2 Localization and Dedekind domains

2.1 Localization of rings

Let A be a commutative ring (unital, as always), and let S be a multiplicative subset of A; this means that S is closed under finite products (including the empty product, so $1 \in S$), and S does not contain zero. To simplify matters let us further assume that S contains no zero divisors of A; equivalently, the map $A \xrightarrow{\times s} A$ is injective for all $s \in S$.

Definition 2.1. The *localization* of A with respect to S is the ring of equivalence classes

$$S^{-1}A := \{a/s : a \in A, s \in S\} / \sim$$

where $a/s \sim a'/s'$ if and only if $as' = a's$. This ring is also sometimes denoted $A[S^{-1}]$.

We canonically embed A in $S^{-1}A$ by identifying each $a \in A$ with the equivalence class $a/1$ in $S^{-1}A$; our assumption that S has no zero divisors ensures that this map is injective. We thus view A as a subring of $S^{-1}A$, and when A is an integral domain (the case of interest to us), we may regard $S^{-1}A$ as a subring of the fraction field of A., which can be defined as $A^{-1}A$, the localization of A with respect to itself. If $S \subseteq T$ are multiplicative subsets of A (neither containing zero divisors), we may view $S^{-1}A$ as a subring of $T^{-1}A$.

If $\varphi\colon A \to B$ is a ring homomorphism and $\mathfrak{b}$ is a B-ideal, then $\phi(A^{-1})$ is an A-ideal called the *contraction* of $\mathfrak{b}$ (to A) and sometimes denoted b^{c}; when A is a subring of B and φ is the inclusion map we simply have $\mathfrak{b}^{\mathrm{c}} = \mathfrak{b} \cap A$. If $\mathfrak{a}$ is an A-ideal then $\varphi(\mathfrak{a})$ is in general not a B-ideal; but the B-ideal $(\varphi(\mathfrak{a}))$ generated by $\varphi(\mathfrak{a})$ is called the *extension* of $\mathfrak{a}$ (to B) and sometimes denoted $\mathfrak{a}^{\mathrm{e}}$. In our setting with $B = S^{-1}A$ and φ inclusion, and we have

$$\mathfrak{a}^{e} = \mathfrak{a}B := \{ab : a \in \mathfrak{a}, b \in B\}. \tag{1}$$

Note that we can write any sum $a_1/s_1 + \cdots a_n/s_n$ as a/s' for some $a \in A$ with $s = s_1 \cdots s_n$ in S (here we are assuming S has no zero divisors), so $\mathfrak{a}B$ is in fact an ideal.

We clearly have $\mathfrak{a} \subseteq \varphi^{-1}((\varphi(\mathfrak{a}))) = \mathfrak{a}^{\mathrm{ec}}$ and $\mathfrak{b}^{\mathrm{ce}} = (\varphi(\varphi^{-1}(\mathfrak{b}))) \subseteq \mathfrak{b}$; one might ask whether these inclusions are equalities. In general the first is not: if $B = S^{-1}A$ and $\mathfrak{a} \cap S \neq \emptyset$ then $\mathfrak{a}^{\mathrm{e}} = \mathfrak{a}B = B$ and $\mathfrak{a}^{\mathrm{ec}} = B \cap A$ are unit ideals, but we may still have $\mathfrak{a} \subsetneq A$. However when $B = S^{-1}A$ the second inclusion is always an equality; see [1, Prop. 11.19] or [2, Prop. 3.11] for a short proof. We also note the following theorem.

Theorem 2.2. *The map $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ defines a bijection from the set of prime ideals of $S^{-1}A$ and the set of prime ideals of A that do not intersect S. The inverse map is $\mathfrak{p} \mapsto \mathfrak{p}S^{-1}A$.*

Proof. See [1, Cor. 11.20] or [2, Prop. 3.11.iv]. □

Remark 2.3. An immediate consequence of (1) is that if $a_1, \ldots, a_n \in A$ generate $\mathfrak{a}$ as an A-ideal, then they also generate $\mathfrak{a}^{\mathrm{e}} = \mathfrak{a}B$ as a B-ideal. As noted above, when $B = S^{-1}A$ we have $\mathfrak{b} = \mathfrak{b}^{\mathrm{ce}}$, so every B-ideal is of the form $\mathfrak{a}^{e}$ (take $\mathfrak{a} = \mathfrak{b}^{\mathrm{c}}$). It follows that if A is noetherian then so are all its localizations, and if A is a PID then so are all of its localizations.

An important special case of localization occurs when $\mathfrak{p}$ is a prime ideal in an integral domain A and $S = A - \mathfrak{p}$ (the complement of the set $\mathfrak{p}$ in the set A). In this case it is customary to denote $S^{-1}A$ by

$$A_{\mathfrak{p}} := \{a/b : a \in A, b \notin \mathfrak{p}\}/\sim, \tag{2}$$

and call it the *localization of A at $\mathfrak{p}$*. The prime ideals of $A_\mathfrak{p}$ are then in bijection with the prime ideals of A that lie in $\mathfrak{p}$. It follows that $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal of A and $A_\mathfrak{p}$ is therefore a local ring (when the term *localization*). We have

$$A \subseteq A_\mathfrak{p} \subseteq \operatorname{Frac} A.$$

If $\mathfrak{p} = (0)$ then $A_\mathfrak{p} = \operatorname{Frac} A$, but otherwise $A_\mathfrak{p}$ is properly contained in $\operatorname{Frac} A$.

Warning 2.4. The notation in (2) makes it tempting to assume that if a/b is an element of $\operatorname{Frac} A$, then $a/b \in A_\mathfrak{p}$ if and only if $b \notin \mathfrak{p}$. This is not necessarily true! As an element of $\operatorname{Frac} A$, the notation "a/b" represents an equivalence class $[a/b]$, and if $[a/b] = [a'/b']$ with $b' \notin A_\mathfrak{p}$, then in fact $[a/b] \in A_\mathfrak{p}$. As a trivial example, take $A = \mathbb{Z}$, $\mathfrak{p} = (3)$, $a/b = 9/3$ and $a'/b' = 3/1$. You may object that we should write a/b in lowest terms, but when A is not a unique factorization domain it is not clear what this means.

Example 2.5. For a field k, let $A = k[x]$ and $\mathfrak{p} = (x - 2)$. Then

$$A_\mathfrak{p} = \{f \in k(x) : f \text{ is defined at } 2\}.$$

The ring A is a PID, so $A_\mathfrak{p}$ is a PID with a unique nonzero maximal ideal, hence a DVR. Its maximal ideal is

$$\mathfrak{p}A_\mathfrak{p} = \{f \in k(x) : f(2) = 0\}.$$

The valuation on the field $k(x) = \operatorname{Frac} A$ corresponding to the valuation ring $A_\mathfrak{p}$ measures the order of vanishing of functions $f \in k(x)$ at 2. The residue field is $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq k$, and the quotient map $A_\mathfrak{p} \twoheadrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ sends f to $f(2)$.

Example 2.6. Let $p \in \mathbb{Z}$ be a prime. Then $\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z}, p \nmid b\}$. As in the previous example, $\mathbb{Z}$ is a PID and $\mathbb{Z}_{(p)}$ is a DVR; the valuation on $\mathbb{Q}$ is the p-adic valuation.

2.2 Localization of modules

The concept of localization generalizes to modules. As above, let A be a ring and let S a multiplicative subset of A If M is an A-module such that the map $M \xrightarrow{\times s} M$ is injective for all $s \in S$ (this is a strong assumption that imposes constraints on both S and M, but it holds in the cases we care about), then the set

$$S^{-1}M := \{m/s : m \in M, s \in S\}/\sim$$

is an $S^{-1}A$-module (the equivalence is $m/s \sim m'/s' \Leftrightarrow s'm = sm'$, as usual). We could equivalently define $S^{-1}M := M \otimes_A S^{-1}A$; see [2, Prop. 3.5]. We will usually take $S = A - \mathfrak{p}$, in which case we write $M_\mathfrak{p}$ for $S^{-1}M$, just as we write $A_\mathfrak{p}$ for $S^{-1}A$.

Proposition 2.7. *Let A be a subring of a field K, and let M be an A-module contained in a K-vector space V (equivalently, for which the map $M \to M \otimes_A K$ is injective).*[1] *Then*

$$M = \bigcap_\mathfrak{m} M_\mathfrak{m} = \bigcap_\mathfrak{p} M_\mathfrak{p},$$

where $\mathfrak{m}$ ranges over the maximal ideals of A and $\mathfrak{p}$ ranges over the prime ideals of A; the intersections takes place in V.

[1] The image is a tensor product of A-modules that is also a K-vector space. We need the natural map to be injective in order to embed M in it. Note that V necessarily contains a subspace isomorphic to $M \otimes_A K$.

Proof. The fact that $M \subseteq \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$ is immediate. Now suppose $x \in \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$. The set $\{a \in A : ax \in M\}$ is an A-ideal $\mathfrak{a}$, and it is not contained in any maximal ideal $\mathfrak{m}$, since $\mathfrak{a} \subseteq \mathfrak{m}$ implies $x \notin M_{\mathfrak{m}}$. Therefore $\mathfrak{a} = A$, so $x = 1 \cdot x \in M$, since $1 \in \{a \in A : ax \in M\}$.

We now note that each $M_{\mathfrak{p}}$ contains some $M_{\mathfrak{m}}$ (since each $\mathfrak{p}$ is contained in some $\mathfrak{m}$), and every maximal ideal is prime, so $\cap_{\mathfrak{m}} M_{\mathfrak{m}} = \cap_{\mathfrak{p}} M_{\mathfrak{p}}$. □

Several important special cases of this proposition occur when A is an integral domain, K is its fraction field, and M is an A-submodule of K. The ideals I of A are precisely its A-submodules, each of which can be localized as above, and the result is just the extension of the ideal to the corresponding localization of A. In particular, if $\mathfrak{p}$ is a prime ideal then

$$I_{\mathfrak{p}} = IA_{\mathfrak{p}},$$

and more generally, $M_{\mathfrak{p}} = MA_{\mathfrak{p}}$. We also have the following corollary of Proposition 2.7.

Corollary 2.8. *Let A be an integral domain. Every ideal I of A (including $I = A$) is equal to the intersection of its localizations at the maximal ideals of A (and also to the intersection of its localizations at the prime ideals of A).*

Example 2.9. If $A = \mathbb{Z}$ then $\mathbb{Z} = \bigcap_p \mathbb{Z}_{(p)}$ in $\mathbb{Q}$.

2.3 Dedekind domains

Proposition 2.10. *Let A be a noetherian domain. The following are equivalent:*

(i) *For every nonzero prime ideal $\mathfrak{p} \subset A$ the local ring $A_{\mathfrak{p}}$ is a DVR.*

(ii) *The ring A is integrally closed and $\dim A \leq 1$.*

Proof. If A is a field then (i) and (ii) both hold, so let us assume that A is not a field, and put $K := \operatorname{Frac} A$. We first show that (i) implies (ii). Recall that $\dim A$ is the supremum of the length of all chains of prime ideals. It follows from Theorem 2.2 that every chain of prime ideals $(0) \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ extends to a corresponding chain in $A_{\mathfrak{p}_n}$ of the same length; conversely, every chain in $A_{\mathfrak{p}}$ contracts to a chain in A of the same length. Thus

$$\dim A = \sup\{\dim A_{\mathfrak{p}} : \mathfrak{p} \in \operatorname{Spec} A\} = 1,$$

since every $A_{\mathfrak{p}}$ is either a DVR ($\mathfrak{p} \neq (0)$), in which case $\dim A_{\mathfrak{p}} = 1$, or a field ($\mathfrak{p} = (0)$), in which case $\dim A_{\mathfrak{p}} = 0$. Any $a \in K$ that is integral over A is integral over every $A_{\mathfrak{p}}$ (since they all contain A), and the $A_{\mathfrak{p}}$ are integrally closed. So $a \in \bigcap_{\mathfrak{p}} A_{\mathfrak{p}} = A$, and therefore A is integrally closed, which shows (ii).

To show that (ii) implies (i), we first show that the following properties are all inherited by localizations of a ring: (1) no zero divisors, (2) noetherian, (3) dimension at most one, (4) integrally closed. (1) is obvious, (2) was noted in Remark 2.3, and (3) follows from the fact that every chain of prime ideals in $A_{\mathfrak{p}}$ extends to a chain of prime ideals in A of the same length, so $\dim A_{\mathfrak{p}} \leq \dim A$. To show (4), suppose $x \in K$ is integral over $A_{\mathfrak{p}}$. Then

$$x^n + \frac{a_{n-1}}{s_{n-1}} x^{n-1} + \cdots + \frac{a_1}{s_1} x + \frac{a_0}{s_0} = 0$$

for some $a_0, \ldots, a_{n-1} \in A$ and $s_0, \ldots, s_{n-1} \in A - \mathfrak{p}$. Multiplying both sides by s^n, where $s = s_0 \cdots s_{n-1} \in S$, shows that sx is integral over A, hence an element of A, since A is integrally closed. But then $sx/s = x$ is an element of $A_\mathfrak{p}$, so $A_\mathfrak{p}$ is integrally closed as claimed.

Thus (ii) implies that every $A_\mathfrak{p}$ is an integrally closed noetherian local domain of dimension at most 1, and for $\mathfrak{p} \neq (0)$ we must have $\dim A_\mathfrak{p} = 1$. Thus for every nonzero prime ideal $\mathfrak{p}$, the localization $A_\mathfrak{p}$ is an integrally closed noetherian local domain of dimension 1, and therefore a DVR, by Theorem 1.14. $\square$

Definition 2.11. A noetherian domain satisfying either of the equivalent properties of Proposition 2.10 is called a *Dedekind domain*.

Corollary 2.12. *Every PID is a Dedekind domain. In particular, $\mathbb{Z}$ is a Dedekind domain, as is $k[x]$ for any field k.*

Remark 2.13. Every PID is both a UFD and a Dedekind domain. Not every UFD is a Dedekind domain (consider $k[x,y]$, for any field k), and not every Dedekind domain is a UFD (consider $\mathbb{Z}[\sqrt{-13}]$, in which $(1+\sqrt{-13})(1-\sqrt{-13}) = 2 \cdot 7 = 14$). However (as we shall see), every ring that is both a UFD and a Dedekind domain is a PID.

We will see in later lectures that the ring of integers of a number field is always a Dedekind domain. More generally, we will prove that if A is a Dedekind domain and L is a finite separable extension of its fraction field, then the integral closure of A in L is a Dedekind domain. For global function fields K, the analog of the ring of integers is the integral closure of $\mathbb{F}_q[t]$ in K, which is also a Dedekind domain (for a suitable choice of t).

Remark 2.14. Unlike $\mathbb{Q}$, not every finite extension of $\mathbb{F}_q(t)$ is separable. But every finite extension K of $\mathbb{F}_q(t)$ contains a subfield isomorphic to $\mathbb{F}_q(t)$ over which it is separable; one can always pick a *separating element* $s \in K$ that is transcendental over $\mathbb{F}_q$ such that $K/\mathbb{F}_q(s)$ is separable. More generally, by a theorem of Schmidt, every finitely generated extension of a perfect field k is *separably generated*, meaning that it is a separable algebraic extension of a purely transcendental extension of k; see [3, Thm. 7.20] for a proof.

References

[1] Allen Altman and Steven Kleiman, *A term of commutative algebra*, Worldwide Center of Mathematics, 2013.

[2] Michael Atiyah and Ian MacDonald, *Introduction to commutative algebra*, Addison–Wesley, 1969.

[3] Anthony W. Knapp, *Advanced Algebra*, Digital Second Edition, 2016.