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 factorization of ideals. As we noted last time, Dedekind domains are typically not unique factorization domains (this occurs if and only if it is also a principal ideal domain), but ideals can be uniquely factored into prime ideals.

3.1 Invertible fractional ideals and the ideal class group

In this section A is a noetherian domain (not necessarily a Dedekind domain) and K is its fraction field. Recall that a fractional ideal of A is a finitely generated A-submodule of K, and if I and J are fractional ideals, so is the colon ideal

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

and we that a fractional ideal I is invertible if $IJ = A$ for some fractional ideal J. The definition of $(A : I)$ implies $I(A : I) \subseteq A$, and Lemma 2.20 implies that I is invertible precisely when this inclusion is an equality, in which case the inverse of I is $(A : I)$.

Ideal multiplication is commutative and associative, thus the set of nonzero fractional ideals of a noetherian domain form an abelian monoid under multiplication with $A = (1)$ as the identity. It follows that the subset of invertible fractional ideals is an abelian group.

Definition 3.1. The *ideal group* $\mathcal{I}_A$ of a noetherian domain A is the group of invertible fractional ideals. Note that, despite the name, elements of $\mathcal{I}_A$ need not be ideals.

Every nonzero principal fractional ideal (x) is invertible (since $(x)^{-1} = (x^{-1})$), and a product of principal fractional ideals is principal (since $(x)(y) = (xy)$), as is the unit ideal (1), thus the set of nonzero principal fractional ideals $\mathcal{P}_A$ is a subgroup of $\mathcal{I}_A$.

Definition 3.2. Let A be a noetherian domain. The quotient $\mathrm{cl}(A) := \mathcal{I}_A/\mathcal{P}_A$ is the *ideal class group* of A; it is also called the *Picard group* of A and denoted $\mathrm{Pic}(A)$.[1]

Example 3.3. If A is a DVR with uniformizer π then its nonzero fractional ideals are the principal fractional ideals (π^n) with $n \in \mathbb{Z}$ (including $n \le 0$). We have $(\pi^m)(\pi^n) = (\pi^{m+n})$, thus the ideal group of A is isomorphic to $\mathbb{Z}$ (under addition). In this case $\mathcal{P}_A = \mathcal{I}_A$ and the ideal class group $\mathrm{cl}(A)$ is trivial.

Remark 3.4. A Dedekind domain is a UFD if and only if its ideal class group is trivial (see Corollary 3.19 below), thus $\mathrm{cl}(A)$ may be viewed as a measure of how far A is from being a UFD. More generally, the ideal class group of an integrally closed noetherian domain A

[1] In general, the Picard group of a commutative ring A as the group of isomorphism classes of A-modules that are invertible under tensor product (equivalently, projective modules of rank one). When A is a noetherian domain, the Picard group of A is canonically isomorphic to the ideal class group of A and the two notions may be used interchangeably.

is trivial when A is a UFD, and the converse holds if one replaces the ideal class group with the *divisor class group*. One defines a divisor as an equivalence class of fractional ideals modulo the equivalence relation $I \sim J \Leftrightarrow (A : I) = (A : J)$, and in an integrally closed noetherian domain A (or more generally, a Krull domain), the set of divisors forms a group that contains principal divisors as a subgroup; the divisor class group is defined as the quotient, and it is trivial if and only if A is a UFD (this holds more generally for any Krull domain, see [2, Thm. 8.34]). In a Dedekind domain, fractional ideals are always distinct as divisors and every nonzero fractional ideal is invertible, so the ideal class group and divisor class group coincide.[2]

3.2 Invertible ideals in Dedekind domains

In order to prove that every nonzero fractional ideal in a Dedekind domain is invertible, we first note that arithmetic of fractional ideals behaves well under localization.

Lemma 3.5. *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. $I_\mathfrak{p} = IA_\mathfrak{p}$ is a finitely generated $A_\mathfrak{p}$-module (since I is a finitely generated A-module; see Remark 2.2), 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 $(I+J)A_\mathfrak{p} = IA_\mathfrak{p} + JA_\mathfrak{p}$. We also have

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

since $(IJ)A_\mathfrak{p} \subseteq I_\mathfrak{p} J_\mathfrak{p}$ obviously holds and by writing sums of fractions over a common denominator we can 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 set of the from $A - \mathfrak{p}$. □

Theorem 3.6. *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 of A is invertible, equivalently, if and only if its localization at every prime ideal 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 3.5, 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 $\mathfrak{m}$. Applying Lemma 3.5 and Proposition 2.6 yields

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

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

[2] In general, the divisor class group and the ideal class group (or Picard group) of an integrally closed noetherian domain A may differ when $\dim A > 1$; see [1, Thm. 19.38] for a dimension 2 an example in which the ideal class group is trivial but the divisor class group is not (implying that A is not a UFD).

Corollary 3.7. *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. It follows from Theorem 3.6 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 in later lectures.

Lemma 3.8. *A nonzero fractional ideal I in a noetherian local domain A is invertible if and only if it is principal.*

Proof. If I is principal then it is 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 $II^{-1} = A$. One of the products $a_i b_i$, say $a_1 b_1$, must be a unit, otherwise the sum would not be a unit (note that $A = \mathfrak{m} \sqcup A^\times$, since A is a local ring). For every $x \in I$ we have $a_1 b_1 x \in (a_1)$, since $b_1 x \in A$ (because $x \in I$ and $b_1 \in I^{-1}$). It follows that $x = (a_1 b_1)^{-1} a_1 b_1 x \in (a_1)$, since $(a_1 b_1)^{-1} \in A$, so we have $I \subseteq (a_1) \subseteq I$, which shows that $I = (a_1)$ is principal. □

Corollary 3.9. *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

We are now ready to prove the main result of this lecture, that every nonzero ideal in a Dedekind domain has a unique factorization into prime ideals. As a first step we need to show that every ideal is contained in only finitely many prime ideals.

Lemma 3.10. *Let A be a Dedekind domain and let $a \in A$ be nonzero. The set of prime ideals that contain a is finite.*

Proof. Consider the following subsets S and T of the ideal group $\mathcal{I}_A$:

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

The sets S and T are both non-empty (they contain A) and partially ordered by inclusion. The elements of S are all ideals, and we have bijections

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

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.

Now if a 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

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

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 3.11. *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 3.10 to any nonzero $a \in I$. □

Example 3.12. The Dedekind domain $A = \mathbb{C}[t]$ contains uncountably many nonzero prime ideals $\mathfrak{p}_r = (t - r)$, one for each $r \in \mathbb{C}$. But any nonzero $f \in \mathbb{C}[t]$ lies in only finitely many of them, namely, the $\mathfrak{p}_r$ for which $f(r) = 0$; equivalently, f has finitely many roots.

Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain A with fraction field K, let π be a uniformizer for the discrete valuation ring $A_\mathfrak{p}$, and let I be a nonzero fractional ideal of A. The localization $I_\mathfrak{p}$ is a nonzero 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 3.13. *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 3.14. *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 3.11 and Lemma 3.13. 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 $I = (x)$, for any $x \in K^\times$. □

We are now ready to prove our main theorem.

Theorem 3.15. *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

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

Proof. Corollary 3.14 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 2.7. To see that it is surjective, note that Lemma 3.13 implies that for any vector $(\dots, e_{\mathfrak{p}}, \dots)$ in the image we have

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

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

Remark 3.16. When A is a DVR, the isomorphism given by Theorem 3.15 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 3.17. *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 $\mathfrak{p}$.*[3]

Remark 3.18. Every integral domain with unique ideal factorization is a Dedekind domain (see Problem Set 2).

The isomorphism of Theorem 3.15 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. Recall that 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 leads to another characterization of Dedekind domains (see Problem Set 2).

[3] 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.

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).[4]

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 $\mathfrak{p}$.

Corollary 3.19. *A Dedekind domain is a UFD if and only if it is a PID, equivalently, if and only if its class group is trivial.*

Proof. Every PID is a UFD, so we only need to prove the reverse implication. The fact that we have unique factorization of ideals implies that it is enough to to show that every prime ideal is principal. Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain A that is also a UFD, let $a \in \mathfrak{p}$ nonzero, and let $a = p_1 \cdots p_n$ be the unique factorization of a into irreducible elements. Now $\mathfrak{p}$ contains and therefore divides $(a) = (p_1) \cdots (p_n)$, so $\mathfrak{p}$ divides (and therefore contains) some (p_i), which is necessarily a prime ideal (in a UFD, irreducible elements generate prime ideals). But A has dimension one, so we must have $\mathfrak{p} = (p_i)$. □

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 A-ideals I and J are said to be *relatively prime*, or *coprime*, if $I + J = A$; equivalently, $\gcd(I, J) = (1)$.

Lemma 3.20. *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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the nonzero prime ideals dividing I' (a finite list, by Corollary 3.11). For $1 \leq i \leq n$ define the ideal $\mathfrak{a}_i := \mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_n$ and choose $a_i \in I$ so that

$$a_i \in \mathfrak{a}_i I \qquad \text{and} \qquad a_i \notin \mathfrak{p}_i I.$$

Note that $\mathfrak{a}_i I \cap \mathfrak{p}_i I \subsetneq \mathfrak{a}_i I$ because $v_{\mathfrak{p}_i}(\mathfrak{a}_i I \cap \mathfrak{p}_i I) = v_{\mathfrak{p}_i}(\mathfrak{p}_i I) > v_{\mathfrak{p}_i}(I) = v_{\mathfrak{p}_i}(\mathfrak{a}_i I)$, so such an a_i exists. Each a_i is necessarily nonzero, and satisfies $v_{\mathfrak{p}_i}(a) = v_{\mathfrak{p}_i}(I)$ since

$$v_{\mathfrak{p}_i}(a_i) \geq v_{\mathfrak{p}_i}(\mathfrak{a}_i I) = v_{\mathfrak{p}_i}(I) \qquad \text{and} \qquad v_{\mathfrak{p}_i}(a_i) < v_{\mathfrak{p}_i}(\mathfrak{p}_i I) = v_{\mathfrak{p}_i}(I) + 1,$$

and for $j \neq i$ we have $v_{\mathfrak{p}_j}(a_i) \geq v_{\mathfrak{p}_j}(\mathfrak{p}_j I) > v_{\mathfrak{p}_j}(I)$. We now define $a := a_1 + \cdots + a_n$, so that $v_{\mathfrak{p}_i}(a) = v_{\mathfrak{p}_i}(a_i) = v_{\mathfrak{p}_i}(I)$ for $1 \leq i \leq n$ (by the nonarchimedean triangle equality; see Problem Set 1). We thus have $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(I)$ for all prime ideals $\mathfrak{p}|I'$.

Now (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 prime ideal $\mathfrak{p}|I'$ we have $v_{\mathfrak{p}}(J) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(I) = 0$, so J is coprime to I', and $IJ = (a)$ is principal as desired. □

[4] 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).

One can show that every integral domain satisfying Lemma 3.20 is a Dedekind domain (see Problem Set 2).

Corollary 3.21 (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 3.20, 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 3.22. *Let I be a nonzero ideal in a Dedekind domain A. The quotient ring A/I is a principal ideal ring (every ideal in 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 in A; then $I \subseteq J$, and $\bar{J} \simeq J/I$ as (A/I)-modules. By Corollary 3.21 we may choose $a \in J$ so that $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(J)$ for all nonzero prime ideals $\mathfrak{p}|I$. For every nonzero prime ideal $\mathfrak{p}$ we then have $v_{\mathfrak{p}}(J) \le v_{\mathfrak{p}}(I)$ and

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

so $(a) + I = J$ (here we are using unique factorization of ideals; in a Dedekind domain two ideals with the same valuation at every nonzero prime ideal must be equal). If follows that $\bar{J} \simeq J/I = ((a)+I)/I = \varphi((a)) = (\varphi(a))$ is principal. □

The converse of Corollary 3.22 also holds; an integral domain whose quotients by nonzero ideals are principal ideal rings is a Dedekind domain (see Problem Set 2).

Definition 3.23. A ring that has only finitely many maximal ideals is called *semilocal*.

Example 3.24. The ring $\mathbb{Z}_{(3)} \cap \mathbb{Z}_{(5)}$ is semilocal, it has just two maximal ideals.

Corollary 3.25. *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 3.20 to any ideal I we will necessarily have $J = A$ and $IJ = I$ principal. □

Theorem 3.26. *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 3.20 there is an ideal J coprime to I' such that IJ is principal, so $IJ = (b)$ for some $b \in I$. We have $\gcd((a),(b)) = \gcd(II', IJ) = I$, since $\gcd(I', J) = (1)$, and it follows that $I = (a, b)$. □

Theorem 3.26 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 Theorem 3.26 holds.

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

Theorem 3.27. *Let A be an integral domain. The following are equivalent:*

- *A is an integrally closed noetherian domain 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. □

References

[1] Pete L. Clark, *Commutative algebra*, 2015.

[2] Max D. Larsen and Paul J. McCarthy, *Multiplicative thoery of ideals*, Academic Press, 1971.

18.785 Number Theory I
Fall 2019