. Show that $I \subsetneq I'$. Iterate this process to find an ascending chain and use the ascending chain condition.

Corollary 77. *Let R be a Dedekind domain. Every fractional ideal I of R can written in the form*

$$I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$$

where $k \geq 0$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are distinct prime ideals of R, and where $n_i \in \mathbb{Z}$. (Here we defined $\mathfrak{p}_i^0$ to be R, so we can freely drop or add any factor with $n_i = 0$). In particular, the prime ideals generate the group of fractional ideals.

Next we will define discrete valutions of fractional ideals. First we start with fractional ideals of $R_\mathfrak{p}$ where R is a Dedekind domain and where $\mathfrak{p}$ is a nonzero prime ideal. Recall that the map

$$k \mapsto (\mathfrak{p}R_\mathfrak{p})^k$$

defines an isomorphism between the additive group $\mathbb{Z}$ and the multiplicative group $\mathcal{I}(R_\mathfrak{p})$ of fractional ideals of $R_\mathfrak{p}$ (See Proposition 30). We define the valuation isomorphism to be the inverse of this isomorphism. We call this map $v_\mathfrak{p}$ (when there is no risk of confusion with the valuation $v_\mathfrak{p}$ on elements):

$$v_\mathfrak{p} \colon \mathcal{I}(R_\mathfrak{p}) \to \mathbb{Z}, \qquad (\mathfrak{p}R_\mathfrak{p})^k \mapsto k.$$

Now recall that localization map $I \mapsto IR_\mathfrak{p}$ is a surjective group homomorphism from the group $\mathcal{I}(R)$ of fractional ideals of R to $\mathcal{I}(R_\mathfrak{p})$. The valuation on $\mathcal{I}(R)$ is defined as the composition

$$\mathcal{I}(R) \to \mathcal{I}(R_\mathfrak{p}) \to \mathbb{Z}.$$

We also call this map $v_\mathfrak{p}$. Warning: we are now using the symbol $v_\mathfrak{p}$ for three functions:

$$K^\times \to \mathbb{Z}, \qquad \mathcal{I}(R_\mathfrak{p}) \to \mathbb{Z}, \qquad \mathcal{I}(R) \to \mathbb{Z}$$

where K is the fraction field of R. Context will dictate which is meant in any given use. We now summarize the definition of $v_\mathfrak{p} \colon \mathcal{I}(R) \to \mathbb{Z}$:

Definition 10. Let R be a Dedekind domain and let $\mathcal{I}(R)$ be the group of fractional ideals of R. Let $\mathfrak{p}$ be a nonzero prime ideal. Then we define the valuation map

$$v_\mathfrak{p} \colon \mathcal{I}(R) \to \mathbb{Z}$$

as follows: if $I \in \mathcal{I}(R)$ then $v_\mathfrak{p}(I)$ is the unique $k \in \mathbb{Z}$ such that $IR_\mathfrak{p} = (pR_\mathfrak{p})^k$.

From the definition, and the discussion proceeding it, we get the following:

Proposition 78. *Let R be a Dedekind domain and let $\mathcal{I}(R)$ be the group of fractional ideals of R. Let $\mathfrak{p}$ be a nonzero prime ideal. Then the valuation map $\mathcal{I}(R) \to \mathbb{Z}$ is a surjective homomorphism from the multiplicative group $\mathcal{I}(R)$ to the additive group $\mathbb{Z}$.*

Next we show that this new valuation is compatible with the valuation of elements.

Proposition 79. *Let R be a Dedekind domain with fractions field K and let $\mathfrak{p}$ be a nonzero prime ideal. Then for all $x \in K^\times$,*

$$v_\mathfrak{p}(xR) = v_\mathfrak{p}(x).$$

Proof. Write x as $u\pi^k$ where $\pi \in R_\mathfrak{p}$ is a uniformizer and u is a unit of $R_\mathfrak{p}$. Under localization, xR maps to $xR_\mathfrak{p}$, which is $\pi^k R_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^k$. Thus $v_\mathfrak{p}(xR) = k$. But also $v_\mathfrak{p}(x) = v_\mathfrak{p}(u\pi^k) = k$. □

There is another characterization of this valuation map:

Proposition 80. *Let R be a Dedekind domain with fraction field K and let $\mathfrak{p}$ be a nonzero prime ideal. If I is a fractional ideal of R then*

$$v_\mathfrak{p}(I) = \min_{x \in I} \{v_\mathfrak{p}(x)\}.$$

Proof. If $k = v_\mathfrak{p}(I)$ then $IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^k$. But $(\mathfrak{p}R_\mathfrak{p})^k$ is just the set of elements x of $K^\times$ with $v_\mathfrak{p}(x) \geq k$. So if $x \in I$ then $x \in IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^k$ and so $v_\mathfrak{p}(x) \geq k$.

We just need to show that our minimum is k by showing that there is an element $x \in I$ with $v_\mathfrak{p}(x) = k$. To that end, start with an element x/s where $x \in I$

and $s \in R \setminus \mathfrak{p}$ such that $x/s \in IR_\mathfrak{p} = (pR_\mathfrak{p})^k$ but not in $(pR_\mathfrak{p})^{k+1}$. When we localize, s becomes a unit in $R_\mathfrak{p}$ so

$$k = v_\mathfrak{p}(x/s) = v_\mathfrak{p}(x) - v_\mathfrak{p}(s) = v_\mathfrak{p}(x) - 0 = v_\mathfrak{p}(x).$$

□

Remark. In the above we can actually take the minimum of $v_\mathfrak{p}(x)$ for x in a generating set of I.

Lemma 81. *Let R be a Dedekind domain and let $\mathfrak{p}, \mathfrak{q}$ be distinct nonzero prime ideals of R. Then $\mathfrak{q}R_\mathfrak{p} = R_\mathfrak{p}$. Thus $v_\mathfrak{p}(\mathfrak{q}) = 0$.*

Proposition 82. *Let I be a fractional ideal of a Dedekind domain R. Suppose*

$$I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$$

where $k \geq 0$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are distinct nonzero prime ideals of R, and where each $n_i \in \mathbb{Z}$. Then $n_i = v_{\mathfrak{p}_i}(I)$. If a nonzero prime ideal $\mathfrak{p}$ is not any of these $\mathfrak{p}_i$ then $v_\mathfrak{p}(I) = 0$.

Proof. Consider the localization homomorphism $I \mapsto IR_\mathfrak{p}$. □

Remark. This gives the uniqueness of the prime factorization of a fractional ideal. So between this result and existence of prime factorizations (Theorem 76) we can conclude that the group of fractional ideals $\mathcal{I}$ of a Dedekind domain R is a the free Abelian group generated by nonzero prime ideals.

Let $\mathcal{P}$ be the subgroup of principal fractional ideals. The quotient group $\mathcal{I}/\mathcal{P}$ is called the *class group of R* and is one of the most important invariants of R. In some sense it is a measure on how much an Dedekind domain fails to be a PID.

We can summarize our results as follows:

Theorem 83. *Let I be a fractional ideal of a Dedekind domain R. Then $v_\mathfrak{p}(I)$ is 0 for all but a finite number of nonzero prime ideals $\mathfrak{p}$. Suppose $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are distinct prime ideals of R containing at least all nonzero prime ideals $\mathfrak{p}$ with $v_\mathfrak{p}(I) \neq 0$. Then*

$$I = \mathfrak{p}_1^{v_{\mathfrak{p}_i}(I)} \cdots \mathfrak{p}_k^{v_{\mathfrak{p}_k}(I)}.$$

Corollary 84. *Let I, J be fractional ideals of a Dedekind domain R. Then $I = J$ if and only if $v_\mathfrak{p}(I) = v_\mathfrak{p}(J)$ for all nonzero prime ideals $\mathfrak{p}$ of R.*

Lemma 85. *Let R be a Dedekind domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. If $k \leq l$ then $(pR_\mathfrak{p})^l \subseteq (pR_\mathfrak{p})^k$ and so*

$$(pR_\mathfrak{p})^k + (pR_\mathfrak{p})^l = (pR_\mathfrak{p})^k \quad \text{and} \quad (pR_\mathfrak{p})^k \cap (pR_\mathfrak{p})^l = (pR_\mathfrak{p})^l.$$

Proposition 86. *Let R be a Dedekind domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. If I, J are fractional ideals of R, then*

$$v_\mathfrak{p}(IJ) = v_\mathfrak{p}(I) + v_\mathfrak{p}(J),$$
$$v_\mathfrak{p}(I + J) = \min(v_\mathfrak{p}(I), v_\mathfrak{p}(J)),$$
$$v_\mathfrak{p}(I \cap J) = \max(v_\mathfrak{p}(I), v_\mathfrak{p}(J)).$$

Proof. The first is just a statement of the homomorphism property. For the other two, use the above lemma. □

Also, I should mentioned the following straightforward consequence of the above results:

Proposition 87. *Let R be a Dedekind domain and let I be a fractional ideal of R. Then I is an integral ideal if and only if $v_{\mathfrak{p}}(I) \geq 0$ for all nonzero prime ideals $\mathfrak{p}$.*

Exercise 27. Let I_1, I_2, J be fractional ideals of a Dedekind domain. Show that

$$(I_1 + I_2) \cap J = I_1 \cap J + I_2 \cap J$$

and

$$(I_1 \cap I_2) + J = (I_1 + J) \cap (I_2 + J).$$

Which inclusions are valid for general integral domains?

Exercise 28. Let I_1, I_2, J be fractional ideals of a Dedekind domain. Show that

$$(I_1 \cap I_2)J = I_1 J \cap I_2 J.$$

Which inclusion is valid for general integral domains?

9 Divisibility for nonzero ideals

We now discuss divisibility for ideals in a Dedekind domain. Recall that for ideal $I \mid J$ means that there is an ideal I' such that $J = II'$. In this case we also say that J is a *multiple* of I. We define *common divisors* and *common multiples* in the usual way.

Proposition 88. *Divisibility in an integral domain R satisfies the following:*

1. *Let I_1, I_2, I_3 be ideals of R. If $I_1 \mid I_2$ and $I_2 \mid I_3$ then $I_1 \mid I_3$.*
2. *Let I, J be ideals of R. If $I \mid J$ then $J \subseteq I$.*
3. *Let I, J be ideals of R. If $I \mid J$ and $J \mid I$ then $I = J$.*
4. *Let I be an ideal of R. Then $I \mid I$ and $R \mid I$.*

Proof. This is straightforward. Note: the second claim gives the third. □

Using factorization into prime ideals in a Dedekind domain, we get the following:

Proposition 89. *Let I, J be nonzero ideals of a Dedekind domain R. Then $I \mid J$ if and only if $v_{\mathfrak{p}}(I) \leq v_{\mathfrak{p}}(J)$ for all nonzero prime ideals $\mathfrak{p}$ of R.*

Theorem 90. *Let I, J be nonzero ideals of a Dedekind domain R. Then*

$$I \mid J \quad \text{if and only if} \quad J \subseteq I.$$

Proof. Suppose $J \subseteq I$. Let I' be the fractional ideal $I^{-1}J$. Observe that $II' = J$. Observe that I' is actually an integral ideal since

$$I' = I^{-1}J \subseteq I^{-1}I \subseteq R.$$

□

Remark. The above translates into a popular phrase for Dedekind domains:

"To contain is to divide".

It is also interesting to note that this property characterizes Dedekind domains. (See Section 12).

Corollary 91. *Let I, J be nonzero ideals of a Dedekind domain R. Then $I \cap J$ is the least common multiple of I and J.*

Remark. Here "least" means the minimum according to the divisibility relation, not the inclusion relation which reverses the partial order.

Another consequence of Theorem 90 is that this notion of divisibility is compatible with divisibility of elements:

Proposition 92. *Suppose R is a Dedekind domain and that $a, b \in R$ are nonzero. Then $a \mid b$ if and only if $aR \mid bR$.*

Note also the following.

Proposition 93. *Let R be a Dedekind domain. If $a \in R$ is nonzero, and I is a nonzero ideal, then $a \in I$ if and only if $I \mid aR$.*

Proposition 94. *If I, J are nonzero ideals of a Dedekind domain then $I + J$ is the greatest common divisor of I and J.*

Proof. By Proposition 86, for each prime ideal $\mathfrak{p}$,

$$v_{\mathfrak{p}}(I + J) = \min(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)).$$

Now use Proposition 89. (Or you can argue from Theorem 90). □

Remark. Here "greatest" means the maximum according to the divisibility relation, not the inclusion relation.

Definition 11. Let I and J be nonzero ideals of an Dedekind domain R. Then we say that I and J are *relatively prime* if the only common divisor of I and J is R. In other words, $I + J = R$, or equivalently $\min(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)) = 0$ for all nonzero prime ideals $\mathfrak{p}$ of R.

Remark. This is equivalent, of course, to having prime factorizations that share no common prime ideals.

Prime ideals behave as primes with the divisibility relation.

Proposition 95. *Let $\mathfrak{p}$ be a proper nonzero ideal of a Dedekind domain R. Then $\mathfrak{p}$ is a prime ideal if and only if the following holds: For all ideals I, J of R, if $\mathfrak{p}|IJ$ then $\mathfrak{p}|I$ or $\mathfrak{p} \mid J$.*

Finally, we can characterize powers of primes using valuations:

Proposition 96. *Let $\mathfrak{p}$ be a nonzero prime in a Dedekind domain, and let $n \in \mathbb{N}$. Then*

$$\mathfrak{p}^n = \{a \in R \mid v_{\mathfrak{p}}(a) \geq n\}.$$

Proof. If $a \in \mathfrak{p}^n$ then $aR \subseteq \mathfrak{p}^n$, so $\mathfrak{p}^n \mid aR$. Thus $n = v_{\mathfrak{p}}(\mathfrak{p}^n) \leq v_{\mathfrak{p}}(aR) = v_{\mathfrak{p}}(a)$.

Conversely, if $v_{\mathfrak{p}}(a) \geq n$ then $v_{\mathfrak{p}}(\mathfrak{p}^n) \leq v_{\mathfrak{p}}(aR)$. For any other nonzero prime ideal $\mathfrak{q}$, we have $v_{\mathfrak{q}}(\mathfrak{p}^n) = nv_{\mathfrak{q}}(\mathfrak{p}) = 0$, so $v_{\mathfrak{q}}(\mathfrak{p}^n) \leq v_{\mathfrak{q}}(aR)$. Thus $\mathfrak{p}^n \mid aR$, and so $a \in \mathfrak{p}^n$. □

Exercise 29. Let I, J be ideals of a Dedekind domain. Show that

$$(I + J)(I \cap J) = IJ.$$

Which inclusion is valid for general integral domains?

Note this says that the least common multiple of two ideals times the greatest common divisor is just the product. This generalizes a basic identity of integers.

Exercise 30. Let I and J be nonzero ideals in a Dedekind domain R. Show that $IJ \subseteq I \cap J$ with equality if and only if $I + J = R$. Can you generalize at least part of this to ideals in an integral domain? (Hint: see the proof of the Chinese remainder theorem below.)

Exercise 31. Let I be a nonzero ideal of a Dedekind domain R. Show that I is a $k \geq 0$ power if and only if $v_{\mathfrak{p}}(I)$ is a multiple of k for all nonzero prime ideals $\mathfrak{p}$. Does this hold for fractional ideals? Does this hold for elements? What if R is a PID? What if R is $\mathbb{Z}$.

Exercise 32. Show that if $I^n = J^n$ for fractional ideals I, J in a Dedekind domain, then $I = J$. Show that if $I^n \mid J^m$ where $m \leq n$ then $I \mid J$. (Here m, n are positive integers.)

Exercise 33. Suppose $I_1 I_2 = J^k$ for nonzero ideals I_1, I_2, J in a Dedekind domain, and where $k \geq 1$. Show that if I_1 and I_2 are relatively prime then $I_1 = J_1^k$ and $I_2 = J_2^k$ for unique nonzero ideals J_1, J_2. Show also that $J_1 J_2 = J$.

10 Approximation Theorems

Given elements a and b in an integral domain with ideal I, we write

$$a \equiv b \mod I$$

to mean $a - b \in I$. If $\mathfrak{p}$ is a nonzero prime ideal in a Dedekind domain, then we think of $a \equiv b \mod \mathfrak{p}^k$ as indicating that a approximates b from the point of view of $\mathfrak{p}$ (or the valuation $v_{\mathfrak{p}}$). The larger the exponent k, the better the approximation. We can also state this approximation as $v_{\mathfrak{p}}(a - b) \geq k$.

We will be simultaneously approximating with respect to multiple nonzero prime ideals. There is a sense in which different nonzero prime ideals are independent. More generally, if $I+J=R$ where R is an integral domain, then the ideals I and J are independent in some sense. This is expressed by the Chinese remainder theorem (a straightforward generalization of the Chinese remainder theorem of elementary number theory).

Theorem 97 (Chinese remainder theorem)**.** *Suppose R is a commutative ring and suppose I, J are ideals of R where $I+J=R$. Then the natural homomorphism*

$$R/IJ \to (R/I)\times(R/J), \qquad [a]\mapsto([a],[a])$$

is a ring isomorphism.

Proof. Start with the natural homomorphism

$$R \to (R/I)\times(R/J), \qquad a\mapsto([a],[a]).$$

Since $I+J=R$, we can find $e_2\in I$ and $e_1\in J$ such that $e_2+e_1=1$. Observe that e_1 maps to $([1],[0])$ and e_2 maps to $([0],[1])$. So, given $([a],[b])\in(R/I)\times(R/J)$, we can find an element of R mapping to it, namely ae_1+be_2. So surjectivity is established.

Then kernel of $R\to(R/I)\times(R/J)$ is $I\cap J$. Clearly $IJ\subseteq I\cap J$. Suppose that $x\in I\cap J$. Let e_1, e_2 be as before. Then

$$x=(e_2+e_1)x=e_2x+e_1x\in IJ.$$

Thus $IJ=I\cap J$, and the kernel of $R\to(R/I)\times(R/J)$ is IJ. □

Remark. Above we used the Cartesian product of two rings. This is a ring where addition and multiplication are defined componentwise. (Actually for the results in this section, we really only need to consider the product as a group under addition).

Remark. We could have written this isomorphism with $I\cap J$ instead of IJ:

$$R/I\cap J\to(R/I)\times(R/J), \qquad [a]\mapsto([a],[a]).$$

Often all we need is the surjection:

$$R\to(R/I)\times(R/J), \qquad a\mapsto([a],[a]).$$

This allows us to solve systems of congruences involving distinct prime ideals.

Proposition 98. *Let R be a Dedekind domain, let $\mathfrak{p}_1,\dots,\mathfrak{p}_k$ be distinct nonzero prime ideals of R, and let $n_1,\dots,n_k$ be nonnegative integers. Then the natural homomorphism*

$$R\to(R/\mathfrak{p}_1^{n_1})\times\cdots\times(R/\mathfrak{p}_k^{n_k})$$

is a surjection. In other words, given $b_1,\dots,b_k\in R$ we can find an $a\in R$ such that

$$a\equiv b_i \mod \mathfrak{p}_i^{n_i}$$

for all i.

Proof. We use induction and the Chinese remainder theorem to first get an isomorphism involving R/I where $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$. From the isomorphism produce the surjection using $R \to R/I$. □

Theorem 99 (Approximation theorem)**.** *Let R be a Dedekind domain with fraction field K, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be distinct nonzero prime ideals of R, let $x_1, \ldots, x_k \in K$, and let $n_1, \ldots, n_k$ be integers. Then there is an $x \in K$ such that*

$$v_{\mathfrak{p}_i}(x - x_i) \geq n_i$$

for each $\mathfrak{p}_i$, and such that $v_{\mathfrak{p}}(x) \geq 0$ for any other nonzero prime ideal $\mathfrak{p}$.

Proof. Observe that it is enough to prove this for $n_i \geq 0$, so we assume nonnegative n_i. If $x_i \in R$ then we just apply the previous proposition with $b_i = x_i$.

In the general case let $d \in R$ be a common denominator for the x_i, and write each x_i as b_i/d with $b_i \in R$. We then wish to find an $a \in R$ such that

$$v_{\mathfrak{p}_i}(a - b_i) \geq n_i + v_{\mathfrak{p}_i}(d).$$

We also want $v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(d)$ for any other nonzero prime ideal with $v_{\mathfrak{p}}(d) > 0$. We can find such an $a \in R$ by appealing to the first case. Now consider $x = a/d$. □

Theorem 100 (Second Approximation theorem)**.** *Let R be a Dedekind domain with fraction field K, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be nonzero prime ideals of R, and let $n_1, \ldots, n_k$ be integers. Then there is an element $x \in K$ such that $v_{\mathfrak{p}_i}(x) = n_i$ for each $\mathfrak{p}_i$ and such that $v_{\mathfrak{p}}(x) \geq 0$ for any other nonzero prime ideal $\mathfrak{p}$.*

Proof. For each such prime $\mathfrak{p}_i$, let $x_i \in \mathfrak{p}_i^{n_i} \smallsetminus \mathfrak{p}_i^{n_i+i}$. Use the approximation theorem to find an $x \in K$ such that $v_{\mathfrak{p}_i}(x - x_i) \geq n_i + 1$ for each $\mathfrak{p}_i$, and such that $v_{\mathfrak{p}}(x) \geq 0$ for any other nonzero prime ideal $\mathfrak{p}$.

Observe that $v_{\mathfrak{p}_i}(x_i) = n_i$ (Proposition 96). Since $x = x_i + (x - x_i)$,

$$v_{\mathfrak{p}_i}(x) = \min\{v_{\mathfrak{p}_i}(x_i), v_{\mathfrak{p}_i}(x - x_i)\} = v_{\mathfrak{p}_i}(x_i) = n_i.$$

□

Theorem 101. *Let R be a Dedekind domain with a finite number of prime ideals. Then R is a PID.*

Proof. Let I be a nonzero ideal of R. Use the second approximation theorem to find an element $a \in R$ such that $v_{\mathfrak{p}}(a)$ is equal to $v_{\mathfrak{p}}(I)$ for all nonzero prime ideals $\mathfrak{p}$ of R. Thus $v_{\mathfrak{p}}(aR) = v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(I)$ for all such $\mathfrak{p}$. So $aR = I$. □

Theorem 102. *Let R be a Dedekind domain. Then every nonzero ideal I of R can be generated by one or two elements.*

Proof. Let I be a nonzero ideal of R. By the second approximation theorem there is an element $a \in R$ such that $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(aR)$ is equal to $v_{\mathfrak{p}}(I)$ for all nonzero prime ideals $\mathfrak{p}$ of R dividing I. Thus $I \mid aR$.

By the second approximation theorem a second time there is an element $b \in R$ such that $v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(bR)$ is equal to $v_{\mathfrak{p}}(I)$ for all nonzero prime ideals $\mathfrak{p}$ of R that divide aR (including those dividing I).

Observe that $aR + bR$ has the same valuation as I for all valuations $v_{\mathfrak{p}}$ associated to nonzero prime ideals of R. □

Exercise 34. Show that every *fractional* ideal of a Dedekind domain can be generated by one or two elements.

Exercise 35. Show that for every nonzero ideal I in a Dedekind domain, there is a nonzero principal ideal relatively prime to I.

Exercise 36. Let $\mathfrak{p}$ be a nonzero prime ideal and let I be a fractional ideal in a Dedekind domain R. Then the quotient $I/\mathfrak{p}I$ can be thought of as an R-module, as can $R/\mathfrak{p}$. Show that $R/\mathfrak{p}$ is isomorphic as an R-module to $I/\mathfrak{p}I$. Furthermore, show that there is an isomorphism of the form $[r] \mapsto [rx]$ for each $x \in I$ not in $\mathfrak{p}I$.

Hint: start with the composition $R \to I \to I/\mathfrak{p}I$ and show that the kernel is a proper ideal containing $\mathfrak{p}$. For surjectivity, observe that any R-submodule of $I/\mathfrak{p}I$ corresponds to a fractional ideal containing $\mathfrak{p}I$ and contained in I. Now use unique factorization of fractional ideals (or multiply by a nonzero d such that dI is an integral ideal).

11 Gauss's lemma in Dedekind domains

There are other important results for general Dedekind domains including (1) Gauss's lemma for polynomials with coefficients in a Dedekind domain, (2) results about modules, especially finitely generated modules, over a Dedekind domain, and (3) results concerning the relationship between two Dedekind domains $R_1 \subseteq R_2$, especially when the fraction field of R_2 is a finite extension of the fraction field of R_1. We won't treat (2) and (3) in this document, but we will touch on (1) in this section. We will start with the case of a discrete valuation ring.

Let R be a DVR with maximal ideal $\mathfrak{m}$, fraction field K, and valuation v. It is possible to extend v, in a natural way, to a function (also called v)

$$v\colon K[X] \to \mathbb{Z} \cup \{\infty\}$$

which we call the *valuation map on polynomials*. We define $v(0)$ to be ∞. For any nonzero $f \in K[X]$, let $v(f)$ be the minimum of $v(a)$ among coefficients of f. So, of course if $f = a$ is a constant polynomial, then $v(f)$ (using the valuation map on polynomials) agrees with $v(a)$ (using the original valuation map).

Proposition 103. *Let R be a DVR with fraction field K. Let v be the valuation map on polynomials and let $f, g \in K[X]$. Then*

$$v(f+g) \geq \min\{v(f), v(g)\}.$$

Proposition 104. *Let R be a DVR with fraction field K. Let v be the valuation map on polynomials and let $f \in K[X]$. Then $f \in R[X]$ if and only if $v(f) \geq 0$.*

Polynomials f is such that $v(f) = 0$ are called *primitive polynomials*. These include all monic polynomials in $R[X]$. Recall that there is a natural surjective ring homomorphism

$$R[X] \to (R/\mathfrak{m})[X]$$

that acts by replacing each coefficient with its equivalence class. Primitive polynomials are exactly the polynomials in $R[X]$ that have nonzero image.

Proposition 105. *Let R be a DVR with maximal ideal $\mathfrak{m}$. Let v be the valuation map on polynomials and let $f \in R[X]$. Then $v(f) = 0$ if and only if the image of f in $(R/\mathfrak{m})[X]$ is nonzero.*

We wish to show that the valuation map on polynomials is multiplicative. We start with an easy case:

Lemma 106. *Let R be a DVR with fraction field K. Let v be the valuation map on polynomials, let $a \in K^\times$, and let $f \in K[X]$. Then $v(af) = v(a) + v(f)$.*

Proposition 107 (Gauss's lemma for DVRs)**.** *Let R be a DVR with fraction field K. Let v be the valuation map on polynomials and let $f, g \in K[X]$. Then*

$$v(fg) = v(f) + v(g).$$

Proof. The zero case is straightforward, so we assume f and g are nonzero. If π is a uniformizer, then write $f = \pi^k f_0$ and $g = \pi^l g_0$ where k is $v(f)$, where l is $v(g)$, and where $f_0, g_0 \in K[X]$. Observe that $v(f_0) = v(g_0) = 0$. In particular, f_0 and g_0 are in $R[X]$. Also, the images of f_0 and g_0 in $(R/\mathfrak{m})[X]$ are nonzero where $\mathfrak{m}$ is the maximal ideal of R. This means that the product $f_0 g_0$ has nonzero image as well since $R[X] \to (R/\mathfrak{m})[X]$ is a homomorphism and $(R/\mathfrak{m})[X]$ is an integral domain. Thus $v(f_0 g_0) = 0$. Since $fg = \pi^{k+l} f_0 g_0$, we have $v(fg) = k+l+0 = v(f)+v(g)$. □

We can extend the valuation map on polynomials further to a valuation $v\colon K(X)^\times \to \mathbb{Z}$ where $K(X)$ is the fraction field of $K[X]$. We call this the *the valuation of $K(X)$ induced by the valuation v of K*. We use the same symbol v for the valuation of $K(X)$ using context to distinguish the various meanings of v. This valuation is define as follow for $f, g \in K[X]$ both nonzero:

$$v(f/g) \stackrel{\text{def}}{=} v(f) - v(g).$$

Here we are ignoring 0, but we set $v(0) = \infty$ if needed.

Lemma 108. *The above function is well-defined, and extends the valuation map on polynomials.*

Proposition 109. *Let R be a DVR with fraction field K. Let v be the induced valuation on $K(X)$ and let $f, g \in K(X)$. Then*

$$v(f+g) \geq \min\{v(f), v(g)\}.$$

Proof. This is straightforward when f and g are written as fractions with a common denominator □

Proposition 110. *Let R be a DVR with fraction field K. Let v be the induced valuation on $K(X)$ and let $f, g \in K(X)$. Then*

$$v(fg) = v(f) + v(g).$$

Proposition 111. *Let R be a DVR with fraction field K. Then the induced valuation is a valuation map $K(X)^\times \to \mathbb{Z}$. The valuation ring consists of elements of the form rf/g where $f, g \in K[X]$ are primitive polynomials and $r \in R$. The maximal ideal consists of elements of this form rf/g where r is in the maximal ideal of R. If π is a uniformizer of R and if f, g are primitive polynomials, then $v(\pi^k f/g) = k$, so π is a uniformizer for the valuation ring associated to $K(X)^\times \to \mathbb{Z}$.*

Now we shift to a general Dedekind domain R. For every nonzero prime $\mathfrak{p}$ of R we have the valuation $v_\mathfrak{p}$ of $R_\mathfrak{p}$. We extend $v_\mathfrak{p}$ to $K(X)^\times$ as above. (We also have the extension of v to fractional ideals of R which we will also need).

Proposition 112. *Let $f \in K(X)^\times$ where K is the fraction field of a Dedekind domain R. Then $v_\mathfrak{p}(f) \neq 0$ for only a finite number of nonzero prime ideals $\mathfrak{p}$ of R.*

It turns out that these extended valuations are closely connected to the concept of the *content* of a polynomial.

Definition 12. Let R be an integral domain with fraction field K. If

$$f = a_n X^n + \ldots + a_1 X + a_0 \in K[X]$$

then the *content* of f is defined as the following fractional ideal:

$$\text{content}(f) \stackrel{\text{def}}{=} a_n R + \ldots + a_1 R + a_0 R.$$

Proposition 113. *Let R be an integral domain with fraction field K, then*

$$\text{content}(fg) \subseteq \text{content}(f)\,\text{content}(g).$$

for any polynomials $f, g \in K[X]$.

Now we consider the case where R is a Dedekind domain.

Proposition 114. *Let R be a Dedekind domain with fraction field K. If $f \in K[X]$ is nonzero then*

$$\text{content}(f) \;=\; \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(f)}$$

where $\mathfrak{p}$ varies among any given finite set of nonzero prime ideals of R containing at least all primes $\mathfrak{p}$ with $v_\mathfrak{p}(f) \neq 0$.

Proof. By Corollary 61 it is enough to show equality locally for each nonzero prime ideal $\mathfrak{p}$. If the coefficients of f are $a_0, \ldots, a_n \in K$ then

$$\text{content}(f)\, R_\mathfrak{p} = a_0 R_\mathfrak{p} + \ldots + a_n R_\mathfrak{p}.$$

Since $R_\mathfrak{p}$ is a DVR, we can use the classification of fractional ideals in DVRs to simplify (where we temporarily define $\mathfrak{p}^{v_\mathfrak{p}(0)} R_\mathfrak{p} = 0$)

$$\text{content}(f)\, R_\mathfrak{p} = \mathfrak{p}^{v_\mathfrak{p}(a_0)} R_\mathfrak{p} + \ldots + \mathfrak{p}^{v_\mathfrak{p}(a_n)} R_\mathfrak{p} = \mathfrak{p}^{v_\mathfrak{p}(a_i)} R_\mathfrak{p}$$

where $v_\mathfrak{p}(a_i)$ is the minimum of $\{v_\mathfrak{p}(a_1), \ldots, v_\mathfrak{p}(a_n)\}$. By definition, $v_\mathfrak{p}(a_i)$ is just $v_\mathfrak{p}(f)$. Thus

$$\text{content}(f)\, R_\mathfrak{p} = \mathfrak{p}^{v_\mathfrak{p}(f)} R_\mathfrak{p}.$$

This is the desired local equality. The result now follows from Corollary 61. □

The above proposition allows us to extend the definition of content to elements of $K(X)^\times$ (when R is a Dedekind domain):

Definition 13. Let $f \in K(X)^\times$ where K is the fraction field of a Dedekind domain R. Then the *content* of f is defined as the following fractional ideal:

$$\text{content}(f) \stackrel{\text{def}}{=} \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(f)}$$

where $\mathfrak{p}$ varies among any given finite set of nonzero prime ideals of R containing at least all primes $\mathfrak{p}$ with $v_{\mathfrak{p}}(f) \neq 0$.

Proposition 115. *Let $f \in K(X)^\times$ where K is the fraction field of a Dedekind domain R. For every nonzero prime ideal $\mathfrak{p}$*

$$v_{\mathfrak{p}}(f) = v_{\mathfrak{p}}(\text{content}(f)).$$

Theorem 116 (Gauss's lemma for Dedekind domains)**.** *Let $f, g \in K(X)^\times$ where K is the fraction field of a Dedekind domain R. Then*

$$\text{content}(fg) = \text{content}(f)\ \text{content}(g)$$

Proof. By Corollary 61 it is enough to show equality in $R_{\mathfrak{p}}$ for each nonzero prime ideal $\mathfrak{p}$. This amounts to showing

$$\mathfrak{p}^{v_{\mathfrak{p}}(fg)} R_{\mathfrak{p}} = \left(\mathfrak{p}^{v_{\mathfrak{p}}(f)} R_{\mathfrak{p}}\right)\left(p^{v_{\mathfrak{p}}(g)} R_{\mathfrak{p}}\right)$$

However $v_{\mathfrak{p}}(fg) = v_{\mathfrak{p}}(f) + v_{\mathfrak{p}}(g)$ by Theorem 107. □

Remark. Gauss's lemma gives a trick for finding a generating set for the product of two fractional ideals IJ. Suppose $I = a_1R + \ldots + a_mR$, then let f be the following "basis polynomial":

$$f \stackrel{\text{def}}{=} a_1 + a_2X + \ldots + a_mX^{m-1}.$$

Observe that $I = \text{content}(f)$. Let $J = \text{content}(g)$ for a similarly constructed polynomial. Then $IJ = \text{content}(fg)$. Thus the coefficients of the polynomial fg provide a generating set for IJ.

Observe, that if I has m generators and J has n generators, then we get $m+n-1$ generators for IJ this way. Compare this to the mn generators you get if instead you use a_ib_j as your generating set where (a_i) are m generators for I and (b_i) are n generators for J.

For example, in algebraic number theory it is known that $R = \mathbb{Z}[\sqrt{-5}\,]$ is a Dedekind domain. Since $\left(3X + (1 + 2\sqrt{-5})\right)\left(3X + (1 - 2\sqrt{-5})\right) = 9X^2 + 6x + 21$ we conclude that

$$\left(3R + (1 + 2\sqrt{-5})R\right)\ \left(3R + (1 - 2\sqrt{-5})R\right) = 9R + 6R + 21R = 3R$$

which gives a factorization of the ideal $3R$.

Exercise 37. Suppose that R is an integral domain with fraction field K.

1. Show that if $f = a$ is a nonzero constant polynomial, then $\text{content}(f) = aR$.

2. Let $f \in K[X]$ be nonzero. Show that $f \in R[X]$ if and only if the content of f is an integral ideal.

3. A *primitive polynomial* is defined to be a polynomial in $K[X]$ with content equal to the identity ideal R. Show that every monic polynomial in $R[X]$ is primitive.

Exercise 38. Suppose that R is a Dedekind domain and that $f, g, h \in K[X]$ are monic. Show that if $f = gh$ and $f \in R[X]$ then $g, h \in R[X]$ as well.

Exercise 39. Show that if R is a PID with fraction field K, and if $f \in K[X]$ is nonzero, then $\text{content}(f) = aR$ if and only $f = af_0$ where f_0 is a primitive polynomial. Make and justify a similar statement for $f \in K(X)^\times$.

In this case we sometimes say that a is the content. The content considered as an element in $K^\times$ is only defined up to multiplication by a unit of R.

Exercise 40. Suppose $f, g \in R[X]$ are nonzero with nonzero sum $f + g$, where R is a Dedekind domain. Show that

$$\text{content}(f) + \text{content}(g) \mid \text{content}(f + g)$$

(where the sum is the sum of ideals).

If you weaken the assumption that R is a Dedekind domain to just that R is integrally closed, you still get some interesting results about polynomials. In the remaining exercises in this section we consider integral domains that are not always Dedekind domains, but are at least integrally closed.

Exercise 41. Let R be an integral domain that is integrally closed in its fraction field K. Show that if r is a root of a nonzero $f \in R[X]$, and if $a \in R$ is the leading coefficient of f, then $ar \in R$. Hint: multiply f by a^{d-1} where d is the degree of f in order to form a monic polynomial with root ar.

Exercise 42. Let R be an integral domain that is integrally closed in its fraction field K. Show that if $r \in K$ is a root of a nonzero polynomial $f \in R[X]$ then we have $f(X) = q(X)(X - r)$ where q is in $R[X]$. Hint: use (strong) induction on the degree of f and use the previous exercise in the context of the division algorithm in $K[X]$. Pay special attention to the leading coefficient of f.

Exercise 43. The above exercise leads to an interesting characterization of the property of being integrally closed. Let R be an integral domain with fraction field K. Show that *R is integrally closed if and only if, for each nonzero $f \in R[X]$ and each root $r \in K$ of f, we can factor f as $q(X)(X - r)$ where q is in $R[X]$.*

Hint: consider the special case where f is monic and look at the two terms of highest power of $f(x)$ and the product $q(X)(X - r)$.

Exercise 44. Use Gauss's lemma to give a simpler proof of the result of Exercise 42 when the hypothesis is replaced by the hypothesis that R is a Dedekind domain.

Exercise 45. (Assumes some field theory background). Let R be an integral domain that is integrally closed in its fraction field K. Show that if $f \in R[X]$ is a nonzero polynomial that factors as $f = gh$ where $g, h \in K[X]$ and where h is monic, then $g \in R[X]$.

Hint: Extend to the splitting field of h, and use Exercise 43 repeatedly d times where $d = \deg h$.

Exercise 46. Use the previous exercise to show the following when R is an integral domain that is integrally closed in its fraction field K. *If $f \in R[X]$ is a monic polynomial that factors as $f = gh$ where $g, h \in K[X]$ are monic, then $g, h \in R[X]$.*

Does the converse hold? In other words, does this property imply that R is integrally closed?

12 Divisibility domains and cancellation domains

Now we explore integral domains that behave like Dedekind domains in certain ways. If an integral domain behaves like a Dedekind domain by having the property that $J \subseteq I \implies I \mid J$, we will call it a *divisibility domain*. If an integral domain behaves like a Dedekind domain by having a cancellation law for nonzero ideals, we will call it a *cancellation domain*. The terms *divisibility domain* and *cancellation domain* should be regarded as temporary classifications since we will show such rings can be characterized in terms of other types of rings (see Theorem 118 and Theorem 165).

Definition 14. A *divisibility domain* is an integral domain with the property that if $J \subseteq I$, where I and J are nonzero ideals, then $I \mid J$.

Example 2. As we have seen, every Dedekind domain is a divisibility domain.

Example 3. By Theorem 19, any divisibility domain with a unique nonzero maximal ideal is a DVR.

Lemma 117. *Suppose R is a divisibility domain. Then every nonzero ideal is invertible.*

Proof. Let I be a nonzero ideal and let $a \in I$ be a nonzero element. Then $aR \subseteq I$. Hence $I \mid aR$. Thus $IJ = aR$ for some nonzero ideal J of R. Observe that $a^{-1}J$ is an inverse for I. □

Theorem 118. *Let R be an integral domain. Then R is a divisibility domain if and only if it is a Dedekind domain.*

Proof. We have already seen that every Dedekind domain is a divisibility domain (Theorem 90). By the previous lemma and Theorem 69, every divisibility domain is a Dedekind domain since every nonzero ideal is invertible. □

Now we consider integral domains that are similar to Dedekind domains by possessing a cancellation law for nonzero ideals.

Definition 15. A *cancellation domain* is an integral domain with the property that if $I_1 J = I_2 J$, where I_1, I_2 and J are nonzero ideals, then $I_1 = I_2$.

Lemma 119. *Suppose I_1, I_2, and J are fractional ideals of a cancellation domain. If $I_1 J = I_2 J$ then $I_1 = I_2$.*

Lemma 120. *Suppose I_1, I_2, and J are fractional ideals of a cancellation domain. If $I_1 J \subseteq I_2 J$ then $I_1 \subseteq I_2$.*

Proof. If $I_1 J \subseteq I_2 J$ then $(I_1 + I_2)J = I_1 J + I_2 J = I_2 J$. Since R is a cancellation domain, $I_1 + I_2 = I_2$. Thus $I_1 \subseteq I_2$. □

Here is a simple, but tricky lemma:

Lemma 121. *Suppose $x \in K^\times$ where K is the fraction field of a cancellation domain R. Then $xR \subseteq x^2 R + R$.*

Proof. Let $I_1 = xR$ and $I_2 = x^2 R + R$. Let $J = xR + R$. Then $I_1 J \subseteq I_2 J$. Thus $I_1 \subseteq I_2$. □

Lemma 122. *Suppose $x \in K^\times$ where K is the fraction field of a cancellation domain R. Then $ax^2 + x + b = 0$ for some $a, b \in R$.*

Proof. This is a consequence of the previous lemma. □

Lemma 123. *Every cancellation domain R is integrally closed.*

Proof. Suppose x is in the fraction field K of R and is integral over R. Then the R-submodule $I = R[x]$ of K must be a finitely generated as an R-module. Observe that $II = I$, so by cancellation $I = R$. Thus $x \in R$ as desired. □

Lemma 124. *Let R be a cancellation domain R with fraction field K. Let $\mathfrak{p}$ be a nonzero prime ideal of R. Then for every $x \in K^\times$ either $x \in R_\mathfrak{p}$ or $x^{-1} \in R_\mathfrak{p}$.*

Proof. By Lemma 122 we have that $ax^2 + x + b = 0$ for some $a, b \in R$. This gives us $(ax)^2 + (ax) + ab = 0$. Since R is integrally closed, $ax \in R$. Observe that $(1+ax)x = -b$ so $(1+ax)x \in R$. Now $R_\mathfrak{p}$ is a local ring so either ax or $1+ax$ is a unit in $R_\mathfrak{p}$. If ax is a unit, then $1/x \in R_\mathfrak{p}$. If $1+ax$ is a unit, then $x \in R_\mathfrak{p}$. □

Proposition 125. *Let R be a Noetherian cancellation domain R. Then $R_\mathfrak{p}$ is a DVR for every nonzero prime ideal of R.*

Proof. Since $R_\mathfrak{p}$ must be Noetherian, it must be a DVR by the previous lemma and Proposition 15. □

Theorem 126. *Let R be an integral domain. Then R is a Dedekind domain if and only if it is a Noetherian cancellation domain.*

Proof. If R is a Dedekind domain, it is Noetherian by definition and every nonzero ideal is invertible (Theorem 69), which makes it a cancellation domain.

If R is a Noetherian cancellation domain, then $R_\mathfrak{p}$ is a DVR for every nonzero maximal ideal $\mathfrak{p}$ of R by the above proposition, which makes it a Dedekind Domain (see Theorem 64). □

In Appendix E we will consider cancellation domains that are not necessarily Noetherian.[8] The following exercises applies to such general cancellation domains, and will be used in Appendix E.

Exercise 47. Show that if R is a cancellation domain and if $a \in R$ is not a unit then

$$\bigcap_{k=1}^{\infty} a^k R = \{0\}.$$

Hint: call this intersection I and show $(aR)I = I$.

Exercise 48. Suppose that R is an integral domain with maximal ideal $\mathfrak{m}$. Derive the identity

$$\left(\mathfrak{m}^k R_{\mathfrak{m}}\right) \cap R = \mathfrak{m}^k.$$

Hint: For each $a \in \left(\mathfrak{m}^k R_{\mathfrak{m}}\right) \cap R$, form the ideal $I_a = \{r \in R \mid ra \in \mathfrak{m}^k\}$. Show that I_a contains the ideal $\mathfrak{m}^k + sR$ for some $s \in R \setminus \mathfrak{m}$. Conclude that $I_a = R$.

Exercise 49. Let $\mathfrak{m}$ be a nonzero maximal ideal in a cancellation domain R. Show that $\mathfrak{m}^2 \subsetneq \mathfrak{m}$. Use the previous exercise to show that this strict inclusion continues to hold in $R_{\mathfrak{m}}$:

$$\mathfrak{m}^2 R_{\mathfrak{m}} \subsetneq \mathfrak{m} R_{\mathfrak{m}}.$$

Exercise 50. Let $\mathfrak{m}$ be a nonzero maximal ideal in a cancellation domain R. Show that $R_{\mathfrak{m}}$ is a valuation ring whose maximal ideal is principal. Hint: see Exercise 6 for the definition of valuation ring, and Exercise 9 to help show the maximal ideal is principal. Also, use the previous exercise.

13 Characterizing Dedekind domains

Here we summarize results, mainly from Sections 7 and 12, concerning what properties are necessary and sufficient for an integral domain to be a Dedekind domain.

Before doing so, we derive a few more such characteristic properties. These are properties that have been established or can easily be established for Dedekind domains, but, as we will see, any Integral domain with these properties must be a Dedekind domain.

Theorem 127. *Suppose that R is an integral domain such that every nonzero proper ideal is the product of maximal ideals. Then R is a Dedekind domain.*

Proof. Let $\mathfrak{m}$ be a nonzero maximal ideal of R and let $a \in \mathfrak{m}$ be nonzero. Then by assumption aR is the product of maximal ideal: $aR = \mathfrak{m}_1 \cdots \mathfrak{m}_k$. By Proposition 21, each $\mathfrak{m}_i$ is invertible. Next observe that $\mathfrak{m}_1 \cdots \mathfrak{m}_k \subseteq \mathfrak{m}$. This implies that $\mathfrak{m} = \mathfrak{m}_i$ for some i. Thus $\mathfrak{m}$ is invertible.

Since every nonzero maximal ideal is invertible, any product of such ideals is invertible. By assumption every nonzero proper ideal is the product of (nonzero) maximal ideals. Thus every nonzero ideal is invertible and, by Theorem 69, R is a Dedekind domain. □

[8] We will see that an integral domain is a cancellation domain if and only if it is an almost Dedekind domain.

Theorem 128. *Suppose that R is an integral domain. Then R is a Dedekind domain if and only if for every nonzero ideal I there is a nonzero ideal J such that IJ is principal.*

Proof. Suppose R is a Dedekind domain and I is a nonzero ideal. Let $a \in I$ be nonzero. Thus $aR \subseteq I$ and $I \mid aR$ as desired.

By Proposition 21, if I and J are nonzero ideals such that IJ is principal, then I and J are invertible. So if for every nonzero ideal I there is a nonzero ideal J such that IJ is principal, then every nonzero ideal I must be invertible. Now use Theorem 69. □

Now we are ready for a list of characterizations of Dedekind domains.

Theorem 129. *Let R be an integral domain. Then the following are equivalent:*

1. *R is a Dedekind domain. In other words, R is an integrally closed Noetherian domain whose nonzero prime ideals are maximal.*
2. *Every nonzero ideal of R is invertible. (see Theorem 69)*
3. *The fractional ideals of R form a group under multiplication. (see Cor. 67)*
4. *Every nonzero proper ideal is the product of maximal ideals. (Theorem 127)*
5. *R is Noetherian and $R_{\mathfrak{m}}$ is a DVR for each nonzero maximal ideal $\mathfrak{m}$. (Th. 64)*
6. *R is Noetherian and $R_{\mathfrak{p}}$ is a DVR for each nonzero prime ideal $\mathfrak{p}$.*
7. *R is a divisibility domain. In other words, R has the property that if $J \subseteq I$, where I and J are nonzero ideals, then $I \mid J$.v(see Theorem 118)*
8. *R is a Noetherian cancellation domain. In other words, R is a Noetherian domain such that if $I_1 J = I_2 J$ then $I_1 = I_2$ for all nonzero ideals I_1, I_2, J. (Theorem 126).*
9. *For every nonzero ideal I of R there is an nonzero ideal J of R such that IJ is principal. (Theorem 128)*

Proof. From Section 7 we use Theorem 64, Corollary 67, and Theorem 69. From Section 8 we use Theorem 76. From Section 12 we use Theorem 118 and Theorem 126. From the current section we use Theorem 127 and Theorem 128. These results give most of the needed implications. The rest are straightforward. □

Remark. Observe that many of these characterizations are simpler than the traditional definition of Dedekind domain (Definition 1). *Why then is the traditional definition still commonly used?* Perhaps because it is the easiest to verify for rings such as the ring of integers in a number field.

Exercise 51. Let R be a Dedekind domain. Show that R is a PID if and only if R is a UFD. Generalize this to any integral domain R with the property that every nonzero prime ideal is maximal.

(Recall that a UFD is an integral domain such that every nonzero non-unit element $a \in R$ can be written uniquely as the product of irreducible elements.

Uniqueness means that if $a = p_1 \dots p_k = q_1 \dots q_l$ are two such products, then $k = l$, and we can rearrange the order of the terms such that, for each i, the elements p_i and q_i are associates (p_i is a unit times q_i). An irreducible element is an nonzero non-unit element that is not the product of two nonzero non-unit elements.)

Hint for one direction: Suppose R is a UFD. First show that if π is irreducible, then πR is a prime ideal. Given a nonzero prime ideal $\mathfrak{p}$, let $a \in \mathfrak{p}$ be nonzero, and factor a into irreducibles. Use that factorization to show that $\mathfrak{p}$ is principal. Conclude that all ideals are principal. (To go from prime ideals principal to all ideas principal is immediate in a Dedekind domain. For more general rings, given a nonzero idea I factor $a \in I$ where a is not zero, and work from there.)

Appendix A: The non-local approach to ideal factorization

One of the main theorems for Dedekind domains, perhaps the main theorem, is that ideals factor uniquely into prime ideals. Initially we assumed this result as background since this document is in some sense a part two in the theory of Dedekind domains, and most introductory accounts give a (non-local) proof of the result

Although we did end up giving an independent proof of this result built on the local approach (see Theorem 76 together with Proposition 82), we now give, for the convenience of the reader, a somewhat standard non-local proof so the reader can more easily compare the two approaches.[9] In particular, the proof in this appendix does not use localization, local rings, or discrete valuation rings. This proof does use fractional ideals, and so depends on some of the material from Sections 3 to 5.[10] So the reader should look over these sections, up to Corollary 42, before reading this appendix (skipping any parts of those sections dealing with localizations or discrete valuation rings).

We will especially draw on Corollary 42 from Section 5 which immediately implies the following result which will label our first lemma:

Lemma 130. *Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain. If there is a fractional ideal I not contained in R such that $I\mathfrak{p} \subseteq R$, then $\mathfrak{p}$ is invertible.*

Next we use the Noetherian property:

Lemma 131. *Let I be a nonzero proper ideal of a Noetherian domain R. Then there are nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_k$, where $k \geq 1$, such that*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq I.$$

[9] The approach in this appendix is largely similar to the standard approach given by B. L. van der Waerden in his *Algebra*, and has been adopted by many other textbooks. Van der Waerden attributes this approach to W. Krull (1928).

[10] Some authors, including Marcus, prove this result using only ideals, not fractional ideals. So the use of fractional ideals is not strictly necessary. All standard proofs, however, require something like the result that every element of $\mathcal{R}(I)$ is integral, at least in the case of I an ideal, which we covered in Section 5 above. Aside from that, the concepts related to fractional ideals presented in Sections 3 and 4 are fairly straightforward and are central to the subject, so I feel comfortable requiring this of the reader even in this basic non-local proof.

Proof. Suppose there are nonzero proper ideals where this fails. Using the Noetherian property, we can find a maximal such ideal I. Note that I is not a prime ideal, so there are $x, y, \in R$ such that $xy \in I$ but x, y are not in I. We can assume the result for $I + xR$ and $I + yR$. Finally, observe that $(I + xR)(I + yR) \subseteq I$. □

Our goal will be to show that the inclusion in the above lemma is an equality when the number of primes k is minimized.

Definition 16. A *prime bounding sequence* $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of an ideal I is a sequence of nonzero prime ideals such that $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq I$. If k is as small as possible, then we call the sequence a *minimal prime bounding sequence* of I. If $I = R$ we consider the empty sequence to be the minimal prime bounding sequence.

Lemma 132. *Let R be a Noetherian domain such that every nonzero prime ideal is maximal. If I is a nonzero ideal and if $\mathfrak{p}$ is a nonzero prime ideal containing I then $\mathfrak{p}$ appears in any prime bounding sequence of I. In particular, I is contained in a finite number of prime ideals.*

Proof. If $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq I \subseteq \mathfrak{p}$ where $\mathfrak{p}_i$ are nonzero prime ideals, then $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i. Hence $\mathfrak{p}_i = \mathfrak{p}$. □

Next we prove invertibility for prime ideals:

Lemma 133. *Every nonzero prime ideal $\mathfrak{p}$ in a Dedekind domain R is invertible.*

Proof. Let $a \in \mathfrak{p}$ be a nonzero element and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be a minimal prime bounding sequence for aR. By the previous lemma, $\mathfrak{p}$ is in the sequence. Permute the terms of the sequence so that $\mathfrak{p} = \mathfrak{p}_k$. By minimality, $\mathfrak{p}_1 \cdots \mathfrak{p}_{k-1}$ is not contained in aR, so the fractional ideal $I = a^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_{k-1}$ is not contained in R. (if $k = 1$, let $I = a^{-1}R$). Also $I\mathfrak{p} \subseteq R$, so $\mathfrak{p}$ is invertible by Lemma 130. □

Lemma 134. *Every nonzero ideal I in a Dedekind domain R is the product of the prime ideals in its minimal prime bounding sequence.*

Proof. We prove this by induction on the size k of the sequence. The base case $k = 0$ is the empty sequence with $I = R$. Suppose now that $\mathfrak{p}_1, \ldots, \mathfrak{p}_{k+1}$ is a minimal prime bounding sequence for I. Let $\mathfrak{p}$ be a prime ideal containing I which is necessarily in the sequence. Permute the sequence so that $\mathfrak{p} = \mathfrak{p}_{k+1}$. Thus

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k = (\mathfrak{p}_1 \cdots \mathfrak{p}_{k+1})\mathfrak{p}^{-1} \subseteq I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R.$$

Note that $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ must be a minimal prime bounding sequence of $I' = I\mathfrak{p}^{-1}$ (otherwise, we could form a smaller prime bounding sequence for $I = I'\mathfrak{p}$ than the given one). So by the induction hypothesis

$$I\mathfrak{p}_{k+1}^{-1} = I' = \mathfrak{p}_1 \cdots \mathfrak{p}_k, \quad \text{and so} \quad I = \mathfrak{p}_1 \cdots \mathfrak{p}_{k+1}.$$

□

We now just need uniqueness:

Lemma 135. *Suppose that I is a proper nonzero ideal of a Dedekind domain with prime ideal factorizations:*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_k = \mathfrak{q}_1 \cdots \mathfrak{q}_l.$$

Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ is a permutation of $\mathfrak{q}_1, \ldots, \mathfrak{q}_l$

Proof. Using properties of prime ideals we can show that $\mathfrak{p}_k = \mathfrak{q}_i$ for some index i. After permuting the factors, we can assume that $\mathfrak{p}_k = \mathfrak{q}_l$. We multiply both factorizations by $\mathfrak{p}_k^{-1}$. Continuing in this way[11] we get uniqueness. □

Theorem 136. *Every nonzero ideal in a Dedekind domain is uniquely the product of nonzero prime ideals. (Uniqueness is up the order of the terms).*

Appendix B: The singular case

In algebraic number theory and algebraic geometry there are important situations where rings arise that are like Dedekind domains except for not being integrally closed. For example, nonmaximal orders in algebraic number fields have this property. In this appendix we consider such rings.

Definition 17. An *integral domain of dimension* 1, or a *1-domain* for short, is an integral domain that is not a field and such that every nonzero prime ideal is maximal.[12]

If a Noetherian 1-domain is not integrally closed, and so is not a Dedekind domain, then we say that it is *singular*. Any nonzero prime ideal $\mathfrak{p}$ of R such that $R_\mathfrak{p}$ fails to be a DVR is called a *singular prime ideal*.

By the results we have established, especially Theorem 129, we have the following facts about any singular Noetherian 1-domain R:

1. The fractional ideals of R do not form a group: some nonzero ideals of R are not invertible.
2. There is at least one singular prime ideal $\mathfrak{p}$.
3. There are nonzero ideals $J \subseteq I$ where $I \mid J$ fails.
4. There is a nonzero proper ideal of R that is not the product of prime ideals. Since R is Noetherian, every nonzero proper ideal is the product of irreducible ideals (Exercise 22), so this means that there are irreducible ideals (in the sense of Exercise 22) that are not prime. Below we will see that such irreducible ideals must be primary ideals, and will give examples.

[11] We can make this into a more formal induction by setting n to be the minimum of k and l and proceed by induction on n. Another approach is to prove the following statement using induction on n: for any two sequences of prime ideals whose products are equal, if a prime $\mathfrak{p}$ occurs exactly n times in one sequence, it occurs exactly n times in the other.

[12] This notion of dimension 1 is based on the notion of Krull dimension. The Krull dimension of a commutative ring is is one less than the length of the longest proper chain of prime ideals. In our case, since every nonzero prime ideal is maximal, the longest chain is of the form $0 \subsetneq \mathfrak{p}$. So the Krull dimension is one.

5. R is not a PID or a UFD (since it is not integrally closed).

6. Cancellation fails: there are nonzero ideals $I_1 \neq I_2$ and J such that $I_1 J = I_2 J$.

Let $\mathfrak{p}$ be a singular prime of a Noetherian 1-domain. By the results developed above (especially in the last part of Section 2) we have the following:

1. The ring $R_{\mathfrak{p}}$ has ideals that are not principal, including its maximal ideal. All such non-principal ideals are not invertible.

2. The ring $R_{\mathfrak{p}}$ is local, but not strongly local. In particular, there are nonmaximal ideals not contained in $(\mathfrak{p}R_{\mathfrak{p}})^2$. We will give examples below.

3. If $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$ is the maximal ideal of $R_{\mathfrak{p}}$, then $\mathfrak{m}/\mathfrak{m}^2$ has dimension greater than one over the field $R/\mathfrak{p} \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.

4. The ring $R_{\mathfrak{p}}$ is not integrally closed in K.

5. There are elements $x \in K^\times$ such that neither x and x^{-1} are in $R_{\mathfrak{p}}$.

6. There are irreducible ideals of $R_{\mathfrak{p}}$ (in the sense of Exercise 22) that are not prime ideals because factorization into nonzero prime ideals fails. We will give examples below.

7. $R_{\mathfrak{p}}$ is not a UFD (since it is not integrally closed).

8. There are nonzero ideals $J \subseteq I$ where $I \mid J$ fails.

9. Cancellation fails: there are nonzero ideals $I_1 \neq I_2$ and J such that $I_1 J = I_2 J$.

In addition, the fact that $R_{\mathfrak{p}}$ is not integrally closed can be seen using elements (or even generators) of the fractional ideal $(\mathfrak{p}R_{\mathfrak{p}})^{-1}$.

Proposition 137. *Let R be a Noetherian domain with unique nonzero prime ideal $\mathfrak{p}$. Suppose that R is not integrally closed. Then there are integral elements $x \notin R$ in the fractional ideal $\mathfrak{p}^{-1}$. Moreover, we can find such an x in any set of generators of the fractional ideal $\mathfrak{p}^{-1}$.*

Proof. Let K be the fraction field of R. By Lemma 43, there are $x \in K^\times$ not in R such that $x\mathfrak{p} \subseteq R$. Such x is in $\mathfrak{p}^{-1}$. As mentioned above $\mathfrak{p}$ is not invertible. So, by Proposition 40, $\mathfrak{p}^{-1} \subseteq \mathcal{R}(\mathfrak{p})$, and so every such x is integral over R.

Given a set of generators of $\mathfrak{p}^{-1}$, at least one is not in R. Otherwise Lemma 43 would fail. □

Even for singular Noetherian 1-domains, there is a factorization theorem. To explain how it works, we begin with the theory of localization which contains the result that $I \mapsto IR_{\mathfrak{p}}$ is a surjection from the set of ideal of R to the set of ideals of $R_{\mathfrak{p}}$. In fact, if J is an ideal of $R_{\mathfrak{p}}$, then $J \cap R$ is an ideal of R that will map to J under this mapping: $(J \cap R)R_{\mathfrak{p}} = J$. In fact, $J \cap R$ is the maximum among ideals of R that map to J under the mapping $I \mapsto IR_{\mathfrak{p}}$.

Our factorization will make use of ideals of R the form $J \cap R$ where J is an ideal of $R_{\mathfrak{p}}$. One desirable property of such ideals is the property of being $\mathfrak{p}$-primary:

Definition 18. Let R be a 1-domain and let I be a nonzero ideal of R. We say that I is *primary* if I is contained in exactly one prime ideal. If I is a primary ideal contained in the prime ideal $\mathfrak{p}$ then we say that I is $\mathfrak{p}$-*primary.*[13]

We now state a convenient characterization of $\mathfrak{p}$-primary. It is a special case of a well-know result from commutative algebra.[14] We give a short proof here for the convenience of the reader.

Proposition 138. *Let R be a 1-domain. Suppose $I \subseteq \mathfrak{p}$ where I is a nonzero ideal and where $\mathfrak{p}$ is a prime ideal. Then I is $\mathfrak{p}$-primary if and only if for each $a \in \mathfrak{p}$ there is a $k \in \mathbb{N}$ such that $a^k \in I$.*

Proof. Suppose that I is $\mathfrak{p}$-primary, and that $a \in \mathfrak{p}$. We have what we want when $a = 0$, so suppose a is not zero. Consider the multiplicative system S consisting of powers a^k where $k \geq 0$.

We start with the following claim: the ideal $S^{-1}I$ is all of $S^{-1}R$. If not, then $S^{-1}I$ would have to be contained in a maximal ideal, which, by the theory of localization, has form $S^{-1}\mathfrak{q}$ where $\mathfrak{q}$ is a prime ideal of R not intersecting S. In particular, $\mathfrak{q}$ is not $\mathfrak{p}$. Also

$$I \subseteq (S^{-1}\mathfrak{q}) \cap R = \mathfrak{q},$$

contradicting the definition of $\mathfrak{p}$-primary. Thus the claim is established.

So $1 \in S^{-1}I$, which means $1 = b/a^k$ for some $b \in I$ and $k \geq 0$. Thus $a^k = b \in I$.

Suppose, conversely, that I is not $\mathfrak{p}$-primary. Then there is another prime ideal $\mathfrak{q}$ such that $I \subseteq \mathfrak{q}$. Let $a \in \mathfrak{p} \setminus \mathfrak{q}$. Then a^k cannot be in $\mathfrak{q}$, and so cannot be in I. □

Example 4. Let R be a 1-domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. Then $\mathfrak{p}^k$ is a $\mathfrak{p}$-primary ideal for all $k \geq 1$ by the above proposition. Also, any ideal I with $\mathfrak{p}^k \subseteq I \subseteq \mathfrak{p}$ is $\mathfrak{p}$-primary.

Exercise 52. Let R be a 1-domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. Show that the product of two $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.

Proposition 139. *Let R be a 1-domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. If J is a nonzero proper ideal of $R_\mathfrak{p}$ then $J \cap R$ is a $\mathfrak{p}$-primary ideal of R.*

Proof. We have $J \cap R \subseteq (\mathfrak{p}R_\mathfrak{p}) \cap R = \mathfrak{p}$, so we can use the above criterion (Proposition 138). Suppose $a \in \mathfrak{p}$, then $a \in \mathfrak{p}R_\mathfrak{p}$. Clearly all proper nonzero ideals of $R_\mathfrak{p}$ are $\mathfrak{p}R_\mathfrak{p}$-primary, so $a^k \in J$ for some $k \in \mathbb{N}$. Hence $a^k \in J \cap R$. □

Proposition 140. *Let R be a 1-domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. If I is a $\mathfrak{p}$-primary ideal of R and if $\mathfrak{q}$ is a prime ideal not equal to $\mathfrak{p}$ then $IR_\mathfrak{q} = R_\mathfrak{q}$.*

Proof. Since I is not contained in $\mathfrak{q}$, there is an element $a \in I$ not in $\mathfrak{q}$. Observe that a is a unit in $R_\mathfrak{q}$. □

[13] The zero idea 0 of an integral domain is considered to be 0-primary, but we are only interested in nonzero primary ideals here. There is a more elaborate definition of primary ideal and $\mathfrak{p}$-primary ideal for general commutative rings which we will not mention here. We just note that the general definitions of these concepts are equivalent to the definitions given here in the special case of 1-domains.

[14] The result states that the radical of an ideal I is the intersection of prime ideals containing I.

Proposition 141. *Let R be a 1-domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. Then the map $I \mapsto IR_{\mathfrak{p}}$ is an order preserving bijection from the set of $\mathfrak{p}$-primary ideals of R to the set of nonzero proper ideals of $R_{\mathfrak{p}}$. The inverse map is $J \to J \cap R$.*

Proof. Given J a nonzero proper ideal of $R_{\mathfrak{p}}$, we know that $J \cap R$ is a $\mathfrak{p}$-primary ideal of R that maps to J. So the map is surjective.

Suppose that I and I' are $\mathfrak{p}$-primary ideals of R such that $IR_{\mathfrak{p}} = I'R_{\mathfrak{p}}$. For any maximal ideal $\mathfrak{q}$ not equal to $\mathfrak{p}$, we have $IR_{\mathfrak{q}} = R_{\mathfrak{q}} = I'R_{\mathfrak{q}}$ by the previous proposition. Thus, by Corollary 61, $I = I'$. So the map is injective. □

Exercise 53. Let R be a Noetherian 1-domain and let $\mathfrak{p}$ be a nonzero prime ideal of R. Show that I is $\mathfrak{p}$-primary if and only if there is a $k \geq 1$ such that

$$\mathfrak{p}^k \subseteq I \subseteq \mathfrak{p}.$$

Exercise 54. Let R be a 1-integral domain. Let I be a $\mathfrak{p}$-primary ideal where $\mathfrak{p}$ is a maximal ideal of R. Show that there is a ring isomorphism

$$R/I \to R_{\mathfrak{p}}/IR_{\mathfrak{p}}.$$

Hint: $(IR_{\mathfrak{p}}) \cap R = I$. If $s \in R \setminus \mathfrak{p}$, what is $sR + I$?

We are ready for the main factorization theorem. Recall that if R is a Noetherian 1-domain then the number of prime ideals containing any given nonzero ideal is finite (see Lemma 132).

Theorem 142. *Let R be a Noetherian 1-domain. Then every nonzero ideal I can be written as the product of primary ideals. More precisely, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the distinct prime ideals containing I. Then*

$$I = I_1 I_2 \cdots I_k$$

where I_i is $\mathfrak{p}_i$-primary. Moreover, this product is unique.

Proof. For each $\mathfrak{p}_i$ let $I_i = IR_{\mathfrak{p}_i} \cap R$. As we have seen, I_i is $\mathfrak{p}_i$-primary. Now define $I' = I_1 I_2 \cdots I_k$. Observe that, for each i,

$$I'R_{\mathfrak{p}_i} = (I_1 R_{\mathfrak{p}_i}) \cdots (I_k R_{\mathfrak{p}_i}) = I_i R_{\mathfrak{p}_i} = IR_{\mathfrak{p}_i}.$$

For any other nonzero prime ideal $\mathfrak{q}$ of R we have

$$I'R_{\mathfrak{q}} = R_{\mathfrak{q}} = IR_{\mathfrak{q}}.$$

Thus, by Corollary 61, $I' = I$. This establishes existence.

Now suppose $I = I_1' I_2' \cdots I_k'$ where I_i' is $\mathfrak{p}_i$-primary. For each i

$$IR_{\mathfrak{p}_i} = (I_1 R_{\mathfrak{p}_i}) \cdots (I_k R_{\mathfrak{p}_i}) = I_i R_{\mathfrak{p}_i} \qquad IR_{\mathfrak{p}_i} = (I_1' R_{\mathfrak{p}_i}) \cdots (I_k' R_{\mathfrak{p}_i}) = I_i' R_{\mathfrak{p}_i}.$$

By the injectivity of the ideal map on the set of $\mathfrak{p}_i$-primary ideals, we deduce from $I_i R_{\mathfrak{p}_i} = I_i' R_{\mathfrak{p}_i}$ the desired conclusion: $I_i = I_i'$. □

Exercise 55. Let R be a Noetherian 1-domain. Show that every irreducible ideal must be a primary ideal. (An irreducible ideal is a nonzero proper ideal that is not the product of two proper ideals.)

Let I be a $\mathfrak{p}$-primary ideal. Show I is an irreducible ideal of R if and only if $IR_{\mathfrak{p}}$ is an irreducible ideal of $R_{\mathfrak{p}}$. Conclude a $\mathfrak{p}$-primary ideal I of R is an irreducible non-prime ideal if and only if $IR_{\mathfrak{p}}$ is an irreducible non-prime ideal.

Let R be a singular Noetherian 1-domain. Then there must be at least one irreducible non-prime ideal I. This is because factorization into nonzero prime ideals fails for some nonzero ideals, but factorization into irreducible ideals holds (Exercise 22). The above exercise shows that such an irreducible I must be a $\mathfrak{p}$-primary ideal for some prime ideal $\mathfrak{p}$. Also, $IR_{\mathfrak{p}}$ must be an irreducible non-prime ideal by the above exercise, and so $R_{\mathfrak{p}}$ is not a DVR. In other words, $\mathfrak{p}$ is singular. So any irreducible non-prime ideal is $\mathfrak{p}$-primary for some singular prime ideal $\mathfrak{p}$.

Conversely, if $\mathfrak{p}$ is singular, $R_{\mathfrak{p}}$ must have an irreducible non-prime ideal J. There is a unique $\mathfrak{p}$-primary ideal I of R with $IR_{\mathfrak{p}} = J$, and by the above exercise this I an irreducible non-prime ideal.

So when we look for irreducible non-prime ideals, we can focus on the local situation at a singular prime. So from now on we will limit our attention to singular local Noetherian 1-domains, i.e., Noetherian domains with exactly one prime ideal that are not DVRs. The next results shows that we can find irreducible non-prime ideals among the principal ideals:

Proposition 143. *Let R be a singular local Noetherian 1-domain. Let $a \in R$ be a nonzero non-unit element. Then aR is the product of irreducible non-prime ideals.*

Proof. Factor $aR = I_1 \cdots I_k$ where each I_i is irreducible (Exercise 22). Since aR is invertible, each I_i must also be invertible. Thus each I_i is principal (Proposition 35) and can be written as $a_i R$ for some $a_i \in R$. Since R is singular, its maximal ideal is not principal. Thus each $a_i R$ is an irreducible non-prime ideal. □

We can identify another source of irreducible non-prime ideals (there may be overlap between our two categories).

Proposition 144. *Let R be a singular local Noetherian 1-domain with maximal ideal $\mathfrak{m}$. If I is an ideal such that $\mathfrak{m}^2 \subsetneq I \subsetneq \mathfrak{m}$ then I is an irreducible non-prime ideal.*

Proof. Suppose such an I factors as proper ideals: $I = J_1 J_2$. Since $J_i \subseteq \mathfrak{m}$, the product $I = J_1 J_2$ is contained in $\mathfrak{m}^2$, a contradiction. □

Are there ideals I such that $\mathfrak{m}^2 \subsetneq I \subsetneq \mathfrak{m}$? The answer is that there are a lot of them when R is singular. Assume R is a singular local Noetherian 1-domain with maximal ideal $\mathfrak{m}$. Consider $\mathfrak{m}/\mathfrak{m}^2$ which is a vector space over the residue field $R/\mathfrak{m}$ (Exercise 20). Since $\mathfrak{m}$ is a finitely generated, the vector space $\mathfrak{m}/\mathfrak{m}^2$ is finite dimensional. Note that $\mathfrak{m} \neq \mathfrak{m}^2$ by Exercise 15, so $\mathfrak{m}/\mathfrak{m}^2$ has positive dimension. Since R is singular, the dimension cannot be one (Exercise 21). So $\mathfrak{m}/\mathfrak{m}^2$ has dimension at least two. Such vector spaces have multiple proper nonzero subspaces.

There is a one-to-one correspondence between ideals I with $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$ and subspaces of the vector space $\mathfrak{m}/\mathfrak{m}^2$. (See the next appendix for the relationship

between ideals of R containing $\mathfrak{m}^2$ and the ideals of $R/\mathfrak{m}^2$. Note that every vector subspace of $\mathfrak{m}/\mathfrak{m}^2$ is an ideal of $R/\mathfrak{m}^2$.) So we get the following:

Proposition 145. *There are multiple ideals I such that $\mathfrak{m}^2 \subsetneq I \subsetneq \mathfrak{m}$. These are in one-to-one correspondence with the proper, nonzero subspaces of $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$.*

So this gives another source of irreducible non-prime ideals in the local singular case, and hence in the general singular case.

Appendix C: A note on ideals in quotient groups

We have frequently used the correspondence between ideals of an integral domain R and ideals of a localization $S^{-1}R$. Prime ideals are well-behaved under this correspondence. This correspondence is also well-behaved with respect to products (and other operations). In fact the map $I \mapsto S^{-1}I$ yields a surjective homomorphism from the monoid of ideals of R to the monoid of ideals of $S^{-1}R$. We extended this surjection to fractional ideals.

There is a similar correspondence between ideals of a ring R and ideals of a quotient ring R/I. However, this situation is trickier since this correspondence is really two levels of correspondence where each level has properties that the other does not. This discrepancy between the two levels actually gives us a method of finding irreducible ideals that are not prime ideals, which we will use later. For simplicity, we will stick to commutative rings, and we will not attempt to extend the correspondence to fractional ideals.

The purpose of this appendix is introduce the ideal correspondence for quotient rings, which is of key importance in commutative algebra, and to prepare the groundwork for the next appendix on prime ideal factorization.

So let R be a commutative ring and let I be an ideal. As mentioned above, there are two levels to the correspondence between ideals of R and ideals of R/I. At first we will consider only ideals J of R that contain I. In this case, the Abelian group J/I is actually a subset of R/I: for each $a \in J$, the coset $a + I$ as an element of J/I is also a coset appearing as an element of R/I. We will often write this coset as $[a]$. Checking that J/I is an ideal of R/I is straightforward, as are most of the claims of the following:

Proposition 146. *Let I be an ideal of a commutative ring R. Then the natural map $J \mapsto J/I$ is an inclusion preserving bijection from the set of ideals containing I to the set of ideals of R/I. Restricting this bijection to prime ideals yields a bijection from the set of prime ideals containing I to the set of prime ideal of R/I.*

In particular, if R is a local ring with maximal ideal $\mathfrak{m}$, and if I is a proper ideal of R, then R/I is a local ring with maximal ideal $\mathfrak{m}/I$.

Proof. The claims are straightforward. For surjectivity, given $\tilde{J}$ an ideal of R/I consider the following ideal of R:

$$J = \left\{ a \in R \;\middle|\; [a] \in \tilde{J} \right\}.$$

□

This bijection is compatible with ideal operations:

Proposition 147. *Let I be an ideal of a commutative ring R. Then the natural bijection $J \mapsto J/I$ respects the operations of addition and intersection:*

$$(J_1 + J_2)/I = (J_1/I) + (J_2/I), \qquad (J_1 \cap J_2)/I = (J_1/I) \cap (J_2/I).$$

This bijection sends any principal ideal aR containing I to the principal ideal $[a](R/I)$. Finally, if J_1, J_2, and $J_1 J_2$ all contain I then

$$(J_1 J_2)/I = (J_1/I)(J_2/I).$$

Proof. This is straightforward. □

A major limitation of the bijection $J \mapsto J/I$ is that it is not in general a monoid homomorphism with respect to products for the simple reason that the domain is not in general closed under products: just because J_1 and J_2 contain I does not guarantee that $J_1 J_2$ will contain I. (Addition fares better with respect to closure, but note that the additive identity $\{0\}$ is not in general in the domain)

We can fix this problem by expanding this correspondence. This second level of correspondence is based on the following idea: Given a homomorphism $\varphi : R_1 \to R_2$ between rings, if J is an ideal of R_1 we define $\varphi[J]$ to be the image of J under this map. If φ is surjective, then $\varphi[J]$ is seen to be an ideal of R_2.

Proposition 148. *Let I be an ideal of a commutative ring R and let $\varphi\colon R \to R/I$ be the canonical homomorphism $a \mapsto [a]$. Then the map $J \mapsto \varphi[J]$ is an order preserving surjective function from the set of ideals of R to the set of ideals of R/I. This map extends the bijection $J \to J/I$ defined above which was defined only when $I \subseteq J$.*

Given ideals J_1, J_2 of R, we have

$$\varphi[J_1 J_2] = \varphi[J_1]\varphi[J_2], \quad \varphi[J_1 + J_2] = \varphi[J_1] + \varphi[J_2].$$

In fact, $J \mapsto \varphi[J]$ is a surjective homomorphism from the monoid of ideals of R under products to the monoid of ideals of R/I under products. Similarly for the monoids under addition.

In addition, this map sends any principal ideal aR to the principal ideal $[a](R/I)$, and yields a surjection from the monoid of principal ideals of R (under multiplication) to the monoid of principal ideals of R/I.

Proof. This is straightforward. □

Since the second level correspondence is not in general injective, we should address the kernel and the issue of injectivity:

Proposition 149. *Let I be an ideal of a commutative ring R and let $\varphi\colon R \to R/I$ be the canonical homomorphism $a \mapsto [a]$. Under the map $J \mapsto \varphi[J]$, an ideal J maps to zero if and only if $J \subseteq I$. Two ideals J_1 and J_2 map to the same ideal in R/I if and only if $J_1 + I = J_2 + I$.*

If J is an ideal of R, then $I + J$ is the unique ideal J' of R containing I such that $\varphi[J] = \varphi[J']$.

So there are two levels of the correspondence; the first is bijective and the second is only surjective. For some purposes the first correspondence works better, for other purposes the second works better. So both are of use. For example, the first has the advantage that the correspondence is bijective and sends primes ideals to prime ideals. The second has the advantage that it is a monoid homomorphism for ideal multiplication and ideal addition. The second is a surjection for principal ideals, while the first is an injection. The first works better for intersections of ideals.

We will now illustrate how having this difference in properties, especially with respect to products, can be exploited to produce ideals that are irreducible but not prime. (Recall that an ideal is irreducible if it is nonzero and proper, and it cannot be written as the product of two proper ideals. In the previous appendix we gave examples of rings with nonprime irreducible ideals, but these integral domains were not integrally closed. In this appendix we will give examples that include integrally closed integral domains).

Recall that in a Dedekind domain every nonzero ideal is the product of prime ideals, so there is no nonprime irreducible ideals. Since every PID is a Dedekind domain, this property also holds for PIDs as well. Does this happen for most nice integral domains? Consider the polynomial ring $R = F[X, Y]$ in two variables where F is a field. We won't prove it here, but this ring is a UFD and is a fairly well-behaved ring. In particular it is integrally closed. Surprisingly, this ring has nonprime irreducible ideals, and we will prove this. It will be a bit of work, but the construction nicely shows off a lot of the techniques we are interested in. The proof also works in more generality than this particular example, and will work in the context of the rings in the following appendix.

Observe that in our example $R = F[X, Y]$, the quotient $R/\langle X\rangle$ is isomorphic to $F[Y]$ which is a PID, so the ideal $\langle X\rangle$ is prime. These are key properties for our construction. More generally, let R be any integral domain with a nonzero prime ideal $\mathfrak{p}_1$ such that $R/\mathfrak{p}_1$ is a PID, or even a Dedekind domain. Assume that $\mathfrak{p}_2$ is a prime ideal such that $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$, but that $\mathfrak{p}_1$ is not contained in $\mathfrak{p}_2^k$ for some $k \geq 2$, and assume k is minimal with this property. For example, if $R = F[X, Y]$ we could choose $\mathfrak{p}_1 = XR$, $\mathfrak{p}_2 = XR + YR$. We check that $\mathfrak{p}_1$ is not contained in $\mathfrak{p}_2^2$ in this case. In this example, $\mathfrak{p}_2$ is not only prime but is maximal since $R/\mathfrak{p}_2$ is isomorphic to the field F.

Given this general set-up, consider the homomorphism $\varphi : R \to R/\mathfrak{p}_1$. Let $\mathfrak{p}_2'$ be the nonzero prime ideal of $R/\mathfrak{p}_1$ corresponding to $\mathfrak{p}_2$. In other words $\mathfrak{p}_2'$ is $\varphi[\mathfrak{p}_2]$, or equivalently $\mathfrak{p}_2/\mathfrak{p}_1$. Let J' be $(\mathfrak{p}_2')^k$ where $k \geq 2$ is as above. By Proposition 146 there is a unique ideal J of R containing $\mathfrak{p}_1$ which maps to J', and J is a nonzero proper ideal of R. Because of the problems of the correspondence of Proposition 146 mentioned above involving products of ideals, J might not be $\mathfrak{p}_2^k$ as you might expect. On the contrary, J will turn out to be irreducible.

Lemma 150. *The ideal J constructed above is an irreducible ideal in R, but is not a prime ideal.*

Proof. First observe that J is not a prime ideal since J' is not a prime ideal in the Dedekind domain $R/\mathfrak{p}_1$ (see Proposition 146).

Suppose J is reducible in the sense that $J = I_1 I_2$ where I_1, I_2 are proper ideals. Observe $\mathfrak{p}_1 \subseteq J = I_1 I_2 \subseteq I_i$. Let I_1' and I_2' be the respective images in $R/\mathfrak{p}_1$. By the homomorphism property (Proposition 148), $I_1' I_2' = J' = (\mathfrak{p}_2')^k$. We are assuming that $R/\mathfrak{p}_1$ is a Dedekind domain, so $I_1' = (\mathfrak{p}_2')^{l_1}$ and $I_2' = (\mathfrak{p}_2')^{l_2}$ where $l_1 + l_2 = k$ and $l_1, l_2 > 0$ (since I_1', I_2' are proper ideals).

By the injectivity of the correspondence (Proposition 146), we have $I_1 = (\mathfrak{p}_2)^{l_1}$ and $I_2 = (\mathfrak{p}_2)^{l_2}$. So $J = (\mathfrak{p}_2)^k$. In particular, $\mathfrak{p}_1 \subseteq J = \mathfrak{p}_2^k$ contradicting the choice of k. □

Remark. So J is not $\mathfrak{p}_2^k$, but they map to the same ideal in $R/\mathfrak{p}_1$. Thus, by Proposition 149 we have $J = \mathfrak{p}_1 + \mathfrak{p}_2^k$ since J contains $\mathfrak{p}_1$.

Example 5. In our original example with $R = F[X, Y]$, the irreducible ideal produced in our construction is $J = XR + (XR + YR)^2$ which can be written as $XR + Y^2R$ or $\langle X, Y^2 \rangle$.

We summarize our construction:

Theorem 151. *Suppose R is an integral domain with nonzero prime ideals $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$. Suppose that $\mathfrak{p}_1$ is not contained in $\mathfrak{p}_2^k$ for some $k \geq 2$. Finally, suppose $R/\mathfrak{p}_1$ is a Dedekind domain. Then R has an irreducible ideal that is not a prime ideal.*

Corollary 152. *If F is a field, then the polynomial ring $F[X, Y]$ has an irreducible ideal that is not a prime ideal.*

Exercise 56. Show that the polynomial ring $F[X_1, \ldots, X_n]$ has an irreducible ideal that is not a prime ideal where $n \geq 2$ and where F is a field.

Exercise 57. Suppose R is a PID with ideal I. Use Proposition 148 to show that every ideal of R/I is principal.

Exercise 58. Extend the above exercise to Dedekind domains. In other words, show that if I is a nonzero ideal of a Dedekind domain R, then every ideal of R/I is principal.

Hint: Let S consist of all $s \in R$ not in any prime ideal containing I. Is S a multiplicative system? Why is $S^{-1}R$ a PID? You can also take the following standard result as given: If S is a multiplicative system of R disjoint from every maximal ideal containing I, then we have a natural isomorphism

$$R/I \cong S^{-1}R/S^{-1}I.$$

Appendix D: A note on prime ideal factorization

Above we proved that if R is an integral domain such that every nonzero proper ideal is the product of maximal ideals then R is a Dedekind domain (Theorem 127). What if we have an integral domain with the weaker property that every nonzero proper ideal is the product of prime ideals? It turns out that this is enough to give a Dedekind domain. In other words, we can strengthen Theorem 127 by changing the hypothesis where we replace products of maximal ideals with products of prime

ideals, but it will take us some effort even using local methods.[15] Fortunately some of the heavy lifting was done in a previous appendix in the proof of Theorem 151.

To prove the stronger version of Theorem 127 we will switch between integral domains sharing the key property. So it will be useful to label the property:

Definition 19. An integral domain is said to have the *prime ideal factorization* (PIF) property if every nonzero proper ideal is the product of prime ideals.

Our goal, then, is to show that any integral domain with the PIF property is a Dedekind domain. As we have seen, it is often easiest to work first with local integral domains, and leverage the results to arbitrary integral domains. When we work locally in the context of the PIF property, we get a UFD:

Lemma 153. *Any local integral domain R with the PIF property is a UFD.*

Proof. Given a nonzero non-unit $a \in R$, the ideal aR factors as the product of prime ideals: $aR = \mathfrak{p}_1 \cdots \mathfrak{p}_k$. By Proposition 21, each of these prime ideals is invertible. By Proposition 35, each of these invertible prime ideals is actually principal. This means that $a = \pi_1 \cdots \pi_k$ where each π_i is a prime element. (Define a prime element π to be a nonzero element such that πR is a prime ideal).

So every nonzero non-unit element factors as the product of prime elements. It is an easy exercise to show that (1) each prime element is irreducible, and (2) if a nonzero non-unit element has such a prime factorization, then it has a unique factorization into irreducible elements. We conclude that R is a UFD. (See Exercise 51 for the definition of UFD, irreducible, and the meaning of unique here). □

Using what we know about localization and quotient rings, it is straightforward to prove the following.

Lemma 154. *If R is an integral domain with the PIF property, then so is $S^{-1}R$ for any multiplicative system S of R.*

We have a similar result for quotients $R/\mathfrak{p}$.

Lemma 155. *If R is an integral domain with the PIF property, then so is $R/\mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of R.*

Proof. Let J' be a nonzero proper ideal of $R/\mathfrak{p}$. Let J be the ideal of R containing $\mathfrak{p}$ that maps to J' under the bijection in Proposition 146. Since J' is nonzero, it follows that $\mathfrak{p} \subsetneq J$. Also J must be a proper ideal. So use the PIF property to factor J into prime ideals of R:

$$J = \mathfrak{p}_1 \cdots \mathfrak{p}_k.$$

Since $J \subseteq \mathfrak{p}_i$, it follows that $\mathfrak{p} \subsetneq \mathfrak{p}_i$. This implies that $\mathfrak{p}_i'$ is a nonzero prime ideal of $R/\mathfrak{p}$ where $\mathfrak{p}_i'$ is the image (i.e., $\mathfrak{p}_i/\mathfrak{p}$) of $\mathfrak{p}_i$ under the canonical map (see Proposition 146). By the homomorphism property (Proposition 148),

$$J' = \mathfrak{p}_1' \cdots \mathfrak{p}_k'.$$

[15] Paulo Ribenboim attributes this stronger version of Theorem 127 to Matusita. He mentions this in Section 7.1 of his *Classical Theory of Algebraic Numbers* (Springer 2001). In this section Ribenboim gives a short, but tricky proof. It is a non-local proof that uses the quotient ring correspondence (our Proposition 146).

□

Lemma 156. *If R is a UFD then every nonzero principal prime ideal πR is a minimal nonzero prime ideal of R.*

Proof. Let $\mathfrak{p}$ be any nonzero prime ideal contained in the prime ideal πR, and let $a \in \mathfrak{p}$ be a nonzero element. Write $a = \pi_1 \cdots \pi_k$ where π_i are irreducible. Since $a \in \mathfrak{p}$, there is an i such that $\pi_i \in \mathfrak{p}$. So

$$\pi_i R \subseteq \mathfrak{p} \subseteq \pi R.$$

Since π_i is irreducible, π_i and π are associates, so $\pi_i R = \mathfrak{p} = \pi R$. □

Our intermediate goal is to show that a local integral domain with the PIF property is a DVR. The next lemma shows that we just need to show the maximal ideal is principal.

Lemma 157. *Let R be a local integral domain with the PIF property. If the maximal ideal of R is nonzero and principal then R is a DVR.*

Proof. Let πR be the maximal ideal of R. By Lemma 153, R is a UFD. By the above lemma (Lemma 156), πR is the unique nonzero prime ideal of R. Since R has the PIF property, every nonzero proper ideal is a power of πR. This means that every ideal of R is principal. By Corollary 12, R is a DVR. □

Proposition 158. *Let R be a local integral domain with the PIF property that is not a field. Then R is a DVR.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of R. If $\mathfrak{m}$ is principal, we are done by the previous lemma. So we will assume $\mathfrak{m}$ is not principal and derive a contradiction.

By Lemma 153, R is a UFD, and in a UFD every irreducible element is a prime element. Let $a \in \mathfrak{m}$ be nonzero and let π_1 be an irreducible factor of a. So $\pi_1 R$ is a nonzero prime idea, call it $\mathfrak{p}_1$. Observe that $\mathfrak{p}_1 \subsetneq \mathfrak{m}$ since $\mathfrak{m}$ is not principal.

By Lemma 155, the quotient $R/\mathfrak{p}_1$ has the PIF property, and so is a UFD by Lemma 153. The image $\tilde{\mathfrak{m}}$ of $\mathfrak{m}$ in $R/\mathfrak{p}_1$ is a nonzero prime ideal since $\mathfrak{p}_1 \subsetneq \mathfrak{m}$. Let $[b] \in \tilde{\mathfrak{m}}$ be nonzero where $b \in R$. Let $[\pi_2]$ be an irreducible factor of $[b]$, where $\pi_2 \in R$. So $[\pi_2](R/\mathfrak{p}_1)$ is a nonzero prime ideal of $R/\mathfrak{p}_1$.

The ideal $\pi_1 R + \pi_2 R$ maps to $[\pi_2](R/\mathfrak{p}_1)$ under the mapping of Proposition 146. So $\pi_1 R + \pi_2 R$ is a prime ideal of R, call it $\mathfrak{p}_2$.

Let R' be $R_{\mathfrak{p}_2}$ and let $\mathfrak{p}_2'$ be its maximal ideal. So $\mathfrak{p}_2' = \pi_1 R' + \pi_2 R'$. Let $\mathfrak{p}_1'$ be $\pi_1 R'$. By the correspondence between prime ideals of R contained in $\mathfrak{p}_2$ and prime ideals of R', the ideal $\mathfrak{p}_1'$ is a prime ideal and $\mathfrak{p}_1' \subsetneq \mathfrak{p}_2'$. Also note that R' has the PIF property by Lemma 154.

Our goal is to apply Theorem 151 to the ring R' to help derive a contradiction. So we wish to show that $R'/\mathfrak{p}_1'$ is a Dedekind domain. By Lemma 155 this ring has the PIF property. The image of $\mathfrak{p}_2'$ is its unique maximal ideal. Observe $\mathfrak{p}_2'$ is principal with generator $[\pi_2]$ and is nonzero. So, by Lemma 157, the ring $R'/\mathfrak{p}_1'$ is a DVR, and so is a Dedekind domain.

To use Theorem 151, we also wish to show that $\mathfrak{p}_1'$ is not contained in $(\mathfrak{p}_2')^2$. Suppose otherwise. Then

$$\pi_1 R' \subseteq (\pi_1 R' + \pi_2 R')^2 = \pi_1^2 R' + \pi_1\pi_2 R' + \pi_2^2 R',$$

and so $\pi_1 = a\pi_1^2 + b\pi_1\pi_2 + c\pi_2^2$ for some $a, b, c \in R'$. This equation yields the equation $[0] = [c][\pi_2]^2$ in $R'/\mathfrak{p}_1'$. But $[\pi_2]$ is nonzero, so $[c]$ is zero. Thus $c = d\pi_1$ for some $d \in R'$. Dividing both sides of the equation by π_1 yields $1 = a\pi_1 + b\pi_2 + d\pi_2^2$. This shows $1 \in \mathfrak{p}_2'$, a contradiction. Thus we have established that $\mathfrak{p}_1'$ is not contained in $(\mathfrak{p}_2')^2$.

Now we can use Theorem 151 to conclude that R' has an irreducible ideal that is not a prime ideal. This contradicts the fact that R' has the PIF property. □

Lemma 159. *If R is an integral domain with the PIF property, then every nonzero prime of R is maximal.*

Proof. Let $\mathfrak{p}$ be a nonzero prime ideal, and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. By Lemma 154, the ring $R_\mathfrak{m}$ also has the PIF property. By Proposition 158, the ring $R_\mathfrak{m}$ is a DVR. Now $\mathfrak{p}R_\mathfrak{m}$ is a nonzero prime ideal, hence $\mathfrak{p}R_\mathfrak{m} = \mathfrak{m}R_\mathfrak{m}$ since DVRs have a unique nonzero prime ideal. This implies $\mathfrak{p} = \mathfrak{m}$. □

We are now ready to state and prove the stronger version of Theorem 127.

Theorem 160. *Suppose that R is an integral domain such that every nonzero proper ideal factors as the product of prime ideals. Then R is a Dedekind domain.*

Proof. By the previous lemma, we see that every nonzero proper ideal factors as the product of maximal ideals. Then R is a Dedekind domain by Theorem 127. □

Appendix E: Almost Dedekind domains and Prüfer domains

Dedekind domains are both Noetherian and integrally closed. In Appendix B we considered a generalization of Dedekind domains that are not necessarily integrally closed, but are, however, Noetherian. In this appendix we consider generalizations of Dedekind domains that are not necessarily Noetherian, but are, however, integrally closed.

We begin with almost Dedekind domains which we introduced in Section 7.

Definition 20. An *almost Dedekind domain* is an integral domain R with the property that $R_\mathfrak{m}$ is a DVR for all nonzero maximal ideals of R.[16]

Example 6. We won't construct any non-Noetherian almost Dedekind domains here, but they are known to exist. We cite two known examples.

Let K be the algebraic number field generated by pth roots of unity for each prime p. Then the ring of integers in K is a non-Noetherian almost Dedekind domain. This was the first non-Noetherian integral domain R identified as having the property of that $R_\mathfrak{m}$ is a DVR for all nonzero maximal ideals of R (N. Nakano 1953).

[16] I was tempted to call these *locally Dedekind domains*, but the term *almost Dedekind domain* is now standard.

Let K be be the algebraic number field generated by the square roots of p for every prime p. Then the ring of integers in K is a non-Noetherian almost Dedekind domain. (C. Hashbarger 2010)

Remark. The term *almost Dedekind domain* was coined by Robert Gilmer (1964) who pioneered the study of such rings. It is interesting that non-Noetherian almost Dedekind domains exists since they are locally Noetherian but not themselves Noetherian.

Proposition 161. *An almost Dedekind domain is integrally closed and has the property that every non-zero prime ideal is maximal. Thus an almost Dedekind domain is a Dedekind domain if and only if it is Noetherian.*

Proof. Since DVRs are integrally closed and has the property that every non-zero prime ideal is maximal, it follows that almost Dedekind domains must also have these properties. See Proposition 62 and Proposition 63. □

We know that invertible maximal ideals are finitely generated (Section 4). In Exercise 23 we learned that the converse is true for almost Dedekind domains. So we have the following

Proposition 162. *A fractional ideal of an almost Dedekind domain is invertible if and only if it is finitely generated.*

Recall that in Section 12 we defined a cancellation domain to be an integral domain with the property that if $I_1J = I_2J$, where I_1, I_2 and J are nonzero ideals, then $I_1 = I_2$ (Definition 15).

Lemma 163. *Every almost Dedekind domain is a cancellation domain.*

Proof. Suppose $I_1J = I_2J$ where I_1, I_2, J are nonzero ideals of an almost Dedekind domain R. For each maximal ideal $\mathfrak{m}$ we have

$$(I_1R_{\mathfrak{m}})(JR_{\mathfrak{m}}) = (I_2R_{\mathfrak{m}})(JR_{\mathfrak{m}}).$$

Now every nonzero ideal in a DVR has an inverse. Thus $(I_1R_{\mathfrak{m}}) = (I_2R_{\mathfrak{m}})$. This holds for each maximal ideal $\mathfrak{m}$, so $I_1 = I_2$ (Corollary 61). □

The surprise here is that the converse of the above lemma holds:

Lemma 164. *If $\mathfrak{m}$ is a nonzero maximal ideal of a cancellation domain R then $R_{\mathfrak{m}}$ is a DVR.*

Proof. By Exercise 50, $R_{\mathfrak{m}}$ is a valuation ring with principal maximal ideal. Let π be a generator of the maximal idea of $R_{\mathfrak{m}}$. By clearing denominators if necessary we can choose π in R. By Exercise 47,

$$\bigcap_{k=1}^{\infty} \pi^k R = \{0\}.$$

We claim that, furthermore, that

$$\bigcap_{k=1}^{\infty} \pi^k R_{\mathfrak{m}} = \{0\}.$$

To see this let a/s be in this intersection where $a \in R$ and $s \notin \mathfrak{m}$. From the identity $\left(\pi^k R_{\mathfrak{m}}\right) \cap R = \pi^k R$ (see Exercise 48), we get that $a \in \pi^k R$ for all $k \geq 1$. Thus a is in the intersection so $a = 0$. Since $a/s = 0$, this establishes the claim.

This implies that every nonzero element of $R_{\mathfrak{m}}$ is of the form $u\pi^k$ where u is a unit of $R_{\mathfrak{m}}$. By Corollary 10, $R_{\mathfrak{m}}$ is a DVR. □

Combining the previous two lemmas gives us the following;

Theorem 165. *Let R be an integral domain. Then R is a cancellation domain if and only if R is an almost Dedekind domain.*

We address the issue of ideal factorization in an almost Dedekind domain in the next two exercises.

Exercise 59. Show that if a nonzero ideal of an almost Dedekind domain factors as the product of nonzero prime ideals then that factorization is unique.

Exercise 60. Let I be a nonzero proper ideal of an almost Dedekind domain. Show that I factors as the product of nonzero prime ideals if and only if I is contained in only a finite number of maximal ideals. Hint: construct a plausible factorization of I based on images in DVRs and use Corollary 61 to verify it.

Exercise 61. Let R be an almost Dedekind domain. Show that R is a Dedekind domain if and only if every nonzero element of R is contained in only a finite number of maximal ideals.

Hint: Observe that if I is an ideal and if some element $a \in I$ is only contained in a finite number of maximal ideals, then I is contained in only a finite number of maximal ideals. Now use the previous exercise.

By Proposition 162 every nonzero finitely generated ideal of an almost Dedekind domain is invertible. As we saw in Section 4, this is the best result we can hope for in a non-Noetherian ring. This helps motivate the next concept:

Definition 21. A *Prüfer domain* is an integral domain such that every nonzero finitely generated ideal is invertible.

Remark. Prüfer domain are named for Heinz Prüfer who introduced such rings in 1932.

The following three propositions are straightforward given our earlier results.

Proposition 166. *Every almost Dedekind domain is a Prüfer domain.*

Proposition 167. *A Prüfer domain is a Dedekind domain if and only if it is Noetherian.*

Proposition 168. *A fractional ideal of a Prüfer domain is invertible if an only if it is finitely generated.*

Prüfer domains have a cancellation law that is weaker than almost Dedekind domains. This is expressed with the next concept.

Definition 22. A *weak cancellation domain* is an integral domain with the property that for all nonzero ideals I_1 and I_2 and for all finitely generated nonzero ideals J if $I_1J = I_2J$ then $I_1 = I_2$.

From the definition of Prüfer domain we have the following:

Proposition 169. *Every Prüfer domain is a weak cancellation domain.*

Several of the lemmas we proved for cancellation domains (Lemma 119 to Lemma 124) generalize almost immediately to the current setting:

Lemma 170. *Suppose I_1, I_2, and J are fractional ideals of a weak cancellation domain where J is finitely generated. If $I_1J = I_2J$ then $I_1 = I_2$.*

Lemma 171. *Suppose I_1, I_2, and J are fractional ideals of a weak cancellation domain where J is finitely generated. If $I_1J \subseteq I_2J$ then $I_1 \subseteq I_2$.*

Lemma 172. *Suppose $x \in K^\times$ where K is the field of fractions of a weak cancellation domain R. Then $xR \subseteq x^2R + R$.*

Lemma 173. *Suppose $x \in K^\times$ where K is the field of fractions of a weak cancellation domain R. Then $ax^2 + x + b = 0$ for some $a, b \in R$.*

Lemma 174. *Every weak cancellation domain R is integrally closed.*

Lemma 175. *Let R be a weak cancellation domain R with field of fractions K. Let $\mathfrak{p}$ be a prime ideal of R. Then for every $x \in K^\times$ either $x \in R_\mathfrak{p}$ or $x^{-1} \in R_\mathfrak{p}$. In other words, $R_\mathfrak{p}$ is a valuation ring.*

So weak cancellation domains can differ from cancellation domains (i.e., almost Dedekind domains) in that the local rings are valuation rings but not necessarily *discrete* valuation rings.

Lemma 176. *Suppose that R is an integral domain and that $R_\mathfrak{m}$ is a valuation ring for every maximal ideal $\mathfrak{m}$ of R. Then every nonzero finitely generated ideal I is invertible. In other words, R is a Prüfer domain.*

Proof. Assume I is nonzero and finitely generated. Then $IR_\mathfrak{m}$ is nonzero and finitely generated for each maximal ideal $\mathfrak{m}$. By assumption, $R_\mathfrak{m}$ is a valuation ring, and so every finitely generated ideal is principal (Exercise 6). So $IR_\mathfrak{m}$ is principal, and hence invertible by Proposition 35. In particular, if $J = II^{-1}$ then

$$JR_\mathfrak{m} = (IR_\mathfrak{m})(IR_\mathfrak{m})^{-1} = R_\mathfrak{m}$$

(see Proposition 50). This holds for each maximal ideal $\mathfrak{m}$, so $J = R$ (Corollary 61). Thus I is invertible. □

Theorem 177. *Let R be an integral domain. Then R is a Prüfer domain if and only if it is a weak cancellation domain.*

Proof. We have already established one direction (Proposition 169), so let R be a weak cancellation domain. By Lemma 175, $R_{\mathfrak{m}}$ is a valuation ring for every nonzero maximal ideal $\mathfrak{m}$. So by Lemma 176, R is a Prüfer domain □

Theorem 178. *Let R be an integral domain. Then the following are equivalent*

1. *R is a Prüfer domain.*
2. *$R_{\mathfrak{p}}$ is a valuation ring for all prime ideals $\mathfrak{p}$.*
3. *$R_{\mathfrak{m}}$ is a valuation ring for all maximal ideals $\mathfrak{m}$.*

Proof. Note that if $\mathfrak{p}$ is the zero ideal then $R_{\mathfrak{p}}$ is a valuation ring since it is a field.
(1) $\Rightarrow$ (2). This follows from Lemma 175.
(2) $\Rightarrow$ (3). All maximal ideals are prime ideals.
(3) $\Rightarrow$ (1). This follows from Lemma 176 □

We restate Lemma 174 in terms of Prüfer domains.

Theorem 179. *Every Prüfer domain is integrally closed.*

Example 7. The following claim (which we state without proof) shows the importance of Prüfer domains:

Suppose that R is a Prüfer domain with fraction field K, and suppose that L is an algebraic extension of K, then the integral closure of R in L is also a Prüfer domain.

For example, the ring of algebraic integers in the algebraic closure of $\mathbb{Q}$, or in any algebraic extension of $\mathbb{Q}$, is a Prüfer domain.

Exercise 62. Recall that if I and J are ideals in a Dedekind domain then

$$(I+J)(I\cap J)=IJ$$

(see Exercise 29). Suppose that R is an integral domain where this identity holds. Show that if I and J are invertible ideals then so are $I+J$ and $I\cap J$. Conclude that all finitely generated fractional ideals must be invertible. Conclude further that R is a Prüfer domain.

Exercise 63. (1) Why is every valuation ring a Prüfer domain? Because of this fact, every valuation ring is integrally closed by Theorem 179. (2) Give a simple direct proof that every valuation ring is integrally closed (i.e., a proof that does not use the notions of Prüfer domain or weak cancellation domain).

Finally we mention (but do not develop) the ideal of a *Krull domain*. These were introduced by W. Krull in 1931. Suppose $\{v_i\}_{i\in I}$ is a family of discrete valuations of a field K such that, for each $x\in K^\times$ there are only a finite number of $i\in I$ such that $v_i(x)\neq 0$. Then the corresponding intersection intersection of DVRs

$$R=\bigcap_{i\in I}\mathcal{O}_{v_i}$$

is called the *Krull domain* associated to $\{v_i\}_{i\in I}$. An integral domain is called a *Krull domain* if it can be represented as such an intersection for some such $\{v_i\}_{i\in I}$.

Example 8. Every Dedekind domain R is a Krull domain. Here we take $\{v_i\}_{i \in I}$ to be the collection of valuations associated with the set of nonzero prime ideals of R.

If R happens to be a field K, then this gives an empty family. The empty intersection in this case is defined to be just K itself.

Example 9. We won't justify the following, but these examples shows the scope of the notion of a Krull domain:

If R is Noetherian domain then it is a Krull domain if and only if R is integrally closed. However, there are non Noetherian Krull domains. Even Noetherian Krull domains do not have to have the property that every nonzero prime ideal is maximal. If R is a Krull domain, then so is $R[X]$. Every UFD is a Krull domain.

Proposition 180. *Let R be a Krull domain. Then R is integrally closed.*

Proof. Observe that R is the intersection of integrally closed domains, so is integrally closed. □

Appendix F: Another route to unique factorization

We know by Theorem 128 that an integral domain is a Dedekind domain if and only if has the following property: for each nonzero ideal I there is a nonzero ideal J such that IJ is principal. Call this the *principal-complement property*. This property is sometimes used as a route to unique factorization of ideals, and was the main route before the 1920s.

In this appendix we explore a more concrete approach to Theorem 128. More specifically, we show how to derive unique factorization of ideals for rings such as the ring of integers $\mathcal{O}_K$ in an algebraic number field K, assuming that we have somehow established the principal-complement property for $\mathcal{O}_K$ (it doesn't matter how). Our proof of the unique factorization of ideal (Theorem 188) will be low-tech and not require the concepts of Noetherian, fractional ideal, integrally closed, discrete valuation ring, or localization. It does use, however, the concepts of prime and maximal ideal, and the correspondence of ideals for quotient rings (see Proposition 146 in Appendix C), concepts that are fairly ubiquitous in an introductory abstract algebra sequence. (Of course, to establish the principal-complement property in the first place you will certainly need some of the more advanced concepts — certainly the integrally closed property since this is a defining property of $\mathcal{O}_K$.)

As mentioned above, this approach is important from a historical perspective. In fact, before the abstract concept of a Dedekind domain arose with Emmy Noether, proofs of the unique factorization of ideals in $\mathcal{O}_K$, for instance Hurwitz's proof, establish the principal-complement property for $\mathcal{O}_K$ as a step to unique factorization of ideals. Such proofs also exploit the fact that $\mathcal{O}_K/I$ is finite for nonzero ideals I.[17]

In this appendix we will explore this route to unique factorization of ideals in a ring R that has similarities to $\mathcal{O}_K$. So up through Theorem 188 we assume the following:

1. R is an integral domain such that, for each nonzero I, the ring R/I is finite.

[17] See Hilbert's famous *Zahlbericht* of 1897 for an example of this approach. Hilbert states he is following Hurwitz.

2. For every nonzero ideal I of R there is a nonzero ideal J such that IJ is principal.

Now we derive some consequences of these two assumptions:

Proposition 181. *Every nonzero prime ideal $\mathfrak{p}$ of R is a maximal ideal.*

Proof. By assumption on R the quotient ring $R/\mathfrak{p}$ is a finite. However, every finite integral domain is a field (we leave this as an exercise). Thus $\mathfrak{p}$ is maximal. □

Proposition 182. *Every proper nonzero ideal I of R is contained in a prime ideal.*

Proof. By assumption on R, the quotient ring R/I is finite. Thus R/I must have a maximal ideal, which must be a prime ideal. By the correspondence of ideals, this gives a prime ideal of R containing I. □

Proposition 183. *The cancellation law holds in R: if I_1, I_2, J are nonzero ideals such that $I_1J = I_2J$ then $I_1 = I_2$.*

Proof. If J is a nonzero principal ideal, then this is straightforward. In general, let J' be a nonzero ideal such that $JJ' = aR$. Multiply both sides of $I_1J = I_2J$ by J' to get $I_1JJ' = I_2JJ'$. Thus $I_1(Ra) = I_2(Ra)$. Hence $I_1 = I_2$. □

Proposition 184. *Let I and J be nonzero ideals of R. Then $J \subseteq I$ if and only if $I \mid J$.*

Proof. One direction is straightforward, so assume that $J \subseteq I$. First we consider the case where $I = aR$. If $I' = \{b/a \mid b \in J\}$ then it is straightforward to show that I' is an ideal such that $J = (aR)I'$. In general, let I'' be such that II'' is of the form aR. Then $JI'' \subseteq II'' = aR$. As before, there is an I' such that

$$JI'' = (aR)I' = (II'')I' = (II')I''.$$

By cancellation, $J = II'$. □

Proposition 185. *Let $\mathfrak{p}$ be a nonzero prime ideal of R. If I and J are nonzero ideals of R such that $\mathfrak{p} \mid IJ$ then $\mathfrak{p} \mid I$ or $\mathfrak{p} \mid J$.*

Proposition 186. *Let $\mathfrak{p}_1, \mathfrak{p}_2$ be nonzero prime ideals of R. If $\mathfrak{p}_1 \mid \mathfrak{p}_2$ then $\mathfrak{p}_1 = \mathfrak{p}_2$.*

Lemma 187. *If $I \mid J$ but $I \neq J$ then R/I has fewer elements than R/J.*

Proof. This follows from the isomorphism $(R/J)/(I/J) \cong R/I$. □

Theorem 188. *Every nonzero proper ideal I of R is uniquely the product of nonzero prime ideals of R. (Uniqueness is up to order).*

Proof. Let $\mathfrak{p}_1$ be a prime ideal containing I (Proposition 182). Observe that $\mathfrak{p}_1 \mid I$ so $I = \mathfrak{p}_1 I_1$ for some nonzero ideal I_1 (Proposition 184). If $I_1 = R$ we are done. Otherwise, continue by writing $I_1 = \mathfrak{p}_2 I_2$ with $\mathfrak{p}_2$ a prime ideal and I_2 a nonzero ideal. We continue in this way. If, at any point, $I_i = R$ we stop, and have the existence of a prime factorization of I.

We still need to argue that this process stops. Observe that if I_i is a proper ideal then $I_i \neq I_{i+1}$. Otherwise $I_i = \mathfrak{p}_{i+1} I_{i+1} = \mathfrak{p}_{i+1} I_i$, which implies $\mathfrak{p}_{i+1} = R$ by the cancellation law. This contradicts the definition of prime ideal. So, by the above lemma, R/I_{i+1} has fewer elements than R/I_i. Since each R/I_i is finite we must eventually have $I_i = R$.

Finally, we prove uniqueness in the usual way (using Proposition 185, Proposition 186, and the cancellation law). □

The above approach quite simple and appealing, so much so that it is natural to suspect that the primary difficulty in pursuing this route is showing the principal-complement property. How do we establish this property in a relatively concrete manner? There are two approaches that I am aware of. One is related to Gauss's lemma, and was used by Hurwitz in one of his proofs.[18] We will not pursue the Gauss's lemma approach here.[19] The other is related to the finiteness of the class group of $\mathcal{O}_K$.[20] We will not discuss how one would establish this finiteness claim, but will instead show how this finiteness claim can be used to establish the principal-complement property. We will work in a general integral domain R, but of course in practice we have in mind the ring of integers $\mathcal{O}_K$ in an algebraic number field K. (Dedekind domains arising in algebraic geometry typically have infinite class group.) In what follows we will make use of fractional ideals and the notions of Noetherian and integrally closed.

Definition 23. Two fractional ideals I and J in an integral domain R are *equivalent modulo principal ideals* if $I = (xR)J$ for some principal fractional ideal xR.

Remark. If you prefer to just use integral ideals, then I and J are equivalent if and only if $aI = bJ$ for some $a, b \in R$ nonzero.

Proposition 189. *The above relation is an equivalence relation on the set of fractional ideals. Every class contains an integral ideal.*

Lemma 190. *Suppose I_1 and I_2 are fractional ideals that are equivalent modulo principal ideals. Then $I_1 J$ is equivalent to $I_2 J$ for all fractional ideals J.*

[18] See E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen* for a proof which Hecke attributes to Hurwitz, with simplifications he attributes to Steinitz, that uses a basic form of Gauss's lemma (see also Lemma 2 of Hilbert's *Zahlbericht* for the basic form of Gauss's lemma needed). Note: what I am calling "Gauss's lemma" (See Section 11 above) is a generalization of the classical Gauss's lemma for $\mathbb{Z}[X]$ and this generalization is related to Kronecker's theory of forms developed the 19th century.

[19] I can mention that it depends on proving a special case of Gauss's lemma for integrally closed integral domains, and then setting up a polynomial f such that I is the content of f. One then finds another polynomial g such that the content of fg is principal. The desired J is then the content of g.

[20] A proof based on proving the class number is finite is given in *A Classical Introduction to Modern Number Theory*, by K. Ireland and M Rosen. Their approach is also based on results of Hurwitz.

Definition 24. Let R be an integral domain. Let $[I]$ and $[J]$ be equivalence classes under the relation of Definition 23. Then define the product $[I][J]$ as $[IJ]$. This is well-defined by the above lemma. We call the set of such equivalence classes under products the *class monoid of* R.

Proposition 191. *The class monoid of an integral domain R is a commutative monoid with unit $[R]$.*

Theorem 192. *Let R be an integrally closed Noetherian ring whose class monoid R is finite. Then for every ideal I there is an ideal J such that IJ is principal.*

Proof. By finiteness, $[I]^m = [I]^n$ for integers m, n with $0 < m < n$. This means that $I^m = I^n(xR)$ for some principal fractional ideal xR. We can write this as

$$I^m(aR) = I^m I^k(bR)$$

where $k = n - m$, and $a, b \in R$ nonzero such that $x = a/b$. By Exercise 17 we cancel to get $aR = I^k(Rb)$. Let J be $I^{k-1}(Rb)$. □

Remark. This approach is fairly concrete. This proof uses Exercise 17, which in turn uses standard properties resulting from R being integrally closed. Exercise 17 also depends on Exercise 16 which can be established using linear algebra. The proof uses fractional ideals for convenience, but it is easily adapted to an approach that uses integral ideals only. The notion of Noetherian can be replaced by showing directly in $\mathcal{O}_K$ that ideals (and fractional ideals) have a finite $\mathbb{Z}$-basis.

The above result also establishes invertibility of each $[I]$, so the class monoid is seen to be a group. Observe that for a Dedekind domain, the class monoid is just the class group of fractional ideals modulo fractional principal ideals.

Exercise 64. Show that two fractional ideals I and J of an integral domain R are isomorphic as R-modules if and only if they are equivalent modulo principal ideals (Definition 23). So in some sense the class monoid classifies isomorphism types of fractional ideals. As a first step, show that any isomorphism between R-submodules of the fraction field K is of the form $x \mapsto cx$ where $c \in K^\times$.

Hint: if $\varphi : I \to J$ is an isomorphism between R-submodules of K, and if one nonzero value is given, $x_2 = \varphi(x_1)$ say, show that $\varphi(x) = cx$ where $c = x_2/x_1$.