9. Discrete valuation rings

9.1. **discrete valuations.** Recall the definition of a *valuation ring.* This is a subring A of a field K so that $K = A \cup A^{-1}$. In other words, for all $x \in K^* = K - 0$, either $x \in A$ or $x^{-1} \in A$. Many valuation rings (and all Noetherian valuation rings) are given by the following construction.

Definition 9.1. A **discrete valuation** on a field K is a surjective function

$$v : K^* \to \mathbb{Z}$$

so that

(1) $v(xy) = v(x) + v(y)$. So, v is a homomorphism ($\Rightarrow v(1) = 0$ and $v(x^{-1}) = -v(x)$.)
(2) $v(x+y) \geq \min(v(x), v(y))$ assuming $x + y \neq 0$.

Extend v to $0 \in K$ by letting $v(0) = +\infty$. Then both conditions above hold and

$$A = \{x \in K \mid v(x) \geq 0\}$$

is called the **valuation ring** of v.

An integral domain A is called a **discrete valuation ring** if there is a discrete valuation v on the field of quotients of A so that A is the valuation ring of v.

Example 9.2. (1) Let $K = \mathbb{Q}$ and for each prime p let $v_p : \mathbb{Q}^* \to \mathbb{Z}$ be the function given by $v_p(p^k a/b) = k$ if a, b are integers relatively prime to p. This is a discrete valuation with valuation ring equal to $\mathbb{Z}_{(p)}$, the integers localized at the prime (p).
(2) Let $K = k(x)$, the field of rational functions $f(x)/g(x)$ in a variable x with coefficients in a field k. Each nonzero polynomial $f(x)$ can be written uniquely as $f(x) = x^n f_0(x)$ where the constant term of $f_0(x)$ is nonzero. Let $v_x(f) = n$ and let

$$v_x(f/g) = v_x(f) - v_x(g)$$

This is a discrete valuation with valuation ring equal to $k[x]_{(x)}$, the polynomial ring $k[x]$ localized at the maximal ideal (x).

Proposition 9.3. (1) *A is a local ring with unique maximal ideal*

$$\mathfrak{m} = \{x \in K \mid v(x) \geq 1\}$$

(2) $\mathfrak{m}^n = \{x \in K \mid v(x) \geq n\}$
(3) $\mathfrak{m} = (x)$ *for any* $x \in K$ *with* $v(x) = 1$.
(4) $\mathfrak{m}^n = (x^n)$ *for all* $n \geq 1$
(5) *Every nonzero ideal in A is equal to $\mathfrak{m}^n$ for some $n \geq 1$.*

Any x as above is called a **uniformizer** of A. Note that each element of A can be written uniquely in the form ux^n where u is a unit.

Corollary 9.4. *A is a Noetherian local domain with dimension 1.*

Conversely, suppose that A is a Noetherian local domain of dimension 1. Then 0 and $\mathfrak{m}$ are the only prime ideals in A. So, all other ideals $\mathfrak{a}$ are $\mathfrak{m}$-primary. ($A/\mathfrak{a}$ has only one prime ideal. So, it is Artin local. So, the maximal ideal in $A/\mathfrak{a}$ is nilpotent which implies that $\mathfrak{m}^n \subseteq \mathfrak{a}$ for some n.)

Proposition 9.5. *Suppose that A is a Noetherian local domain with dimension one. Then the following are equivalent.*

1. $\mathfrak{m} = (x)$ *is principal.*
2. $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$ *where* $k = A/\mathfrak{m}$.
3. $\mathfrak{m}^n$ *is principal for all* $n \geq 1$
4. *Every nonzero ideal in A is equal to $\mathfrak{m}^n$ for some $n \geq 1$.*
5. *A is a discrete valuation ring.*
6. *A is integrally closed.*

Proof. It is easy to see that the first 4 conditions are equivalent. Given these conditions, every element of A can be written uniquely in the form ux^n where u is a unit. Then a discrete valuation on A can be given by $v(ux^n) = n$ which is the largest number so that $\mathfrak{m}^n$ contains the element. This can be extended to a discrete valuation on the fraction field by $v(a/b) = v(a) - v(b)$. So, A is a discrete valuation ring. So, A is integrally closed by Prop. 5.26.

Finally, we show that (6) ⇒ (1). Suppose not. Take $a \in \mathfrak{m}$, $a \notin \mathfrak{m}^2$. Then (a) is $\mathfrak{m}$-primary. So there is an $n \geq 2$ so that $\mathfrak{m}^n \subseteq (a)$. Take n minimal. Then there is some $b \in \mathfrak{m}^{n-1}$ so that $b \notin (a) = aA$.

Let $c = b/a \in K = Q(A)$. Then $b \notin aA \Rightarrow c \notin A$. So, c is not integral over A (A being integrally closed).

But $b \in \mathfrak{m}^{n-1} \Rightarrow b\mathfrak{m} \subseteq aA \Rightarrow c\mathfrak{m} \subseteq A$. Since this is an A-module, it is an ideal in A. But $c\mathfrak{m}$ is not contained in $\mathfrak{m}$. (Otherwise, $\mathfrak{m}$ would be a f.g. faithful $A[c]$-module contradicting the fact that c is not integral over A. Therefore, $c\mathfrak{m} = A$. So, $b\mathfrak{m} = aA$. But this is a contradiction since $b\mathfrak{m} \subseteq \mathfrak{m}^2$ and $a \notin \mathfrak{m}^2$. □

Exercise 9.6. Show that a Noetherian domain is a valuation ring if and only if it is a discrete valuation ring.

Exercise 9.7. Given a discrete valuation ring A with valuation $v : K^* \twoheadrightarrow \mathbb{Z}$ and uniformizer x, show that the A-submodules of K are: $0, K$ and x^nA for $n \in \mathbb{Z}$. (These are called *fractional ideals.*)

9.2. **Dedekind domains.**

Definition 9.8. A **Dedekind domain** is a Noetherian domain A of dimension one satisfying any of the following equivalent conditions.

(1) A is integrally closed.
(2) Every primary ideal in A is a power of a prime ideal.
(3) The localization $A_{\mathfrak{p}}$ of A at any nonzero prime ideal is a discrete valuation ring.

For example, the ring of integers $\mathbb{Z}$ is a Dedekind domain since its primary ideals are (p^k) for prime numbers p. The unique factorization of integers can be expressed as a unique factorization of ideals into products of powers of prime ideals:

$$n = \prod p_i^{k_i} \Rightarrow (n) = \prod (p_i)^{k_i}$$

To show that the conditions in the definition are equivalent, note that (1) $\Leftrightarrow$ (3) since "integrally closed" is a local condition. To show (2) $\Leftrightarrow$ (3) note that there is a bijection between $\mathfrak{p}$-primary ideals and the nonzero ideals in the local ring $A_{\mathfrak{p}}$.

Theorem 9.9. *If A is a Dedekind domain then every ideal $\mathfrak{a}$ can be expressed uniquely as a product of powers of prime ideals:*

$$\mathfrak{a} = \prod \mathfrak{p}_i^{k_i}$$

Proof. Since A is a domain with dimension 1, every nonzero prime ideal is maximal. Therefore, any two nonzero primes are coprime. So, any nonzero primary ideals with distinct radicals are coprime. So, in the primary decomposition of $\mathfrak{a}$ we can replace intersection with product and the terms are powers of prime ideals by the definition of a Dedekind domain. □

Theorem 9.10. *The ring of integers in any number field is a Dedekind domain.*

A number field K is a finite extension of the rational numbers. The ring of integers A in K is the integral closure of $\mathbb{Z}$ in K. In the "going up" theorem we showed that any prime ideal $\mathfrak{p}$ in A is maximal if and only if $\mathfrak{p} \cap \mathbb{Z}$ is maximal in $\mathbb{Z}$. Also, if $\mathfrak{p} \subsetneq \mathfrak{p}'$ in A then $\mathfrak{p} \cap \mathbb{Z} \subsetneq \mathfrak{p}' \cap \mathbb{Z}$.

9.3. **fractional ideals.**

Definition 9.11. If A is an integral domain with fraction field K then by a **fractional ideal** of A we mean an A-submodule $M \subseteq K$ so that $xM \subseteq A$ for some $x \neq 0 \in K$.

Here are some trivial observations.

1. Every ideal is a fractional ideal.
2. Any finitely generated A-submodule of K is a fractional ideal.
3. $xM \cong M$ as an A-module.
4. If A is a PID then every fractional ideal is also principal (generated by one element).
5. If A is Noetherian, every fractional ideal is finitely generated.
6. M is a fractional ideal if and only if
$$(A : M) \neq 0$$

Definition 9.12. An A-submodule $M \subseteq K$ is an **invertible ideal** if
$$M(A : M) = A$$

Proposition 9.13. *M is an invertible ideal iff there exist $x_1, \cdots, x_n \in M$ and $y_1, \cdots, y_n \in (A : M)$ so that*
$$1 = \sum x_i y_i$$

Corollary 9.14. *Every invertible ideal is a fractional ideal which is finitely generated. In fact it is generated by the elements x_i in the above proposition.*

Proof. Any $x \in M$ can be written as:
$$x = \sum (xy_i)x_i$$
where $xy_i \in A$ since $y_i M \subseteq A$. □

Corollary 9.15. *Suppose that A is a local domain with unique maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}$ is invertible if and only if it is principal.*

Proof. If $\mathfrak{m} = (x)$ then $1 = xx^{-1}$ with $x^{-1} \in (A : \mathfrak{m})$. So, $\mathfrak{m}$ is invertible.

Conversely, suppose the $\mathfrak{m}$ is invertible. Then
$$1 = \sum x_i y_i$$
where $y_i \in (A : \mathfrak{m})$. The elements $x_i y_i$ cannot all be in $\mathfrak{m}$. So, at least one term, say $u = x_j y_j \in A - \mathfrak{m}$ is a unit. Then $1 = u^{-1} x_j y_j$ which implies that $\mathfrak{m} = (u^{-1} x_j) = (x_j)$ by the previous corollary. □

The property of being invertible is a local property of M.

Proposition 9.16. *Suppose that $M \subseteq K$ is an A-module. Then the following are equivalent.*

1. *M is invertible.*
2. *M is f.g. and $M_\mathfrak{p}$ is an invertible $A_\mathfrak{p}$ ideal for all prime ideals $\mathfrak{p}$ in A.*
3. *M is f.g. and $M_\mathfrak{m}$ is an invertible $A_\mathfrak{m}$ ideal for all maximal ideals $\mathfrak{m}$ in A.*

Note that all three conditions imply that M is a fractional ideal.

Proof. Certainly (2) ⇒ (3). To show (1) ⇒ (2) we use the equation $1 = \sum x_i y_i$. We just need to recall that

$$(A : M)_\mathfrak{p} = (A_\mathfrak{p} : M_\mathfrak{p})$$

which holds since M is finitely generated.

(3) ⇒ (1). Let $M(A : M) = \mathfrak{a} \subseteq A$. If this is a proper ideal in A then it is contained in a maximal ideal $\mathfrak{m}$ and we get

$$M_\mathfrak{m}(A_\mathfrak{m} : M_\mathfrak{m}) = \mathfrak{a}_\mathfrak{m} \subseteq \mathfrak{m}_\mathfrak{m} \subsetneq A_\mathfrak{m}$$

which contradicts (3). Therefore $\mathfrak{a} = A$ and M is invertible. □

Proposition 9.17. *Suppose that A is a local domain. Then A is a DVR iff every nonzero fractional ideal is invertible.*

Proof. ⇒: We did this already.

⇐: if every nonzero ideal is invertible then in particular the maximal ideal $\mathfrak{m}$ is invertible and thus principal. So, A is a DVR. □

Theorem 9.18. *Suppose that A is an integral domain. Then A is Dedekind iff every fractional ideal is invertible.*

Proof. Both conditions are local and imply that A is Noetherian. □

Corollary 9.19. *The nonzero fractional ideals of a Dedekind domain form a group.*

This group is called the **group of ideals** of A. It is an abelian group which the book calls I. The principal ideals form a subgroup P. The quotient H is called the **ideal class group** of A. Since every principal ideal is generated by an element of K^* we get a homomorphism $K^* \to P$ whose kernel is the group of units U of A. This gives an exact sequence

$$1 \to U \to K^* \to I \to H \to 1$$

If A is the ring of integers in a number field K then it is well-known that H is a finite group. The order of H is called the **class number** of K. U is a finitely generated group whose rank is given by the *Dirichlet unit theorem* which can be proved using *Reidemeister torsion.*