Ash Notes
Chapter 3

Wiliam M. Faucette

1. The Definition and Some Basic Properties

Definition. A **Dedekind doman** is an integral domain A satisfying the following three conditions:

(i) A is a Noetherian ring;

(ii) A is integrally closed;

(iii) Every nonzero prime ideal of A is maximal. [That is, A has height 1.]

Proposition. *In the AKLB setup, B is integrally closed, regardless of A. If A is an integrally closed Noetherian, then B is also a Noetherian ring, as well as a finitely generated A-module.*

Proof. B is integrally closed in L, which is the field of fractions on B. If A is integrally closed, then B is a submodule of a free A-module M of rank n. If A is Noetherian, then M is a Noetherian A-module, and B is a Noetherian submodule. An ideal of B is, in particular, an A-submodule of B, hence is finitely generated over A and therefore over B. It follows that B is a Noetherian ring. □

Theorem. *In the AKLB setup, if A is a Dedekind domain, then so is B. In particular, the ring of algebraic integers in a number field is a Dedekind domain.*

Proof. From the last result, we need only show that every nonzero prime ideal Q of B is maximal. Since B is integral over A and Q is a nonzero prime ideal, then $Q \cap A$ is a prime ideal and nonzero. So, it's maximal (since A is a Dedekind domain). Thus Q is also maximal. □

2. Fractional Ideals

Recall the definition of the product of ideals.

If a prime ideal P contains a product of ideals $I_1 \dots I_n$, then $P \supseteq I_j$ for some j.

Proposition. *If I is a nonzero ideal of the Noetherian integral domain R, then I is contains a product of nonzero prime ideals.*

Proof. Let $\mathcal{S}$ be the collection of all nonzero ideals that do not contain a product of nonzero prime ideals. Use the fact that if $\mathcal{S}$ is not empty, it must have a maximal element J. The ideal J cannot be prime, so there exist $a, b \in R$ so that $a \notin J$, $b \notin J$, and $ab \in J$. By maximality of J, the ideals $J + Ra$ and $J + Rb$ contain a product of nonzero prime ideals. But then so does their product, which is contained in J. Contradiction. □

Corollary. *If I is an ideal of the Noetherian ring R (not necessarily an integral domain), then I contains a product of prime ideals.*

Proof. Repeat the proof of the proposition with the word "nonzero" deleted. □

Definition. Let R be an integral domain with fraction field K, and let I be an R-submodule of K. We say I is a **fractional ideal** of R if $rI \subset R$ for some nonzero $r \in R$. We call r a **denominator** of I. An ordinary ideal of R is a fractional ideal (take $r = 1$), and will often be referred to as an **integral ideal**.

Lemma. (i) *If I is a finitely generated R-submodule of K, then I is a fractional ideal.*

(ii) *If R is Noetherian and I is a fractional ideal of R, then I is finitely generated R-submodule of K.*

(iii) *If I and J are fractional ideals with denominators r and s respectively, then $I \cap J$, $I + J$, and IJ are fractional ideals with respective denominators r (or s), rs, and rs.*

Lemma. *Let I be a nonzero prime ideal of the Dedekind domain R, and let J be the set of all elements $x \in K$ such that $xI \subseteq R$. Then $R \subsetneq J$.*

Proof. Since $RI \subseteq R$, it follows that R is a subset of J. Pick a nonzero element $a \in I$, so that I contains a principal ideal Ra. Let n be the smallest positive integer such that Ra contains a product $P_1 \cdots P_n$ of n nonzero prime ideals. Since R is Noetherian, there is such an n since every ideal in R contains a product of prime ideals. Hence I contains one of the P_i, say P_1. But in a Dedekind domain, every nonzero prime ideal is maximal, so $I = P_1$.

Assuming $n \geq 2$, set $I_1 = P_2 \cdots P_n$, so that $Ra \not\supseteq I_1$ by minimality of n. Choose $b \in I_1$ with $b \notin Ra$. Now $II_1 = P_1 \cdots P_n \subset Ra$, in particularly, $Ib \subseteq Ra$, hence $Iba^{-1} \subseteq R$. (note that a has an inverse in K but not necessarily in R.). Thus, $ba^{-1} \in J$, but $ba^{-1} \notin R$, for if so, $b \in Ra$, contradicting the choice of b.

The case $n = 1$ must be handled separately. In this case, $P_1 = I \supseteq Ra \supseteq P_1$, so $I = Ra$. Thus Ra is a proper ideal, and we can choose $b \in R$ with $b \notin Ra$. Then $ba^{-1} \notin R$, but $ba^{-1}I = ba^{-1}Ra = bR \subseteq R$, so $ba^{-1} \in J$. □

We prove that J is the inverse of I.

Proposition. *Let I be a nonzero prime ideal of the Dedekind domain R, and let $J = \{x \in K \mid xI \subseteq R\}$. Then J is a fractional ideal and $IJ = R$.*

Proof. If r is a nonzero element of I and $x \in J$, then $rx \in R$, so $rJ \subseteq R$ and J is a fractional ideal. Now $IJ \subseteq R$ by definition of J, so IJ is an integral ideal. By the lemma, we have $I = IR \subseteq IJ \subseteq R$, and maximality of I implies that either $IJ = I$ or $IJ = R$. In the latter case, $IJ = R$ and we're done. So suppose $IJ = I$.

If $x \in J$, then $xI \subseteq IJ \subseteq R$, and by induction $x^n I \subseteq I$ for all $n \in \mathbb{N}$. Let r be any nonzero element of I. Then $rx^n \in x^n I \subseteq I \subseteq R$, so $R[x]$ is a fractional ideal. Since R is Noetherian, part (ii) implies that $R[x]$ is a finitely generated R-submodule of K. Then x is integral over R. But R, a Dedekind domain, is integrally closed, so $x \in R$. Therefore $J \subseteq R$, contradicting the last lemma. □

Theorem. *If R is a Dedekind domain, then R is a UFD if and only if R is a PID.*

Proof. Recall from basic algebra that a (commutative) ring R is a PID iff R is a UFD and every nonzero prime ideal of R is maximal. □

3. Unique Factorization of Ideals

Theorem. *If I is a nonzero fractional ideal of the Dedekind domain R, then I can be factored uniquely at $P_1^{n_1} P_2^{n_2} \cdots P_r^{n_r}$, where n_i are integers. Consequently, the nonzero fractional ideals form a group under multiplication.*

Proof. First consider the existence of such a factorization. Without loss of generality, we can restrict to integral ideals. [Note that if $r \neq 0$ and $rI \subseteq R$, then $I = (rR)^{-1}(rI)$.]

By convention, we regard R as the product of the empty collection of prime ideals, so let $\mathcal{S}$ be the set of all nonzero proper ideals of R that cannot be factored in the given form, with all n_i *positive* integers. (This trick will yield the useful result that the factorization of integral ideals only involves positive exponents.) Since R is Noetherian, $\mathcal{S}$, if nonempty, has a maximal element I_0, which is contained in a maximal ideal I. Since every nonzero prime ideal in a Dedekind domain is invertible, I has an inverse fractional ideal J. Thus, by the lemma and proposition at the end of section 2,

$$I_0 = I_0 R \subseteq I_0 J \subseteq IJ = R.$$

Therefore $I_0 J$ is an integral ideal, and we claim that $I_0 \subset I_0 J$. For it $I_0 = I_0 J$, then the last paragraph of the proof of the last proposition in Section 2 can be reproduced with I replaced by I_0 to reach a contradiction. By maximality of I_0, $I_0 J$ is a product of prime ideals, say $I_0 J = P_1 \cdots P_r$ (with repetition allowed). Multiply both sides by the prime ideal I to conclude that I_0 is a product of prime ideals, contradicting $I_0 \in \mathcal{S}$. Thus $\mathcal{S}$ must be empty, and the existence of the desired factorization is established.

Uniqueness is on p. 5 in box. □

Corollary. *A nonzero fractional ideal I is an integral ideal if and only if all exponents in the prime factorization of I are nonnegative.*

Proof. The "only if" part was noted in the proof of the last theorem. The "if" part follows because a power of an integral ideal is still an integral ideal. □

Corollary. *Denote by $n_P(I)$ the exponent of the prime ideal P in the factorization of I. (If P does not appear, take $n_P(I) = 0$.) If I_1 and I_2 are nonzero fractional ideals, then $I_1 \supseteq I_2$ if and only if for every prime ideal P of R, $n_P(I_1) \leq n_P(I_2)$.*

Proof. We have $I_2 \subseteq I_1$ iff $I_2 I_1^{-1} \subseteq R$, and by the last corollary, this happens iff for every P, $n_P(I_2) - n_P(I_1) \geq 0$. □

Definition. Let I_1 and I_2 be nonzero integral ideals. We say that I_1 **divides** I_2 if $I_2 = JI_1$ for some integral ideal J. Just as with integers, an equivalent statement is that each prime factor of I_1 is a factor of I_2.

Corollary. *If I_1 and I_2 are nonzero integral ideals, then I_1 divides I_2 if and only if $I_1 \supseteq I_2$. In other words, for these ideals,*

DIVIDES MEANS CONTAINS.

Proof. By the definition, I_1 divides I_2 iff $n_P(I_1) \leq n_P(I_2)$ for every prime ideal P. By the last corollary, this is equivalent to $I_1 \supseteq I_2$. $\square$

GCD's and LCM's

In a Dedekind domain, we can compute the GCD and LCM of two nonzero ideals. The GCD is the smallest ideal containing both I and J, that is, $I + J$. The least common multiple is the largest ideal contains in both I and J, which is $I \cap J$.

A Dedekind domain comes close to being a PID in the sense that every nonzero integral ideal, in fact every nonzero fractional ideal, divides some principal ideal.

Proposition. *Let I be a nonzero fractional ideal of the Dedekind domain R. Then there is a nonzero integral ideal J such that IJ is a principal ideal of R.*

Proof. By the theorem on factorization of fractional ideals in a Dedekind domain R, there is a nonzero fractional ideal I' such that $II' = R$. By definition of fractional ideal, there is a nonzero element $r \in R$ such that rI' is an integral ideal. If $J = rI'$, then $IJ = Rr$, a principal ideal of R. $\square$

4. Some Arithmetic in Dedekind Domains

Page 7 in box.