Local fields

Emile T. Okada

March 15, 2019

Contents

CHAPTER 1

Discrete valuation rings and Dedekind domains

1.1 Discrete valuation rings

Definition 1.1.1. Let K be a field. A *discrete valuation* on K is a surjective function $v : K \to \mathbb{Z} \cup \{\infty\}$ satisfying

1. $v(x) = \infty$ iff $x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x + y) \geq \inf(v(x), v(y))$.

If (K, v) is a field with a discrete valuation then $R = \{x \in K : v(x) \geq 0\}$ is a subring of K called the valuation ring of v.

Definition 1.1.2. A domain R is called a *discrete valuation ring* if there is a valuation v on $K = \mathrm{Frac}(R)$ for which R is the valuation ring.

Lemma 1.1.3. *Any DVR is a Noetherian local domain of Krull dimension 1.*

Proof. Let $t \in R$ be such that $v(t) = 1$. Then all the ideals of R are in the chain

$$R \supsetneq (t) \supsetneq (t^2) \supsetneq (t^3) \supsetneq \cdots \supseteq 0. \tag{1.1}$$

■

Thm 1.1.4. *Let R be a Noetherian local domain with Krull dimenstion 1 and maximal ideal $\mathfrak{m}$. The following are equivalent*

1. *R is a DVR*
2. *$\mathfrak{m}$ is principal*
3. *R is normal.*

Proof. From the conditions on R we know the only prime ideals are 0 and $\mathfrak{m}$.

(1) $\Rightarrow$ (3) Let $x \in K = \mathrm{Frac}(R)$ and suppose it is integral over R. Then there are $a_0, \ldots, a_{n-1} \in R$ such that $x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 = 0$. Suppose that $v(x) < 0$. Then

$$nv(x) = v(x^n) \geq \inf(v(a_i x^i)) \geq (n-1)v(x) \tag{1.2}$$

and so $v(x) \geq 0$ which is a contradiction and so $v(x) \geq 0$ and hence $x \in r$.

(3) $\Rightarrow$ (2) Let $0 \neq x \in \mathfrak{m}$. Then $\mathrm{rad}((x)) = \mathfrak{m}$ and so since R is Noetherian there is an $n \in \mathbb{N}$ such that $\mathfrak{m}^n \subseteq (x) \subseteq \mathfrak{m}$. Let n be minimal with this property.

Remark 1.1.5. Morally we now have $(x) = \mathfrak{m}^n$.

Let $y \in \mathfrak{m}^{n-1}$ be such that $y \notin (x)$. Set $z = x/y \in K$. Then $z^{-1} \notin R$ so z^{-1} is not integral over R. But this means that $z^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$ my theorem 2.3.1. But $y\mathfrak{m} \subset (x)$ and so $z^{-1}\mathfrak{m} \subseteq R$ and hence $z^{-1}\mathfrak{m} = R$ and so $\mathfrak{m} = (z)$.

(2) $\Rightarrow$ (1) Define obvious valuation. ∎

Proposition 1.1.6. *R is a DVR iff it is a Noetherian local ring and its maximal ideal is generated by a non-nilpotent element π.*

Proof. By theorem 2.4.1 every element in R can be written as $\pi^n u$ for u a unit and $n \in \mathbb{N}_0$. It follows that R must be an integral domain, and so this expression is unique. Setting $v(\pi^n u) = n$ one can easily check that this defines valuation on $\mathrm{Frac}(R)$ with valuation ring R. ∎

Summary of useful properties of DVRs

1. If $a, b \in K = \mathrm{Frac}(R)$ have $\nu(a) \neq \nu(b)$ then $\nu(a+b) = \min(\nu(a), \nu(b))$.

1.2 Dedekind domains

Definition 1.2.1. A *Dedekind domain* is a normal Noetherian domain of Krull dimension 1.

Lemma 1.2.2. *Let R be a Noetherian domain of Krull dimension 1. Then R is a Dedekind domain iff every local ring $R_\mathfrak{p}$ for $\mathfrak{p} \neq 0$ is a DVR.*

1.2.1 Examples

PIDs

Thm 1.2.3. *Let R be a PID. Then R is a Dedekind domain.*

Proof. Certainly Noetherian. Also clearly has Krull dimension 1. Finally, $R_\mathfrak{p}$ is a local PID and hence a DVR for all $0 \neq \mathfrak{p} \lhd R$. ∎

Rings of integers

Thm 1.2.4. *Let $K/\mathbb{Q}$ be a number field and $\mathcal{O}_K$ its ring of algebraic integers. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. If $\alpha \in \mathrm{Frac}(\mathcal{O}_K) = K$ is integral over $\mathcal{O}_K$ then it is integral over $\mathbb{Z}$ and so lies in $\mathcal{O}_K$. Thus $\mathcal{O}_K$ is normal. To see that $\mathcal{O}_K$ is Noetherian note that it is finite over $\mathbb{Z}$ and hence Noetherian. Finally, $\mathcal{O}_K$ has Krull dimension 1 since it is integral over $\mathbb{Z}$ and $\mathbb{Z}$ has Krull dimension 1. ■

Coordinate rings

Thm 1.2.5. *Let V be an affine variety defined over an algebraically closed field k. Then $k[V]$ is a Dedekind domain iff V is non-singular, irreducible and of dimension 1.*

Proof. $k[V]$ is always Noetherian. V is irreducible iff $k[V]$ is a domain. V is of dimension 1 iff $k[V]$ has Krull dimension 1.

Now suppose $k[V]$ is a Dedekind domain. Then we know that all the local rings are normal Noetherian local domains i.e. DVRs and hence V must be non-singular. Conversely, suppose V is non-singular. Then all the local rings of $k[V]$ are DVRs and so $k[V]$ is a Dedekind domain. ■

1.2.2 Properties of Dedekind domains

1. Consider $\mathrm{Spec}(R)$ where R is a Dedekind domain. Then $\mathrm{Spec}(R)$ consists of closed points and a generic point.

2. For any prime ideal $\mathfrak{p} \lhd R$, we have natural inclusions $R \subseteq R_\mathfrak{p} \subseteq K = \mathrm{Frac}(R)$.

3. If we interpret K as the rational functions on $\mathrm{Spec}(R)$, then $\nu_\mathfrak{p}(k)$ is the degree of the pole/zero of k at the point $\mathfrak{p}$. Rational functions on $\mathrm{Spec}(R)$ have finitely many zeros/poles.

4. $\mathfrak{p} = R \cap (\mathfrak{p}R_\mathfrak{p})$. Thus for $r \in R$, $r \in \mathfrak{p}$ iff $\nu_\mathfrak{p}(r) \geq 1$.

5. An element $k \in K$ is in R iff $\nu_\mathfrak{p}(k) \geq 0$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$.

Rigorous part

Definition 1.2.6. Let R be a Dedekind domain with $K = \mathrm{Frac}(R)$. We call an R-submodule of K a fractional ideal if it is finitely generated as an R-module.

Remark 1.2.7. One can define the product of fractional ideals in the obvious way. Then the products of fractional ideals are fractional ideals.

lemma:frac_DVR **Lemma 1.2.8.** *Let R be a DVR with uniformising element π. Then all the non-zero fractional ideals of R are of the form $\pi^n R$ for $n \in \mathbb{Z}$.*

Proof. Elements in $K = \mathrm{Frac}(R)$ can uniquely be written in the form $\pi^n u$ for $n \in \mathbb{Z}, u \in R^\times$. The fact that fractional ideals are finitely generated ensures that they have an element with minimal valuation. The result follows. ■

Thm 1.2.9. *Let R be a Dedekind domain. Then all non-zero fractional ideals are invertible.*

Proof. Let $0 \neq \mathfrak{a}$ be a fractional ideal of R and $\mathfrak{a}' = (R : \mathfrak{a})$. It suffices to show that $\mathfrak{a}.\mathfrak{a}' = R$. But by lemma 1.2.8, we have $\mathfrak{a}_\mathfrak{p}\mathfrak{a}'_\mathfrak{p} = R_\mathfrak{p}$ for all prime ideals $0 \neq \mathfrak{p} \lhd R$. If $\mathfrak{p} = 0$ then $\mathfrak{a}_\mathfrak{p}\mathfrak{a}'_\mathfrak{p} = R_\mathfrak{p}$ holds by inspection. But $\mathfrak{a}.\mathfrak{a}' \subseteq R$ always holds and so we must have equality. ■

Corollary 1.2.10. *The set of non-zero fraction ideals of R form a group under multiplication.*

Remark 1.2.11. Note that $(R : xR) = x^{-1}R$.

lemma:DCC

Lemma 1.2.12. *Let $x \in R \backslash 0$. Then the set of ideals containing x satisfy the descending chain condition.*

Proof. Let $R \supseteq \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq xR$. Then $xR \subseteq x\mathfrak{a}_1^{-1} \subseteq x\mathfrak{a}_2^{-1} \subseteq \cdots \subseteq R$. The result now follows from the fact that R is a Noetherian domain. ■

prop:finite_prime

Proposition 1.2.13. *Let $x \in R \backslash 0$. Then only finitely many prime ideals contain x.*

Proof. Suppose $x \in \mathfrak{p}_1, \mathfrak{p}_2, \ldots$. By lemma 1.2.12, $\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supseteq \cdots$ must stabilise. Thus there is an n such that $\mathfrak{p}_n \supseteq \cap_{i=1}^{n-1}\mathfrak{p}_i$. But then there is an i such that $1 \leq i < n$ and $\mathfrak{p}_n \supseteq \mathfrak{p}_i$. Since R has Krull dimension 1 this forces $\mathfrak{p}_n = \mathfrak{p}_i$ and so we obtain a contradition. ■

Corollary 1.2.14. *Let $\nu_\mathfrak{p}$ denote the valution on $K = Frac(R)$ obtained from $R_\mathfrak{p}$ for $\mathfrak{p} \lhd R$ a prime. Then for $0 \neq x \in K$, the numbers $\nu_\mathfrak{p}(x)$ are almost all* 0.

Definition 1.2.15. Let $\mathfrak{a} \lhd R$ be a fractional ideal and let $\mathfrak{p} \lhd R$ be a prime ideal. Then $\mathfrak{a}_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^n$ for some $n \in \mathbb{Z}$. Define $\nu_\mathfrak{p}(\mathfrak{a}) = n$.

Remark 1.2.16. It follows from proposition 1.2.13 that the numbers $\nu_\mathfrak{p}(\mathfrak{a})$ are almost all 0.

Thm 1.2.17. *Let $0 \neq \mathfrak{a}$ be a fractional ideal. Then*

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}. \tag{1.3}$$

Proof. Localise. ■

Lemma 1.2.18. *Let $n_1, \ldots, n_k$ be integers, $x_1, \ldots, x_k \in R$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be distinct prime ideals of R. Then there exists an $x \in R$ such the $\nu_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all i.*

Proof. WLOG the $n_i \geq 0$. If $k = 1$ the result is trivial. Suppose $k \geq 2$. Let $\mathfrak{a} = \mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_k^{n_k}$. Then $\nu_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all $\mathfrak{p}$ and so $\mathfrak{a} = R$. Thus we can write $x_1 = y_{(1)} + x_{(1)}$ with $y_{(1)} \in \mathfrak{p}_1^{n_1}$ and $x_{(1)} \in \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_k^{n_k}$. It follows that $\nu_{\mathfrak{p}_1}(x_{(1)} - x_1) \geq n_1$ and $\nu_{\mathfrak{p}_i}(x_{(1)}) \geq n_i$ for all $i \neq 1$. If we define $x_{(i)}$ similarly and let $x = \sum_i x_{(i)}$ then we obtain $\nu_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all i. ■

Corollary 1.2.19. *Let $n_1, \ldots, n_k$ be integers, $x_1, \ldots, x_k \in K = Frac(R)$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be distinct prime ideals of R. Then there exists an $x \in K$ such the $\nu_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all i, and $\nu_{\mathfrak{q}}(x) \geq 0$ for $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k$.*

Proof. Write $x_i = a_i/s$ for $a_i \in R$ and $0 \neq s \in R$. Let $a \in R$ be such that $\nu_{\mathfrak{p}_i}(a - a_i) \geq n_i + \nu_{\mathfrak{p}_i}(s)$ and $\nu_{\mathfrak{q}}(a) \geq \nu_{\mathfrak{q}}(s)$ for $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Such an a exists since there are only finitely many $\mathfrak{q}$ for which $\nu_{\mathfrak{q}}(s) > 0$. Then $\nu_{\mathfrak{p}_i}(a/s - a_i/s) \geq n_i$ and $\nu_{\mathfrak{q}}(a/s) \geq 0$ for all $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k$. ■

Corollary 1.2.20. *Let $\mathfrak{a}$ be a fractional ideal of R. Then*

$$\mathfrak{a} = \{k \in K : \nu_{\mathfrak{p}}(k) \geq \nu_{\mathfrak{p}}(\mathfrak{a})\}. \tag{1.4}$$

Proof. Let $I = \{k \in K : \nu_{\mathfrak{p}}(k) \geq \nu_{\mathfrak{p}}(\mathfrak{a})\}$ and let $\mathfrak{p} \lhd R$ be a prime ideal. Then certainly $I_{\mathfrak{p}} \subseteq \mathfrak{a}_{\mathfrak{p}}$. Now suppose $k \in \mathfrak{a}_{\mathfrak{p}}$. To see that $k \in I_{\mathfrak{p}}$ we must show that there exists an $r \in R \backslash \mathfrak{p}$ such that $rk \in I$.

Let $r \in R$ be such that $\nu_{\mathfrak{q}}(r) \geq \nu_{\mathfrak{q}}(\mathfrak{a}) - \nu_{\mathfrak{q}}(k)$ for all $\mathfrak{q} \neq \mathfrak{p}$ and $\nu_{\mathfrak{p}}(r-1) \geq 1$. Such an r exists because there are only finitely many $\mathfrak{q}$ such that $\nu_{\mathfrak{q}}(\mathfrak{a}) - \nu_{\mathfrak{q}}(k) \neq 0$. Then $\nu_{\mathfrak{p}}(r) = \nu_{\mathfrak{p}}(r - 1 + 1) = 0$ and so $r \in R \backslash \mathfrak{p}$. Moreover, since $k \in \mathfrak{a}_{\mathfrak{p}}$ we also have $\nu_{\mathfrak{p}}(k) \geq \nu_{\mathfrak{p}}(\mathfrak{a})$. Therefore $\nu_{\mathfrak{q}}(rk) \geq \nu_{\mathfrak{q}}(\mathfrak{a})$ for all $\mathfrak{q}$. Thus $rk \in I$ and $r \in R \backslash \mathfrak{p}$. ■

Corollary 1.2.21. *A Dedekind domain with only finitely many prime ideals is principal.*

Proof. For every $\mathfrak{p} \lhd R$ there exists an $r \in R$ such that $\nu_{\mathfrak{q}}(r) = \delta_{\mathfrak{p},\mathfrak{q}}$. It follows that $\mathfrak{p} = (r)$. Thus all the prime ideals are principal, and hence all ideals are principal (since all ideals are a product of prime ideals). ■

Remark 1.2.22. To see why such a r exists, note that there exists a $\pi \in R$ such that $\nu_{\mathfrak{p}}(\pi) = 1$. Then let r be such that $\nu_{\mathfrak{p}}(r - \pi) \geq 2$ and $\nu_{\mathfrak{q}}(r - 1) \geq 1$.

Corollary 1.2.23. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be prime ideals in R and $n_1, \ldots, n_k \in \mathbb{Z}$. Then there exists a $x \in K := Frac(R)$ such that $\nu_{\mathfrak{p}_i}(x) = n_i$.*

Proof. Follows from the previous remark. ■

Definition 1.2.24. Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of R. We say that $\mathfrak{a} \mid \mathfrak{b}$ if there is an ideal $\mathfrak{c}$ of R such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

Corollary 1.2.25. *Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of R. Then $\mathfrak{a} \mid \mathfrak{b}$ iff $\mathfrak{a} \supseteq \mathfrak{b}$.*

Proof. ($\Rightarrow$) Obvious. ($\Leftarrow$) $\mathfrak{a} \supseteq \mathfrak{b}$ implies that $\nu_{\mathfrak{p}}(\mathfrak{b}) \geq \nu_{\mathfrak{p}}(\mathfrak{a})$ for all $\mathfrak{p}$. Thus $\nu_{\mathfrak{p}}(\mathfrak{a}^{-1}\mathfrak{b}) \geq 0$ for all $\mathfrak{p}$ and so is an ideal of R. ■

1.3 Extensions

Notation 1.3.1. Let K be a field and L a finite extension of K. Write n for $|L : K|$. Let A denote a Noetherian domain with $\mathrm{Frac}(A) = K$. We denote by B the integral closure of A in L. Note that if we let $S = A^\times$, then $B[S^{-1}] = B.K$ is the integral closure of K in L i.e. the whole of L. We say that (F) is satisfied if B is a finitely generated A-module.

Proposition 1.3.2. *Suppose hypothesis (F) is satisfied. If A is Dedekind then B is Dedekind.*

Proof. It is clear that B is Noetherian and normal. By the going up theorem $\dim(B) = \dim(A) = 1$ and so B is Dedekind. ∎

Definition 1.3.3. Suppose hypothesis (F) is satisfied. Let $\mathfrak{B}$ be a non-zero prime ideal of B. If $\mathfrak{p} = \mathfrak{B} \cap A$ then we say that $\mathfrak{B}$ divides $\mathfrak{p}$. This is a good definition because $\mathfrak{B}$ divides $\mathfrak{p}$ iff $\mathfrak{B}$ divides $\mathfrak{p}B$. We define $e_{\mathfrak{B}} = \nu_{\mathfrak{B}}(\mathfrak{p}B)$ and call it the ramification index of $\mathfrak{B}$ in the extension L/K. Note that

$$\mathfrak{p}B = \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}}}. \tag{1.5}$$

If $\mathfrak{B}$ divides $\mathfrak{p}$ then note that $B/\mathfrak{B}$ is a field extension of $A/\mathfrak{p}$. We call the degree of the extension $f_{\mathfrak{B}}$. This number is finite as B is finitely generated over A. When there is only one prime ideal $\mathfrak{B}$ dividing $\mathfrak{p}$ and $f_{\mathfrak{b}} = 1$ we say that L/K is *totally ramified* at $\mathfrak{p}$.

Thm 1.3.4. *Suppose hypothesis (F) is satisfied. Let $\mathfrak{p}$ be a non-zero prime ideal of A. The ring $B/\mathfrak{p}B$ is a $A/\mathfrak{p}$-algebra of degree n isomorphic to $\prod_{\mathfrak{B}|\mathfrak{p}} B/\mathfrak{B}^{e_{\mathfrak{B}}}$. Moreover*

$$n = \sum_{\mathfrak{B}|\mathfrak{p}} e_{\mathfrak{B}} f_{\mathfrak{B}}. \tag{1.6}$$

Proof. The isomorphism follows from the Chinese remainder theorem. Note that $A \cap \mathfrak{p}B = \mathfrak{p}$ and so $A/\mathfrak{p} \hookrightarrow B/\mathfrak{p}B$. It follows from 2.5.2 that the dimension of $B/\mathfrak{p}B$ as an $A/\mathfrak{p}$ vector space is $\sum_{\mathfrak{B}|\mathfrak{p}} e_{\mathfrak{B}} f_{\mathfrak{B}}$. It remains to show that this number is n. Let $S = A \backslash \mathfrak{p}$ and write $A' = A[S^{-1}]$ and $B' = B[S^{-1}]$. We have that $A/\mathfrak{p}A \cong A'/\mathfrak{p}A'$. To see that $B'/\mathfrak{p}B'$ note that S maps to $(A/\mathfrak{p})^\times$ in $B/\mathfrak{p}B$. By proposition 2.5.3, B' is a free A' module of rank n. It follows that $B/\mathfrak{p}B \cong B \otimes_A A/\mathfrak{p}$ is a dimension n $A/\mathfrak{p}$ vector space. ∎

Remark 1.3.5. Let $\mathfrak{B} \mid \mathfrak{p}$ and $x \in K$. Then $\nu_{\mathfrak{B}}(x) = e_{\mathfrak{B}} \nu_{\mathfrak{p}}(x)$. This follows from the fact that $\nu_{\mathfrak{B}}(x) = \nu_{\mathfrak{B}}(xB)$ and $\nu_{\mathfrak{p}}(x) = \nu_{\mathfrak{p}}(xA)$. We say that the valuation $\nu_{\mathfrak{B}}$ prolongs or extends $\nu_{\mathfrak{p}}$ with index $e_{\mathfrak{B}}$.

Proposition 1.3.6. *Let w be a discrete valuation on L extending $\nu_{\mathfrak{p}}$ with index e. Then there is a prime divisor $\mathfrak{B}$ of $\mathfrak{p}$ with $w = \nu_{\mathfrak{B}}$ and $e = e_{\mathfrak{B}}$.*

Proof. Let W be the ring of w and $\mathfrak{q}$ its maximal ideal. Since w extends $\nu_\mathfrak{p}$, $A \subseteq W$. Since W is integrally closed in L, $B \subseteq W$. Let $\mathfrak{B} = \mathfrak{q} \cap B$. Then it is clear that $\mathfrak{B} \cap A = \mathfrak{p}$ and so $\mathfrak{B}$ divides $\mathfrak{p}$. Moreover $B_\mathfrak{B} \subseteq W$. But $B_\mathfrak{B}$ is a maximal subring of L and so $W = B_\mathfrak{B}$. Thus $w = \nu_\mathfrak{B}$ and $e = e_\mathfrak{B}$. ∎

1.3.1 Hypthesis (F)

Proposition 1.3.7. *Hypothesis* (F) *is satisfied if* L/K *is a separable extension.*

Proof. $\mathrm{Tr} : L \to K$ gives rise to a symmetric non-degenerate K-bilinear form on L by composing it with the mulitplication map. Note that if $x \in B$ then $\mathrm{Tr}(x) \in A$ by integrality considerations.

Now let $\{e_i\}_i$ be a basis of L over K with the $e_i \in B$ (this exists because $B.K = L$) and let V be the free A-module spanned by the e_i's. For every A-submodule M of L, define

$$M^* = \{x \in L : \mathrm{Tr}(xy) \in A \ \forall y \in M\}. \tag{1.7}$$

Clearly $V \subseteq B \subseteq B^* \subseteq V^*$. Since A is Noetherian it thus suffices to show that V^* is a finitely generated A-module. Let $\{f_i\}$ be the dual basis of $\{e_i\}$ with respect to Tr. Then it is clear that V^* is the free A-module generated by the f_i. This completes the proof. ∎

1.4 Norm and Inclusion

Definition 1.4.1. Let A, B be as in the previous section and write I_A, I_B for their respective ideal groups. Define the homomorphisms $i : I_A \to I_B, N : I_B \to I_A$ by $i(\mathfrak{p}) = \mathfrak{p}B = \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_\mathfrak{B}}$ and $N(\mathfrak{B}) = \mathfrak{p}^{f_\mathfrak{B}}$ where $\mathfrak{B} \mid \mathfrak{p}$ and extend linearly.

1.4.1 Grothendieck Ring

Proposition 1.4.2. *Let* $\mathfrak{a}$ *be a fractional ideal of* A *and* $\mathfrak{p} \lhd A$ *a non-zero prime ideal of* A*. Then* $\mathfrak{a}/\mathfrak{p}\mathfrak{a} \cong A/\mathfrak{p}$ *as* A*-modules.*

Proof. Write $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{a_i}$ and wlog $\mathfrak{p} = \mathfrak{p}_1$. Let $x \in K := \mathrm{Frac}(A)$ be such that $\nu_{\mathfrak{p}_i}(x) = a_i$. Then $x \in \mathfrak{a} \backslash \mathfrak{p}\mathfrak{a}$. Now define the map $A \to \mathfrak{a}/\mathfrak{p}\mathfrak{a}$ by $r \mapsto rx$. It clearly descends to $A/\mathfrak{p}$ and so we obtain a map $\phi : A/\mathfrak{p} \to \mathfrak{a}/\mathfrak{p}\mathfrak{a}$. Since $\mathfrak{p}$ is maximal the kernel must be trivial. For surjectivity note that $\mathfrak{p}\mathfrak{a} \subsetneq \mathfrak{p}\mathfrak{a} + Ax \subseteq \mathfrak{a}$ and so by looking at the prime factorisation we must have $\mathfrak{p}\mathfrak{a} + Ax = \mathfrak{a}$. ∎

Definition 1.4.3. Let $\mathcal{C}_A$ be the category of A-modules of finite length. This is an abelian category so let $R(\mathcal{C}_A)$ denote the Grothendieck group of $\mathcal{C}_A$.

If $M \in \mathcal{C}_A$ we have a composition series $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_m = M$. The quotients M_i/M_{i-1} are isomorphic to $A/\mathfrak{p}_i$ for some $\mathfrak{p}_i$ a non-zero prime ideal of A. Define $\chi_A(M) = \prod_i \mathfrak{p}_i \in I_A$. This is well defined by the Jordan-Holder theorem. Moreover it is clear that $\chi_A : (R(\mathcal{C}_A), +) \to I_A$ is a homomorphism.

Proposition 1.4.4. *Let $\mathfrak{a} \subseteq \mathfrak{b}$ be fractional ideals of A. Then $\chi_A(\mathfrak{b}/\mathfrak{a}) = \mathfrak{a} \cdot \mathfrak{b}^{-1}$. In particular $\chi_A(A/\mathfrak{a}) = \mathfrak{a}$ for ideals $\mathfrak{a} \lhd A$.*

Proof. Take the obvious composition series. ∎

Corollary 1.4.5. *χ_A is an isomorphism.*

Remark 1.4.6. Note that $\mathcal{C}_B$ naturally includes into $\mathcal{C}_A$.

Proposition 1.4.7. *Let $M \in \mathcal{C}_B$. Then $\chi_A(M) = N(\chi_B(M))$. In other words*

$$\begin{tikzcd} I_B \arrow[r, "N"] & I_A \\ R(\mathcal{C}_B) \arrow[u, "\chi_B"] \arrow[r] & R(\mathcal{C}_A) \arrow[u, "\chi_A"'] \end{tikzcd} \tag{1.8}$$

commutes.

Remark 1.4.8. Tensoring by B gives a functor $\otimes_A B : \mathcal{C}_A \to \mathcal{C}_B$.

Proposition 1.4.9. *$\otimes_A B$ is an exact functor.*

Proof. Suffices to check locally. But $B_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module. ∎

Proposition 1.4.10. *The following diagram commutes*

$$\begin{tikzcd} I_A \arrow[r, "i"] & I_B \\ R(\mathcal{C}_A) \arrow[u, "\chi_A"] \arrow[r, "R(\otimes_A B)"] & R(\mathcal{C}_B). \arrow[u, "\chi_B"'] \end{tikzcd} \tag{1.9}$$

Proof. Suffices to check for $A/\mathfrak{p}$. But $i(\chi_A(A/\mathfrak{p})) = \mathfrak{p}B = \chi_B(B/\mathfrak{p}B)$. ∎

Proposition 1.4.11. *Let $x \in L$. Then $N(xB) = N_{L/K}(x)A$.*

1.5 Simple extensions

Let A be a local ring with maximal ideal $\mathfrak{m}$ and residue field k, $f \in A[x]$ and $B_f := A[x]/f$. We have

$$\bar{B}_f := B_f/\mathfrak{m}B_f \cong A[x]/(\mathfrak{m}, f) \cong k[x]/(\bar{f}) \tag{1.10}$$

where $\bar{f}$ is the reduction of f to $k[x]$. Let $\bar{f} = \prod_i \phi_i^{e_i}$ be the decomposition of $\bar{f}$ into irreducibles, and for each ϕ pick a $g_i \in A[x]$ such that $\bar{g}_i = \phi_i$. Write $\mathfrak{m}_i$ for the ideal in B_f generated by $\mathfrak{m}$ and the image of g_i in B_f.

Proposition 1.5.1. *The ideals $\mathfrak{m}_i$ are maximal and distint and are all the maximal ideals of B_f. Moreover $B_f/\mathfrak{m}_i \cong k_i := k[x]/(\phi_i)$.*

Proof. $\mathfrak{m}_i$ is the preimage of $(\phi_i)/(f) \lhd \bar{B}_f$ in B_f. Thus $B_f/\mathfrak{m}_i \cong k_i$ and so the $\mathfrak{m}_i$ are distinct and maximal. To show that every maximal ideal is one of the $\mathfrak{m}_i$ it suffices to show that if $\mathfrak{n}$ is maximal it contains $\mathfrak{m}$. If not then $\mathfrak{m}B_f + \mathfrak{n} = B_f$ which would imply that $\mathfrak{n} = B_f$ (by Nakayama) which is a contradiction. ■

1.5.1 Unramified case

Suppose $\bar{f}$ is irreducible and A is a DVR. Then B_f is a DVR with maximal ideal $\mathfrak{m}B_f$ and residue field $k[x]/(\bar{f})$.

1.6 Galois Extensions

Let A, B be as before, but suppose additionally that L/K is a Galois extension. Write $G(L/K)$ for the Galois gorup of the extension.

Proposition 1.6.1. *$G(L/K)$ acts transitively on the set of primes in B dividing $\mathfrak{p} \lhd A$.*

Corollary 1.6.2. *Let $\mathfrak{p}$ be a non-zero prime ideal of A. Then integers $e_{\mathfrak{B}}$ and $f_{\mathfrak{B}}$ (for $\mathfrak{B} \mid \mathfrak{p}$) only depend on $\mathfrak{p}$. If we denote these numbers $e_{\mathfrak{p}}, f_{\mathfrak{p}}$, and $g_{\mathfrak{p}}$ for the number of prime ideals in B dividing $\mathfrak{p}$ then $n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$.*

Definition 1.6.3. Define $D_{\mathfrak{B}}(L/K) =_{G(L/K)} (\mathfrak{B})$.

CHAPTER 2

Appendix - Commutative algebra results

2.1 Prime ideals

lemma:prime_avoidance **Lemma 2.1.1.** *(Prime avoidance lemma). Let $I \lhd R$ be an ideal and let $P_1, \dots, P_k \lhd R$ be prime ideals. If $I \subseteq \cup_i P_i$ then there exists an i such that $I \subseteq P_i$.*

2.2 Localisation

Proposition 2.2.1. *Let $\mathfrak{a}, \mathfrak{b} \lhd R$ be ideals and $\mathfrak{p} \lhd R$ a prime ideal. Then*

$$(1)\ (\mathfrak{a}+\mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} + \mathfrak{b}_{\mathfrak{p}}, \quad (2)\ (\mathfrak{a}.\mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}.\mathfrak{b}_{\mathfrak{p}}, \quad (3)\ (\mathfrak{a}:\mathfrak{b})_{\mathfrak{p}} = (\mathfrak{a}_{\mathfrak{p}}:\mathfrak{b}_{\mathfrak{p}}) \tag{2.1}$$

where (3) *additionally requires $\mathfrak{b}$ to be finitely generated.*

Proof. (1) and (2) are trivial. For (3) note that $(\subseteq)$ always holds. Now suppose $\mathfrak{b} = (b_1, \dots, b_k)$. If $r/s \in (\mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}})$ then so is $r/1$. Thus we have $(r/1)(b_i/1) = a_i/s_i$ for some $a_i \in \mathfrak{a}, s_i \notin \mathfrak{p}$. Thus there is a $u_i \notin \mathfrak{p}$ such that $(u_i s_i)(r b_i) = u_i a_i \in \mathfrak{a}$. Let $u = \prod_i (u_i s_i)$. Then $(ur)b_i \in \mathfrak{a}$ for all i. Thus $ur \in (\mathfrak{a} : \mathfrak{b})$ and so $r/1 = ur/u \in (\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}}$ and so r/s is too. ■

Proposition 2.2.2. *Let $\mathfrak{a}, \mathfrak{b}$ be R-submodules of $K = Frac(R)$ and $\mathfrak{p} \lhd R$ a prime ideal. Then*

$$(1)\ (\mathfrak{a}+\mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} + \mathfrak{b}_{\mathfrak{p}}, \quad (2)\ (\mathfrak{a}.\mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}.\mathfrak{b}_{\mathfrak{p}}, \quad (3)\ (\mathfrak{a}:\mathfrak{b})_{\mathfrak{p}} = (\mathfrak{a}_{\mathfrak{p}}:\mathfrak{b}_{\mathfrak{p}}) \tag{2.2}$$

where (3) *additionally requires $\mathfrak{b}$ to be finitely generated and $(\mathfrak{a} : \mathfrak{b}) := \{k \in K : k\mathfrak{b} \subseteq \mathfrak{a}\}$.*

Proof. First note that $\mathfrak{a}_{\mathfrak{p}} = \{\frac{1}{s}k : s \in R \backslash \mathfrak{p}, k \in \mathfrak{a}\}$. Then (1) and (2) follow. For (3), $(\subseteq)$ always holds. If $\mathfrak{b}$ is additionally finitely generated, let $k_1, \dots, k_n$ be its generators. For $k \in (\mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}})$, we have that for each i there are $a_i \in \mathfrak{a}, s_i \notin \mathfrak{p}$ such that $kk_i = \frac{1}{s_i} a_i$. Let $s = \prod_i s_i$. Then $skk_i \in \mathfrak{a}$ for all i. Thus $sk \in (\mathfrak{a} : \mathfrak{b})$ and so $k \in (\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}}$. ■

2.3 Integrality

thm:int_dep **Thm 2.3.1.** *Let $S \subseteq R$ be rings and $x \in R$. The following are equivalent:*

1. *x is integral over S*
2. *$S[x]$ is a finite S-algebra*
3. *$S[x]$ is contained ina subring $T \subseteq R$ that is a finite S-alg*
4. *There is an $S[x]$-module M such that $Ann_{S[x]}(M) = 0$ and M is finitely generated as a S-module.*

Lemma 2.3.2. *Let $S \subseteq R$ be an integral extension of rings. Let $Q \lhd R$ be a prime ideal, and set $P = Q \cap S$. Then Q is maximal in R iff P is maximal in S.*

Lemma 2.3.3. *(Incomparability). Let $S \subseteq R$ be an integral extension of rings. Let $Q, Q' \lhd R$ be prime ideals with $Q \subseteq Q'$ and $Q \cap S = Q' \cap S$. Then $Q = Q'$.*

Lemma 2.3.4. *(Lying over). Let $S \subseteq R$ be an integral extension of rings. Let $P \lhd S$ be prime. Then there exists a prime $Q \lhd R$ such that $Q \cap S = P$.*

thm:going_up **Thm 2.3.5.** *(Going up). Let $S \subseteq R$ be an integral extension of rings. Let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$ be a chain of primes in S and $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ with $0 \leq m < n$ be a chain of primes in R with $Q_i \cap S = P_i$. Then the chain can be extended to $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_n$ with $Q_i \cap S = P_i$.*

thm:going_down **Thm 2.3.6.** *(Going down). Let $S \subseteq R$ be an integral extension of domains such that S is normal. Let $P_1 \supseteq P_2 \supseteq \cdots \supseteq P_n$ be a chain of primes in S and $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_m$ with $0 \leq m < n$ be a chain of primes in R with $Q_i \cap S = P_i$. Then the chain can be extended to $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_n$ with $Q_i \cap S = P_i$.*

Proposition 2.3.7. *Let $A \subset R$ be rings and S a multiplicativly subset of A. If B is the integral closure of A in R then $B[S^{-1}]$ is the integral closure of $A[S^{-1}]$ in $R[S^{-1}]$.*

2.4 Noetherian Local Rings

thm:noeth_loc_ring **Thm 2.4.1.** *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then $\cap_n \mathfrak{m}^n = 0$.*

2.5 Miscellaneous Results on DVRs and Dedekind domains

Proposition 2.5.1. *Let R be a Dedekind domain and $\mathfrak{p} \lhd R$ be a prime ideal. Then for any $n \geq 1$,*

$$R/\mathfrak{p}^n \cong R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}^n. \tag{2.3}$$

Proof. We have the short exact sequence

$$0 \to \mathfrak{p}^n \to R \to R/\mathfrak{p}^n \to 0. \tag{2.4}$$

Localising at $\mathfrak{p}$ we get that

$$R_{\mathfrak{p}}/\mathfrak{p}^n_{\mathfrak{p}} \cong (R/\mathfrak{p}^n)_{\mathfrak{p}/\mathfrak{p}^n} \tag{2.5}$$

and so it suffices to show that all the elements not in $\mathfrak{p}/\mathfrak{p}^n$ are invertible in $R/\mathfrak{p}^n$. For this let $r \in R\backslash\mathfrak{p}$. Then $(r) + \mathfrak{p} = R$ and so $(r) + \mathfrak{p}^n = R$. It follows that $r + \mathfrak{p}^n$ is invertible in $R/\mathfrak{p}^n$. ■

prop:q_dim **Proposition 2.5.2.** *Let R be a DVR with maximal ideal $\mathfrak{m}$ and let k be a field in $R/\mathfrak{m}^n$. Then $\dim_k(R/\mathfrak{m}^n) = n \cdot |R/\mathfrak{m} : k|$.*

Proof. We have the following chain of ideals, and hence k vector spaces

$$0 \subseteq \mathfrak{m}^{n-1}/\mathfrak{m}^n \subseteq \cdots \subseteq \mathfrak{m}/\mathfrak{m}^n \subseteq R/\mathfrak{m}^n. \tag{2.6}$$

It follows that $\dim_k(R/\mathfrak{m}^n) = \sum_{i=0}^{n-1} \dim_k(\mathfrak{m}^i/\mathfrak{m}^{i+1})$. But $\mathfrak{m}^i/\mathfrak{m}^{i+1} \cong \mathfrak{m}^i \otimes_R R/\mathfrak{m} \cong R/\mathfrak{m}$ since $\mathfrak{m}^i \cong R$ as R-modules. As k naturally lives inside $R/\mathfrak{m}$ the result follows. ■

prop:DVR_closure **Proposition 2.5.3.** *Let R be a DVR and $K = Frac(R) \leq L$ be a finite field extension. Let S be the integral closure of R in L, and suppose that S is a finitely generated R-module. Then S is a free module of rank $|L : K|$.*

Proof. R is a PID so S is a free R-module. Suppose $\alpha_1, \ldots, \alpha_k$ are an R-basis for S. Since $K.S = L$, $\alpha_1, \ldots, \alpha_k$ span L as a K vector space. But since $K = \mathrm{Frac}(R)$, they are also linearly independent over K and so $k = |L : K|$. ■

Proposition 2.5.4. *Let R be a DVR. Then R is a maximal subring of $Frac(R)$.*

Proof. Obvious. ■