3 Properties of Dedekind domains

In the previous lecture we defined a Dedekind domain as a noetherian domain A that satisfies either of the following equivalent conditions:

- the localizations of A at its nonzero prime ideals are all discrete valuation rings;
- A is integrally closed and has dimension at most one.

In this lecture we will establish several additional properties enjoyed by Dedekind domains, the most significant of which is unique ideal factorization. As we noted last time, a Dedekind domain is typically not a unique factorization domain (this occurs if and only if it is also a principal ideal domain), but its ideals can all be uniquely factored into prime ideals.

3.1 Fractional ideals

Throughout this subsection, A is a noetherian domain (not necessarily a Dedekind domain) and K is its fraction field.

Definition 3.1. A *fractional ideal of* A is a finitely generated A-submodule of K.

Despite the nomenclature, fractional ideals are typically not ideals, because they need not be subsets of A. But they do generalize the notion of an ideal: when A is noetherian the ideals of A are precisely the finitely generated A-submodules of A, and when A is also a domain we can extend this notion to its fraction field. Some authors use the term *integral ideal* to distinguish fractional ideals that are actually ideals but we will not do so.

Remark 3.2. Fractional ideals can be defined more generally in domains that are not necessarily noetherian; in this case they are A-submodules I of K for which there exists an element $r \in A$ such that $rI \subseteq A$. When A is noetherian this coincides with our definition.

Lemma 3.3. *Let A be a noetherian domain with fraction field K, and let $I \subseteq K$ be an A-module. Then I is finitely generated if and only if $aI \subseteq A$ for some nonzero $a \in A$.*

Proof. For the forward implication, if $r_1/s_1, \dots, r_n/s_n$ generate I as an A-module, then $aI \subseteq A$ for $a = s_1 \cdots s_n$. Conversely, if $aI \subseteq A$, then aI is an ideal, hence finitely generated (since A is noetherian), and if $a_1, \dots, a_n$ generate aI then $a_1/a, \dots, a_n/a$ generate I. □

Corollary 3.4. *Every fractional ideal of A can be written in the form $\frac{1}{a}I$, for some nonzero $a \in A$ and ideal I.*

Example 3.5. The set $I = \frac{1}{2}\mathbb{Z} = \{\frac{n}{2} : n \in \mathbb{Z}\}$ is a fractional ideal of $\mathbb{Z}$. As a $\mathbb{Z}$-module it is generated by $1/2 \in \mathbb{Q}$, and we have $2I \subseteq \mathbb{Z}$.

Definition 3.6. A fractional ideal of A if *principal* if it is generated as an A-module by one element. We use (x) or xA to denote the principal fractional ideal generated by $x \in K$.

Like ideals, fractional ideals may be added and multiplied:

$$I + J := (i + j : i \in I, j \in J), \qquad IJ := (ij : i \in I, j \in J).$$

Here the notation (S) means the A-module generated by $S \subseteq K$. As with ideals, we actually have $I + J = \{i + j : i \in I, j \in J\}$, but the ideal IJ is typically not the same as set

$\{ij : i \in I, j \in J\}$, it consists of all finite sums of elements in this set. We also have a new operation, corresponding to division. For any fractional ideals I, J with J nonzero, the set

$$(I : J) := \{x \in K : xJ \subseteq I\}$$

is called a *colon ideal*, or *ideal quotient* of I by J. Note that it is **not** a quotient of A-modules ($2\mathbb{Z}/2\mathbb{Z} = \{0\}$ but $(2\mathbb{Z} : 2\mathbb{Z}) = \mathbb{Z}$), and we do not assume $I \subseteq J$ (or $J \subseteq I$). If $I = (x)$ and $J = (y)$ are principal fractional ideals then $(I : J) = (x/y)$, so colon ideals can be viewed as a generalization of division in $K^\times$.

The colon ideal $(I : J)$ is an A-submodule of K, and it is finitely generated, hence a fractional ideal. This is easy to see when $I, J \subseteq A$: let j be any nonzero element of $J \subseteq A$ and note that $j(I : J) \subseteq I \subseteq A$, so $(I : J)$ is finitely generated, by Lemma 3.3. More generally, choose a and b so that $aI \subseteq A$ and $bJ \subseteq A$. Then $(I : J) = (abI : abJ)$ with $abI, abJ \subseteq A$ and we may apply the same argument.

Definition 3.7. A fractional ideal I is *invertible* if $IJ = A$ for some fractional ideal J.

Lemma 3.8. *A fractional ideal I of A is invertible if and only if $I(A : I) = A$, in which case $(A : I)$ is its unique inverse.*

Proof. We first note that inverses are unique when they exist: if $IJ = A = IJ'$ then $J = JA = JIJ' = AJ' = J'$. Now suppose I is invertible, with $IJ = A$. Then $jI \subseteq A$ for all $j \in J$, so $J \subseteq (A : I)$, and $A = IJ \subseteq I(A : I) \subseteq A$, so $I(A : I) = A$. □

Theorem 3.9. *The set $\mathcal{I}_A$ of invertible fractional ideals of A form an abelian group under multiplication in which the set of nonzero principal fractional ideals is a subgroup.*

Proof. To see that $\mathcal{I}_A$ is an abelian group note that: (1) commutativity and associativity of fractional ideal multiplication follows from the commutativity and associativity of K, (2) inverse exist by definition, and (3) $A = (1)$ is a (necessarily unique) multiplicative identity. Every nonzero principal ideal (a) has an inverse $(1/a)$, and a product of principal ideals is principal, so they form a subgroup. □

Definition 3.10. The group $\mathcal{I}_A$ of invertible fractional ideals of A is the *ideal group* of A. The subgroup of principal fractional ideals is denoted $\mathcal{P}_A$, and the quotient $\mathrm{cl}(A) := \mathcal{I}_A/\mathcal{P}_A$ is the *ideal class group* of A, also called the *Picard group* of A and denoted $\mathrm{Pic}(A)$.[1]

Example 3.11. If A is a DVR with uniformizer π then its nonzero fractional ideals are the principal fractional ideals (π^n) for $n \in \mathbb{Z}$ (including $n < 0$), all of which are invertible. We have $(\pi^m)(\pi^n) = (\pi^{m+n})$, thus the ideal group of A is isomorphic to $\mathbb{Z}$ (under addition). We have $\mathcal{P}_A = \mathcal{I}_A$, since A is a PID, so the ideal class group $\mathrm{cl}(A)$ is the trivial group.

Remark 3.12. The ideal class group of A is trivial if and only if A is a PID and it can thus be viewed as a measure of "how far" the domain A is from being a PID. When A is a Dedekind domain it is equivalently a measure of how far A is from being a UFD.

[1] In general one defines the Picard group of a commutative ring A as the group of isomorphism classes of A-modules that are invertible under tensor product. For noetherian domains the Picard group is canonically isomorphic to the ideal class group we have defined and the two terms may be used interchangeably.

3.2 Fractional ideals under localization

The arithmetic operations $I+J$, IJ, and $(I:J)$ on fractional ideals respect localization.

Lemma 3.13. *Let I and J be fractional ideals of A of a noetherian domain A, and let $\mathfrak{p}$ be a prime ideal of A. Then $I_\mathfrak{p}$ and $J_\mathfrak{p}$ are fractional ideals of $A_\mathfrak{p}$, as are*

$$(I+J)_\mathfrak{p} = I_\mathfrak{p} + J_\mathfrak{p}, \qquad (IJ)_\mathfrak{p} = I_\mathfrak{p}J_\mathfrak{p}, \qquad (I:J)_\mathfrak{p} = (I_\mathfrak{p}:J_\mathfrak{p}).$$

The same applies if we localize with respect to any multiplicative subset S of A.

Proof. We first note that $I_\mathfrak{p} = IA_\mathfrak{p}$ is a finitely generated $A_\mathfrak{p}$-module (by generators of I as an A-module), hence a fractional ideal of $A_\mathfrak{p}$, and similarly for $J_\mathfrak{p}$. We have

$$(I+J)_\mathfrak{p} = (I+J)A_\mathfrak{p} = IA_\mathfrak{p} + JA_\mathfrak{p} = I_\mathfrak{p} + J_\mathfrak{p},$$

where we use the distributive law in K to get $(I+J)A_\mathfrak{p} = IA_\mathfrak{p} + JA_\mathfrak{p}$, and

$$(IJ)_\mathfrak{p} = (IJ)A_\mathfrak{p} = I_\mathfrak{p}J_\mathfrak{p},$$

where we note that $(IJ)A_\mathfrak{p} \subseteq I_\mathfrak{p}J_\mathfrak{p}$ obviously holds and by writing sums of fractions over a common denominator we see that $I_\mathfrak{p}J_\mathfrak{p} \subseteq (IJ)A_\mathfrak{p}$ also holds. Finally

$$(I:J)_\mathfrak{p} = \{x \in K : xJ \subseteq I\}_\mathfrak{p} = \{x \in K : xJ_\mathfrak{p} \subseteq I_\mathfrak{p}\} = (I_\mathfrak{p}:J_\mathfrak{p}).$$

For the last statement, note that no part of our proof depends on the fact that we localized with respect to a multiplicative of the from $A - \mathfrak{p}$ □

Theorem 3.14. *Let I be a fractional ideal of a noetherian domain A. Then I is invertible if and only if its localization at every maximal ideal $\mathfrak{m}$ of A is invertible (equivalently, if and only if its localization at every prime ideal $\mathfrak{p}$ of A is invertible).*

Proof. Suppose I is invertible. Then $I(A:I) = A$, and for any maximal ideal $\mathfrak{m}$ we have $I_\mathfrak{m}(A_\mathfrak{m} : I_\mathfrak{m}) = A_\mathfrak{m}$, by Lemma 3.13, so $I_\mathfrak{m}$ is also invertible.

Now suppose $I_\mathfrak{m}$ is invertible for every maximal ideal $\mathfrak{m}$. Then $I_\mathfrak{m}(A_\mathfrak{m} : I_\mathfrak{m}) = A_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$. Using Lemma 3.13 and $A = \cap_\mathfrak{m} A_\mathfrak{m}$ (see Proposition 2.7) we obtain

$$\bigcap_\mathfrak{m} I_\mathfrak{m}(A_\mathfrak{m} : I_\mathfrak{m}) = \bigcap_\mathfrak{m} A_\mathfrak{m} = A$$
$$\bigcap_\mathfrak{m} (I(A:I))_\mathfrak{m} = A$$
$$I(A:I) = A.$$

Therefore I is invertible. The exact same proof works for prime ideals. □

Corollary 3.15. *In a Dedekind domain every nonzero fractional ideal is invertible.*

Proof. If A is Dedekind then all of its localizations at maximal ideals are DVRs, hence PIDs, and in a PID every nonzero fractional ideal is invertible (see Example 3.11). It follows from Theorem 3.15 that every nonzero fractional ideal of A is invertible. □

An integral domain in which every nonzero ideal is invertible is a Dedekind domain (see Problem Set 2), so this gives another way to define Dedekind domains. Let us also note an equivalent condition that will be useful later.

Lemma 3.16. *A nonzero fractional ideal I in a noetherian local domain A is invertible if and only if it is principal.*

Proof. Nonzero principal fractional ideals are always invertible, so we only need to show the converse. Let I be an invertible fractional ideal, and let $\mathfrak{m}$ be the maximal ideal of A. We have $II^{-1} = A$, so $\sum_{i=1}^{n} a_i b_i = 1$ for some $a_i \in I$ and $b_i \in I^{-1}$, and each $a_i b_i$ lies in II^{-1} and therefore in A. One of the products $a_i b_i$, say $a_1 b_1$, must be a unit (otherwise the sum would lie in $\mathfrak{m}$; in a local ring every non-unit must lie in $\mathfrak{m}$ because there is only one maximal ideal). For every $x \in I$ we have $a_1 b_1 x \subseteq a_1 I$, since $a_1 \in I$ and $b_i x \in A$, and therefore $x \in A_1 I$, since $a_1 b_1$ is a unit, so $I \subseteq (a_1) \subseteq I$ and $I = (a_1)$ is principal. □

Corollary 3.17. *A nonzero fractional ideal in a noetherian domain A is invertible if and only if it is locally principal, that is, its localization at every maximal ideal of A is principal.*

3.3 Unique factorization of ideals in Dedekind domains

Lemma 3.18. *Let x be a nonzero element of a Dedekind domain A. The set of prime ideals that contain x is finite.*

Proof. Let us define two subsets S and T of $\mathcal{I}_A$:

$$S := \{I \in \mathcal{I}_A : (x) \subseteq I \subseteq A\},$$
$$T := \{I \in \mathcal{I}_A : A \subseteq I \subseteq (x^{-1})\}.$$

The sets S and T are non-empty (they both contain A) and partially ordered by inclusion. We have bijections

$$\begin{aligned} \varphi_1 \colon S &\to T & \qquad \varphi_2 \colon T &\to S \\ I &\mapsto I^{-1} & \qquad I &\mapsto xI \end{aligned}$$

with φ_1 order-reversing and φ_2 order-preserving. The composition $\varphi := \varphi_2 \circ \varphi_1$ is thus an order-reversing permutation of S. Since A is noetherian, the set S satisfies the ascending chain condition: every chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals in S is eventually constant. By applying our order-reversing permutation φ we see that S also satisfies the descending chain condition: every chain $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ of ideals in S is eventually constant (and nonzero, since they all contain $x \neq 0$).

Now if x lies in infinitely many distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots$ then

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supseteq \cdots$$

is a descending chain of ideals in S that must stabilize. Thus for n sufficiently large we have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n-1} \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n \subseteq \mathfrak{p}_n.$$

The prime ideal $\mathfrak{p}_n$ contains the product $\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}$, so it must contain one of the factors $\mathfrak{p}_1, \cdots, \mathfrak{p}_{n-1}$ (this is what it means for an ideal to be prime). But this contradicts $\dim A \leq 1$: we cannot have a chain of prime ideals $(0) \subsetneq \mathfrak{p}_i \subsetneq \mathfrak{p}_n$ of length 2 in A. □

Corollary 3.19. *Let I be a nonzero ideal of a Dedekind domain A. The number of prime ideals of A that contain I is finite.*

Proof. Apply Lemma 3.19 to any nonzero $a \in I$. □

Example 3.20. The Dedekind domain $A = \mathbb{C}[t]$ contains uncountably many nonzero prime ideals $\mathfrak{p}_a = (t-a)$, one for each $a \in \mathbb{C}$. But any nonzero $f \in \mathbb{C}[t]$ lies in only finitely many of them, namely the $\mathfrak{p}_a$ for which $f(a) = 0$; equivalently, f has finitely many roots.

Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain A with fraction field K, let I be a fractional ideal of A, and let π be a uniformizer for the discrete valuation ring $A_\mathfrak{p}$. The localization $I_\mathfrak{p}$ is a fractional ideal of $A_\mathfrak{p}$, hence of the form (π^n) for some $n \in \mathbb{Z}$ that does not depend on the choice of π (note that n may be negative). We now extend the valuation $v_\mathfrak{p} \colon K \to \mathbb{Z} \cup \{\infty\}$ to fractional ideals by defining $v_\mathfrak{p}(I) := n$ and $v_\mathfrak{p}((0)) := \infty$; for any $x \in K$ we have $v_\mathfrak{p}((x)) = v_\mathfrak{p}(x)$.

The map $v_\mathfrak{p} \colon \mathcal{I}_A \to \mathbb{Z}$ is a group homomorphism: if $I_\mathfrak{p} = (\pi^m)$ and $J_\mathfrak{p} = (\pi^n)$ then

$$(IJ)_\mathfrak{p} = I_\mathfrak{p} J_\mathfrak{p} = (\pi^m)(\pi^n) = (\pi^{m+n}),$$

so $v_p(IJ) = m+n = v_\mathfrak{p}(I) + v_\mathfrak{p}(J)$. It is order-reversing with respect to the partial ordering on $\mathcal{I}_A$ by inclusion and the total order on $\mathbb{Z}$: for any $I, J \in \mathcal{I}_A$, if $I \subseteq J$ then $v_\mathfrak{p}(I) \geq v_\mathfrak{p}(J)$.

Lemma 3.21. *Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain A. If I is an ideal of A then $v_\mathfrak{p}(I) = 0$ if and only if $\mathfrak{p}$ does not contain I. In particular, if $\mathfrak{q}$ is any nonzero prime ideal different from $\mathfrak{p}$ then $v_\mathfrak{q}(\mathfrak{p}) = v_\mathfrak{p}(\mathfrak{q}) = 0$.*

Proof. If $I \subseteq \mathfrak{p}$ then $v_p(I) \geq v_\mathfrak{p}(\mathfrak{p}) = 1$ is nonzero. If $I \not\subseteq \mathfrak{p}$ then pick $a \in I - \mathfrak{p}$ and note that $0 = v_\mathfrak{p}(a) \geq v_\mathfrak{p}(I) \geq v_\mathfrak{p}(A) = 0$ since $(a) \subseteq I \subseteq A$. The prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ are nonzero, hence maximal (since $\dim A \leq 1$), so neither contains the other and $v_\mathfrak{q}(\mathfrak{p}) = v_\mathfrak{p}(\mathfrak{q}) = 0$. □

Corollary 3.22. *Let A be a Dedekind domain with fraction field K. For each nonzero fractional ideal I we have $v_\mathfrak{p}(I) = 0$ for all but finitely many prime ideals $\mathfrak{p}$. In particular, if $x \in K^\times$ then $v_\mathfrak{p}(x) = 0$ for all but finitely many $\mathfrak{p}$.*

Proof. For $I \subseteq A$ this follows from Corollary 3.20 and Lemma 3.22. For $I \not\subseteq A$ let $I = \frac{1}{a}J$ with $a \in A$ and $J \subseteq A$. Then $v_\mathfrak{p}(I) = v_\mathfrak{p}(J) - v_\mathfrak{p}(a) = 0 - 0 = 0$ for all but finitely many prime ideals $\mathfrak{p}$. This holds in particular for $I = (x)$ with $v_\mathfrak{p}((x)) = v_\mathfrak{p}(x)$ for any $x \in K^\times$. □

Theorem 3.23. *Let A be a Dedekind domain. The ideal group $\mathcal{I}_A$ of A is the free abelian group generated by its nonzero prime ideals $\mathfrak{p}$. The isomorphism*

$$\mathcal{I}_A \simeq \bigoplus_\mathfrak{p} \mathbb{Z}$$

is given by the inverse maps

$$I \mapsto (\dots, v_\mathfrak{p}(I), \dots)$$
$$\prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}} \hookleftarrow (\dots, e_\mathfrak{p}, \dots)$$

Proof. Corollary 3.23 implies that the first map is well defined (the vector associated to $I \in \mathcal{I}_A$ has only finitely many nonzero entries and is thus an element of the direct sum). For each nonzero prime ideal $\mathfrak{p}$, the maps $I \mapsto v_\mathfrak{p}(I)$ and $e_\mathfrak{p} \mapsto \mathfrak{p}^{e_\mathfrak{p}}$ are group homomorphisms, and it follows that the maps in the theorem are both group homomorphisms. To see that the first map is injective, note that if $v_\mathfrak{p}(I) = v_\mathfrak{p}(J)$ then $I_\mathfrak{p} = J_\mathfrak{p}$, and if this holds for

every $\mathfrak{p}$ then $I = \cap_{\mathfrak{p}} I_{\mathfrak{p}} = \cap_{\mathfrak{p}} J_{\mathfrak{p}} = J$, by Corollary 2.8. To see that it is surjective, note that Lemma 3.22 implies that for any vector $(\dots, e_{\mathfrak{p}}, \dots)$ in the image we have

$$v_{\mathfrak{q}}\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}\Big) = \sum_{\mathfrak{p}} e_{\mathfrak{p}} v_{\mathfrak{q}}(\mathfrak{p}) = e_{\mathfrak{q}},$$

and this implies that $\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ is the pre-image of $(\dots, e_{\mathfrak{p}}, \dots)$; this also shows that the second map is the inverse of the first map, which completes the proof. □

Remark 3.24. When A is a DVR, the isomorphism given by Theorem 3.24 is just the discrete valuation map $v_{\mathfrak{p}} \colon \mathcal{I}_A \xrightarrow{\sim} \mathbb{Z}$, where $\mathfrak{p}$ is the unique maximal ideal of A.

Corollary 3.25. *In a Dedekind domain every nonzero fractional ideal I has a unique factorization $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ into nonzero prime ideals $\mathfrak{p}$.*[2]

Remark 3.26. Every integral domain with unique ideal factorization is a Dedekind domain (see Problem Set 2).

The isomorphism of Theorem 3.24 allows us to reinterpret the operations we have defined on fractional ideals. If $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ and $J = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}}$ are nonzero fractional ideals then

$$\begin{aligned} IJ &= \prod \mathfrak{p}^{e_{\mathfrak{p}} + f_{\mathfrak{p}}}, \\ (I : J) &= \prod \mathfrak{p}^{e_{\mathfrak{p}} - f_{\mathfrak{p}}}, \\ I + J &= \prod \mathfrak{p}^{\min(e_{\mathfrak{p}}, f_{\mathfrak{p}})} = \gcd(I, J), \\ I \cap J &= \prod \mathfrak{p}^{\max(e_{\mathfrak{p}}, f_{\mathfrak{p}})} = \operatorname{lcm}(I, J). \end{aligned}$$

and for all $I, J \in \mathcal{I}_A$ we have

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

A key consequence of unique factorization is that $I \subseteq J$ if and only if $e_{\mathfrak{p}} \geq f_{\mathfrak{p}}$ for all $\mathfrak{p}$; this implies that J contains I if and only if J divides I. In any commutative ring, if J divides I (i.e. $JH = I$ for some ideal H) then J contains I (the elements of I are H-linear, hence A-linear, combinations of elements of J and so lie in J), whence the slogan *to divide is to contain*. In a Dedekind domain the converse is also true: *to contain is to divide*. This turns out to be another characteristic property of Dedekind domains (see Problem Set 2).

Given that inclusion and divisibility are equivalent in a Dedekind domain, we may view $I + J$ as the greatest common divisor of I and J (it is the smallest ideal that contains, hence divides, both I and J), and $I \cap J$ as the least common multiple of I and J (it is the largest ideal contained in, hence divisible by, both I and J).[3]

We also note that

$$x \in I \iff (x) \subseteq I \iff v_{\mathfrak{p}}(x) \geq e_{\mathfrak{p}} \text{ for all } \mathfrak{p},$$

(where $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ as above), and therefore

$$I = \{x \in K : v_{\mathfrak{p}}(x) \geq e_{\mathfrak{p}} \text{ for all } \mathfrak{p}\}.$$

We have $I \subseteq A$ if and only if $e_{\mathfrak{p}} \geq 0$ for all $\mathfrak{p}$.

[2] We view $A = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(A)} = \prod_{\mathfrak{p}} \mathfrak{p}^0 = (1)$ as an (empty) product of prime ideals.

[3] It may seem strange at first glance that the greatest common divisor of I and J is the *smallest* ideal dividing I and J, but note that if $A = \mathbb{Z}$ then $\gcd((a), (b)) = \gcd(a, b)$ for any $a, b \in \mathbb{Z}$, so the terminology is consistent (note that bigger numbers generate smaller ideals).

3.4 Representing ideals in a Dedekind domain

Not all Dedekind domains are PIDs; a typical Dedekind domain will contain ideals that require more than one generator. But it turns out that two generators always suffice, and we can even pick one of them arbitrarily. To prove this we need the following lemma, Recall that two ideals I and J are said to be *relatively prime*, or *coprime*, if $I + J = A$.

Lemma 3.27. *Let A be a Dedekind domain and let I and I' be nonzero ideals. There exists an ideal J coprime to I' such that IJ is principal.*

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the nonzero prime ideals dividing I' (a finite list, by Corollary 3.20) For each $\mathfrak{p}_i$ let us choose

$$a_i \in (\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_n)I - \mathfrak{p}_i I.$$

This is clearly possible, since the two products are divisible by different powers of $\mathfrak{p}_i$ and cannot coincide; note that a_i is necessarily nonzero. Now let $a = a_1 + \cdots + a_n \neq 0$. Then $v_{\mathfrak{p}_i}(a) = v_{\mathfrak{p}_i}(a_i) = v_{\mathfrak{p}_i}(I)$ (by the nonarchimedean triangle equality; see Problem Set 1).

The (a) is contained in I and therefore divisible by I (since A is a Dedekind domain), so $(a) = IJ$ for some ideal J. For each $\mathfrak{p}_i$ we have $v_{\mathfrak{p}_i}(J) = v_{\mathfrak{p}_i}(a) - v_{\mathfrak{p}_i}(I) = 0$, so J is coprime to I' and $IJ = (a)$ is principal, as desired. □

One can show that any integral domain satisfying Lemma 3.28 is a Dedekind domain (in fact this remains true even if without the constraint that J and I' are coprime), see Problem Set 2.

Corollary 3.28 (Finite approximation)**.** *Let I be a nonzero fractional ideal in a Dedekind domain A and let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be a finite set of nonzero prime ideals of A. Then I contains an element x for which $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(I)$ for $1 \le i \le n$.*

Proof. Let $I = \frac{1}{s}J$ with $s \in A$ and J an ideal. As in the proof of Lemma 3.28, we can pick $a \in J$ so that $v_{\mathfrak{p}_i}(a) = v_{\mathfrak{p}_i}(J)$ for $1 \le i \le n$. If we now let $x = a/s$ then we have $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(a) - v_{\mathfrak{p}_i}(s) = v_{\mathfrak{p}_i}(J) - v_{\mathfrak{p}_i}(s) = v_{\mathfrak{p}_i}(I)$ for $1 \le i \le n$ as desired. □

Corollary 3.29. *Let I be a nonzero ideal in a Dedekind domain A. Every ideal in the quotient ring A/I is principal.*

Proof. Let $\varphi\colon A \to A/I$ be the quotient map, let $\bar{J}$ be an (A/I)-ideal and let $J := \varphi^{-1}(J)$ be its inverse image; then $I \subseteq J$ and $\bar{J} \simeq J/I$ as (A/I)-modules. By Corollary 3.29 we may choose $a \in J$ so that $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(J)$ for nonzero prime ideals $\mathfrak{p}$ dividing I. We have $v_{\mathfrak{p}}(J) \le v_{\mathfrak{p}}(I)$ for all nonzero prime ideals $\mathfrak{p}$ (since $I \subseteq J$) and

$$v_{\mathfrak{p}}((a) + I) = \begin{cases} \min(v_{\mathfrak{p}}(J), v_{\mathfrak{p}}(I)) = v_{\mathfrak{p}}(J) & \text{if } \mathfrak{p} | I, \\ \min(v_{\mathfrak{p}}(a), 0) = 0 = v_{\mathfrak{p}}(J) & \text{if } \mathfrak{p} \nmid I, \end{cases}$$

so $(a) + I = J$. If follows that $\bar{J} \simeq J/I = ((a) + I)/I = (a)/I \simeq (\varphi(a))$ is principal. □

The converse of Corollary 3.30 also holds; an integral domain whose quotients by nonzero ideals are principal ideal rings is a Dedekind domain (see Problem Set 2).

Definition 3.30. A ring that has only finitely many maximal ideals is called *semilocal*.

Example 3.31. The ring $\mathbb{Z}_{(3)} \cap \mathbb{Z}_{(5)}$ is semilocal, it has just two maximal ideals.

Corollary 3.32. *Every semilocal Dedekind domain is a principal ideal domain.*

Proof. If we let I' be the product of all the prime ideals in A and apply Lemma 3.28 to any ideal I we will necessarily have $J = A$ and $IJ = I$ principal. □

Theorem 3.33. *Let I be a nonzero ideal in a Dedekind domain A and let $a \in I$ be nonzero. Then $I = (a, b)$ for some $b \in I$.*

Proof. We have $(a) \subseteq I$, so I divides (a) and we have $II' = (\alpha)$ for some nonzero ideal I'. By Lemma 3.28 there is an ideal J coprime to I' such that IJ is principal, so let $IJ = (b)$ for some b (which necessarily lies in I). We have $\gcd((a), (b)) = \gcd(II', IJ) = I$, since $\gcd(I', J) = (1)$, and it follows that $I = (a, b)$. □

Theorem 3.34 gives us a convenient way to represent ideals I in the ring of integers of a global field. We can always pick $a \in \mathbb{Z}$ or $a \in \mathbb{F}_q[t]$; we will see in later lectures that there is a natural choice for a (the absolute norm of I). It also gives us yet another characterization of Dedekind domains: they are precisely the integral domains for which the theorem holds.

We end this section with a theorem that summarizes the various equivalent definitions of a Dedekind domain we have seen.

Theorem 3.34. *Let A be an integral domain. The following are equivalent:*

- *A is an integrally closed noetherian ring of dimension at most one.*
- *A is noetherian and its localizations at nonzero prime ideals are DVRs.*
- *Every nonzero ideal in A is invertible.*
- *Every nonzero ideal in A is a (finite) product of prime ideals.*
- *A is noetherian and "to contain is to divide" holds for ideals in A.*
- *For every ideal I in A there is an ideal J in A such that IJ is principal.*
- *Every quotient of A by a nonzero ideal is a principal ideal ring.*
- *For every nonzero ideal I in A and nonzero $a \in I$ we have $I = (a, b)$ for some $b \in I$.*

Proof. See Problem Set 2. □

18.785 Number Theory I
Fall 2016