3 Unique factorization of ideals in Dedekind domains

3.1 Fractional ideals

Throughout this subsection, A is a noetherian 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 not necessarily ideals, because they need not be subsets of A. But they do generalize the notion of an ideal: in a noetherian domain an ideal is a finitely generated A-submodule of $A \subseteq K$. Some authors use the term *integral ideal* to distinguish fractional ideals that are actually ideals.

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 exist 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 $r_1/s_1, \ldots, r_n/s_n$ are fractions whose equivalence classes generate I as an A-module, then $aI \subseteq A$ for $a = s_1 \cdots s_n$. For the reverse implication, if $aI \subseteq A$, then aI is an ideal, hence finite generated (since A is noetherian), and if $a_1, \ldots, a_n$ generate aI then $a_1/a, \ldots, a_n/a$ generate I. □

Corollary 3.4. *Every fractional ideal of A can be written as $\frac{1}{a}I$, where $a \in A$ is nonzero and I is an ideal.*

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 *principal fractional ideal* is a fractional ideal with a single generator. For any $x \in K$ we use (x) or xA to denote the principal fractional ideal generated by x.

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 $S \subseteq K$. In the case of $I + J$ this is just the set of sums $i + j$, but IJ is typically not the set of products ij, it is the set of all finite sums of such products. We also have a new operation, corresponding to division. For any nonzero fractional ideal J, the set

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

is called a *colon ideal*, or *generalized ideal quotient* of I by J (but note that J need not be contained in I, so $(I : J)$ is typically not a quotient of A-modules). If $I = (x)$ and $J = (y)$ are principal fractional ideals then $(I : J) = (x/y)$, so it 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 previous case.

Lecture by Andrew Sutherland

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 $J \subseteq (A : I)$. Now $A = IJ \subseteq I(A : I) \subseteq A$, so $I(A : I) = A$. □

Theorem 3.9. *The invertible fractional ideals of A form an abelian group under multiplication in which the nonzero principal fractional ideals form a subgroup.*

Proof. This first statement is immediate: multiplication is commutative and associative, inverses exist by definition, and $A = (1)$ is the 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 $\operatorname{cl}(A) := \mathcal{I}_A/\mathcal{P}_A$ is the *ideal class group*.

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 also note that $(\pi^m) + (\pi^n) = (\pi^{\min(m,n)})$. The ideal class group of A is trivial, since A is necessarily a PID.

3.2 Fractional ideals under localization

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

Lemma 3.12. *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 $A_\mathfrak{p}$ and*

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

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

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

Similarly,

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

where we note that in the fraction field of a domain and can put sums of fractions over a common denominator to get $I_\mathfrak{p} J_\mathfrak{p} \subseteq (IJ)A_\mathfrak{p}$ (the reverse containment is clear). Finally

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

Theorem 3.13. *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. Assume I is an 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 3.12, so $I_\mathfrak{m}$ is also invertible.

To prove the converse, suppose every $I_\mathfrak{m}$ is invertible. Then $I_\mathfrak{m}(A_\mathfrak{m}:I_\mathfrak{m})=A_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$. Applying Lemma 3.12 and the fact that $A=\cap_\mathfrak{m}A_\mathfrak{m}$ (see Proposition 2.8) we have

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

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

Corollary 3.14. *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, and in a DVR every fractional ideal is principle, hence invertible (see Example 3.11). It follows from Theorem 3.13 that every fractional ideal of A is invertible. □

One can show that an integral domain in which every nonzero ideal is invertible is a Dedekind domain (see Problem Set 2), which gives another way to define Dedekind domains.

Let us also note an equivalent condition.

Lemma 3.15. *A nonzero factional ideal I in a 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 $\sum_{i=1}^n a_ib_i=1$ for some $a_i\in I$ and $b_i\in I^{-1}$, and each a_ib_i lies in II^{-1} and therefore in A. One of the products a_ib_i, say a_1b_1, must be a unit (otherwise the sum would lie in $\mathfrak{m}$). For every $x\in I$ we have $x=a_1b_1x\subseteq a_1I$, since $b_ix\in A$, so $I\subseteq(a_1)\subseteq I$, thus $I=(a_1)$ is principal. □

Corollary 3.16. *A 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 3.17. *Let x be a nonzero element of a Dedekind domain A. Then the number of prime ideals that contain x is finite.*

Proof. Define subsets S and T of $\mathcal{I}_A$:

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

where S and T are partially ordered by inclusion. We then have bijections

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

with φ_1 order-reversing and φ_2 order-preserving. The composition $\varphi := \varphi_2 \circ \varphi_1$ is then an order-reversing permutation of S. Since A is noetherian, every ascending chain of ideals containing (x) eventually stabilizes, and after applying our order-reversing permutation this implies that every descending chain of ideals containing (x) stabilizes.

Now suppose for the sake of contradiction that x lies in infinitely many distinct nonzero prime ideals $\mathfrak{p}_i$. 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 that must stabilize. For any sufficiently large n we must have

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

Now $\mathfrak{p}_n$ is prime, so it must contain one of the nonzero prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_{n-1}$. This is a contradiction because $\dim A \le 1$, so we cannot have a chain $(0) \subsetneq \mathfrak{p}_i \subsetneq \mathfrak{p}_n$. □

Corollary 3.18. *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 3.17 to a nonzero $a \in I$. □

Example 3.19. 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 and let π be a uniformizer for the discrete valuation ring $A_\mathfrak{p}$. For each nonzero fractional ideal I of A, its 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 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 also order-reversing with respect to the partial ordering of $\mathcal{I}_A$ given by containment and the total order on $\mathbb{Z}$.

Lemma 3.20. *Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain A. For all $I, J \in \mathcal{I}_A$, if $I \subseteq J$ then $v_\mathfrak{p}(I) \ge v_\mathfrak{p}(J)$.*

Proof. Let π be a uniformizer for $A_\mathfrak{p}$, and let $I_\mathfrak{p} = (\pi^m)$ and $J_\mathfrak{p} = (\pi^n)$, where $m = v_\mathfrak{p}(I)$ and $n = v_\mathfrak{p}(J)$. If $I \subseteq J$, then $I_\mathfrak{p} \subseteq J_\mathfrak{p}$ and therefore $m \ge n$. □

Corollary 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, and 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 $v_p(I) \ge v_\mathfrak{p}(\mathfrak{p}) = 1$ is nonzero. If $I \not\subseteq \mathfrak{p}$ then pick $a \in I - \mathfrak{p}$ and note that $0 = v_\mathfrak{p}(a) \ge v_\mathfrak{p}(I) \ge v_\mathfrak{p}(A) = 0$ since $(a) \subseteq I \subseteq A$. For the second statement, note that $\mathfrak{p}$ and $\mathfrak{q}$ must both be maximal ideals, since $\dim A \le 1$, so neither contains the other. □

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 immediately from Corollaries 3.18 and 3.21. If $I \not\subseteq A$ then write I as $\frac{1}{a}J$ 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 $\mathfrak{p}$. $\square$

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 $\mathfrak{p}$, and the isomorphism*

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

is given by the inverse maps

$$\begin{aligned} I &\mapsto (\ldots, v_\mathfrak{p}(I), \ldots) \\ \prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}} &\leftarrow\!\shortmid (\ldots, e_\mathfrak{p}, \ldots) \end{aligned}$$

Proof. Corollary 3.22 implies that the first map is well defined (the vector associated to each $I \in \mathcal{I}_A$ has only finitely many nonzero entries, thus it is an element of the direct sum). For each $\mathfrak{p}$ 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 2.9. To see that it is surjective, note that Corollary 3.21 implies that for any $(\ldots, e_\mathfrak{p}, \ldots)$ 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 $(\ldots, e_\mathfrak{p}, \ldots)$; this also shows that the second map is the inverse of the first map. $\square$

Remark 3.24. When A is a DVR, the isomorphism given by Theorem 3.23 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 prime ideals.*

Conversely, one can show that an integral domain in which every nonzero proper ideal has a unique factorization into prime ideals is a Dedekind domain (see Problem Set 2), so this gives yet another way to define a Dedekind domain.

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

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

Another 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. It is generally true that if one nonzero ideals divides another than it contains it, but in a Dedekind domain the converse also holds: *to contain is to divide.* We also note that

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

thus

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

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

3.4 Approximation theorems

The weak approximation theorem is a general result about field valuations that is useful in many contexts.

Theorem 3.26 (Weak Approximation)**.** *Let K be a field and let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent nontrivial absolute values on K. Let $a_1, \ldots, a_n \in K$ and let $\epsilon_1, \ldots, \epsilon_n$ be positive real numbers. Then there exists an $x \in K$ such that $|x - a_i|_i < \epsilon_i$ for $1 \leq i \leq n$.*

Proof. See Problem Set 2. □

The strong approximation theorem is a stronger version of the weak approximation theorem that is specific to global fields; recall that a global field is any finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$; see [1] for an axiomatic characterization of global fields.

Theorem 3.27 (Strong Approximation)**.** *Let K be a global field, and let $|\cdot|_0, |\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent nontrivial absolute values on K. Let $a_1, \ldots, a_n \in K$ and let $\epsilon_1, \ldots, \epsilon_n$ be positive real numbers. Then there exists an $x \in K$ such that $|x - a_i|_i < \epsilon_i$ for $1 \leq i \leq n$ and $|x| \leq 1$ for all absolute values $|\cdot|$ that are not equivalent to any of $|\cdot|_0, |\cdot|_1, \ldots, |\cdot|_n$.*

The strong approximation theorem applies to fewer fields than the weak approximation theorem, but it imposes a constraint for all but one equivalence class of absolute values, whereas the weak approximation theorem constrains only a finitely many.

Example 3.28. Let $K = \mathbb{Q}$ and let $|\cdot|_0$ be the usual archimedean absolute value on $\mathbb{Q}$. Then there exists $x \in \mathbb{Q}$ such that $|x - 17|_2 \leq 2^{-10}$, $|x - 5|_3 \leq 3^{-100}$, $|x - 42| \leq 5^{-1000}$ and $|x|_p \leq 1$ for all finite primes p. The last constraint implies that $x \in \cap_p \mathbb{Z}_{(p)} = \mathbb{Z}$, while the first three imply $x \equiv 17 \bmod 2^{10}$, and $x \equiv 5 \bmod 3^{100}$, and $x \equiv 42 \bmod 5^{1000}$. The Chinese Remainder Theorem implies that such an integer x actually exists. But notice that the more tightly we constrain the p-adic valuations of $x \in \mathbb{Z}$, the larger we may need to make x, which is why it is important that we do not constrain $|x|_0$. Alternatively, if we put $|\cdot|_0 = |\cdot|_p$ for some finite prime p, then we can constrain the archimedean valuation of x, at the cost of permitting x to have a denominator that may be a very large power of p.

We will prove the strong approximation theorem in a later lecture; for now we will just prove a "pretty strong" approximation theorem that suffices for our immediate needs; it constrains the absolute value of x at all *finite places* (equivalence classes of absolute values arising from the valuation associated to a prime ideal), which is all but finitely many of them. When K is $\mathbb{Q}$ or $\mathbb{F}_q(t)$ there is only one infinite place, but in general there may be several infinite places (up to the degree of K over $\mathbb{Q}$ or $\mathbb{F}_q(t)$).

Theorem 3.29 (Pretty Strong Approximation). *Let A be a Dedekind domain with fraction field K. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct nonzero primes of A, let $a_1, \ldots, a_n \in K$, and let $e_1, \ldots, e_n \in \mathbb{Z}$. Then there exists $x \in K$ such that*

$$v_{\mathfrak{p}_i}(x - a_i) \geq e_i \quad (1 \leq i \leq n)$$

and $v_{\mathfrak{q}}(x) \geq 0$ for all $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Proof. We can assume $n > 1$ (if $n = 1$ let $a_2 = 0$ and $e_2 = 0$ and use $n = 2$), and we can assume $e_i > 0$ for all i, since this only makes the theorem stronger. We consider 3 cases:

Case 1: $a_1, \ldots, a_n \in A$ with all but a_1 equal to zero. The ideals $\mathfrak{p}_1^{e_1}$ and $\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n}$ are relatively prime, so we can write $a_1 = y + x$ with $y \in \mathfrak{p}_1^{e_1}$ and $x \in \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n}$. Then $v_{\mathfrak{p}_1}(x - a_1) = v_{\mathfrak{p}_1}(y) = e_1$ and $v_{\mathfrak{p}_i}(x - a_i) = v_{\mathfrak{p}_i}(x) = e_i$ for $2 \leq i \leq n$, since $a_i = 0$. And $x \in A$, so $v_{\mathfrak{q}}(x) \geq 0$ for all primes $\mathfrak{q}$, thus the theorem holds.

Case 2: $a_1, \ldots, a_n \in A$. Use case 1 to approximate $(a_1, 0, \ldots, 0)$ by x_1, $(0, a_2, 0, \ldots, 0)$ by x_2, $\ldots$, and $(0, \ldots, 0, a_n)$ by x_n, using the same $e_1, \ldots, e_n$ in each case. By the triangle inequality, $x = x_1 + \cdots + x_n$ satisfies the theorem.

Case 3: $a_1, \ldots, a_n \in K$. Write $a_i = b_i/s$ with $b_i, s \in A$. Use case 2 to obtain $y \in A$ such that $v_{\mathfrak{p}_i}(y - b_i) \geq e_i + v_{\mathfrak{p}_i}(s)$ and $v_q(y) \geq v_q(s)$ for all other primes $\mathfrak{q}$ (note that $v_{\mathfrak{q}}(s) = 0$ for all but finitely many $\mathfrak{q}$). Then $x = y/s$ satisfies the theorem. ☐

Corollary 3.30. *Let A be a Dedekind domain with fraction field K and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be nonzero primes of A. For any $e_1, \ldots, e_n \in \mathbb{Z}$ there exists $x \in K$ with $v_{\mathfrak{p}_i}(x) = e_i$ for $1 \leq i \leq n$ and $v_{\mathfrak{q}}(x) \geq 0$ for all primes $\mathfrak{q} \notin \{\mathfrak{p}_i\}$.*

Proof. Let $a_i = \mathfrak{p}_i^{e_i}$ and apply the theorem to $a_1, \ldots, a_n$ and $e_1 + 1, \ldots, e_n + 1$ to get $x \in K$ with $v_{\mathfrak{p}_i}(x - a_i) \geq e_i + 1$ for $1 \leq i \leq n$ and $v_{\mathfrak{q}}(x) \geq 0$ for $\mathfrak{q} \notin \{\mathfrak{p}_i\}$. We must then have $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(a_i) = e_i$, since if they differed then the nonarchimedean "triangle equality" would imply

$$v_{\mathfrak{p}_i}(x - a_i) = \min(v_{\mathfrak{p}_i}(x), v_{\mathfrak{p}_i}(-a_i)) = \min(v_{\mathfrak{p}_i}(x), v_{\mathfrak{p}_i}(a_i)) \leq e_i.$$ ☐

Definition 3.31. A ring that has only finitely many maximal ideals is called *semilocal.*

Example 3.32. The ring $\mathbb{Z}_{(3)} \cap \mathbb{Z}_{(5)}$ is semilocal, it has just two maximal ideals.

Corollary 3.33. *A semilocal Dedekind domain is a PID*

Proof. Let A be a semilocal Dedekind domain and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ its maximal ideals. Since $\dim A = 1$, the nonzero prime ideals of A are $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Every nonzero ideal I of A factors uniquely as $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ for some $e_1, \ldots, e_n \in \mathbb{Z}_{\geq 0}$. By Corollary 3.30 there exists $x \in A$ such that $v_{\mathfrak{p}_i}(x) = e_i$ for $1 \leq i \leq n$. Therefore $(x) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, so $I = (x)$ is principal. ☐

Not all Dedekind domains are PIDs, so in general a Dedekind domain will contain ideals that require more than one generator. But it turns out that two always suffice. Moreover, we can pick one of them arbitrarily.

Theorem 3.34. *Let I be a nonzero ideal in a Dedekind domain A and let α be a nonzero element of I. Then $I = (\alpha, \beta)$ for some $\beta \in I$.*

Proof. Let $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ be the prime factorization of I, and let $(\alpha) = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_m^{f_m} \mathfrak{q}_1^{g_1} \cdots \mathfrak{q}_n^{g_n}$ be the prime factorization of (α). By Corollary 3.30 there exists $\beta \in A$ such that $v_{\mathfrak{p}_i}(\beta) = e_i$ and $v_{\mathfrak{q}_j}(\beta) = 0$. Then $\beta \in I$ and $\gcd((\alpha), (\beta)) = I$; therefore $I = (\alpha, \beta)$. ☐

One can show that Theorem 3.34 gives another characterization of Dedekind domains: they are precisely the domains A for which the theorem holds (see Problem Set 2).

References

[1] Emil Artin and George Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. **51** (1945), 469–492.

18.785 Number Theory I
Fall 2015