6 Extensions of Dedekind rings

6.1 Modules over Dedekind rings

Let A be a Dedekind ring with quotient field K.

$A = \mathbb{Z}$

Definition 6.1.1: Consider an A-module M.

$\exists n \neq 0 : n \cdot m = 0$

(a) An element $m \in M$ is called *torsion* if there exists $a \in A \setminus \{0\}$ such that $am = 0$.

(b) The module M is called *torsion* if every element of M is torsion.

(c) The module M is called *torsion-free* if no non-zero element of M is torsion.

Theorem 6.1.2: Any finitely generated A-module is isomorphic to the direct sum of a torsion module and a torsion-free module.

Theorem 6.1.3: Any non-zero finitely generated torsion-free A-module is isomorphic to $\mathfrak{a} \oplus A^{r-1}$ for a non-zero ideal $\mathfrak{a} \subset A$ and an integer $r \geqslant 1$.

Theorem 6.1.4: Any finitely generated torsion A-module is isomorphic to

(a) $\bigoplus_{i=1}^{r} A/\mathfrak{p}_i^{e_i}$ for $r \geqslant 0$ and maximal ideals $\mathfrak{p}_i \subset A$ and integral exponents $e_i \geqslant 1$.

(b) $\bigoplus_{i=1}^{s} A/\mathfrak{a}_i$ for $s \geqslant 0$ and non-zero ideals $\mathfrak{a}_s \subset \ldots \subset \mathfrak{a}_1 \subsetneq A$.

Proposition 6.1.5: Consider a K-vector space V of finite dimension n and a finitely generated A-submodule $M \subset V$ that generates V over K. Then M is isomorphic to a direct sum of n fractional ideals of A.

Proof: Induction on n.

$n=0$ clear.

$n>0$: Choose $\ell : V \twoheadrightarrow K$ K-linear.

$\Rightarrow$ $\ell(M) \subset K$ nonzero fin. gen. A-module

$\Rightarrow$ $\mathfrak{a} = \ell(M)$ = fractional ideal of A.

Recall $\mathfrak{a}^{-1}\cdot\mathfrak{a} = A$.

Choose $a_1,\dots,a_n$ generators of $\mathfrak{a}$ and $b_1,\dots,b_n \in \mathfrak{a}^{-1}$ with $\sum b_i a_i = 1$.

Choose $m_i \in M$ with $\ell(m_i) = a_i$.

$$0 \to V' := \ker(\ell) \to V \xrightarrow{\ell} K \to 0$$

$$0 \to M' := M \cap V' \to M \underset{s}{\leftrightarrows} \mathfrak{a} \to 0, \qquad m_i \mapsfrom a_i$$

well defined.

A-linear map: $\sum_i (x b_i) m_i \longleftarrow\!\!\shortmid\; x$ $\quad (\in \mathfrak{a}\cdot\mathfrak{a}^{-1} = A)$

$$\ell\circ s(x) = \sum_i x b_i \cdot \ell(m_i) = \sum x b_i a_i = x.$$

$\mathrm{id} - s\circ\ell : M \to M'$ because $\ell\circ(\mathrm{id}-s\circ\ell) = \ell - \ell\circ s\circ\ell = \ell - \ell = 0$.

$\Rightarrow$ $\boxed{M' \oplus \mathfrak{a} \cong M}$, $(m', x) \mapsto m' + s(x)$; $\quad ((\mathrm{id}-s\ell)(m), \ell(m)) \mapsfrom m$

M' fin. gen. A-module generating V' over K.

Finish by induction. qed

Proposition 6.1.6: For any fractional ideals $\mathfrak{a}, \mathfrak{b}$ of A there is a natural isomorphism

$$\mathfrak{b}\mathfrak{a}^{-1} \xrightarrow{\sim} \mathrm{Hom}_A(\mathfrak{a},\mathfrak{b}), \quad c \mapsto (\varphi_c : a \mapsto ca).$$

$n, m > 0$

$n\mathbb{Z} \to m\mathbb{Z}$

$\in \mathfrak{b}\mathfrak{a}^{-1}\cdot\mathfrak{a} = \mathfrak{b}$

$\Rightarrow$ well defined.

Proof:

Localize over K $\leadsto$ injective.

Take $\psi \in \mathrm{Hom}_A(\mathfrak{a},\mathfrak{b})$.

Pick $a \in \mathfrak{a}$, $a \neq 0$ and set $c := \psi(a)\cdot a^{-1} \in K$.

Then $\psi(a) = ca$.

$\forall a' \in \mathfrak{a}$: Choose $x' \in A\setminus\{0\}$ and $x \in A$, $a'x' = ax$.

$\Rightarrow$ $\psi(a')x' = \psi(a'x') = \psi(ax) = \psi(a)x = cax = ca'x'$

$\Rightarrow$ $\psi(a') = ca'$.

So $c\cdot\mathfrak{a} \subset \mathfrak{b}$ $\Rightarrow$ $c \in c\mathfrak{a}\mathfrak{a}^{-1} \subset \mathfrak{b}\mathfrak{a}^{-1}$

So $\psi = \varphi_c$ qed

$$\begin{array}{ccccc} L & \supset & B & \supset & \mathfrak{q} \\ | & & | & & | \\ K & \supset & A & \supset & \mathfrak{p} = \mathfrak{q} \cap A \end{array}$$

that generates L as K-vector space

6.2 Decomposition of prime ideals

For the rest of this chapter we take a finite separable field extension L/K of degree n. Then the integral closure B of A in L is a finitely generated ~~projective~~ A-module ~~of rank n~~ and itself a Dedekind ring. For any maximal ideal $\mathfrak{p} \subset A$ we abbreviate the residue field by $k(\mathfrak{p}) := A/\mathfrak{p}$, and likewise for any maximal ideal of B. Where applicable we let C be the integral closure of B in a finite separable extension M/L.

Consider a maximal ideal $\mathfrak{p} \subset A$. Then $\mathfrak{p}B$ is a non-zero ideal of B and therefore has a prime factorization

unique

$$\mathfrak{p}B \;=\; \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

with distinct maximal ideals $\mathfrak{q}_i \subset B$ and integral exponents $e_i \geqslant 1$.

Proposition 6.2.1: (a) The ideals $\mathfrak{q}_i$ are precisely the prime ideals of B above $\mathfrak{p}$.

(b) For each i the residue field $k(\mathfrak{q}_i)$ is a finite extension of the residue field $k(\mathfrak{p})$.

(c) Letting f_i denote the degree of this residue field extension, we have

$$\boxed{\sum_{i=1}^{r} e_i f_i = n.}$$

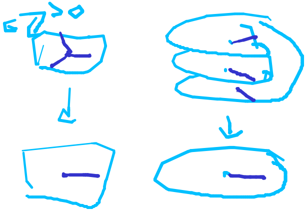
Proof: (a) $\mathfrak{p} \subset \mathfrak{p}B \subset \mathfrak{q}_i \Rightarrow \underset{\text{maximal}}{\mathfrak{p}} \subset \mathfrak{q}_i \cap A$ = prime ideal of A. $\Rightarrow \mathfrak{p} = \mathfrak{q}_i \cap A$, i.e.: $\mathfrak{q}_i$ over $\mathfrak{p}$.

$\mathfrak{q} \subset B$ prime ideal over $\mathfrak{p} \Rightarrow \mathfrak{p} \subset \mathfrak{q} \Rightarrow \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} = \mathfrak{p}B \subset \mathfrak{q} \Rightarrow \exists i : \underset{\text{maximal}}{\mathfrak{q}_i} \subset \mathfrak{q}$. $\Rightarrow \mathfrak{q}_i = \mathfrak{q}$.

(b–c) 6.1.5: $B \cong \bigoplus_{i=1}^{n} \mathfrak{a}_i \Rightarrow B/\mathfrak{p}B \cong \bigoplus_{i=1}^{n} \mathfrak{a}_i/\mathfrak{p}\mathfrak{a}_i \cong \bigoplus_{i=1}^{n} A/\mathfrak{p}$ by 1.11.9 $\Rightarrow B/\mathfrak{p}B$ is a $k(\mathfrak{p})$-vector space of dimension n. $B/\mathfrak{p}B = B/\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ is a successive extension of e_i copies of $B/\mathfrak{q}_i$ for all i by 1.11.9

$$\Rightarrow \quad n = \dim_{k(\mathfrak{p})}(B/\mathfrak{p}B) = \sum_{i=1}^{r} e_i \cdot \dim_{k(\mathfrak{p})}(B/\mathfrak{q}_i) = \sum_{i=1}^{r} e_i \cdot f_i \qquad \text{qed.}$$

Example: $\mathbb{C} \to \mathbb{C}$, $z \mapsto z^e$, for $e \in \mathbb{Z}_{>0}$.



$$\mathbb{C}[z] \leftarrow \mathbb{C}[z]$$

$$f(z^e) \leftarrow\!\!| \; f(z)$$

Definition 6.2.2:

(a) The number $e_{\mathfrak{q}_i|\mathfrak{p}} := e_i$ is called the *ramification degree of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$.

(b) The number $f_{\mathfrak{q}_i|\mathfrak{p}} := f_i$ is called the *inertia degree of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$.

(c) We call $\mathfrak{q}_i$ *unramified over* $\mathfrak{p}$ if $e_i = 1$.

(d) We call $\mathfrak{q}_i$ *ramified over* $\mathfrak{p}$ if $e_i > 1$.

Definition 6.2.3:

(a) We call $\mathfrak{p}$ *unramified in* B if all $e_i = 1$, that is, if $\mathfrak{p}B = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ ← with distinct prime factors $\mathfrak{q}_i$.

(b) We call $\mathfrak{p}$ *ramified in* B if some $e_i > 1$.

(c) We call $\mathfrak{p}$ *totally split in* B if all $e_i = f_i = 1$, that is, if $r = n$ and $\mathfrak{p}B = \mathfrak{q}_1 \cdots \mathfrak{q}_n$.

(d) We call $\mathfrak{p}$ *totally inert in* B if $r = e_1 = 1$, that is, if $\mathfrak{p}B$ is prime.

(e) We call $\mathfrak{p}$ *totally ramified in* B if $r = f_1 = 1$, that is, if $\mathfrak{p}B = \mathfrak{q}^n$ for a prime $\mathfrak{q} \subset B$.

Proposition 6.2.4: Suppose that $B = A[\beta]$ and let $f \in A[X]$ be the minimal polynomial of β above K. Set $\bar f := f \bmod \mathfrak{p}$ and write $\bar f = \prod_{i=1}^r \bar f_i^{e_i}$ with inequivalent irreducible factors $\bar f_i \in k(\mathfrak{p})[X]$ and integral exponents $e_i \geqslant 1$. Choose $f_i \in A[X]$ with $\bar f_i = f_i \bmod \mathfrak{p}$. Then $\mathfrak{p}B = \prod_{i=1}^r \mathfrak{q}_i^{e_i}$ with the distinct prime ideals $\mathfrak{q}_i := \mathfrak{p}B + f_i(\beta)B$.

Proof: $B \cong A[X]/(f)$, $\quad \beta \leftarrow X$

$\Rightarrow B/\mathfrak{p}B \cong A[X]/(\mathfrak{p}A[X] + (f))$

$\cong (A/\mathfrak{p})[X]/(\bar f)$

$= k(\mathfrak{p})[X]/(\prod_{i=1}^r \bar f_i^{e_i})$

$\mathfrak{q} \subset B$ over $\mathfrak{p}$ $\Rightarrow B/\mathfrak{q} \twoheadleftarrow B/\mathfrak{p}B$.

$\supset (\mathfrak{p}A[X] + (f_i)) \longleftarrow \mathfrak{p}B + (f_i(\beta))$

$\updownarrow$

$\supset$ maximal ideals $(\bar f_i)$

Compute $\prod_{i=1}^r \mathfrak{q}_i^{e_i} = \prod_{i=1}^r (\mathfrak{p}B + (f_i(\beta)))^{e_i} \subset \mathfrak{p}B + (\prod_{i=1}^r f_i(\beta)^{e_i})$

$= \mathfrak{p}B + (f(\beta)) = \mathfrak{p}B.$

$n = \dim_{k(\mathfrak{p})}(B/\mathfrak{p}B) = \deg(\bar f) = \sum_{i=1}^r \deg(\bar f_i)\cdot e_i = \sum_{i=1}^r \dim_{k(\mathfrak{p})}(B/\mathfrak{q}_i)\cdot e_i = \dim_{k(\mathfrak{p})}(B/\prod_{i=1}^r \mathfrak{q}_i^{e_i})$

So $B/\prod \mathfrak{q}_i^{e_i} \twoheadrightarrow B/\mathfrak{p}B$. $\Rightarrow$ equality. So $\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$.

qed

Example 6.2.5: Take $L = \mathbb{Q}(\sqrt{d}\,)$ with $d \in \mathbb{Z} \smallsetminus \{1\}$ squarefree. Then an odd prime p of $\mathbb{Z}$ with

$2 = \sum e_i f_i$

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{is (totally) ramified in } \mathcal{O}_L, \\ 1 & \text{is (totally) decomposed in } \mathcal{O}_L, \\ -1 & \text{is (totally) inert in } \mathcal{O}_L. \end{cases}$$

$r = 1,\ f_1 = 1,\ e_1 = 2$

$r = 2,\ f_i = e_i = 1$

$r = 1,\ f_1 = 2,\ e_1 = 1$

Proposition 6.2.6: For any a prime $\mathfrak{r} \subset C$ above $\mathfrak{q} \subset B$ above $\mathfrak{p} \subset A$ we have

$$e_{\mathfrak{r}|\mathfrak{p}} = e_{\mathfrak{r}|\mathfrak{q}} \cdot e_{\mathfrak{q}|\mathfrak{p}} \qquad \text{and} \qquad f_{\mathfrak{r}|\mathfrak{p}} = f_{\mathfrak{r}|\mathfrak{q}} \cdot f_{\mathfrak{q}|\mathfrak{p}}.$$