Unique Factorization of Ideals and Dedekind domains

Lemma

A noetherian ring. For any nontrivial ideal I of A there exists a finite set of prime ideals $P_1, \dots, P_s$ and integers $e_1, \dots, e_s \geq 1$ s.t

$$P_1^{a_1} \cdots P_s^{a_s} \subseteq I \subseteq P_1 \cap \cdots \cap P_s$$

Proof

By contradiction, assume that Σ, the set of ideal not satisfying the lemma, is nonempty. A noetherian $\Rightarrow$ Σ has a maximal element I. I is not prime of course $\Rightarrow$ $\exists\, a, b \in A \setminus I$, $ab \in I$. Define $I_a = \langle I, a \rangle$, $I_b = \langle I, b \rangle$.

Then,

$$I_a I_b = \langle I^2, aI, bI, ab \rangle \subseteq I \subseteq I_a \cap I_b$$

Note that $I_a, I_b \neq A$ since $I_a I_b \subseteq I \subsetneq A$. That is I_a, I_b are non-trivial ideal that contan I and so, by maximality of I, $I_a, I_b \notin \Sigma$.

Thus,

$$P_1^{e_1} \cdots P_s^{e_s} \subseteq I_x \subseteq P_1 \cap \cdots \cap P_s$$

$$Q_1^{f_1} \cdots Q_t^{f_t} \subseteq I_y \subseteq Q_1 \cap \cdots \cap Q_t \qquad P_i, Q_i \in \operatorname{Spec} A \quad e_i, f_i \geq 1$$

$\Rightarrow$

$$I \subseteq I_x \cap I_y \subseteq P_1 \cap \cdots \cap Q_t$$

$$P_1^{e_1} \cdots Q_t^{f_t} \subseteq I_x I_y \subseteq I$$

$\Rightarrow$ $I \notin \Sigma$. Contradiction. ∎

The above lemma only exploited noetherianity. We'll now assume that the dimension is one. Before, we need to simple lemmas.

Lemma

P prime in a ring A. I, J ideals. Then, $IJ \subseteq P \Rightarrow I \subseteq P$ or $J \subseteq P$

Proof

If $I \not\subseteq P$ and $J \not\subseteq P$ $\exists\, i \in I \setminus P$, $j \in J \setminus P$ but $ij \in IJ \subseteq P$ contradicting P prime.

Lemma

A ring. $I_1, \dots, I_n$ ideals of A that are pairwise coprime. Then,

(1) $I_1 \cdots I_s$ coprime to I_{s+1} $\quad s = 1, \dots, n-1$

(2) $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

Proof

(1) Fix s. Take $x_j \in I_{s+1}$ and $y_j \in I_j$ s.t. $x_j + y_j = 1$. Then,

$$1 = \prod_{j=1}^{s} (x_j + y_j) \in \langle x_1, \dots, x_s, \prod_{i=1}^{s} y_i \rangle \subseteq I_{s+1} + I_1 \cdots I_s .$$

(2) By induction. $n = 2$: Take $x \in I_1$ $y \in I_2$ s.t. $x + y = 1$. Take $z \in I_1 \cap I_2$.

Then, $z = z \cdot 1 = zx + zy \in I_1 I_2 \implies I_1 \cap I_2 \subseteq I_1 I_2$. $I_1 I_2 \subseteq I_1 \cap I_2$ of course always holds.

For $n > 2$, by (1) $I_1 \cdots I_s$ and I_{s+1} are coprime. Hence, $(I_1 \cdots I_s) \cap I_{s+1} = \bigcap_{i=1}^{s+1} I_i$.

By induction, $I_1 \cdots I_s = I_1 \cap \cdots \cap I_s$. ∎

Lemma

A noetherian, $\dim A = 1$. I nontrivial ideal of A. Then, there are only finitely many maximal ideal $M_1, \dots, M_s \in \operatorname{Max} A$ containing I. Further, $\exists$ integers $e_1, \dots, e_s \geq 1$ s.t.

$$\prod_{i=1}^{s} M_i^{e_i} \subseteq I \subseteq \prod_{i=1}^{s} M_i$$

Proof

The first lemma + $\dim A = 1$ implies that $\exists$ max ideals $M_1, \dots, M_s$ and $e_1, \dots, e_s \geq 1$ s.t.

$$\prod M_i^{e_i} \subseteq I \subseteq \cap M_i$$

Maximal ideals are always coprime and so

$$\prod M_i^{e_i} \subseteq I \subseteq \prod M_i$$

Now, assume M is some max ideal containg I. Then $M \supseteq \prod M_i^{e_i}$ and so by a previous lemma, since M is prime $\exists i$ s.t. $M \supseteq M_i$. By maximality $M = M_i$ and so all maximal ideals that contain I in fact participate in this "semi factorization". ∎

Proposition

A noetherian, $\dim A = 1$. FAE:

(1) A has UFI

(2) A_M has UFI $\forall M \in \operatorname{Max} A$.

Proof

$1 \to 2$: Fix $M \in \operatorname{Max} A$. Let $\varphi : A \hookrightarrow A_M$ be the natural embedding: $\varphi(a) = \frac{a}{1}$.

Take I ideal of A_M. Consider the ideal $\varphi^{-1}(I)$. By assumption

$$\varphi^{-1}(I) = P_1^{e_1} \cdots P_s^{e_s} \qquad P_i \in \operatorname{Max} A.$$

Recall that there is a 1:1 correspondence between the prime ideals of A_M and those of A that are contained in M. The correspondence is induced by φ^{-1} and so $\varphi^{-1}(I) \subseteq M$. By a previous lemma, $\exists i$: $P_i \subseteq M$. Since $\dim A = 1$ $P_i \in \operatorname{Max} A$ $\Rightarrow$ $P_i = M$.

Recall that in general if I is an ideal of $S^{-1}A$ and $\varphi: A \hookrightarrow S^{-1}A$ $\varphi(a) = \frac{a}{1}$

then $S^{-1}\varphi^{-1}(I) = I$. In our case

$$
\begin{aligned}
I &= (\varphi^{-1}(I))_M \\
&= (P_1^{e_1} \cdots P_s^{e_s} A)_{P_i} \\
&= (P_1^{e_1} A)_{P_i} \cdots (P_s^{e_s} A)_{P_i} \\
&= (P_i A_{P_i})^{e_i} \\
&= (M A_M)^{e_i}
\end{aligned}
$$

$S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$

$(QA)_P = A_P$ whenever $Q \not\subseteq P$

and so I can be factored into a product of max ideals in A_M.

As for uniqueness. Recall that in general:

Claim

If $J \subseteq I$ are ideals in A then $J = I \iff J_M = I_M$ $\forall M \in \operatorname{Max} A$, $M \supseteq J$.

By UFI of A, for every integer a, $M^{a+1} \subsetneq M^a$. Note that M is the only max ideal of A that contains M^{a+1} and so by the claim $(MA_M)^a \neq (MA_M)^{a+1}$.

$2 \Leftarrow 1$: Take $0 \neq I \subseteq A$. Since A noetherian and $\dim A = 1$, $\exists$ finite set of max ideals of A, $M_1, \dots, M_s$ that contain I. Let $\varphi_i : A \longrightarrow A_{M_i}$ $\quad a \mapsto \frac{a}{1}$.
By assumption A_{M_i} has UFI. Further, A_{M_i} is a local ring of dim 1 (since $\dim A = 1$) and so $\varphi_i(I) = (M_i A_{M_i})^{a_i}$ for some unique $a_i \geq 1$.

We'll now show that $I = M_1^{a_1} \cdots M_s^{a_s}$. First just by set-theoretic arguments

$$I \subseteq \varphi_1^{-1}((M_1 A_{M_1})^{a_1}) \cap \cdots \cap \varphi_s^{-1}((M_s A_{M_s})^{a_s})$$

As $M_i^{a_i} \subseteq \varphi_i^{-1}((M_i A_{M_i})^{a_i})$ and since M_i is the only max ideal in A that contains $M_i^{a_i}$, we get $M_i^{a_i} = \varphi_i^{-1}((M_i A_{M_i})^{a_i})$.

Note that $M_i^{a_i}$ and $M_j^{a_j}$ are coprime for $i \neq j$ and so

$$\bigcap_{i=1}^{s} M_i^{a_i} = \prod_{i=1}^{s} M_i$$

$\Rightarrow$ $I \subseteq M_1^{a_1} \cdots M_s^{a_s}$. But $I_{M_i} = (M_i A_{M_i})^{a_i} = (M_1^{a_1} \cdots M_s^{a_s})_{M_i}$

we deduce $I = M_1^{a_1} \cdots M_s^{a_s}$.

As for uniqueness, note that I must be of the form $I = M_1^{b_1} \cdots M_s^{b_s}$. Localizing at M_i we get that $(I_{M_i}) = (M_i A_{M_i})^{a_i} = (M_i A_{M_i})^{b_i}$. By UFI of A_{M_i} we get $a_i = b_i$.

$\blacksquare$

Proposition

A noetherian local domain of dimension 1. TFAE:

(1) A has UFI

(2) A is a PID

(3) A is integrally closed

Proof

Let M denotes A's unique max ideal.

$1 \to 2$: Take any $x \in M \setminus M^2$. Such exists by UFI. By UFI $\langle x \rangle$ can be factored into a product of prime ideals of A. However, M is the only nonzero prime ideal of A and so $\langle x \rangle = M^a$ for some $a \geq 1$. As $x \notin M^2$ $a=1$ and so $M = \langle x \rangle$. Since we prove principality of all prime ideals (indeed only M) then by a lemma we proved, A is a PID.

$2 \to 1$: PID $\Rightarrow$ UFD and so also UFI.

$2 \to 3$: We already proved that UFDs are integrally closed, let alone PIDs

$3 \to 2$: Take $0 \neq x \in M$. If $M = \langle x \rangle$ we're done. Otherwise, by noetherianity and $\dim A = 1$ $\exists n \geq 1$ s.t. $M^n \subseteq \langle x \rangle$ yet $M^{n-1} \not\subseteq \langle x \rangle$. Take $y \in M^{n-1} \setminus \langle x \rangle$.

Let $K = \mathrm{Frac}\, A$. Then $\frac{y}{x} \in K \setminus A$. As A is integrally closed, $\frac{y}{x}$ is not integral over A. Now, by noetherianity of A, M is a f.g. A-module and $M \subseteq K$ (and so M is an A-submodule of K) it follows that $\left(\frac{y}{x}\right) M \not\subseteq M$. But $\frac{y}{x} M \subseteq A$ since $yM \subseteq M^n \subseteq \langle x \rangle$. Thus, $(y/x) M$ is an ideal of A not containd in M $\Rightarrow$ $\frac{y}{x} M = A$ $\Rightarrow$ $M = \langle \frac{x}{y} \rangle$ principal $\Rightarrow$ A PID.

$\blacksquare$

Theorem (Fundamental theorem of Dedekind domains)

A noetherian, $\dim A = 1$. FAE:

1) A Dedekind domain ($\Leftrightarrow$ integrally closed).

2) A has UFI

Proof

We know that A is i.c. $\Leftrightarrow A_m$ is i.c $\forall m \in \operatorname{Max} A$. By the previous proposition, A_m i.c $\Leftrightarrow A_m$ has UFI. We proved that UFI is also a local property of noetherian rings of dim 1.

$\blacksquare$

Some notation

A Dedekin domain. I nonzero ideal of A. If P is a max ideal s.t. $I = PJ$ for some ideal J, we say that P **divides** I and write $P \mid I$. The **order** of I at P for $P \mid I$ is the unique integer a s.t. $I = P^a P_2^{a_2} \cdots P_s^{a_s}$ in the factorization of I to prime ideals. We define the order to be 0 for $P \nmid I$. We denote the order of I at P by $\operatorname{ord}_P(I)$. So,

$$I = \prod_{P \in \operatorname{Max} A} P^{\operatorname{ord}_P(I)}$$

Observe that $\operatorname{ord}_P(I)$ is local as it only depends on $IA_P \subseteq A_P$. Indeed, If A_P is a Dedekin domain then for every ideal I of A

$$\operatorname{ord}_P(I) = \operatorname{ord}_{PA_P}(IA_P).$$