Michiel Filip Kosters
mkosters@math.leidenuniv.nl

Anisotropic modules and the integral closure

Master Thesis, defended on June 21, 2010

Thesis advisor: prof.dr. H.W. Lenstra

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction

All rings and algebras are assumed to be commutative with 1.

1. Summary

Let $K \supset \mathbf{Q}$ be a number field. An important problem in algebraic number theory is to find $\mathcal{O}_K$, the ring of integers inside K. This is defined to be the integral closure of $\mathbf{Z}$ inside K. In general one starts with an order, say $\mathbf{Z}[\alpha] \subseteq \mathcal{O}_K$ with $\mathbf{Q}(\alpha) = K$. The first step for finding $\mathcal{O}_K$, is to factor the discriminant of this order. After this has been done, most algorithms keep finding bigger orders until one obtains the integral closure. In this thesis, we will develop a method for this last step which uses techniques different from most algorithms. With these techniques, one can sometimes find the ring of integers without doing much work, and just write it down directly.

We will now explain these techniques in some more detail. In this thesis we have considered a bit more general situation. Let R be a Dedekind domain (Definition 1.4.3). We define an *order* over R to be an R-algebra A which is a finitely generated and torsion-free R-module which has a non-degenerate trace map on its total quotient ring $Q(A)$ (Definition 1.4.11 and Definition 1.3.7). If $A \neq 0$ we have an inclusion $R \subseteq A$ and we want to know the integral closure $\overline{A}$ of R inside $Q(A)$ (this is the set of elements in $Q(A)$ which are a zero of a monic polynomial in $R[x]$). There are various approaches for calculating this integral closure. In this thesis we will approach this problem from a rather unusual perspective. We will try to get as much information about the integral closure by just looking at the trace map itself.

Now let A be an order with trace map $\mathrm{Tr}_{Q(A)/Q(R)}$. We define its *trace dual* as follows:

$$A^\dagger = \{x \in Q(A) : \mathrm{Tr}_{Q(A)/Q(R)}(xA) \subseteq R\}.$$

Then one can show that $A \subset \overline{A} \subset A^\dagger \subset Q(A)$ and $\overline{A}$ is itself an order (Lemma 1.4.15).

We say that A is tame at a nonzero prime $\mathfrak{p} \subset R$ if the radical of the map

$$\begin{aligned} A/\mathfrak{p}A \times A/\mathfrak{p}A &\to R/\mathfrak{p} \\ (x, y) &\mapsto \mathrm{Tr}_{A/\mathfrak{p}A/R/\mathfrak{p}}(xy) \end{aligned}$$

is the nilradical of $A/\mathfrak{p}A$ (Definition 1.3.11).

Then we have the following theorem (Theorem 2.3.1), which will be the main result of Chapter 2.

Theorem 1. *Let A be an order over a Dedekind domain R. Let $\mathfrak{p} \subset R$ be a nonzero prime ideal and assume that A is tame at $\mathfrak{p}$. Then $\mathfrak{p} \mid \mathrm{Ann}_R(\overline{A}/A)$ iff $\mathfrak{p}^2 \mid \mathrm{Ann}_R(A^\dagger/A)$.*

If $R = \mathbf{Z}$ then $A^\dagger/A$ is just a finite group and we see whether A is integrally closed at a tame prime $(p) \subset \mathbf{Z}$ by just looking if $A^\dagger/A$ has an element of order p^2.

We will now try to exploit this theorem. Let $M = A^\dagger/A$. If we let $I = \mathrm{Ann}_R(M)$, then the trace map induces a non-degenerate symmetric R/I-bilinear form

$$\langle\ ,\ \rangle : M \times M \to I^{-1}/R$$

(Lemma 4.1.3). One can see that $M' = \overline{A}/A$ satisfies $\sqrt{0}_{R/I} \cdot M'^{\perp} \subseteq M' \subseteq M'^{\perp}$ under some tameness assumptions. One can also show that the *lower root* of M,

$$\mathrm{lr}(M) \quad = \quad \sum_{r \in R/I} (rM) \cap M[r],$$

satisfies these properties (Lemma 3.5.6). We now define such a non-degenerate symmetric bilinear map $\langle\ ,\ \rangle : M \times M \to I^{-1}/R$ to be *anisotropic* if $\mathrm{lr}(M)$ is the unique submodule $L \subseteq M$ with $\sqrt{0}_{R/I} \cdot L^{\perp} \subseteq L \subseteq L^{\perp}$ (Definition 3.5.7). We then have the following theorem (Theorem 4.2.3).

Theorem 2. *Let A be an order over a Dedekind domain R. Let $\mathrm{Ann}_R(A^\dagger/A) = I$. Suppose that $\overline{A}$ is tame at all nonzero primes of R. Suppose that $\langle\ ,\ \rangle : A^\dagger/A \times A^\dagger/A \to I^{-1}/R$ is anisotropic. Then $\overline{A}/A = \mathrm{lr}(A^\dagger/A)$.*

From the considerations above we see that it is important to understand the intersection of all modules $L \subset M$ with $\sqrt{0}_{R/I} \cdot L^{\perp} \subseteq L \subseteq L^{\perp}$ (we will call this the *radical root*) and we will also study this.

We define a *uniserial ring* to be a local zero-dimensional principal ideal ring. One can show that instead of looking at non-degenerate symmetric bilinear forms over zero-dimensional principal ideal rings (such as R/I), we can look at forms over uniserial rings. This will give us local versions of the previous theorem. So suppose that R is a uniserial ring, M a finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric bilinear form. Let $\mathfrak{m}$ be the maximal ideal of R. In this case we say that the form $\langle\ ,\ \rangle$ is *anisotropic* if it is non-degenerate and the only submodule $L \subseteq M$ satisfying $\sqrt{0} \cdot L^{\perp} \subseteq L \subseteq L^{\perp}$ is $\mathrm{lr}(M)$. This definition coincides with the normal definition of anisotropy if R is a field (Remark 5.3.2). From $\langle\ ,\ \rangle$ we obtain two symmetric $R/\mathfrak{m}$-bilinear forms, $\langle\ ,\ \rangle_{\mathrm{even}}$ and $\langle\ ,\ \rangle_{\mathrm{odd}}$ (see Definition 3.4.10 for more details). We will prove the following theorem (part of Theorem 5.3.10).

Theorem 3. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Consider the following statements:*

i. *$\langle\ ,\ \rangle$ is anisotropic;*
ii. *both $\langle\ ,\ \rangle_{\mathrm{even}}$ and $\langle\ ,\ \rangle_{\mathrm{odd}}$ are anisotropic;*
iii. *the form $\langle\ ,\ \rangle$ is non-degenerate and if $x \in M$ satisfies $\langle x, x\rangle = 0$, then $x \in \mathrm{lr}(M)$.*

Then i $\iff$ ii $\implies$ iii. *If* $\mathrm{char}(R/\mathfrak{m}) \neq 2$, *then all statements are equivalent.*

This theorem shows that the question if a form is anisotropic is completely reduced to the case where we have forms over fields. From this theorem one can easily deduce the following corollary (Corollary 5.3.12).

Corollary 4. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a non-degenerate symmetric R-bilinear form. The following statements hold.*

i. *Suppose that M is cyclic. Then $\langle\ ,\ \rangle$ is anisotropic.*

ii. *Suppose that M is generated by two elements and* $\text{length}_R(M)$ *is odd. Then* $\langle\ ,\ \rangle$ *is anisotropic.*

This last corollary can be used to determine the integral closure in some cases. It shows that if $A^\dagger/A$ is cyclic, then one can find the integral closure directly by lifting the lower root. To make it more concrete, suppose we are given an irreducible polynomial $x^2+ax+b \in \mathbf{Z}[x]$ where a is odd. Let $\alpha \in \mathbf{C}$ be a root of f and consider the order $A = \mathbf{Z}[\alpha]$. For $n \in \mathbf{Z}_{\geq 0}$ define $\text{lr}(n)$ to be the largest non-negative integer whose square divides n. Then $A^\dagger/A$ is cyclic and one can directly find the integral closure, namely

$$\overline{A} \quad = \quad \mathbf{Z}\cdot 1 + \mathbf{Z}\cdot\alpha + \mathbf{Z}\cdot\frac{1}{\text{lr}(\Delta(f))}(2\alpha+a)$$

(See Section 2 of Chapter 7).

We will later define the notion *quasi-anisotropy* (Definition 6.1.1), which is a bit weaker than anisotropy. This quasi-anisotropy also has some nice applications in number theory. One of the most interesting results in this thesis, is Theorem 6.2.3. We will state the theorem below.

Theorem 5. *Let A be an order over a Dedekind domain R and let $\mathfrak{p} \subset R$ be a nonzero prime. Let $B = \left(A^\dagger/A\right)_\mathfrak{p}$ and let $I = \text{Ann}_R(A^\dagger/A)$. Assume that $\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) < \text{char}(R/\mathfrak{p})$ or $\text{char}(R/\mathfrak{p}) = 0$. Let $\langle\ ,\ \rangle : B \times B \to \left(I^{-1}/R\right)_\mathfrak{p}$ be the induced form (Corollary 4.1.4). Suppose that $\langle\ ,\ \rangle$ is quasi-anisotropic. Then $\left(\overline{A}/A\right)_\mathfrak{p} = \text{lr}(B)$.*

2. Overview of the text

In Chapter 1 we will discuss a few topics such as symmetric bilinear forms, trace forms, artinian rings, algebras over fields, Dedekind domains and orders. Most readers will be familiar with large parts of this chapter and we have written this chapter for completeness.

In Chapter 2 we will show that instead of looking at orders over Dedekind domains, we can look at local orders over complete discrete valuation rings. We will study these local orders over complete discrete valuation rings. We will also prove the first theorem of our introduction in this chapter.

In Chapter 3 we will study zero-dimensional principal ideal rings. We will also study uniserial rings and modules over such rings. Finally, we will introduce the notion of anisotropy.

In Chapter 4 we combine Chapter 2 and Chapter 3 to give some nice results concerning the integral closure (such as the second theorem of the introduction).

In Chapter 5 we will give equivalent definitions of anisotropy. We will also introduce the notion of the radical root and give a method for calculating it in certain cases.

In Chapter 6 we will study the notion of quasi-anisotropy and give applications in number theory.

In Chapter 7 we will give examples of the theory discussed in the previous sections and we will test how often we can find the integral closure using our techniques.

Finally, in Chapter 8 we will discuss some problems which are still open and we will give further suggestions for research.

3. Acknowledgements

First of all, I would like to thank my supervisor, professor Hendrik Lenstra. Without his help, I wouldn't be able to write this thesis. He is also the person who suggested the topic of this thesis.

I would also like to thank my friends and family for supporting me during the last few years.

CHAPTER 1

Preliminaries

In this chapter we will cover theory which is largely well-known, but we will state it for completeness.

1. Symmetric bilinear forms

In this section we fix a ring R. We let M, N be R-modules.

Definition 1.1.1. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear map. Then $\langle\ ,\ \rangle$ is called *non-degenerate* if the map

$$\begin{array}{rcl} \varphi : M & \to & \mathrm{Hom}_R(M, N) \\ m & \mapsto & \langle m, \cdot \rangle \end{array}$$

is an isomorphism.

Remark 1.1.2. In the above case, a submodule $M' \subseteq M$ inherits a symmetric R-bilinear form. We will sometimes use statements as 'M' is non-degenerate', which means that the restriction of this form to $M' \times M'$ is non-degenerate.

Definition 1.1.3. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Let $T \subseteq M$. Then we define the *orthogonal complement* of T as

$$T^{\perp} = \{x \in M : \langle x, T\rangle = 0\} = \{x \in M |\ \forall t \in T : \langle x, t\rangle = 0\}.$$

Definition 1.1.4. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. We define the *radical* of $\langle\ ,\ \rangle$ to be $M^{\perp}$.

Lemma 1.1.5. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form where M, N are R-modules. Let $T, T' \subseteq M$. Then:*

i. *$T^{\perp}$ is an R-module;*
ii. *$T \subseteq (T^{\perp})^{\perp}$;*
iii. *If $T \subseteq T'$, then $T'^{\perp} \subseteq T^{\perp}$;*
iv. *$(T + T')^{\perp} = T^{\perp} \cap T'^{\perp}$.*

Proof. All proofs are obvious and left to the reader. □

Notation 1.1.6. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Let $M_1, M_2 \subseteq M$ be submodules such that $M = M_1 \oplus M_2$. Then we write $M = M_1 \perp M_2$ if $M_2 \subseteq M_1^{\perp}$.

Theorem 1.1.7. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Suppose that $M = M_1 \perp M_2$ for submodules $M_1, M_2 \subseteq M$. Then M is non-degenerate iff M_1 and M_2 are non-degenerate.*

Proof. This is an easy exercise and left to the reader. □

Theorem 1.1.8. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric bilinear form and let $M' \subseteq M$ be a submodule which is non-degenerate. Then $M = M' \perp M'^{\perp}$. Furthermore, $\langle\ ,\ \rangle$ is non-degenerate iff $M'^{\perp}$ is non-degenerate.*

PROOF. Consider the map

$$\begin{aligned} \varphi : M &\to \operatorname{Hom}_R(M', N) \\ m &\mapsto \langle m, \cdot \rangle. \end{aligned}$$

This map has kernel equal to $M'^{\perp}$ and if we restrict φ to M' we obtain an isomorphism. Let ψ be the inverse of this latter isomorphism. Then we have an exact sequence as follows:

$$0 \longrightarrow M'^{\perp} \longrightarrow M \xrightarrow{\psi \circ \varphi} M' \longrightarrow 0.$$

Notice that the inclusion $M' \to M$ gives a splitting of this sequence and hence we have $M = M' \oplus M'^{\perp}$. As this decomposition is orthogonal, we have $M = M' \perp M'^{\perp}$.

The last part follows from Theorem 1.1.7. □

2. Trace on projective modules

Lemma 1.2.1. *Let R be a ring and let P be a finitely generated projective R-module. Then we have an R-linear isomorphism*

$$\begin{aligned} \varphi : \operatorname{Hom}_R(P, R) \otimes_R P &\to \operatorname{End}_R(P) \\ \psi \otimes p &\mapsto (p' \mapsto \psi(p')p). \end{aligned}$$

Let $f : R^n \to P$ be a surjective morphism and let $f' : P \to R^n$ be a splitting of f. Let e_i be the i-th standard basis vector of R^n and let π_i be the projection on the i-th coordinate. Then for $\phi \in \operatorname{End}_R(P)$ we have

$$\varphi^{-1}(\phi) = \sum_{i=1}^{n} (x \mapsto \pi_i \circ f' \circ \phi(x)) \otimes f(e_i).$$

PROOF. We will first show that φ is an isomorphism. Consider the following R-linear map for R-modules N and M

$$\begin{aligned} \varphi' : \operatorname{Hom}_R(M, R) \otimes_R N &\to \operatorname{Hom}_R(M, N) \\ \psi \otimes n &\mapsto (m \mapsto \psi(m)n). \end{aligned}$$

Notice that this map is an isomorphism if $N = R$. Then observe that it is an isomorphism for $N = N_1 \oplus N_2$ iff it is an isomorphism for both $N = N_1$ and $N = N_2$. As a finitely generated projective R-module P is a direct summand of R^n for some n, it follows that we have an isomorphism if we take $N = P$. Now take $M = P$ as well and we obtain the first result.

We will now show that our second map is indeed the inverse. Let $x \in P$ and $\phi \in \operatorname{End}_R(P)$. Then we find

$$\begin{aligned} \phi(x) &= f\left(f'\left(\phi(x)\right)\right) \\ &= \sum_{i=1}^{n} f\left(\pi_i\left(f'\left(\phi(x)\right)\right) e_i\right) \\ &= \sum_{i=1}^{n} \pi_i\left(f'\left(\phi(x)\right)\right) f(e_i). \end{aligned}$$

Hence we find

$$\phi \quad = \quad \varphi\left(\sum_{i=1}^{n}(x \mapsto \pi_i \circ f' \circ \phi(x)) \otimes f(e_i)\right).$$

and we obtain the last result. □

Definition 1.2.2. Let R be a ring and let P be an R-module. Then we have a natural R-linear map

$$\begin{aligned} \mathrm{Tr}_{P/R} : \mathrm{Hom}_R(P,R) \otimes_R P &\to R \\ \varphi \otimes p &\mapsto \varphi(p). \end{aligned}$$

Now suppose that P is a finitely generated projective R-module. By Lemma 1.2.1 we obtain a natural R-linear map $\mathrm{Tr}_{P/R} : \mathrm{End}_R(P) \to R$.

Remark 1.2.3. Let R be a ring and let P be a finitely generated projective R-module. Then Lemma 1.2.1 also gives a direct formula for the trace. If $f : R^n \to P$ is a surjection, and if $f' : P \to R^n$ is a splitting of f, then we have for $\psi \in \mathrm{End}_R(P)$

$$\mathrm{Tr}_{P/R}(\psi) \quad = \quad \mathrm{Tr}(f' \circ \psi \circ f)$$

(the latter is the well known-trace of an endomorphism on R^n).

Lemma 1.2.4. *Let R be a ring and let P be a finitely generated projective R-module. Let $f : R \to R'$ be a ring morphism. Then $P \otimes_R R'$ is a finitely generated projective R'-module. Furthermore, we have the following commutative diagram*

$$\begin{array}{ccc} \mathrm{End}_R(P) & \xrightarrow{\varphi \mapsto \varphi \otimes \mathrm{id}_{R'}} & \mathrm{End}_{R'}(P \otimes_R R') \\ \downarrow \sim & & \downarrow \sim \\ \mathrm{Hom}_R(P,R) \otimes_R P & \xrightarrow{\psi \otimes p \mapsto (\psi \otimes \mathrm{id}_{R'}) \otimes (p \otimes 1)} & \mathrm{Hom}_{R'}(P \otimes_R R', R') \otimes_{R'} (P \otimes_R R') \\ \downarrow \mathrm{Tr}_{P/R} & & \downarrow \mathrm{Tr}_{P \otimes R'/R'} \\ R & \xrightarrow{f} & R'. \end{array}$$

Proof. Recall that a module P is projective over a ring R iff P is a free summand of $R^{(I)}$ for some set I. As tensoring commutes with taking direct sums, it follows that $P \otimes_R R'$ is a finitely generated projective R'-module. Then one defines the maps using the universal property of the tensor product. When this is done, one can easily verify that both squares commute. □

Definition 1.2.5. Let R be a ring and let P be an R-algebra which is finitely generated and projective as R-module (for example, it is free over R). Then we have a natural inclusion

$$\begin{aligned} \cdot : P &\to \mathrm{End}_R(P) \\ x &\mapsto \cdot x. \end{aligned}$$

We now define (with some ambiguity)

$$\begin{aligned} \mathrm{Tr}_{P/R} : P &\to R \\ x &\mapsto \mathrm{Tr}_{P/R}(\cdot x). \end{aligned}$$

Remark that this map is R-linear.

We now have the following lemma.

Lemma 1.2.6. *Let R be a ring and let P be an R-algebra which is finitely generated and projective as R-module. Let $f : R \to R'$ be a morphism of rings. Then for $x \in P$ we have*

$$f(\mathrm{Tr}_{P/R}(x)) = \mathrm{Tr}_{P\otimes_R R'/R'}(x \otimes 1).$$

PROOF. This follows from Lemma 1.2.4. Indeed we find

$$\begin{aligned} f\left(\mathrm{Tr}_{P/R}(x)\right) &= f\left(\mathrm{Tr}_{P/R}(\cdot x)\right) \\ &= \mathrm{Tr}_{P\otimes_R R'/R'}(\cdot x \otimes \mathrm{id}_{R'}) \\ &= \mathrm{Tr}_{P\otimes_R R'/R'}\left(\cdot(x \otimes 1)\right) \\ &= \mathrm{Tr}_{P\otimes_R R'/R'}\left(x \otimes 1\right). \end{aligned}$$

□

3. Artinian rings and algebras over fields

Lemma 1.3.1. *Let A be a nonzero artinian ring. Then $\dim(A) = 0$ and A has only finitely many maximal ideals. Also $A \cong \prod_{\mathfrak{p}\in \mathrm{Spec}(A)} A_{\mathfrak{p}}$.*

PROOF. The first statements follow from [**1**] Proposition 8.1 and Proposition 8.2. For the last statement, see [**4**] Exercise 10.9f. □

Definition 1.3.2. Let A be a ring and let B be an A-algebra. Then B is called a *finite A-algebra* if B is finitely generated as A-module.

Lemma 1.3.3. *Let k be a field and let A be a finitely generated k-algebra. Then the following are equivalent:*

i. *A is a finite k-algebra;*
ii. *A is artinian.*

PROOF. See [**1**], Exercise 8.3. □

Definition 1.3.4. Let R be a ring and let A be an R-algebra which is free of rank n as an R-module. Let $e_1, \ldots, e_n$ be a basis of A over R. We define the *discriminant* of A over R (using Definition 1.2.5) to be

$$\Delta(A/R) \quad = \quad \det\left(\mathrm{Tr}_{A/R}(e_i e_j)_{i,j=1}^n\right) \in R/R^{*2}.$$

One can again show that this is well-defined and independent of the chosen basis. For more details, see Chapter 4 from [**9**].

Lemma 1.3.5. *Let k be a field and let $U \subseteq V$ be finite dimensional k-vector spaces. Let φ be a k-endomorphism of V such that $\varphi(U) \subseteq U$. Let ψ be the endomorphism obtained from φ on V/U. Then $\mathrm{Tr}(\varphi) = \mathrm{Tr}(\varphi|_U) + \mathrm{Tr}(\psi)$.*

PROOF. Let $x_1, \ldots, x_m$ be a basis of U, and extend this to a basis $x_1, \ldots, x_n$ over V. From the matrix respresentation of φ in this basis one easily deduces the result. □

Lemma 1.3.6 (Trace formula)**.** *Let A be a finite k-algebra where k is a field. Then for $x \in A$ we have*

$$\mathrm{Tr}_{A/k}(x) = \sum_{\mathfrak{p}\in \mathrm{Spec}(A)} e_{\mathfrak{p}} \cdot \mathrm{Tr}_{(A/\mathfrak{p})/k}(x + \mathfrak{p})$$

where $e_{\mathfrak{p}} = \mathrm{length}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}})$.

PROOF. By Lemma 1.3.3, the ring A is artinian, hence all prime ideals are maximal and there are only finitely many of them (Lemma 1.3.1). This shows that the formula makes sense.

First suppose that $(A, \mathfrak{p})$ is a local ring. Since A satisfies the descending and ascending chain conditions, there is a composition series $A = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_{e_\mathfrak{p}} = 0$ where the M_i are A-modules and $M_i/M_{i-1} \cong A/\mathfrak{p}$ (see [**1**], Proposition 6.8). Apply Lemma 1.3.5 to the endomorphism which is the multiplication by x to get (where x now stands for the different multiplication by x endomorphisms)

$$\begin{aligned} \mathrm{Tr}_{A/k}(x) &= \mathrm{Tr}_{M_0/k}(x) \\ &= \mathrm{Tr}_{M_1/k}(x) + \mathrm{Tr}_{(M_0/M_1)/k}(x) \\ &= \ldots \\ &= \sum_{i=1}^{e_\mathfrak{p}} \mathrm{Tr}_{(M_i/M_{i-1})/k}(x). \end{aligned}$$

Since we have isomorphisms $M_i/M_{i-1} \cong A/\mathfrak{p}$, all the multiplication maps by x will have the same trace. This shows that $\mathrm{Tr}_{A/k}(x) = e_\mathfrak{p} \cdot \mathrm{Tr}_{(A/\mathfrak{p})/k}(x + \mathfrak{p})$.

Now let A be a finite k-algebra. We know from Lemma 1.3.1 that $A \cong \prod_{\mathfrak{p} \in \mathrm{Spec}(A)} A_\mathfrak{p}$. As the trace is additive and using the fact that $A/\mathfrak{p} \cong A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ by the natural map (by exactness of localization) we obtain

$$\begin{aligned} \mathrm{Tr}_{A/k}(x) &= \sum_{\mathfrak{p} \in \mathrm{Spec}(A)} e_\mathfrak{p} \cdot \mathrm{Tr}_{(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})/k}(x + \mathfrak{p}A_\mathfrak{p}) \\ &= \sum_{\mathfrak{p} \in \mathrm{Spec}(A)} e_\mathfrak{p} \cdot \mathrm{Tr}_{(A/\mathfrak{p})/k}(x + \mathfrak{p}). \end{aligned}$$

□

Definition 1.3.7. Let k be a field and let A be a finite k-algebra. Then A is called *finite étale* if the symmetric k-bilinear map

$$\begin{aligned} \langle\ ,\ \rangle : A \times A &\to k \\ \langle x, y \rangle &\mapsto \mathrm{Tr}_{A/k}(xy) \end{aligned}$$

is non-degenerate.

Remark 1.3.8. One can easily deduce that the non-degeneracy in the previous statement is equivalent to $\Delta(A/k) \neq 0$ (see Exercise 4.10a from [**9**]).

Lemma 1.3.9. *Let l/k be a finite extension of fields. Then l is a finite étale k-algebra iff l/k is separable. If l/k is inseparable, then $\mathrm{Tr}_{l/k}$ is identically 0.*

PROOF. If l/k is inseparable, then $\mathrm{Tr}_{l/k} = 0$ (a proof which we leave to the reader). If l/k is separable, use Theorem 5.5.2 from [**4**] to see that l is a finite étale k-algebra. □

Theorem 1.3.10. *Let k be a field and let A be a finite k-algebra. Then the following are equivalent:*

i. *A is a finite étale algebra;*
ii. *A is isomorphic as k-algebra to a finite product of finite separable field extensions of k.*

PROOF. i $\implies$ ii: From the trace formula (Lemma 1.3.6), it follows that there are no nilpotents in A (as $\sqrt{0} = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(A)} \mathfrak{p}$). From Lemma 1.3.1 it follows that there are only finitely many prime ideals, which are pairwise coprime. Hence $A \cong \prod_{\mathfrak{p}\in \mathrm{Spec}(A)} A/\mathfrak{p}$. Notice that the $A/\mathfrak{p}$ are fields with nonzero discriminant, as $\Delta(A/K) = \prod_{\mathfrak{p}\in \mathrm{Spec}(A)} \Delta(A/\mathfrak{p}/k)$. Now apply Lemma 1.3.9.

ii $\implies$ i: This follows directly from Lemma 1.3.9 by looking at the discriminant. □

Definition 1.3.11. Let A be a finite k-algebra where k is a field. Then A is called *tame* if the radical of the symmetric k-bilinear form

$$\begin{aligned} \langle\ ,\ \rangle : A \times A &\to k \\ \langle x, y\rangle &\mapsto \mathrm{Tr}_{A/k}(xy) \end{aligned}$$

is equal to the nilradical of A. If A is not tame, it is called *wild*. We will refer to the radical of $\langle\ ,\ \rangle$ as the *trace radical*.

Example 1.3.12. A finite étale algebra A is automatically tame. This follows since the trace radical is 0 by definition and the nilradical is zero as well (Theorem 1.3.10).

We will now study this tameness in more detail.

Definition 1.3.13. Let A be a ring. Then we define the *characteristic* of A, $\mathrm{char}(A)$, to be the unique non-negative generator of the kernel of the unique ring morphism $\mathbf{Z} \to A$.

Definition 1.3.14. Let A be a finite k-algebra where k is a field. Then a prime $\mathfrak{p} \subset A$ is called *wild* if $(A/\mathfrak{p})/k$ is inseparable or $\mathrm{char}(k) \mid \mathrm{length}_{A_\mathfrak{p}}(A_\mathfrak{p})$. If $\mathfrak{p}$ is not wild, it is called *tame*. Remark that all primes of A are tame if $\mathrm{char}(k) = 0$.

Corollary 1.3.15. *Let A be a finite k-algebra where k is a field. Then for $x \in A$ we have*

$$\mathrm{Tr}_{A/k}(x) = \sum_{\mathfrak{p}\subset A \text{ tame}} e_\mathfrak{p} \cdot \mathrm{Tr}_{(A/\mathfrak{p})/k}(x + \mathfrak{p})$$

where $e_\mathfrak{p} = \mathrm{length}_{A_\mathfrak{p}}(A_\mathfrak{p})$.

PROOF. If $\mathfrak{p}$ is wild, either $e_\mathfrak{p} = 0 \in k$ or the trace form $\mathrm{Tr}_{(A/\mathfrak{p})/k}$ is identically 0 (Lemma 1.3.9). Now apply Lemma 1.3.6. □

Lemma 1.3.16. *Let A be a finite k-algebra and let $x \in A$. Then x is in the trace radical iff $x \in \bigcap_{\mathfrak{p}\in \mathrm{Spec}(A) \text{ tame}} \mathfrak{p}$.*

PROOF. We use Lemma 1.3.1 and the Chinese remainder theorem to get a surjection $\varphi : A \to \prod_{\mathfrak{p}\in \mathrm{Spec}(A)\text{tame}} A/\mathfrak{p}$. By corollary 1.3.15 and Lemma 1.3.9 we see that x is in the trace radical iff $\varphi(x) = 0$ iff $x \in \bigcap_{\mathfrak{p}\in \mathrm{Spec}(A) \text{ tame}} \mathfrak{p}$. □

Corollary 1.3.17. *Let A be a finite k-algebra. Then A is tame iff all primes of A are tame.*

PROOF. By definition A is tame iff the traceradical is $\sqrt{0}$. We know by Lemma 1.3.16 that the traceradical is equal to $\bigcap_{\mathfrak{p}\subset A \text{ tame}} \mathfrak{p}$. As we have a surjection $\varphi : A \to \prod_{\mathfrak{p}\in \mathrm{Spec(A)}} A/\mathfrak{p}$ by Lemma 1.3.1 and the Chinese remainder theorem, we see that we have an equality iff all primes are tame. □

Remark 1.3.18. Let $A_1, \ldots, A_n$ be finite k-algebras. Then directly from the definition it follows that $\prod_{i=1}^n A_i$ is tame iff all the A_i are tame.

Lemma 1.3.19. *Let k be a field and let A be a finite k-algebra. Then the following statements hold.*

i. *Write $A = \prod_{\mathfrak{p}\in \mathrm{Spec}(A)} A_{\mathfrak{p}}$. Then the trace radical of A, $A^\perp$, is equal to*

$$A^\perp = \prod_{\mathfrak{p}\in \mathrm{Spec}(A) \text{ wild}} A_{\mathfrak{p}} \times \prod_{\mathfrak{p}\in \mathrm{Spec}(A) \text{ tame}} \mathfrak{p}A_{\mathfrak{p}}.$$

ii. *Suppose that A is wild. Then $\dim_k(A) \geq \dim_k(A^\perp) \geq \mathrm{char}(k) > 0$.*

Proof. i. This follows directly from Lemma 1.3.16.

ii. As we are in the wild case, if follows directly that $\mathrm{char}(k) > 0$ (Definition 1.3.14 and Corollary 1.3.17). Also, there is at least one wild prime ideal (Corollary 1.3.17), say $\mathfrak{p} \subset A$. Then $\dim_k(A^\perp) \geq \dim_k(A_{\mathfrak{p}})$ by the previous part. Notice that

$$\begin{aligned} \dim_k(A_{\mathfrak{p}}) &= \mathrm{length}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}) \cdot \dim_k(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}) \\ &= e_{\mathfrak{p}} \cdot \dim_k(A/\mathfrak{p}). \end{aligned}$$

As $\mathfrak{p}$ is wild either $e_{\mathfrak{p}}$ is a strictly positive multiple of $\mathrm{char}(k)$ or the extension $A/\mathfrak{p} \supseteq k$ is not separable. Notice that inseparable extensions have degree at least $\mathrm{char}(k)$. Hence we conclude that $\dim_k(A^\perp) \geq \mathrm{char}(k)$ in the wild case. □

4. Dedekind domains and orders

Definition 1.4.1. A ring R is called a *discrete valuation ring* if R is a local principal ideal domain and not a field.

Theorem 1.4.2. *Let R be a domain which is not a field. Then the following are equivalent:*

i. *every nonzero ideal can be written as a product of prime ideals;*
ii. *the ring R is noetherian, and the localization at each maximal ideal is a discrete valuation ring;*
iii. *every fractional ideal of R is invertible;*
iv. *the ring R is an integrally closed noetherian domain of dimension one.*

Proof. See [**7**], Theorem 5.1. □

Definition 1.4.3. A domain which is not a field satisfying one of the statements of Theorem 1.4.2 is called a *Dedekind domain*.

Definition 1.4.4. Let R be a domain. Then for an R-module M we define the *torsion-submodule* of M as

$$T(M) = \{x \in M : \mathrm{Ann}_R(x) \neq 0\}.$$

The module M is called *torsion-free module* if $T(M) = 0$. The module M is called *torsion* if $T(M) = M$.

Theorem 1.4.5. *Let R be a Dedekind domain and let M be a finitely generated R-module. Then the following statements are equivalent:*

i. *M is torsion-free;*
ii. *M is flat;*
iii. *M is projective.*

PROOF. i $\Longleftrightarrow$ ii: See [**1**], Exercise 9.5.
i $\Longleftrightarrow$ iii: See [**7**], Theorem 7.2. □

Furthermore we have a structure theorem for finitely generated modules over a Dedekind domain.

Theorem 1.4.6. *Let R be a Dedekind domain and let M be a finitely generated R-module. Then $M/T(M)$ is torsion-free and we have a split exact sequence*

$$0 \longrightarrow T(M) \longrightarrow M \longrightarrow M/T(M) \longrightarrow 0.$$

Furthermore, $M/T(M) = 0$ or $M/T(M) \cong R^n \oplus I$ where $n \in \mathbf{Z}_{\geq 0}$ and I a fractional R-ideal where $[I] \in \mathrm{Cl}(R)$ is uniquely determined. We also have

$$T(M) \quad \cong \quad R/\mathfrak{p}_1^{n_1} \oplus \ldots \oplus R/\mathfrak{p}_m^{n_m}$$

for some $m \in \mathbf{Z}_{\geq 0}$, maximal ideals $\mathfrak{p}_i \subset R$ and $n_i \in \mathbf{Z}_{\geq 1}$ where the $(\mathfrak{p}_i, n_i)$ are uniquely determined up to permutation.

PROOF. See [**7**], Theorem 7.3. □

Remark 1.4.7. Let R be a Dedekind domain and let $\mathfrak{p}, \mathfrak{p}' \subset R$ be nonzero primes. Then an easy calculation shows that for $i \in \mathbf{Z}_{\geq 1}$ we have

$$\left(R/\mathfrak{p}^i\right)_{\mathfrak{p}'} = \begin{cases} R/\mathfrak{p}^i & \mathfrak{p} = \mathfrak{p}' \\ 0 & \mathfrak{p} \neq \mathfrak{p}'. \end{cases}$$

Hence if we have a finitely generated torsion R-module M it follows that $M_{\mathfrak{p}} = M[\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathrm{Ann}_R(M))}]$.

Definition 1.4.8. Let R be a ring. Let $S = \{x \in R | \mathrm{Ann}_R(x) = 0\} \subseteq R$ be the set of non zero divisors. Then we define the *total quotient ring* of R as $Q(R) = S^{-1}R$.

Remark 1.4.9. The set of non zero divisors is the largest multiplicatively closed subset S of R such that $R \to S^{-1}R$ is injective.

Theorem 1.4.10. *Let R be a domain and let A be an R-algebra that is torsion-free and finitely generated as R-module. Then $A \otimes_R Q(R) \cong Q(A)$ by the natural map.*

PROOF. Assume that $A \neq 0$. Then $R = R \cdot 1 \subseteq A$ as A is torsion-free. Now let S be the set of nonzero divisors of R and let T be the set of nonzero divisors of A. Then $S \subseteq T$ as A is torsion-free. We will now claim that T is the saturation of S (see [**1**], Exercise 7). We have to show that for any $x \in T$, there exists $y \in A$ with $xy \in S$. Let $x \in T$. As A is integral over R ([**1**], Proposition 5.1), it follows that $x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0$ for some $r_i \in R$. Assume that this relation is of minimal degree. We have $r_0 \neq 0$ as x is not a zero divisor. But this means that $x(x^{n-1} + r_{n-1}x^{n-2} + \ldots + r_1) = -r_0 \in R \setminus \{0\} = S$. Hence $S^{-1}A = T^{-1}A$ and we find (using [**1**], Proposition 3.5)

$$\begin{aligned} A \otimes_R Q(R) &= A \otimes_R S^{-1}R \\ &= S^{-1}A \\ &= T^{-1}A \\ &= Q(A). \end{aligned}$$

□

Definition 1.4.11. Let R be a Dedekind domain. Then an R-algebra A is called an *order* over R if A is a finitely generated torsion-free R-module and $Q(A) = A \otimes_R Q(R)$ is a finite étale algebra over $Q(R)$.

Definition 1.4.12. Let R be a Dedekind domain and let A be an order over R. Let $M \subset Q(A)$ be a finitely generated R-module. Then we define the *trace dual* of M to be the R-module

$$M^\dagger = \{x \in Q(A) : \mathrm{Tr}_{Q(A)/Q(R)}(xM) \subseteq R\}.$$

Definition 1.4.13. Let A be a ring. Then we define the *integral closure* of A in $Q(A)$ as

$$\overline{A} = \{a \in Q(A) : \exists \text{ monic } f(x) \in A[x] : f(a) = 0\}.$$

We want to study the integral closure of an order A over a Dedekind domain R by looking at the structure of $A^\dagger/A$. Now let $M \subset Q(A) = A \otimes_R Q(R)$ be an R-submodule. Then we have

$$M \otimes_R Q(R) \subseteq Q(A) \otimes_R Q(R) \subseteq A \otimes_R Q(R) \otimes_R Q(R) = A \otimes_R Q(R) = Q(A)$$

by flatness of $Q(R)$. We have the following lemma.

Lemma 1.4.14. *Let R be a Dedekind domain and let A be an order over R. Let $M \subset Q(A)$ be a finitely generated R-module. Suppose that $M \otimes_R Q(R) = Q(A)$. Then the map*

$$\begin{aligned} \varphi : M^\dagger &\to \mathrm{Hom}_R(M, R) \\ x &\mapsto \big(m \mapsto \mathrm{Tr}_{Q(A)/Q(R)}(mx)\big) \end{aligned}$$

is an isomorphism of R-modules.

Proof. We will first show that φ is injective. Suppose that $\varphi(x) = 0$ for $x \in M^\dagger$. As $Q(A) = M \otimes_R Q(R) = S^{-1}M$ where $S = R \setminus \{0\}$, we have for any $y \in Q(A)$ the equality $\mathrm{Tr}_{Q(A)/Q(R)}(yx) = 0$. As $Q(A)$ is a finite $Q(R)$-étale algebra, it follows that $x = 0$.

We will now show that our map is surjective. Let $\psi \in \mathrm{Hom}_R(M, R)$. Then consider the map $\psi' = \psi \otimes \mathrm{id}_{Q(R)} : Q(A) \to Q(R)$. As $Q(A)$ is a finite $Q(R)$-étale algebra, we can find $x \in M$ such that $\mathrm{Tr}_{Q(A)/Q(R)}(xy) = \psi'(y)$. But then $x \in M^\dagger$ and $\varphi(x) = \psi$. □

Lemma 1.4.15. *Let R be a Dedekind domain and let $A \neq 0$ be an order over R. Then the following all hold:*

i. *$R \subseteq A$ is integral and $\overline{A}$ is the integral closure of R inside $Q(A)$;*
ii. *every order $B \subset Q(A)$ with $Q(B) = Q(A)$ satisfies $\mathrm{Tr}_{Q(A)/Q(R)}(B) \subseteq R$;*
iii. *$A \subseteq \overline{A} \subseteq A^\dagger$;*
iv. *$A^\dagger$ is a finitely generated R-module and $A^\dagger/A$ is torsion;*
v. *$\overline{A}$ is the unique maximal element (under inclusion) of the set of orders $B \subseteq Q(A)$ with $Q(B) = Q(A)$.*

Proof. i. We have $R \subseteq A$ as $A \neq 0$ is torsion-free. As A is finitely generated over R, we can apply Proposition 5.1 from [**1**] to see that $R \subseteq A$ is integral. The second statement follows from [**1**], Corollary 5.4.

ii. As B is projective over R (Theorem 1.4.5), we can use Definition 1.2.5 and Lemma 1.2.6 to prove ii (let $f : R \to Q(R)$ be the inclusion).

iii., iv. By Lemma 1.4.14 we see that $A^\dagger \cong \mathrm{Hom}_R(A,R)$ and hence $A^\dagger$ is finitely generated over R. Let $x \in \overline{A}$. Then $A[x]$ is an order, hence

$$\mathrm{Tr}_{Q(A)/Q(R)}(A[x]) \subseteq R$$

and $x \in A^\dagger$. As $Q(A)/A$ is torsion we obtain iii and iv.

v. As all orders are integral over R, they are contained in $\overline{A} = \overline{R} \subseteq Q(A)$. As $\overline{A} \subseteq A^\dagger$, it follows that $\overline{A}$ is finitely generated and torsion-free. Also $Q(\overline{A}) = Q(A)$ and hence $\overline{A}$ is an order as well. □

Lemma 1.4.16. *Let R be a Dedekind domain and let A be an order over R. Let*

$$\mathfrak{S} = \{M \subseteq Q(A) : M \text{ fin. gen. } R\text{−module}, M \otimes_R Q(R) = Q(A)\}.$$

The map

$$\begin{array}{rccc} {}^\dagger : \mathfrak{S} & \to & \mathfrak{S} \\ M & \mapsto & M^\dagger \end{array}$$

is a bijection with inverse †.

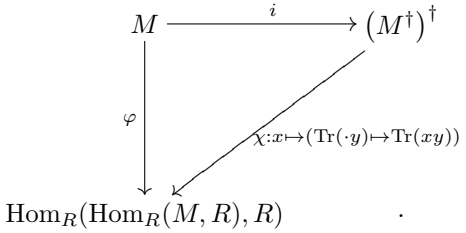
Proof. One first easily shows that the map is well-defined. Then consider for any R-module M the map

$$\begin{array}{rccc} \varphi' : M & \to & \mathrm{Hom}_R(\mathrm{Hom}_R(M,R),R) \\ m & \mapsto & (\psi \mapsto \psi(m)). \end{array}$$

If $M = R$, this map is an isomorphism. Furthermore, it is an isomorphism for $M \oplus N$ iff it is an isomorphism for M and for N. Hence our map is an isomorphism for R^n and also for direct summands of R^n, that is, for finitely generated projective R-modules.

Now let $M \in \mathfrak{S}$ and let φ' be the above isomorphism (M is torsion-free, hence projective by Theorem 1.4.5).

Let $i : M \to \left(M^\dagger\right)^\dagger$ be the natural inclusion. Now consider the following diagram



This diagram commutes and as φ and χ are isomorphisms (Lemma 1.4.14), the map i is an isomorphism as well. □

Definition 1.4.17. Let R be a Dedekind domain and let $A \supseteq R$ be an order over R. Let $\mathfrak{p} \subset R$ be a nonzero prime. Then A is said to be *tame* at $\mathfrak{p}$ if $A/\mathfrak{p}A$ is tame as $R/\mathfrak{p}$-algebra (apply Definition 1.3.11). If A is not tame at $\mathfrak{p}$, it is called *wild*.

As an example, we give the following lemma.

Lemma 1.4.18. *Let $A = \mathbf{Z}[x]/(f)$ where $f(x) \in \mathbf{Z}[x]$ is monic and $\Delta(f) \neq 0$. Then A is an order over $\mathbf{Z}$. Let $p \in \mathbf{Z}$ be prime and write $\overline{f} = \prod_{i=1}^m f_i^{n_i} \in \mathbf{F}_p[x]$ where $(f_i, f_j) = 1$ if $i \neq j$, the $f_i \in \mathbf{F}_p[x]$ are irreducible and $n_i \in \mathbf{Z}_{\geq 1}$. Then A is tame at p if $p \nmid n_i$ for $i = 1, \ldots, m$.*

PROOF. We will first show that $\Delta(A \otimes_Z \mathbf{Q}/\mathbf{Q}) \neq 0$. As the discriminant behaves well under taking tensor products, we consider the order $(A \otimes_{\mathbf{Z}} \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C} = A \otimes_{\mathbf{Z}} \mathbf{C} = \mathbf{C}[x]/(f)$ and we will show that its discriminant is nonzero. As $\Delta(f) \neq 0$, it follows that all roots occur with multiplicity one and hence $\mathbf{C}[x]/(f) \cong \mathbf{C}^{\deg(f)}$ and hence $\mathbf{C}[x]/(f)$ has nonzero discriminant.

Now let $p \in \mathbf{Z}$ be prime. By the Chinese remainder theorem it follows that $A/pA \cong \prod_{i=1}^{m} \mathbf{F}_p[x]/(f_i)^{n_i}$. All the $\mathbf{F}_p[x]/(f_i)^{n_i}$ are local, and localizing at the different prime ideals just give the different $A_i = \mathbf{F}_p[x]/(f_i)^{n_i}$ back. The maximal ideal of such a factor is (f_i). Notice that $A_i/(f_i) \cong \mathbf{F}_p[x]/(f_i)$, and $\#A_i = (\#A_i/(f_i))^{n_i}$, which shows that $\text{length}_{A_i}(A_i) = n_i$. We see that we are in the wild case iff there is an n_i which is divisible by p. □

Example 1.4.19. Let $K \supset \mathbf{Q}$ be a number field. Let $p \in \mathbf{Z}$ be prime. Then $\mathcal{O}_K$ is called tame at p if $p \nmid e(\mathfrak{p}/p)$ for $\mathfrak{p} \in \text{Spec}(\mathcal{O}_K)$ with $\mathfrak{p} \cap \mathbf{Z} = (p)$. Here $e(\mathfrak{p}/p)$ is defined by $p\mathcal{O}_K = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{O}_K) : \mathfrak{p} \cap \mathbf{Z} = (p)} \mathfrak{p}^{e(\mathfrak{p}/p)}$. We then find by the Chinese remainder theorem

$$\mathcal{O}_K/p\mathcal{O}_K \quad \cong \quad \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{O}_K) : \mathfrak{p} \cap \mathbf{Z} = (p)} \mathcal{O}_K/\mathfrak{p}^{e(\mathfrak{p}/p)}.$$

From this last expression we deduce that $e_{\mathfrak{p}/p\mathcal{O}_K} = e(\mathfrak{p}/p)$. As $\mathbf{F}_p$ is a perfect field, we see that the two definitions of tameness are the same in this case.

CHAPTER 2

First main theorem

1. Orders: reduction to the complete local case

In this section we fix a Dedekind domain R and an order A over R. We will also fix a nonzero prime $\mathfrak{p} \subset R$.

Our goal is to study the integral closure of A in its total quotient ring $Q(A) = A \otimes_R Q(R)$. We will first reduce to the case where R is local using localization. Then we will complete our local ring and finally we can make our order A local.

First notice that $R_{\mathfrak{p}}$ is still a Dedekind domain (actually, it is a discrete valuation ring). Let $A_{\mathfrak{p}} = A \otimes_R R_{\mathfrak{p}}$. We have the following lemma.

Lemma 2.1.1. *The following assertions all hold.*

i. *The ring $A_{\mathfrak{p}}$ is an order over $R_{\mathfrak{p}}$.*
ii. *We have $Q(A_{\mathfrak{p}}) = Q(A)$.*
iii. *Furthermore, $\left(A^{\dagger}\right)_{\mathfrak{p}} = (A_{\mathfrak{p}})^{\dagger}$ and $\left(A^{\dagger}/A\right)_{\mathfrak{p}} \cong (A_{\mathfrak{p}})^{\dagger}/A_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$-modules by the natural map.*
iv. *Also we have $\overline{A_{\mathfrak{p}}} = \overline{A}_{\mathfrak{p}}$ and $\left(\overline{A}/A\right)_{\mathfrak{p}} \cong \overline{A}_{\mathfrak{p}}/A_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$-modules by the natural map.*

Proof. i. We directly see that $A_{\mathfrak{p}}$ is projective over $R_{\mathfrak{p}}$. Notice that $Q(R) = Q(R_{\mathfrak{p}})$ and hence by Theorem 1.4.10

$$Q(A_{\mathfrak{p}}) = A \otimes_R R_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} Q(R_{\mathfrak{p}}) = A \otimes_R Q(R) = Q(A).$$

Hence $Q(A_{\mathfrak{p}})$ is a finite $Q(R)$-étale algebra, and it follows that $A_{\mathfrak{p}}$ is an order over $R_{\mathfrak{p}}$.

ii. This follows from the calculation at i.

iii. Let $x \in \left(A^{\dagger}\right)_{\mathfrak{p}}$. Then we directly see that $\mathrm{Tr}_{Q(A)/Q(R)}(xA_{\mathfrak{p}}) \subseteq R_{\mathfrak{p}}$. Hence $\left(A^{\dagger}\right)_{\mathfrak{p}} \subseteq (A_{\mathfrak{p}})^{\dagger}$. Now let $x \in (A_{\mathfrak{p}})^{\dagger}$. As A is finitely generated R-module, there is $w \in R \setminus \mathfrak{p}$ such that $\mathrm{Tr}_{Q(A)/Q(R)}(xA) \subseteq \frac{1}{w}R$. Hence $wx \in A^{\dagger}$ and $x \in \left(A^{\dagger}\right)_{\mathfrak{p}}$. For the second part use that localization is exact ([**1**], Proposition 3.3).

iv. For the first part use [**1**], Proposition 5.12. For the second part use again that localization is exact. □

Lemma 2.1.2. *The ring A is tame at $\mathfrak{p}$ iff $A_{\mathfrak{p}}$ is tame over $\mathfrak{p}R_{\mathfrak{p}}$.*

Proof. We have, using Exercise 2.2 from [**1**] and exactness of localization:

$$\begin{aligned} A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}A_{\mathfrak{p}} &= A_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} (R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}) \\ &= A \otimes_R (R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}) \\ &= A \otimes_R (R/\mathfrak{p}R) \\ &= A/\mathfrak{p}A. \end{aligned}$$

The lemma now follows directly. □

Consider the following exact sequence:

$$0 \longrightarrow R_{\mathfrak{p}} \longrightarrow Q(R) \longrightarrow Q(R)/R_{\mathfrak{p}} \longrightarrow 0.$$

Now we tensor it with A over R, and since A is projective (hence flat), we obtain the following exact sequence:

$$0 \longrightarrow A_{\mathfrak{p}} \longrightarrow Q(A) \longrightarrow (Q(R)/R_{\mathfrak{p}}) \otimes_R A \longrightarrow 0.$$

Let $M = (Q(R)/R_{\mathfrak{p}}) \otimes_R A$. Notice that M is a torsion $R_{\mathfrak{p}}$-module.

Definition 2.1.3. Let B be a local ring with maximal ideal $\mathfrak{m}$. Then the *completion* of B with respect to $\mathfrak{m}$ is

$$\hat{B} \quad = \quad \varprojlim B/\mathfrak{m}^i.$$

Now let N be a B-module. Then we define

$$\hat{N} \quad = \quad \varprojlim N/\mathfrak{m}^i N.$$

See [**3**] Chapter 7 for more details.

Recall that local Dedekind domains are discrete valuation rings and that $R_{\mathfrak{p}}$ is a discrete valuation ring.

Lemma 2.1.4. *Let B be a discrete valuation ring. Then $\hat{B}$ is a discrete valuation ring. Also, the natural map $B \to \hat{B}$ is an inclusion. Furhermore, $Q(\hat{B}) = Q(B) \otimes_B \hat{B}$.*

Proof. From [**3**], Theorem, it follows that $\hat{B}$ is noetherian, and $\hat{B}$ is also local. Let $\mathfrak{m} = (\pi)$ be the maximal ideal of B. From Corollary 7.13 [**3**] it follows that the maximal ideal $\hat{B}$ is $\mathfrak{m}\hat{B} = \pi\hat{B}$, a principal ideal. From Corollary 10.12 from [**3**] we get

$$\dim(\hat{B}) = \dim(B) = 1.$$

Hence $\hat{B}$ is a regular local ring, which is a domain by Corollary 10.14 from [**3**]. It follows that $\hat{B}$ is a noetherian local domain of dimension one with principal maximal ideal, a discrete valuation ring ([**1**], Proposition 9.2). As $\bigcap_{i \in \mathbf{Z}_{\geq 0}} \mathfrak{m}^i = 0$, it follows that our map is injective.

Finally consider the natural inclusion $\hat{B} = B \otimes_B \hat{B} \to Q(B) \otimes_B \hat{B}$. We will now use Corollary 3.2 from [**1**] to show that $Q(B) \otimes_B \hat{B} = Q(\hat{B})$ (so $S = \hat{B} \setminus \{0\}$). As $\hat{B}$ is flat ([**3**], Theorem 7.2), it follows that the second condition in this lemma is fulfilled. One easily sees that the first and third condition are fulfilled (here one use that only π needs to be inverted).

□

Lemma 2.1.5. *Let B be a noetherian local ring with maximal ideal $\mathfrak{m}$ and let N be a B-module. Suppose that for all $m \in N$ we have that $\mathrm{Ann}_B(m) \supseteq \mathfrak{m}^{n_a}$ for some $n_a \in \mathbf{Z}_{\geq 0}$. Then $N \cong N \otimes_B \hat{B}$ by the canonical map.*

Proof. First assume that N is finitely generated as B-module. Then there exists $i \in \mathbf{Z}_{\geq 0}$ such that $\mathfrak{m}^i N = 0$. Hence $\hat{N} \cong N$. As $\hat{N} \cong N \otimes_B \hat{B}$ ([**3**], Theorem 7.2)), we have $N \cong N \otimes_B \hat{B}$. Now we will do the general case. As N is the inductive limit of all finitely generated B-submodules, and tensoring commutes with inductive limits ([**1**], Exercise 2.20), we find $N \cong N \otimes_B \hat{B}$. □

Corollary 2.1.6. *Let B be a discrete valuation ring and let N be a torsion B-module. Then $N \cong N \otimes_B \hat{B}$ by the natural map.*

PROOF. This directly follows from the previous lemma. □

Lemma 2.1.7. *Let R_1, R_2 be Dedekind domains and let $f : R_1 \to R_2$ be an injective ring morphism making R_2 into an R_1-algebra. Let A_1 be an order over R_1. Then $A_1 \otimes_{R_1} R_2$ is an order over R_2.*

PROOF. As A_1 is finitely generated projective over R_1, it follows that $A_1 \otimes_{R_1} R_2$ is finitely generated projective over R_2. Now consider the map $f' : Q(R_1) \to Q(R_2)$ obtained from f which exists since f is injective. Consider the base extension given by f':

$$\begin{aligned}(A_1 \otimes_{R_1} R_2) \otimes_{R_2} Q(R_2) &= A_1 \otimes_{R_1} Q(R_2) \\ &= (A_1 \otimes_{R_1} Q(R_1)) \otimes_{Q(R_1)} Q(R_2).\end{aligned}$$

By Lemma 1.2.6 and Theorem 1.4.10 we see that

$$\Delta(Q(A \otimes_{R_1} R_2)) = f'(\Delta(Q(A))).$$

As f is injective and A was an order, we conclude from Remark 1.3.8 that $Q(A \otimes_{R_1} R_2)$ is a finite étale algebra and hence $A \otimes_{R_1} R_2$ is an order. □

We can apply Lemma 2.1.7 for the inclusion $f : R_\mathfrak{p} \to \hat{R}_\mathfrak{p}$. Using Lemma 2.1.4 we see that $Q(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}) = Q(A_\mathfrak{p}) \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$. We know that $\hat{R}_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module ([**3**], Theorem 7.2). By Lemma 2.1.6 we find the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_\mathfrak{p} & \longrightarrow & Q(A_\mathfrak{p}) & \xrightarrow{f_1} & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} & \longrightarrow & Q(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}) & \xrightarrow{f_2} & M & \longrightarrow & 0. \end{array}$$

Furthermore, as $A_\mathfrak{p}$ is projective (hence flat) as an $R_\mathfrak{p}$-module it follows that $A_\mathfrak{p} \to A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$ is an inclusion. By the five lemma it even follows that the map in the middle is injective as well.

Theorem 2.1.8. *Let $\mathfrak{S}$ be the set of $R_\mathfrak{p}$-submodules N with $A_\mathfrak{p} \subseteq N \subseteq Q(A_\mathfrak{p})$. Let $\mathfrak{T}$ be the set of $\hat{R}_\mathfrak{p}$-submodules N' with $A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} \subseteq N' \subseteq Q(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p})$. Then the map*

$$\begin{aligned}\varphi : \mathfrak{S} &\to \mathfrak{T} \\ N &\mapsto N \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\end{aligned}$$

is a bijection with inverse φ^{-1} given by:

$$\varphi^{-1}(N') = \psi^{-1}(N')$$

Furthermore, the following statements hold for $N \in \mathfrak{S}$:

i. *N is a ring iff $\varphi(N)$ is a ring;*
ii. *N is finitely generated over $R_\mathfrak{p}$ iff $\varphi(N)$ is finitely generated over $\hat{R}_\mathfrak{p}$.*

Finally we have:

i. $\overline{A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}} = \overline{A_\mathfrak{p}} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$;

ii. $\overline{A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}}/A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} \cong \left(\overline{A}/A\right)_\mathfrak{p}$ *as* $\hat{R}_\mathfrak{p}$*-modules.*

PROOF. All $R_\mathfrak{p}$-submodules between $A_\mathfrak{p}$ and $Q(A_\mathfrak{p})$ correspond to $R_\mathfrak{p}$-submodules of M (take the inverse image under f_1). Similarly all $\hat{R}_\mathfrak{p}$=submodules between $A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$ and $Q(A_\mathfrak{p} \otimes_{\mathbf{Z}_p} \hat{R}_\mathfrak{p})$ correspond to $\hat{R}_\mathfrak{p}$-submodules of M (take the inverse image under f_2). Notice that the notion of $R_\mathfrak{p}$- and $\hat{R}_\mathfrak{p}$-submodules of M are the same as M is torsion. Take a submodule $M' \subseteq M$, then as $\psi^{-1} \circ f_2^{-1}(M') = f_1^{-1}(M')$ it follows that the φ^{-1} we defined is indeed the bijection which we are looking for. On the other hand, suppose that $A_\mathfrak{p} \subseteq N \subseteq Q(A_\mathfrak{p})$ with $N/A_\mathfrak{p} = M'$. Then notice that $N/A_\mathfrak{p} = (N/A_\mathfrak{p}) \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} = \left(N \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right) / \left(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right)$ (by flatness of $\hat{R}_\mathfrak{p}$ and Corollary 2.1.6) and hence we see that N corresponds to $N \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$. This gives us our map φ.

Now let $N \in \mathfrak{S}$.

i. If N is a ring, then $N \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$ is obviously closed under the ring operations which it inherits. If N' is a ring, then $\varphi^{-1}(N') = \psi^{-1}(N')$ is also a ring.

ii. This N is finitely generated as an $R_\mathfrak{p}$-module iff $N/A_\mathfrak{p}$ is finitely generated as an $R_\mathfrak{p}$-module iff $N/A_\mathfrak{p}$ is finitely generated as an $\hat{R}_\mathfrak{p}$-module iff $\varphi(N)$ is finitely generated as an $\hat{R}_\mathfrak{p}$-module.

We will now prove the last two statements.

i. Notice that the integral closure of a ring B in its total quotient ring C is equal to the injective limit of all subrings $B \subseteq D$ of B such that D is a finitely generated B-module ([**1**], Proposition 5.1). As tensoring commutes with taking injective limits ([**1**], Exercise 2.20), the result follows from the two previous parts.

ii. First notice that from the previous i, the fact that $\hat{R}_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module and Lemma 2.1.1 iv we obtain $\overline{A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}}/A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} = \left(\overline{A}/A\right)_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$. Apply Corollary 2.1.6 and Lemma 1.4.15 to see that this is isomorphic to $\left(\overline{A}/A\right)_\mathfrak{p}$.

□

Lemma 2.1.9. *We have* $\left(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right)^\dagger = A_\mathfrak{p}^\dagger \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$.

PROOF. First notice that $A_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module (Theorem 1.4.6, as $R_\mathfrak{p}$ is a principal ideal domain). Let $\omega_1, \ldots, \omega_n$ be a basis of $A_\mathfrak{p}$ over $R_\mathfrak{p}$ and let $\omega_1^*, \ldots, \omega_n^*$ be its dual basis with respect to the trace. Then $\omega_1 \otimes 1, \ldots, \omega_n \otimes 1$ forms a basis of $A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$ over $\hat{R}_\mathfrak{p}$ and has a dual basis $\omega_1^* \otimes 1, \ldots, \omega_n^* \otimes 1$. Using this dual basis and Lemma 2.1.1 we obtain the result.

□

Lemma 2.1.10. *The order* A *is tame at* $\mathfrak{p}$ *iff* $A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}$ *is tame at* $\mathfrak{p}\hat{R}_\mathfrak{p}$.

PROOF. The proof uses Lemma 2.1.2 and is left to the reader. □

2. Orders over complete discrete valuation rings

In the previous section we have seen that we can translate many properties from orders over a Dedekind domain R to an order over $\hat{R}_\mathfrak{p}$, a complete discrete valuation ring (see Lemma 2.1.4). **In this section we assume that R is a complete discrete valuation ring with maximal ideal $\mathfrak{p}$.**

An order which is local as a ring, will be called a *local order*.

Theorem 2.2.1. *Let A be an order over R. Then A has only finitely many maximal ideals and the localizations $A_{\mathfrak{m}}$ at a maximal ideal $\mathfrak{m} \subset R$ are complete local orders over R. Furthermore, $A \cong \prod_{\mathfrak{m} \in \mathrm{Maxspec}(A)} A_{\mathfrak{m}}$ as rings by the natural map.*

PROOF. Corollary 7.6 from [**3**] tells us that there are only finitely maximal ideals and the localization $A_{\mathfrak{m}}$ at a maximal ideal $\mathfrak{m} \subset R$ is a complete local ring which is finite over R, and $A \cong \prod_{\mathfrak{m} \in \mathrm{Maxspec}(A)} A_{\mathfrak{m}}$. As A is projective over R and direct summands of projective modules are projective, it follows that the $A_{\mathfrak{m}}$ are also projective over R. Now notice that $A \otimes_R Q(R) = \prod_{\mathfrak{m} \in \mathrm{Maxspec}(A)} (A_{\mathfrak{m}} \otimes_R Q(R))$ and hence

$$\Delta(Q(A)/Q(R)) = \prod_{\mathfrak{m} \in \mathrm{Maxspec}(A)} \Delta(Q(A_{\mathfrak{m}})/Q(R)).$$

As $\Delta(Q(A)/Q(R)) \neq 0$, it follows that $\Delta(Q(A_{\mathfrak{m}})/Q(R)) \neq 0$. Hence by Remark 1.3.8 these $A_{\mathfrak{m}}$ are orders over R. □

By the previous theorem it suffices to study local orders.

Lemma 2.2.2. *Let $(A, \mathfrak{m})$ be a local order over R. Then $\mathfrak{m} : \mathfrak{m} = \{x \in Q(A) : x\mathfrak{m} \subseteq \mathfrak{m}\}$ is an order over R and $A \subseteq \mathfrak{m} : \mathfrak{m} \subseteq \overline{A}$.*

PROOF. First notice that $\mathfrak{m} : \mathfrak{m}$ is a ring containing A. Let $x \in \mathfrak{m} : \mathfrak{m}$. Since R is noetherian, it follows that $\mathfrak{m}$ is a finitely generated R-module. As A is torsion-free, we see that $\mathfrak{m}$ is a faithful R-module. Now apply Proposition 5.1 iii from [**1**] to see that x is integral over A. Hence $\mathfrak{m} : \mathfrak{m} \subseteq \overline{A}$. We see that $\mathfrak{m} : \mathfrak{m}$ is finitely generated as R-module and still torsion-free (as $\mathfrak{m} : \mathfrak{m} \subseteq \overline{A} \subset Q(A)$, use Lemma 1.4.15). As $Q(\mathfrak{m} : \mathfrak{m}) = Q(A)$, it follows that $\mathfrak{m} : \mathfrak{m}$ is an order. □

We will now state and prove the following elegant lemma.

Lemma 2.2.3. *Let $C \subsetneq D$ be rings. Let $J \subseteq C$ be a radical ideal and assume that there is $n \in \mathbf{Z}_{\geq 1}$ such that $J^n D \subseteq C$. Then $C \subsetneq J : J = \{x \in D : xJ \subseteq J\}$.*

PROOF. Take $n \in \mathbf{Z}_{\geq 1}$ maximal such that $J^{n-1}D \not\subset C$. Then $J(J^{n-1}D) \subseteq C$ by assumption. We also have

$$(J^n D)^2 = J^{2n} D^2 = J^n (J^n D) \subseteq J^n \subseteq J.$$

As $J^n D \subseteq C$ and J was radical, we conclude that $J^n D \subseteq J$ and hence $J^{n-1} D \subseteq J : J$. This shows that $C \subsetneq J : J$. □

Theorem 2.2.4. *Let $(A, \mathfrak{m})$ be a local order over R. Then the following statements are equivalent.*

i. $A = \overline{A}$;
ii. $A = \mathfrak{m} : \mathfrak{m}$;
iii. $\mathfrak{m}(A : \mathfrak{m}) = A$;
iv. $\mathfrak{m} : \mathfrak{m} \neq A : \mathfrak{m}$;
v. $\mathfrak{m}$ *is principal;*
vi. A *is a discrete valuation ring.*

PROOF. We first make a few remarks. Recall that $\overline{A}/A$ is a finitely generated torsion module (Lemma 1.4.15 and Theorem 1.4.6). Let $r \in \mathbf{Z}_{\geq 0}$ such that $\mathfrak{p}^r \overline{A} \subseteq A$. As $A/\mathfrak{p}A$ is an artinian ring (Lemma 1.3.3), it follows that $\mathfrak{m}^n \subseteq \mathfrak{p}A$ for some $n \in \mathbf{Z}_{\geq 0}$. Hence there exists $s \in \mathbf{Z}_{\geq 1}$ such that $\mathfrak{m}^s \overline{A} \subseteq A$.

Now we will prove that $A : \mathfrak{m} \supsetneq A$. Suppose that $A : \mathfrak{m} = A$. Pick $n \in \mathbf{Z}_{\geq 1}$ minimal such that $\mathfrak{m}^n \subseteq \mathfrak{p}A$. But then $\mathfrak{m}^{n-1} \subseteq \mathfrak{p}A : \mathfrak{m} = \mathfrak{p}(A : \mathfrak{m}) = \mathfrak{p}A$ (as $\mathfrak{p}$ is a principal ideal), a contradiction.

i $\implies$ ii: This follows from Lemma 2.2.2.

ii $\implies$ iii: We have $\mathfrak{m} \subseteq \mathfrak{m}(A : \mathfrak{m}) \subseteq A$. Suppose that $\mathfrak{m}(A : \mathfrak{m}) \neq A$, then $\mathfrak{m}(A : \mathfrak{m}) = \mathfrak{m}$. Using this and the second remark, we conclude that $\mathfrak{m} : \mathfrak{m} = A : \mathfrak{m} \supsetneq A$, a contradiction.

iii $\iff$ iv: Notice that $\mathfrak{m} : \mathfrak{m} \subseteq A : \mathfrak{m}$. We have $\mathfrak{m}(A : \mathfrak{m}) = A$ iff $\mathfrak{m}(A : \mathfrak{m}) \neq \mathfrak{m}$ iff $A : \mathfrak{m} \supsetneq \mathfrak{m} : \mathfrak{m}$.

iii $\implies$ v: From $(A : \mathfrak{m})\mathfrak{m} = A$ we see that we can write $1 = \sum_{i=1}^{m} x_i y_i$ where $x_i \in (A : \mathfrak{m})$ and $y_i \in \mathfrak{m}$. Pick i such that $x_i y_i \notin \mathfrak{m}$. We claim that $\mathfrak{m} = (y_i)$. Indeed for $x \in \mathfrak{m}$ we find

$$x = y_i \cdot \frac{x x_i}{y_i x_i} \in (y_i).$$

v $\implies$ vi: We know that $\mathfrak{m}$ is principal and that A is local noetherian and has dimension 1 (as it is integral over R). This makes A into a regular local ring. By Corollary 10.14 from [**3**] it follows that A is a domain. Now apply Proposition 9.2 from [**1**] to see that A is a discrete valuation ring.

vi $\implies$ i: Again apply Proposition 9.2 from [**1**] to see that A is integrally closed.

Although we don't need it, using Lemma 2.2.3, there is an elegant proof of ii $\implies$ i. Just use the first remark and this lemma. □

Theorem 2.2.5. *Let $(A, \mathfrak{m})$ be a local order over R which is tame at $\mathfrak{p}$. Then $\mathfrak{p}A^\dagger \subseteq A$ iff A is integrally closed. If $A \subsetneq \overline{A}$, we have $(\mathfrak{m} : \mathfrak{m})/\mathfrak{m} = A/\mathfrak{m} \oplus \left((\mathfrak{m} : \mathfrak{m}) \cap \mathfrak{p}A^\dagger\right)/\mathfrak{m}$.*

Proof. We have the following commutative diagram by Lemma 1.2.4, Remark 1.2.5 and Lemma 1.2.6

$$\begin{array}{ccccc} Q(A) & \longleftarrow & A & \longrightarrow & A/\mathfrak{p}A \\ \downarrow{\scriptstyle \mathrm{Tr}_{Q(A)/Q(R)}} & & \downarrow{\scriptstyle \mathrm{Tr}_{A/R}} & & \downarrow{\scriptstyle \mathrm{Tr}_{A/\mathfrak{p}A/R/\mathfrak{p}}} \\ Q(R) & \longleftarrow & R & \longrightarrow & R/\mathfrak{p}. \end{array}$$

Consider the symmetric bilinear form on $A/\mathfrak{p}A \times A/\mathfrak{p}A \to R/\mathfrak{p}$ obtained from $\mathrm{Tr}_{A/\mathfrak{p}A/R/\mathfrak{p}}$. The radical of this form by tameness is $\mathfrak{m}/\mathfrak{p}A$. Hence we obtain a non-degenerate form $A/\mathfrak{m} \times A/\mathfrak{m} \to R/\mathfrak{p}$. As this trace from comes from the one on $\mathrm{Tr}_{Q(A)/Q(R)}$ and $\mathfrak{p}$ is principal, we see that $\mathfrak{m} = \mathfrak{p}A^\dagger \cap A$.

$\implies$: Suppose that A is not integrally closed and let $T = \mathfrak{m} : \mathfrak{m}$. By Theorem 2.2.4 we have $T \supsetneq A$ and T is an order in $Q(A)$ by Lemma 2.2.2. Hence T comes with a trace form which is induced from $\mathrm{Tr}_{Q(A)/Q(R)}$ (by Lemma 1.2.6). Notice that $\mathfrak{m} \subset T$ is an ideal. Let $p : R \to R/\mathfrak{p}$ be the reduction. Then for $x \in \mathfrak{m}$ we have $p \circ \mathrm{Tr}_{Q(A)/Q(R)}(xT) = 0$. Hence we have the following commutative diagram:

$$\begin{array}{ccc} T/\mathfrak{m} \times T/\mathfrak{m} & \xrightarrow{(t+\mathfrak{m}, t'+\mathfrak{m}) \mapsto p \circ \mathrm{Tr}_{Q(A)/Q(R)}(tt')} & R/\mathfrak{p} \\ \uparrow{\scriptstyle i \times i} & & \uparrow{\scriptstyle \mathrm{id}} \\ A/\mathfrak{m} \times A/\mathfrak{m} & \xrightarrow{(a+\mathfrak{m}, a'+\mathfrak{m}) \mapsto p \circ \mathrm{Tr}_{Q(A)/Q(R)}(aa')} & R/\mathfrak{p}. \end{array}$$

We know that $A/\mathfrak{m} \subsetneq T/\mathfrak{m}$ is non-degenerate. By Theorem 1.1.8 we have

$$\begin{aligned} T/\mathfrak{m} &= A/\mathfrak{m} \perp (A/\mathfrak{m})^{\perp} \\ &= A/\mathfrak{m} \perp \left(T \cap \mathfrak{p}A^{\dagger}\right)/\mathfrak{m}. \end{aligned}$$

As $T/\mathfrak{m} \supsetneq A/\mathfrak{m}$, it follows that $\left(T \cap \mathfrak{p}A^{\dagger}\right)/\mathfrak{m} \neq 0$. As $A \cap \mathfrak{p}A^{\dagger} = \mathfrak{m}$, it follows that $\mathfrak{p}A^{\dagger} \not\subseteq A$.

$\Longleftarrow$: By Theorem 2.2.4 we see that A is a discrete valuation ring. First notice that $\mathfrak{p}A^{\dagger} \subseteq Q(A)$ is an A-module. Now suppose that $\mathfrak{p}A^{\dagger} \not\subseteq A$, then $A \subseteq \mathfrak{p}A^{\dagger}$ (here we use that A is a discrete valuation ring). Hence we have $A \subseteq \mathfrak{p}A^{\dagger} \cap A = \mathfrak{m}$, a contradiction. □

Corollary 2.2.6. *Let $(A, \mathfrak{m})$ be a local order over R which is tame at $\mathfrak{p}$. Let $B = A^{\dagger}/A$. Then*

$$(\mathfrak{m} : \mathfrak{m})/A = (\mathfrak{p}B)[\mathfrak{m}] \underset{A \neq \overline{A}}{=} B[\mathfrak{m}].$$

Proof. We will first prove the statement if $A = \overline{A}$. Then $\mathfrak{m} : \mathfrak{m} = A$ (Theorem 2.2.4) and $\mathfrak{p}B = 0$ (Theorem 2.2.5). The statement in this case now follows directly.

Now suppose that $A \neq \overline{A}$. From Theorem 2.2.4 it follows that $A : \mathfrak{m} = \mathfrak{m} : \mathfrak{m}$. As $\mathfrak{m} : \mathfrak{m} \subseteq \overline{A} \subseteq A^{\dagger}$, it follows that $(\mathfrak{m} : \mathfrak{m})/A = (A : \mathfrak{m})/A = B[\mathfrak{m}]$. Now we obviously have $(\mathfrak{p}B)[\mathfrak{m}] \subseteq B[\mathfrak{m}]$. From Theorem 2.2.5 it follows that $(\mathfrak{m} : \mathfrak{m})/\mathfrak{m} = A/\mathfrak{m} + \left((\mathfrak{m} : \mathfrak{m}) \cap \mathfrak{p}A^{\dagger}\right)/\mathfrak{m}$. Modding out by A gives us

$$(\mathfrak{m} : \mathfrak{m})/A = \left((\mathfrak{m} : \mathfrak{m}) \cap \mathfrak{p}A^{\dagger}\right)/A.$$

This shows that $(\mathfrak{m} : \mathfrak{m})/A \subseteq (\mathfrak{p}B)[\mathfrak{m}]$ and this finishes our proof. □

This last corollary seems rather uninteresting. We will see that it plays a crucial role in the proof of Theorem 6.2.2. Most algorithms for calculating the integral closure of an order, keep calculating $\mathfrak{m} : \mathfrak{m}$ until the chain of orders stabilizes. The last corollary really shows what one is doing inside $A^{\dagger}/A$ in these cases.

3. The general case

We can finally prove one of the theorems of our introduction.

Theorem 2.3.1. *Let A be an order over a Dedekind domain R. Let $\mathfrak{p} \subset R$ be a nonzero prime and assume that A is tame at $\mathfrak{p}$. Then $\mathfrak{p} \mid \operatorname{Ann}_R(\overline{A}/A)$ iff $\mathfrak{p}^2 \mid \operatorname{Ann}_R(A^{\dagger}/A)$.*

Proof. From Theorem 2.1.8 iv we see that $\mathfrak{p} \mid \operatorname{Ann}_R(\overline{A}/A)$ iff

$$\mathfrak{p} \mid \operatorname{Ann}_{\hat{R}_{\mathfrak{p}}}\left(\overline{A_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} \hat{R}_{\mathfrak{p}}}/A_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} \hat{R}_{\mathfrak{p}}\right).$$

Now let $A_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} \hat{R}_{\mathfrak{p}} = \prod_{i=1}^{n} B_i$ where B_i is a local order over $\hat{R}_{\mathfrak{p}}$ which is tame at $\mathfrak{p}$ (use Theorem 2.2.1, Remark 1.3.18 and Lemma 2.1.10). Notice that

$$\overline{\prod_{i=1}^{n} B_i} = \prod_{i=1}^{n} \overline{B_i}$$

and

$$\left(\prod_{i=1}^{n} B_i\right)^{\dagger} = \prod_{i=1}^{n} B_i^{\dagger}.$$

Then $\mathfrak{p} \mid \mathrm{Ann}_{\hat{R}_\mathfrak{p}}\left(\overline{A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}}/A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right)$ iff $\mathfrak{p} \mid \mathrm{Ann}_{\hat{R}_\mathfrak{p}}(\overline{B_i}/B_i)$ for some i. By Theorem 2.2.5 and Lemma 2.1.10 this is equivalent to $\mathfrak{p}^2 \mid \mathrm{Ann}_{\hat{R}_\mathfrak{p}}(B_i^\dagger/B_i)$ for this i. So it is equivalent to $\mathfrak{p}^2 \mid \mathrm{Ann}_{\hat{R}_\mathfrak{p}}(\left(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right)^\dagger / A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p})$. By Lemma 2.1.9, the flatness of $\hat{R}_\mathfrak{p}$ as $R_\mathfrak{p}$-module, Corollary 2.1.6, and the fact that localization is flat we have:

$$\begin{aligned}
\left(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right)^\dagger / \left(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right) &= \left(A_\mathfrak{p}^\dagger \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right) / \left(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right) \\
&= \left(A_\mathfrak{p}^\dagger / A_\mathfrak{p}\right) \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} \\
&= A_\mathfrak{p}^\dagger / A_\mathfrak{p} \\
&= \left(A^\dagger / A\right)_\mathfrak{p}.
\end{aligned}$$

Hence we see that $\mathfrak{p} \mid \mathrm{Ann}_R(\overline{A}/A)$ iff $\mathfrak{p}^2 \mid \mathrm{Ann}_R(\left(A^\dagger/A\right)_\mathfrak{p})$ iff $\mathfrak{p}^2 \mid \mathrm{Ann}_R(A^\dagger/A)$. □

Remark 2.3.2. The tameness condition in Theorem 2.3.1 can't be dropped in any of its implication. For example consider $A = \mathbf{Z}[\sqrt{d}]$ where $d \in \mathbf{Z}$ with $d \neq 1$ and d square-free. Then one can show that $A^\dagger = \frac{1}{2}\mathbf{Z} \oplus \frac{\sqrt{d}}{2d}\mathbf{Z}$. Hence $A^\dagger/A \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2d\mathbf{Z}$. By Lemma 1.4.18 we see that we are indeed in a wild case (look at the prime 2).

Now take $d = 2$. Then from Example 3.21 from [**9**] we see that $\overline{A} = A$. But $A^\dagger/A$ contains an element of order 2^2, which would contradict $\Longleftarrow$ in Theorem 2.3.1.

If we take $d = 5$, then from this example we see that $\overline{A} = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. But in this case $A^\dagger/A$ has no element of order 2^2, and this would contradict $\Longrightarrow$ in Theorem 2.3.1.

4. Tameness

Let R be a Dedekind domain and let A be an order over R. In some later theorems we require $\overline{A}$ to be tame at certain primes. The problem is, that we don't know this $\overline{A}$ in most cases. Hence we want to have conditions which guarantee certain orders to be tame. We have the following lemma, which provides a condition for being tame which can easily be used in algorithms.

Lemma 2.4.1. *Let R be a Dedekind domain and let A be an order over R. Let $\mathfrak{p} \subset R$ be prime. Let $B = A^\dagger/A$. Let A' be an R-order with $A \subseteq A' \subseteq \overline{A}$. Then A' is tame at $\mathfrak{p}$ if $\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) < \mathrm{char}(R/\mathfrak{p})$ or $\mathrm{char}(R/\mathfrak{p}) = 0$. Furthermore, the dimensions of $B/\mathfrak{p}B$ and the trace radical of $A/\mathfrak{p}A$ over $R/\mathfrak{p}$ are equal.*

Proof. As A' satisfies the same hypothesis as A, we may assume that $A' = A$. If $\mathrm{char}(R/\mathfrak{p}) = 0$, $A/\mathfrak{p}A$ will be automatically be tame (Lemma 1.3.19).

Assume that $\mathrm{char}(R/\mathfrak{p}) \neq 0$. Notice that $B/\mathfrak{p}B \cong B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ as $R/\mathfrak{p}$-modules and $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Now use Lemma 2.1.2 and Lemma 2.1.1 to see that we may assume that R is discrete valuation ring with maximal ideal $\mathfrak{p} = (\pi)$. Let $C = A/\mathfrak{p}A$ and assume that C is wild. Then from Lemma 1.3.19 it follows that $\dim_{R/\mathfrak{p}}(C^\perp) \geq \mathrm{char}(R/\mathfrak{p})$. For $x \in A$ we have $[x] \in C^\perp$ iff $\mathrm{Tr}_{Q(A)/Q(R)}(xA) \subseteq (\pi)$ iff $\mathrm{Tr}_{Q(A)/Q(R)}(\frac{x}{\pi}A) \subseteq A$ iff $\frac{x}{\pi} \in A^\dagger$ iff $x \in \pi A^\dagger = \mathfrak{p}A^\dagger$. Hence

$$C^\perp = \left(\mathfrak{p}A^\dagger \cap A\right)/\mathfrak{p}A.$$

We have

$$\begin{aligned}\left(\mathfrak{p}A^\dagger \cap A\right)/\mathfrak{p}A &= \left(\pi A^\dagger \cap A\right)/\pi A \\ &\cong \left(A^\dagger \cap \pi^{-1}A\right)/A \\ &= B[\mathfrak{p}].\end{aligned}$$

Finally consider the following exact sequence:

$$0 \longrightarrow B[\mathfrak{p}] \longrightarrow B \xrightarrow{\cdot\pi} B \longrightarrow B/\mathfrak{p}B \longrightarrow 0.$$

The length as R-module is an additive function ([**1**], Proposition 6.9). Hence $\text{length}_R(B[\mathfrak{p}]) = \text{length}_R(B/\mathfrak{p}B)$, and both lengths are their dimensions over $R/\mathfrak{p}$. So if A is wild at $\mathfrak{p}$ we have

$$\begin{aligned}\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) &= \dim_{R/\mathfrak{p}}(B[\mathfrak{p}]) \\ &= \dim_{R/\mathfrak{p}}(C^\perp) \\ &\geq \text{char}(R/\mathfrak{p}),\end{aligned}$$

and this concludes the proof. □

CHAPTER 3

Zero-dimensional principal ideal rings

1. Structure theorem

Definition 3.1.1. A ring R is called*uniserial* if R is a local zero-dimensional principal ideal ring.

Remark 3.1.2. In some books one uses the term *special rings* instead of *uniserial rings*, but we dislike this terminology.

Theorem 3.1.3. *Let R be a zero-dimensional principal ideal ring. Then R has only finitely many primes and $R \cong \prod_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}}$ by the natural map. All the $R_{\mathfrak{p}}$ are uniserial rings.*

Proof. From Theorem 8.5 from [**1**] it follows that R is artinian. Now apply Lemma 1.3.1. □

Remark 3.1.4. One can generalize the previous theorem for principal ideal rings: a ring is a principal ideal ring iff it is isomorphic to a product of finitely many principal ideal domains and uniserial rings (see [**10**], Page 245, Theorem 33).

We also want such a decomposition for modules.

Corollary 3.1.5. *Let R be an artinian ring. Let M be an R-module. Then $M \cong \bigoplus_{\mathfrak{p}\in \mathrm{Spec(R)}} M_{\mathfrak{p}}$ by the natural map.*

Proof. From Theorem 3.1.3 and Proposition 3.5 from [**1**] we have

$$\begin{aligned} M &\cong M \otimes_R R \\ &\cong M \otimes_R \left(\prod_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}} \right) \\ &\cong \bigoplus_{\mathfrak{p}\in \mathrm{Spec}(R)} M \otimes_R R_{\mathfrak{p}} \\ &\cong \bigoplus_{\mathfrak{p}\in \mathrm{Spec}(R)} M_{\mathfrak{p}}. \end{aligned}$$

□

Recall that all the $M_{\mathfrak{p}}$ are modules over $R_{\mathfrak{p}}$.

Lemma 3.1.6. *Let R be an artinian ring. Let M, N be R-modules. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. We then have $M = \perp_{\mathfrak{p}\in \mathrm{Spec}(R)} M_{\mathfrak{p}}$. Fix a prime $\mathfrak{p} \in \mathrm{Spec}(R)$. Let $i : R_{\mathfrak{p}} \to R$ and $j : M_{\mathfrak{p}} \to M$ be the inclusions. Then*

we have the following commutive diagram:

$$\begin{array}{ccc} M \times M & \xrightarrow{\langle\,,\,\rangle} & R \\ {\scriptstyle j\times j}\uparrow & & \uparrow{\scriptstyle i} \\ M_{\mathfrak{p}} \times M_{\mathfrak{p}} & \xrightarrow{(\frac{x}{s},\frac{y}{t})\mapsto\frac{\langle x,y\rangle}{st}} & R_{\mathfrak{p}}. \end{array}$$

PROOF. By Corollary 3.1.5 we have $M \cong \bigoplus_{\mathfrak{p}\in \mathrm{Spec(R)}} M_{\mathfrak{p}}$. Let $\mathfrak{p}, \mathfrak{p}' \subset R$ be different primes. Take $\mathfrak{m} \in \mathbf{Z}_{\geq 0}$ such that $\mathfrak{p}^m R_{\mathfrak{p}} = 0 \subset R_{\mathfrak{p}}$ and $\mathfrak{p}'^m R_{\mathfrak{p}'} = 0 \subset R_{\mathfrak{p}'}$ (use Proposition 8.6 from [**1**]). But then

$$\mathrm{Ann}_R(\langle M_{\mathfrak{p}}, M_{\mathfrak{p}'}\rangle) \supseteq \mathfrak{p}^m + \mathfrak{p}'^m = R$$

since $\mathfrak{p}^m$ and $\mathfrak{p}'^m$ are coprime. The last part is a calculation which is left to the reader. □

2. Uniserial rings

Lemma 3.2.1. *Let R be a ring. Then R is a principal ideal ring iff R is noetherian and all prime ideals of R are principal.*

PROOF. $\Longrightarrow$: This follows directly.

$\Longleftarrow$: We apply noetherian induction. Let S be the set of ideals of R which are not principal. Suppose $S \neq \emptyset$ and let $I \in S$ be a maximal element of S. Then I is not prime and not the unit ideal. We can choose $x, y \in R \setminus I$ with $xy \in I$. By assumption there is $a \in R$ such that $I + (x) = (a)$. Now consider $I : a = \{r \in R : ra \in I\}$. Notice that $I \subseteq I : a$ and $y \in I : a$, hence $I : a \supsetneq I$. By assumption there is $b \in R$ with $I : a = (b)$. Then by construction $I = (ab)$, a contradiction. Hence $S = \emptyset$ and we are done. □

Lemma 3.2.2. *A ring R is uniserial iff it is a local artinian ring with principal maximal ideal.*

PROOF. $\Longrightarrow$: By Theorem 8.5 from [**1**] it follows that R is artinian and the result follows.

$\Longleftarrow$: By Theorem 8.5 from [**1**] it follows that R is zero-dimensional and noetherian. By Lemma 3.2.1 we conclude that R is a principal ideal ring. □

Lemma 3.2.3. *Let R be a local artinian ring with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}$ is nilpotent and if $\mathfrak{m}^i = \mathfrak{m}^{i+1}$, then $\mathfrak{m}^i = 0$.*

PROOF. This follows from [**1**] Proposition 8.3 and Proposition 8.4. □

Theorem 3.2.4. *Let R be a uniserial ring with maximal ideal $\mathfrak{m}$. Suppose that $\mathfrak{m}^n = 0$ and $\mathfrak{m}^{n-1} \neq 0$. Then:*

i. *there are exactly $n+1$ ideals in R, namely $R = \mathfrak{m}^0 \supsetneq \mathfrak{m} = \mathfrak{m}^1 \supsetneq \mathfrak{m}^2 \supsetneq \ldots \supsetneq \mathfrak{m}^{n-1} \supsetneq 0 = \mathfrak{m}^n$;*
ii. *the ring R has length n as an R-module.*

PROOF. By Lemma 3.2.3 all ideals in the given sequence are different. Let $(\pi) = \mathfrak{m}$. Now consider an ideal $I = (x)$. If $x = 0$, then $(x) = \mathfrak{m}^n$. Now suppose $x \neq 0$. As $\mathfrak{m}$ is nilpotent by Lemma 3.2.3, it follows that there is a unique i with $1 \leq i \leq n$ and $(x) \subseteq \mathfrak{m}^i$, but $(x) \not\subseteq \mathfrak{m}^{i+1}$. We claim that $(x) = \mathfrak{m}^i$. We first write $x = \pi^i r$ where $r \in R$. If $r \in \pi$, then $(x) \subseteq \mathfrak{m}^{i+1}$. Hence $r \in R^*$ and $(x) = (\pi^i) = \mathfrak{m}^i$.

As a consequence $R = \mathfrak{m}^0 \supsetneq \mathfrak{m} = \mathfrak{m}^1 \supsetneq \mathfrak{m}^2 \supsetneq \ldots \supsetneq \mathfrak{m}^{n-1} \supsetneq 0 = \mathfrak{m}^n$ is a composition series for R. □

Remark 3.2.5. Let R is a uniserial ring of length n with maximal ideal $\mathfrak{m}$. Then $\mathrm{Ann}_R(\mathfrak{m}^i) = \mathfrak{m}^{n-i}$ for $0 \leq i \leq n$.

Lemma 3.2.6. *Let $R \neq 0$ be a ring with the property that the set of ideals of R is finite and linearly ordered by inclusion. Then R is uniserial.*

Proof. Let $R = I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \ldots \supsetneq I_n = 0$ be all ideals of R. It directly follows that R satisfies the descending chain condition, hence R is artinian. Of course $I_n = 0$ is principal. Now consider I_j for $0 \leq j < n$ and take $x \in I_j \setminus I_{j+1}$. Then $(x) \subseteq I_j$ and as $(x) \notin I_{j+1}$, it follows that $(x) = I_j$ and we are done. □

3. Modules over uniserial rings

Lemma 3.3.1. *Let R be a local artinian ring with maximal ideal $\mathfrak{m}$ and let M, N be R-modules. Let $\varphi : M \to N$ be an R-linear map. Then the following statements hold:*

i. *φ is surjective iff $\varphi \otimes 1 : M/\mathfrak{m}M = M \otimes_R R/\mathfrak{m} \to N/\mathfrak{m}N = N \otimes_R R/\mathfrak{m}$ is surjective;*
ii. *φ is injective iff $\varphi|_{M[\mathfrak{m}]} : M[\mathfrak{m}] \to N[\mathfrak{m}]$ is injective.*

Proof. i. $\Longrightarrow$: Obvious.
$\Longleftarrow$: It follows that $\varphi(M) + \mathfrak{m}N = N$. Substituting this relation in itself gives $\varphi(M) + \mathfrak{m}^2 N = \varphi(M) + \mathfrak{m}(\varphi(M) + \mathfrak{m}N) = N$. We can repeat the process and we obtain that $\varphi(M) + \mathfrak{m}^i N = N$. By Lemma 3.2.3 it follows that $\mathfrak{m}^n = 0$ for some $n \in \mathbf{Z}_{\geq 0}$. Hence we conclude that $\varphi(M) = N$, that is, φ is surjective.
ii. $\Longrightarrow$: Obvious.
$\Longleftarrow$: Assume that $\ker(\varphi) \neq 0$. We will show that a nonzero R-module M' satisfies $M'[\mathfrak{m}] \neq 0$ and this would prove the implication. As $\mathfrak{m}$ is nilpotent ([**1**], Proposition 8.4), it follows that there is an $r \in \mathbf{Z}_{\geq 0}$ such that $\mathfrak{m}^r M' \neq 0$ and $\mathfrak{m}^{r+1} M' = 0$. Then $\mathfrak{m}^r M' \subseteq M'[\mathfrak{m}]$ and hence $M'[\mathfrak{m}] \neq 0$.

□

Remark 3.3.2. Notice that i from the previous statement is also true if R is just a local ring and M is a finitely generated R-module. The implication $\Longrightarrow$ follows trivially. For $\Longleftarrow$ notice that $\varphi(M) + \mathfrak{m}N = N$ and use [**1**] Corollary 2.7 (Nakayama's Lemma). For our next theorem we need the case for non-finitely generated modules as well.

Theorem 3.3.3. *Let R be a uniserial ring of length n with maximal ideal $\mathfrak{m}$ and let M be an R-module. Then $M \cong \bigoplus_{i=1}^{n} (R/\mathfrak{m}^i)^{(n_i)}$ where the n_i are uniquely determined cardinal numbers.*

Proof. Let $\varphi : M \to M/\mathfrak{m}M$ be the canonical map. Now define the following $R/\mathfrak{m}$-vector spaces:

$$\begin{aligned} V_i &= \varphi(M[\mathfrak{m}^i]) \subseteq M/\mathfrak{m}M \\ W_i &= \mathfrak{m}^i M[\mathfrak{m}^{i+1}] \subseteq M[\mathfrak{m}] \end{aligned}$$

This gives two chains, namely $M/\mathfrak{m}M = V_n \supseteq V_{n-1} \supseteq \ldots \supseteq V_0 = \{0\}$ and $\{0\} = W_n \subseteq W_{n-1} \subseteq \ldots \subseteq W_0 = M[\mathfrak{m}]$. First notice that $\mathfrak{m}M \cap M[\mathfrak{m}^i] = \mathfrak{m}M[\mathfrak{m}^{i+1}]$ and

hence the naturally obtained map $\overline{\varphi} : M[\mathfrak{m}^i]/(M[\mathfrak{m}^{i-1}] + \mathfrak{m}M[\mathfrak{m}^{i+1}]) \to V_i/V_{i-1}$ is an isomorphism. Let $\mathfrak{m} = (\pi)$. Then we have the following diagram:

$$\begin{array}{ccc} V_i/V_{i-1} & & W_{i-1}/W_i \\ \uparrow{\scriptstyle \overline{\varphi}} & & \downarrow{\scriptstyle \mathrm{id}} \\ M[\mathfrak{m}^i]/(M[\mathfrak{m}^{i-1}] + \mathfrak{m}M[\mathfrak{m}^{i+1}]) & \xrightarrow{\cdot\pi^{i-1}} & \mathfrak{m}^{i-1}M[\mathfrak{m}^i]/\mathfrak{m}^i M[\mathfrak{m}^{i+1}]. \end{array}$$

We need to show that the map $\cdot\pi^{i-1}$ is well-defined. For this consider the map $\cdot\pi^{i-1} : M[\mathfrak{m}^i] \to W_{i-1}/W_i$, which is obviously surjective. We determine its kernel. Let $x \in M[\mathfrak{m}^i]$ and suppose that $\pi^{i-1}x = \pi^i y \in \mathfrak{m}^i M[\mathfrak{m}^{i+1}]$ where $y \in M[\mathfrak{m}^{i+1}]$. This means that $\pi^{i-1}(x - \pi y) = 0$, hence $x - \pi y = z \in M[\mathfrak{m}^{i-1}]$ and hence $x = \pi y + z \in \mathfrak{m}M[\mathfrak{m}^{i+1}] + M[\mathfrak{m}^{i-1}]$. Conversely, $\mathfrak{m}M[\mathfrak{m}^{i+1}] + M[\mathfrak{m}^{i-1}]$ is in the kernel. This shows that we have three isomorphisms in the diagram, and this gives us an isomorphism $\psi = \cdot\pi^{i-1} \circ \overline{\varphi}^{-1} : V_i/V_{i-1} \to W_{i-1}/W_i$.

Now let $B_i \subseteq M[\mathfrak{m}^i]$ be a lift of a basis of V_i/V_{i-1} to $M[\mathfrak{m}^i]$. By the above isomorphism, $\pi^{i-1}B_i \subseteq W_{i-1}$ gives a basis of W_{i-1}/W_i.

Now consider the following map:

$$f : F = \bigoplus_{i=1}^{n} (R/\mathfrak{m}^i)^{(B_i)} \to M$$

which maps $(R/\mathfrak{m}^i)^{(B_i)} \to M[\mathfrak{m}^i]$ in the obvious way. We claim that this map is an isomorphism, and for this we use Lemma 3.3.1. By construction $\bigsqcup_{i=1}^{n} B_i$ forms a basis of $V_n = M/\mathfrak{m}M$, which shows that the induced map $F/\mathfrak{m}F \to M/\mathfrak{m}M$ is surjective. By Lemma 3.3.1 f is surjective. Now consider the induced map $F[\mathfrak{m}] \to M[\mathfrak{m}]$, which is injective since $\bigsqcup_{i=1}^{n} \pi^{i-1}B_i$ forms a basis of $M[\mathfrak{m}]$. By Lemma 3.3.1 f is injective.

We will now show the uniqueness of the (n_i). For this remark that $(n_i) = \dim(W_{i-1}/W_i)$ (which follows from an easy calculation). □

Corollary 3.3.4. *Let R be an uniserial ring. The following statements hold.*

i. *The ring R is injective as R-module.*
ii. *Let M be a finitely generated R-module. Then $M \cong \mathrm{Hom}_R(M, R)$.*

Proof. Let n be the length of R and let $\mathfrak{m} = (\pi)$ be the maximal ideal of R.

i. We will first show that R is injective as R-module. We use Baer's criterion ([**6**], 3.7) and Theorem 3.2.4. Let $f : \mathfrak{m}^{n-i} \to R$ be an R-linear map. Then $f(\pi^{n-i}) = r\pi^{n-i}$ for $r \in R$. Then define $f' : R \to R$ by $f(1) = r$.

ii. Now let $M = R/\mathfrak{m}^i$. Then look at the following R-linear map:

$$\begin{array}{rccc} \varphi_i : R & \to & \mathfrak{m}^{n-i} \\ 1 & \mapsto & \pi^{n-i}. \end{array}$$

This map is surjective by definition, and its kernel is equal to $\mathfrak{m}^i$ by Remark 3.2.5. Hence we have an induced isomorphism $\varphi_i' : R/\mathfrak{m}^i \to \mathfrak{m}^{n-i}$. Now let $\psi \in \mathrm{Hom}_R(R/\mathfrak{m}^i, R)$, then ψ is determined by $\psi(1) \in \mathfrak{m}^{n-i}$, and such an element determines a morphism. Hence $\mathrm{Hom}_R(R/\mathfrak{m}^i, R) \cong \mathfrak{m}^{n-i} \cong R/\mathfrak{m}^i$. Use Theorem 3.3.3 to finish the proof of the statement. □

Definition 3.3.5. Let R be a uniserial ring of length n with maximal ideal $\mathfrak{m}$ and M be an R-module. We define the *lower root* of M as

$$\mathrm{lr}(M) = \sum_{k=0}^{n} (\mathfrak{m}^k M) \cap M[\mathfrak{m}^k].$$

We define the *upper root* of M as

$$\mathrm{ur}(M) = \bigcap_{k=0}^{n} \left(\mathfrak{m}^k M + M[\mathfrak{m}^k]\right).$$

Later we will give a definition as in the introduction which works in a more general situation.

Lemma 3.3.6. *Let R be a uniserial ring of length n with maximal ideal $\mathfrak{m}$. Let $M = R/\mathfrak{m}^i$ where $0 \leq i \leq n$. Then $\mathrm{lr}(M) = \mathfrak{m}^{\lceil \frac{i}{2} \rceil}/\mathfrak{m}^i$ and $\mathrm{ur}(M) = \mathfrak{m}^{\lfloor \frac{i}{2} \rfloor}/\mathfrak{m}^i$. Stated differently, the lower root respectively upper root of a cyclic module of length i is the unique submodule of length $\lfloor \frac{i}{2} \rfloor$ respectively $\lceil \frac{i}{2} \rceil$.*

Proof. This is an easy calculation and left to the reader. □

Corollary 3.3.7. *Let R be a uniserial ring with maximal ideal $\mathfrak{m}$. Let M be an R-module. Then we have $\mathfrak{m} \cdot \mathrm{ur}(M) \subseteq \mathrm{lr}(M) \subseteq \mathrm{ur}(M)$.*

Proof. Let M_i be R-modules for $i \in I$. Then $\bigoplus_{i\in I} \mathrm{lr}(M_i) = \mathrm{lr}(\bigoplus_{i\in I} M_i)$. Now apply Theorem 3.3.3 and Lemma 3.3.6. □

Lemma 3.3.8. *Let R be a uniserial ring. Let M, N be R-modules and $\varphi : M \to N$ a morphism. Then we have induced maps from $\varphi_{\mathrm{lr}} : \mathrm{lr}(M) \to \mathrm{lr}(N)$ and $\varphi_{\mathrm{ur}} : \mathrm{ur}(M) \to \mathrm{ur}(N)$.*

Proof. This is an easy calculation and left to the reader. □

4. Non-degenerate symmetric bilinear forms

In this section we fix a uniserial ring R of length n with maximal ideal $\mathfrak{m} = (\pi)$.

4.1. Non-degeneracy conditions.

Theorem 3.4.1. *Let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear map where M is a finitely generated R-module. Then consider the map*

$$\begin{array}{rcl} {}^{\perp} : \{R\text{−submodules of } M\} & \to & \{R\text{−submodules of } M\} \\ N & \mapsto & N^{\perp}. \end{array}$$

Then the following statements are equivalent:

i. $\langle\ ,\ \rangle$ *is non-degenerate;*
ii. $M^{\perp} = 0$*;*
iii. *for all submodules $N \subseteq M$ we have*

$$\mathrm{length}_R(N) + \mathrm{length}_R(N^{\perp}) = \mathrm{length}_R(M);$$

iv. $^{\perp}$ *is an inclusion reversing bijection with inverse* $^{\perp}$*.*

PROOF. i $\implies$ iii: Let $N \subseteq M$ be a submodule. Let $\varphi : M \to \mathrm{Hom}_R(M, R)$ be the isomorphism obtained from $\langle\ ,\ \rangle$. By injectivity of R (Corollary 3.3.4) we know that $0 \to \mathrm{Hom}_R(M/N, R) \to \mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(N, R) \to 0$ is exact. By definition $N^\perp = \varphi^{-1}(\mathrm{Hom}_R(M/N, R))$. We find that $\mathrm{length}_R(N)+\mathrm{length}_R(N^\perp) = \mathrm{length}_R(M)$ by Corollary 3.3.4.

iii $\implies$ iv: Let $N \subseteq M$ be a submodule. We will prove that $N = (N^\perp)^\perp$. By Lemma 1.1.5 we have $N \subseteq (N^\perp)^\perp$. From iii it follows that $\mathrm{length}_R(N) = \mathrm{length}_R(M) - \mathrm{length}_R(N^\perp)$ and $\mathrm{length}_R(N^\perp) = \mathrm{length}_R(M) - \mathrm{length}_R((N^\perp)^\perp)$. Hence we find $\mathrm{length}_R(N) = \mathrm{length}_R((N^\perp)^\perp)$ and since we have an inclusion, $N = (N^\perp)^\perp$.

iv $\implies$ ii: We have

$$M^\perp = (0^\perp)^\perp = 0.$$

ii $\implies$ i: We obtain a morphism $\varphi : M \to \mathrm{Hom}_R(M, R)$ from $\langle\ ,\ \rangle$. By assumption, φ is injective. As $\mathrm{length}_R(\mathrm{Hom}_R(M, R)) = \mathrm{length}_R(M)$ (Corollary 3.3.4), it follows that the map is surjective as well and we have an isomorphism. □

Remark 3.4.2. Let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear map where M is a finitely generated R-module. Then we obtain a symmetric R-bilinear map $\langle\ ,\ \rangle' : M/M^\perp \times M/M^\perp \to R$, which by the above theorem is non-degenerate.

Lemma 3.4.3. *Let $\langle\ ,\ \rangle : M \times M \to R$ be a non-degenerate symmetric R-bilinear map where M is a finitely generated R-module. Let $N, N' \subseteq M$ be submodules. Then:*

$$\begin{aligned} (N + N')^\perp &= N^\perp \cap N'^\perp \\ (N \cap N')^\perp &= N^\perp + N'^\perp. \end{aligned}$$

PROOF. The first equality follows from Lemma 1.1.5. Now in the first equality put $(N^\perp, N'^\perp)$ instead of (N, N') and use Theorem 3.4.1:

$$\begin{aligned} N^\perp + N'^\perp &= \left((N^\perp + N'^\perp)^\perp\right)^\perp \\ &= \left((N^\perp)^\perp \cap (N'^\perp)^\perp\right)^\perp \\ &= (N \cap N')^\perp. \end{aligned}$$

□

Definition 3.4.4. A finitely generated R-module M is called *free over $R/\mathfrak{m}^i$* if it is isomorphic to $(R/\mathfrak{m}^i)^m$ for some $m \in \mathbf{Z}_{\geq 0}$.

Theorem 3.4.5. *Let $M = (R/\mathfrak{m}^r)^s$ ($1 \leq r \leq n$, $s \in \mathbf{Z}_{\geq 0}$). Say that $e_1, \ldots, e_s$ forms a basis of M over $R/\mathfrak{m}^r$. Let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear map. Let $x_{ij} \in R$ with $\langle e_i, e_j \rangle = \pi^{n-r} x_{ij}$. Then $\langle\ ,\ \rangle$ is non-degenerate iff* $\det\left((x_{ij} + \mathfrak{m})_{i,j=1}^s\right) \neq 0$ *in $R/\mathfrak{m}$.*

PROOF. Consider the following isomorphism:

$$\begin{aligned} \varphi : R/\mathfrak{m}^r &\to R[\mathfrak{m}^r] \\ [x] &\mapsto \pi^{n-r} x. \end{aligned}$$

The map $\langle\ ,\ \rangle$ is non-degenerate iff it induces an isomorphism between M and $\mathrm{Hom}_R(M, R)$. As $\mathrm{Hom}_R(M, R) \cong M$ by maps of the form φ one obtains a linear

map $\psi : M \to M$ given on the basis $e_1, \ldots, e_n$ by the matrix $\left(\varphi^{-1}(\langle e_i, e_j\rangle)\right)_{i,j=1}^{n}$. In order for our map to be an isomorphism, it is necessary and sufficient that the determinant of this matrix is in $(R/\mathfrak{m}^r)^*$. We reduce all coefficients modulo $\mathfrak{m}$ and see that this is equivalent to $\det((\varphi^{-1}(\langle e_i, e_j\rangle) + \mathfrak{m})_{i,j=1}^{n}) \neq 0$ in $R/\mathfrak{m}$.

□

4.2. Lower roots and upper roots. The aim of this subsection is to show how we can use upper roots and lower roots to see if a form is non-degenerate.

Lemma 3.4.6. *Let M be a finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Then $\mathrm{lr}(M) \subseteq \mathrm{ur}(M)^\perp \subseteq \mathrm{lr}(M)^\perp$.*

Proof. As $\mathrm{lr}(M) \subseteq \mathrm{ur}(M)$ (and Lemma 1.1.5) we find $\mathrm{ur}(M)^\perp \subseteq \mathrm{lr}(M)^\perp$. Recall that

$$\begin{aligned} \mathrm{lr}(M) &= \sum_{k=0}^{n} (\mathfrak{m}^k M) \cap M[\mathfrak{m}^k] \\ \mathrm{ur}(M) &= \bigcap_{k=0}^{n} \left(\mathfrak{m}^k M + M[\mathfrak{m}^k]\right). \end{aligned}$$

Let $x \in (\mathfrak{m}^k M) \cap M[\mathfrak{m}^k]$ and $y \in \mathrm{ur}(M)$. Then $y \in \mathfrak{m}^k M + M[\mathfrak{m}^k]$. But then obviously $\langle x, y\rangle = 0$. □

In the non-degenerate case, we can prove a stronger statement. We begin with the following lemma.

Lemma 3.4.7. *Let M be a finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to R$ be a non-degenerate symmetric R-bilinear form. Then $(\mathfrak{m}^k M)^\perp = M[\mathfrak{m}^k]$ and $M[\mathfrak{m}^k]^\perp = \mathfrak{m}^k M$.*

Proof. By Theorem 3.4.1 it is enough to prove $(\mathfrak{m}^k M)^\perp = M[\mathfrak{m}^k]$. Let $x \in M$. Then $x \in (\mathfrak{m}^k M)^\perp$ iff $\forall s \in M : \langle x, \pi^k s\rangle = 0$ iff $\forall s \in M : \langle \pi^k x, s\rangle = 0$ iff (non-degeneracy) $\pi^k x = 0$ iff $x \in M[\mathfrak{m}^k]$. □

Theorem 3.4.8. *Let M be a finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to R$ be a non-degenerate symmetric bilinear form. Then $\mathrm{lr}(M)^\perp = \mathrm{ur}(M)$. Especially, $\mathfrak{m} \cdot \mathrm{lr}(M)^\perp \subseteq \mathrm{lr}(M) \subseteq \mathrm{lr}(M)^\perp$.*

Proof. We calculate using the previous lemma and other properties of $^\perp$ (Lemma 3.4.3):

$$\begin{aligned} \mathrm{lr}(M)^\perp &= \left(\sum_{k=1}^{n-1} (\mathfrak{m}^k M) \cap M[\mathfrak{m}^k]\right)^\perp \\ &= \bigcap_{k=1}^{n-1} \left((\mathfrak{m}^k M)^\perp + M[\mathfrak{m}^k]^\perp\right) \\ &= \bigcap_{k=1}^{n-1} \left(M[\mathfrak{m}^k] + \mathfrak{m}^k M\right) \\ &= \mathrm{ur}(M). \end{aligned}$$

The rest follows from Corollary 3.3.7. □

Lemma 3.4.9. *Let M be finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear form. Then we obtain a symmetric bilinear form*

$$\langle\ ,\ \rangle_{\mathrm{odd}} : \mathrm{ur}(M)/\mathrm{lr}(M) \times \mathrm{ur}(M)/\mathrm{lr}(M) \to R.$$

If $\langle\ ,\ \rangle$ is non-degenerate, then $\langle\ ,\ \rangle_{\mathrm{odd}}$ is non-degenerate as well.

Proof. The first statement follows from Lemma 3.4.6. The second statement follows from Theorem 3.4.8 and Theorem 3.4.1. □

Definition 3.4.10. Let M be a finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear form. Then we define $\langle\ ,\ \rangle_{\mathrm{odd}}$ to be the form obtained from $\langle\ ,\ \rangle$ on $\mathrm{ur}(M)/\mathrm{lr}(M)$ as in Lemma 3.4.9. From $\langle\ ,\ \rangle$ we obtain a form $\langle\ ,\ \rangle' : M/M[\mathfrak{m}] \times M/M[\mathfrak{m}] \to R/R[\mathfrak{m}]$. We define $\langle\ ,\ \rangle_{\mathrm{even}} = \langle\ ,\ \rangle'_{\mathrm{odd}}$. Sometimes we use the notation M_{odd} and M_{even} for these modules with their symmetric bilinear forms. Remark that the odd and even forms are forms on vector spaces over $R/\mathfrak{m}$.

We will now divide up this M_{odd} and M_{even} in smaller parts.

Definition 3.4.11. Let M be an R-module. Let $i \in \mathbf{Z}_{\geq 1}$ be odd. Then we define

$$\rho_i(M) \quad = \quad \mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^i] / \left(\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^{i-1}] + \mathfrak{m}^{\lfloor \frac{i}{2} \rfloor + 1} M[\mathfrak{m}^{i+1}] \right).$$

For even $i \in \mathbf{Z}_{\geq 2}$ we define

$$\rho_i(M) \quad = \quad \rho_{i-1}(M/M[\mathfrak{m}]).$$

Remark 3.4.12. Note that by construction these $\rho_i(M)$ are $R/\mathfrak{m}$-vector spaces. If $\mathrm{Ann}_R(M) = \mathfrak{m}^r$ $(0 \leq r \leq n)$, then $\rho_i(M) = 0$ for $i > r$.

Lemma 3.4.13. *Let M be an R-module. Then the natural map*

$$\begin{aligned} \varphi_{\mathrm{odd}} : \bigoplus_{i \in \mathbf{Z}_{\geq 1} \text{ odd}} \rho_i(M) \quad &\to \quad \mathrm{ur}(M)/\mathrm{lr}(M) = M_{\mathrm{odd}} \\ ([x_i])_{i \text{ odd}} \quad &\mapsto \quad [\sum_{i \text{ odd}} x_i] \end{aligned}$$

is an isomorphism of R-modules. Similarly, we obtain an isomorphism of R-modules

$$\begin{aligned} \varphi_{\mathrm{even}} : \bigoplus_{i \in \mathbf{Z}_{\geq 2} \text{ even}} \rho_i(M) \quad &\to \quad \mathrm{ur}(M/M[\mathfrak{m}])/\mathrm{lr}(M/M[\mathfrak{m}]) = M_{\mathrm{even}} \\ ([x_i])_{i \text{ even}} \quad &\mapsto \quad [\sum_{i \text{ even}} x_i]. \end{aligned}$$

Now assume that $M \cong (R/\mathfrak{m}^r)^s$ (where $0 \leq r \leq n$). Then we have an R-linear isomorphism

$$\rho_i(M) \cong \begin{cases} (R/\mathfrak{m})^s & i = r \\ 0 & i \neq r \end{cases}$$

Proof. We will prove the statements for φ_{odd} and by construction the similar statements for φ_{even} will follow. First we will show that our map is well-defined. Let $i \in \mathbf{Z}_{\geq 1}$ be odd. We first need to show that $\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^i] \subseteq \mathrm{ur}(M)$. Indeed, we have $\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^i] \subseteq \mathfrak{m}^k M$ for $k \leq \lfloor \frac{i}{2} \rfloor$ and $\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^i] \subseteq M[\mathfrak{m}^k]$ for $k \geq \lceil \frac{i}{2} \rceil$. Now check the definition. We will show that $\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^{i-1}] + \mathfrak{m}^{\lfloor \frac{i}{2} \rfloor + 1} M[\mathfrak{m}^{i+1}] \subseteq \mathrm{lr}(M)$.

We have $\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^{i-1}] \subseteq (\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M) \cap M[\mathfrak{m}^{\lfloor \frac{i}{2} \rfloor}]$. A similar statement holds for the other term (replace i by $i+2$), and now check the definition.

We will show that φ_{odd} is a bijection. For R-modules N and N' we have $\rho_i(N \oplus N') = \rho_i(N) \oplus \rho_i(N')$ and

$$\text{ur}(N \oplus N')/\text{lr}(N \oplus N') = \text{ur}(N)/\text{lr}(N) \oplus \text{ur}(N')/\text{lr}(N').$$

Now use Theorem 3.3.3 to see that we need to prove the statement only for modules of the form $M = R/\mathfrak{m}^j$. Notice that for $1 \leq i, j \leq n$ and i odd that

$$\rho_i(R/\mathfrak{m}^j) = \begin{cases} \text{ur}(R/\mathfrak{m}^j)/\text{lr}(R/\mathfrak{m}^j) & i = j \\ 0 & i \neq j \end{cases}$$

and hence our map is indeed an isomorphism. This also proves our last statement. □

Definition 3.4.14. Let M be a finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear form. Then we define $\langle\ ,\ \rangle'_{\text{odd}}$ and $\langle\ ,\ \rangle'_{\text{even}}$ to be the maps making the following diagrams commute:

$$\begin{array}{ccc} \bigoplus_{i \in \mathbf{Z}_{\geq 1} \text{ odd}} \rho_i(M) \times \bigoplus_{i \in \mathbf{Z}_{\geq 1} \text{ odd}} \rho_i(M) & \xrightarrow{\langle\ ,\ \rangle'_{\text{odd}}} & R[\mathfrak{m}] \\ \downarrow{\scriptstyle \varphi_{\text{odd}} \times \varphi_{\text{odd}}} & & \downarrow{\scriptstyle \text{id}_{R[\mathfrak{m}]}} \\ M_{\text{odd}} \times M_{\text{odd}} & \xrightarrow[\langle\ ,\ \rangle_{\text{odd}}]{} & R[\mathfrak{m}] \end{array}$$

and

$$\begin{array}{ccc} \bigoplus_{i \in \mathbf{Z}_{\geq 2} \text{ even}} \rho_i(M) \times \bigoplus_{i \in \mathbf{Z}_{\geq 2} \text{ even}} \rho_i(M) & \xrightarrow{\langle\ ,\ \rangle'_{\text{even}}} & R[\mathfrak{m}^2]/R[\mathfrak{m}] \\ \downarrow{\scriptstyle \varphi_{\text{even}} \times \varphi_{\text{even}}} & & \downarrow{\scriptstyle \text{id}_{R[\mathfrak{m}^2]/R[\mathfrak{m}]}} \\ M_{\text{even}} \times M_{\text{even}} & \xrightarrow[\langle\ ,\ \rangle_{\text{even}}]{} & R[\mathfrak{m}^2]/R[\mathfrak{m}]. \end{array}$$

Lemma 3.4.15. *Let M be a finitely generated R-module and let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear form. Then we have orthogonal decompositions*

$$\perp_{i \in \mathbf{Z}_{\geq 1} \text{ odd}} \rho_i(M)$$

and

$$\perp_{i \in \mathbf{Z}_{\geq 2} \text{ even}} \rho_i(M)$$

under $\langle\ ,\ \rangle'_{\text{odd}}$ respectively $\langle\ ,\ \rangle'_{\text{even}}$.

Proof. We again do the odd case only. We need to show that $\rho_i(M)$ and $\rho_j(M)$ are orthogonal if $i \neq j$. Suppose without loss of generality that $i > j$. Take $x \in \rho_i(M)$ and $y \in \rho_j(M)$ and take representatives $\pi^{\lfloor \frac{i}{2} \rfloor} x' \in \mathfrak{m}^{\lfloor \frac{i}{2} \rfloor} M[\mathfrak{m}^i]$ and $\pi^{\lfloor \frac{j}{2} \rfloor} y' \in \mathfrak{m}^{\lfloor \frac{j}{2} \rfloor} M[\mathfrak{m}^j]$. But then we just calculate and obtain:

$$\begin{aligned} \langle x, y \rangle'_{\text{odd}} &= \langle \pi^{\lfloor \frac{i}{2} \rfloor} x', \pi^{\lfloor \frac{j}{2} \rfloor} y' \rangle \\ &= \langle x', \pi^{\lfloor \frac{i}{2} \rfloor + \lfloor \frac{j}{2} \rfloor} y' \rangle \\ &= \langle x', 0 \rangle \\ &= 0. \end{aligned}$$

□

Lemma 3.4.16. *Assume that M be a finitely generated R-module which is free over $R/\mathfrak{m}^r$ $(0 \leq r \leq n)$. Let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear form. Then we obtain a natural symmetric R-bilinear form $\langle\ ,\ \rangle' : M/\mathfrak{m}M \times M/\mathfrak{m}M \to \mathfrak{m}^{n-r}/\mathfrak{m}^{n-r+1}$. If r is odd, we have the following commutative diagram where the vertical maps are isomorphisms*

$$\begin{array}{ccc} M/\mathfrak{m}M \times M/\mathfrak{m}M & \xrightarrow{\langle\ ,\ \rangle'} & \mathfrak{m}^{n-r}/\mathfrak{m}^{n-r+1} \\ \downarrow{\scriptstyle \cdot\pi^{\frac{r-1}{2}} \times \cdot\pi^{\frac{r-1}{2}}} & & \downarrow{\scriptstyle \cdot\pi^{r-1}} \\ M_{\text{odd}} \times M_{\text{odd}} & \xrightarrow{\langle\ ,\ \rangle_{\text{odd}}} & R[\mathfrak{m}]. \end{array}$$

For even r we have the following commutative diagram where the vertical maps are isomorphisms

$$\begin{array}{ccc} M/\mathfrak{m}M \times M/\mathfrak{m}M & \xrightarrow{\langle\ ,\ \rangle'} & \mathfrak{m}^{n-r}/\mathfrak{m}^{n-r+1} \\ \downarrow{\scriptstyle \cdot\pi^{\frac{r}{2}-1} \times \cdot\pi^{\frac{r}{2}-1}} & & \downarrow{\scriptstyle \cdot\pi^{r-2}} \\ M_{\text{even}} \times M_{\text{even}} & \xrightarrow{\langle\ ,\ \rangle_{\text{even}}} & R[\mathfrak{m}^2]/R[\mathfrak{m}]. \end{array}$$

PROOF. The proof is easy and left to the reader. □

Theorem 3.4.17. *Let M be a finitely generated R-module. Let $\langle\ ,\ \rangle : M \times M \to R$ be a symmetric R-bilinear form. The following statements hold.*

i. *The form $\langle\ ,\ \rangle$ is non-degenerate iff $\langle\ ,\ \rangle_{\text{odd}}$ and $\langle\ ,\ \rangle_{\text{even}}$ are non-degenerate.*
ii. *If $\langle\ ,\ \rangle$ is non-degenerate, then we can write $M = M_1 \perp \ldots \perp M_n$ where M_i is non-degenerate and free over $R/\mathfrak{m}^i$. Furthermore, suppose that $M_i' \subseteq M$ is free over $R/\mathfrak{m}^i$ $(1 \leq i \leq n)$. Assume that the map $\rho_i(M_i') \to \rho_i(M)$ is an isomorphism of R-modules. Then there is such a decomposition as above with $M_i = M_i'$.*

PROOF. We will prove the first statement, and along the way we will prove the second one as well.

$\Longrightarrow$: By Lemma 3.4.9 it follows that $\langle\ ,\ \rangle_{\text{odd}}$ is non-degenerate. We claim that $\langle\ ,\ \rangle' : M/M[\mathfrak{m}] \times M/M[\mathfrak{m}] \to R/R[\mathfrak{m}]$ is non-degenerate. Indeed, suppose that $\langle x, M\rangle \subset R[\mathfrak{m}]$. Then $x \in M[\mathfrak{m}]$ by non-degeneracy and we are done. Now use Lemma 3.4.9.

$\Longleftarrow$: First assume that M is free over $R/\mathfrak{m}^r$, say $M = (R/\mathfrak{m}^r)^s$ with basis $e_1, \ldots, e_s$ over $R/\mathfrak{m}^r$. Assume that r is odd. Then we write

$$\langle e_i, e_j\rangle \quad = \quad \pi^{n-r} x_{ij}$$

where $x_{ij} \in R$. Notice that the elements $\pi^{\frac{r-1}{2}} e_i$ give a basis of $\text{ur}(M)/\text{lr}(M)$ and we obtain

$$\begin{aligned} \pi^{r-1}\langle e_i, e_j\rangle &= \langle \pi^{\frac{r-1}{2}} e_i, \pi^{\frac{r-1}{2}} e_j\rangle \\ &= \pi^{n-1} x_{ij}. \end{aligned}$$

By Theorem 3.4.5 we see $\langle\ ,\ \rangle$ is non-degenerate iff $\langle\ ,\ \rangle_{\text{odd}}$ is non-degenerate.

Similarly, one shows that if r is even, that $\langle\ ,\ \rangle$ is non-degenerate iff $\langle\ ,\ \rangle_{\text{even}}$ is non-degenerate.

Now we will do the general case. We will give a proof by induction on $\text{length}_R(M)$, the statement being trivial when $M = 0$. Pick a non-zero $M_i \subset M$ free over $R/\mathfrak{m}^i$

$(1 \leq i \leq n)$ such that the map $\rho_i(M_i') \to \rho_i(M)$ is an isomorphism (we can get such a module by using Theorem 3.3.3 to write $M = N_1 \oplus \ldots \oplus N_n$ where the N_i are free over $R/\mathfrak{m}^i$ and pick a nonzero N_n). Then from the homogeneous case, Lemma 3.4.15 and Theorem 1.1.8 it follows that M_i is non-degenerate. Now write $M = M_i \perp M'$ and by induction M' is non-degenerate (since the odd and even forms stay non-degenerate, use Lemma 3.4.13). Apply Theorem 1.1.8 to conclude that M is non-degenerate. We can also directly prove statement ii. by induction. □

5. Anisotropy

Definition 3.5.1. Let R be a zero-dimensional principal ideal ring and let M be an R-module. Then we define the *lower root* of M as

$$\mathrm{lr}(M) = \sum_{r \in R} (rM) \cap M[r].$$

We define the *upper root* of M as

$$\mathrm{ur}(M) = \bigcap_{r \in R} \left(rM + M[r]\right).$$

Remark 3.5.2. Notice that our previous definition coincides with Definition 3.3.5 in case R is a uniserial ring. Also notice that $\mathrm{lr}(M \oplus N) = \mathrm{lr}(M) \oplus \mathrm{lr}(N)$ and $\mathrm{ur}(M \oplus N) = \mathrm{ur}(M) \oplus \mathrm{ur}(N)$.

Furthermore let R be a zero-dimensional principal ideal ring. Let M be an R-module. Then we can use Corollary 3.1.5 to write $M = \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(R)} M_{\mathfrak{p}}$. Then we have

$$\mathrm{lr}(M) = \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathrm{lr}(M_{\mathfrak{p}}).$$

Similarly, we have

$$\mathrm{ur}(M) = \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathrm{ur}(M_{\mathfrak{p}}).$$

Definition 3.5.3. Let R be a ring and let M be an R-module. Then M is called *semi-simple* if M is a sum of simple submodules.

Remark 3.5.4. Let R be a zero-dimensional principal ideal ring. Let M be an R-module. For $\mathfrak{p} \in \mathrm{Spec}(R)$ let $l_{\mathfrak{p}} = \mathrm{length}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}})$. Then by Corollary 3.1.5 and Theorem 3.3.3 it follows that we can write any R-module as

$$\bigoplus_{\mathfrak{p} \in \mathrm{Spec}(R)} \bigoplus_{i=1}^{l_{\mathfrak{p}}} \left(R/\mathfrak{p}^i\right)^{(n_{\mathfrak{p},i})}$$

where the $(n_{\mathfrak{p},i})$ are uniquely determined cardinal numbers. This shows that an R-module is semisimple iff it is a direct sum of modules of the form $R/\mathfrak{p}$. Equivalently, M is semisimple iff $\sqrt{0} \cdot M = \left(\prod_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}\right) M = 0$.

Lemma 3.5.5. *Let R be a zero-dimensional principal ideal ring and let M be an R-module. Then*

$$\sqrt{0} \cdot \mathrm{ur}(M) \subseteq \mathrm{lr}(M) \subseteq \mathrm{ur}(M).$$

Proof. This follows from Remark 3.5.2 in combination with Corollary 3.3.7. □

Lemma 3.5.6. *Let R be a zero dimensional principal ideal ring. Let M be a finitely generated R-module and let N be a free R-module of rank 1. Let $\langle\ ,\ \rangle : M \times M \to N$ be a non-degenerate symmetric R-bilinear form. Then $\mathrm{lr}(M)^\perp = \mathrm{ur}(M)$. Furthermore, $\sqrt{0} \cdot \mathrm{lr}(M)^\perp \subseteq \mathrm{lr}(M) \subseteq \mathrm{lr}(M)^\perp$.*

Proof. We have a decomposition by Lemma 3.1.6 and each $M_\mathfrak{p}$ is still non-degenerate for $\mathfrak{p} \in \mathrm{Spec}(R)$ (Theorem 1.1.7). Hence by Theorem 3.4.8 and Remark 3.5.2 we have:

$$\begin{aligned} \mathrm{lr}(M)^\perp &= \left(\perp_{\mathfrak{p}\in \mathrm{Spec}(R)} \mathrm{lr}(M_\mathfrak{p})\right)^\perp \\ &= \perp_{\mathfrak{p}\in \mathrm{Spec}(R)} \mathrm{lr}(M_\mathfrak{p})^\perp \\ &= \perp_{\mathfrak{p}\in \mathrm{Spec}(R)} \mathrm{ur}(M_\mathfrak{p}) \\ &= \mathrm{ur}(M). \end{aligned}$$

The last statement follows from the first part and Lemma 3.5.5. □

Lemma 3.5.6 now allows us to give the following definition.

Definition 3.5.7. Let R be a zero-dimensional principal ideal ring. Let M be a finitely generated R-module and let N be a free R-module of rank 1. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Then $\langle\ ,\ \rangle$ is called *anisotropic* if it is non-degenerate and the only submodule $L \subseteq M$ satisfying $\sqrt{0} \cdot L^\perp \subseteq L \subseteq L^\perp$ is $\mathrm{lr}(M)$. It is called *isotropic* if it is not anisotropic.

Definition 3.5.8. Let M be a finitely generated R-module. Let $\langle\ ,\ \rangle : M \times M \to N$ be a non-degenerate symmetric R-bilinear form. Then we define the *radical root* of $(M, \langle\ ,\ \rangle)$ as

$$\mathrm{rr}(M, \langle\ ,\ \rangle) = \bigcap_{L\subseteq M : \sqrt{0}\cdot L^\perp \subseteq L \subseteq L^\perp} L.$$

In most cases $\langle\ ,\ \rangle$ will be fixed and we will just write $\mathrm{rr}(M)$ instead of $\mathrm{rr}(M, \langle\ ,\ \rangle)$.

Remark 3.5.9. Let R be a zero-dimensional principal ideal ring. Then one can easily see from Lemma 3.1.6 that anisotropy is a property which can be checked at the primes. This means that $\langle\ ,\ \rangle : M \times M \to N$ is anisotropic iff all the $M_\mathfrak{p}$ are anisotropic. One can also locally 'calculate' this $\mathrm{rr}(M)$.

CHAPTER 4

Integral closure and uniserial rings

1. Orders and uniserial rings

Lemma 4.1.1. *Let R be a Dedekind domain and let $I \neq 0, R$ be an ideal. Then R/I is a zero-dimensional principal ideal ring.*

PROOF. By Theorem 1.4.2 and the Chinese remainer theorem we find

$$R/I \cong \prod_{\mathfrak{p} \in \mathrm{MaxSpec}(R) : \mathrm{ord}_{\mathfrak{p}}(I) > 0} R/\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(I)}.$$

Notice that by exactness of localization we have $R/\mathfrak{p}^m = R_{\mathfrak{p}}/\mathfrak{p}^m R_{\mathfrak{p}}$. As $R_{\mathfrak{p}}$ is a discrete valuation ring (Theorem 1.4.2), it follows that R/I is isomorphic to a finite product of zero-dimensional principal ideal rings. This shows that R/I is a zero-dimensional principal ideal ring. □

Lemma 4.1.2. *Let R be a Dedekind domain and let $I \subset R$ be a nonzero ideal. Then I^{-1}/R is a free rank one R/I-module.*

PROOF. Take a nonzero $x \in R$ such that $xI^{-1} \subseteq R$. Then notice that $R/(x)$ is a principal ideal ring (Lemma 4.1.1, if $I = R$, it is still a principal ideal ring), and hence $xI^{-1} = aR + xR$ for some $a \in R$. Hence we obtain a surjective R-linear map $\psi : R \to I^{-1}/R$ with $\psi(1) = \frac{a}{x}$ which has kernel I. □

Lemma 4.1.3. *Let A be an order over a Dedekind domain R. Let $I = \mathrm{Ann}_R(A^\dagger/A)$. Then the trace map induces a non-degenerate symmetric R/I-bilinear form as follows:*

$$\begin{aligned} \langle\ ,\ \rangle : A^\dagger/A \times A^\dagger/A &\to I^{-1}/R \\ ([x],[y]) &\mapsto \mathrm{Tr}_{Q(A)/Q(R)}(xy) + R. \end{aligned}$$

PROOF. First remark that $I \neq 0$ as $A^\dagger/A$ is a finitely generated torsion module (Lemma 1.4.15).

Notice that the map is well defined, since for $x \in A$ we have $\mathrm{Tr}_{Q(A)/Q(R)}(xA^\dagger) \subseteq R$ by definition and as $IA^\dagger \subseteq A$, it follows that we land in I^{-1}/R.

We only have to check that $\langle\ ,\ \rangle$ is non-degenerate. By Lemma 4.1.2, we have $I^{-1}/R \cong R/I$ as R-modules. First notice that $A^\dagger/A \cong \mathrm{Hom}_{R/I}(A^\dagger/A, R/I)$ as R/I-modules (use Theorem 1.4.6 and then some calculation). Hence we need to show that the induced map

$$\begin{aligned} \varphi : A^\dagger/A &\to \mathrm{Hom}_{R/I}(A^\dagger/A, I^{-1}/R) \\ x &\mapsto \langle x, \cdot \rangle \end{aligned}$$

is an isomorphism. It follows from Lemma 1.4.16 that this map is injective ($A^{\dagger\dagger} = A$), and as both lengths as R/I-modules are equal, we have an isomorphism. □

Let A be an order over a Dedekind domain R. Recall that $A^\dagger/A \cong \bigoplus_{i=1}^m R/\mathfrak{p}_i^{n_i}$ for some $m \in \mathbf{Z}_{\geq 0}$, $n_i \in \mathbf{Z}_{\geq 1}$ and $\mathfrak{p}_i \in \mathrm{MaxSpec}(R)$ (Theorem 1.4.6). From Remark 1.4.7 we know what happens when we localize at a prime $\mathfrak{p}$, we only keep the terms where $\mathfrak{p}_i = \mathfrak{p}$. One can also see that

$$\left(A^\dagger/A\right)_\mathfrak{p} = \left(A^\dagger/A\right)[\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathrm{Ann}_R(A^\dagger/A))}].$$

Also remark that we have by natural maps

$$\begin{aligned}\left(I^{-1}/R\right)_\mathfrak{p} &\cong \mathfrak{p}^{-\mathrm{ord}_\mathfrak{p}(I)}R_\mathfrak{p}/R_\mathfrak{p} \\ &\cong \mathfrak{p}^{-\mathrm{ord}_\mathfrak{p}(I)}/R.\end{aligned}$$

Now we can formulate the local version of Lemma 4.1.3 .

Corollary 4.1.4. *Let A be an order over a Dedekind domain R. Let $I = \mathrm{Ann}_R(A^\dagger/A)$. Let $\mathfrak{p} \in \mathrm{MaxSpec}(R)$. Then the map $\langle\ ,\ \rangle$ from Lemma 4.1.3 induces a non-degenerate symmetric $(R/I)_\mathfrak{p}$-bilinear form as follows:*

$$\begin{aligned}\langle\ ,\ \rangle : \left(A^\dagger/A\right)_\mathfrak{p} \times \left(A^\dagger/A\right)_\mathfrak{p} &\to (I^{-1}/R)_\mathfrak{p} \\ (\frac{[x]}{s}, \frac{[y]}{t}) &\mapsto \frac{\langle x, y\rangle}{st}.\end{aligned}$$

Proof. If $\mathrm{ord}_\mathfrak{p}(I) = 0$, our statement is trivially correct. If $\mathrm{ord}_\mathfrak{p}(I) > 0$, we apply Lemma 4.1.3, Lemma 3.1.6 (as R/I is an artinian ring) and Theorem 1.1.7. □

2. Anisotropic spaces and the integral closure

In this section we will combine Theorem 2.3.1 and the theory of uniserial rings (and anisotropy).

Lemma 4.2.1. *Let A be an order over a Dedekind domain R and let $\mathfrak{p} \in \mathrm{MaxSpec}(R)$. Suppose that $\overline{A}$ is tame at $\mathfrak{p}$. Then $B = \left(\overline{A}/A\right)_\mathfrak{p} \subseteq \left(A^\dagger/A\right)_\mathfrak{p}$ satisfies $\mathfrak{p}B^\perp \subseteq B \subseteq B^\perp$ (using the form from Corollary 4.1.4).*

Proof. A simple calculation shows that $B^\perp = \left(\overline{A}^\dagger/A\right)_\mathfrak{p}$. As $\overline{A} \subseteq A^\dagger$ by Lemma 1.4.15 we have $B \subseteq B^\perp$. The tameness assumption implies by Theorem 2.3.1 that $\mathfrak{p}\left(\overline{A}^\dagger/A\right)_\mathfrak{p} \subseteq \left(\overline{A}/A\right)_\mathfrak{p}$ and hence $\mathfrak{p}B^\perp \subseteq B$. □

This lemma has some nice consequences.

Theorem 4.2.2. *Let A be an order over a Dedekind domain R and let $\mathfrak{p} \in \mathrm{MaxSpec}(R)$. Suppose that $\overline{A}$ is tame at $\mathfrak{p}$. Let $B = \left(A^\dagger/A\right)_\mathfrak{p}$. Consider the form $\langle\ ,\ \rangle$ from Corollary 4.1.4. Let $D \subset Q(A)$ such that $D/A = \mathrm{rr}(B)$. Then the following statements hold.*

i. *We have $\mathrm{rr}(B) = D/A \subseteq A[D]/A \subseteq \left(\overline{A}/A\right)_\mathfrak{p}$.*
ii. *Suppose that $\langle\ ,\ \rangle$ is anisotropic. Then $\left(\overline{A}/A\right)_\mathfrak{p} = \mathrm{lr}(B)$.*
iii. *Suppose that $\mathrm{rr}(B)$ satisfies $\mathfrak{p}\cdot\mathrm{rr}(B)^\perp \subseteq \mathrm{rr}(B)$. Assume that $A[D]$ is tame at $\mathfrak{p}$. Then $\left(\overline{A}/A\right)_\mathfrak{p} = A[D]/A$.*

PROOF. i. We have $\mathrm{rr}(B) = D/A \subseteq \left(\overline{A}/A\right)_{\mathfrak{p}}$ by Lemma 4.2.1. As $\overline{A}$ is a ring, it follows that $A[D] \subseteq \overline{A}$. Notice that $A[D]/A \subseteq \left(\overline{A}/A\right)_{\mathfrak{p}}$ and the result follows.
ii. We directly obtain the result by definition of anisotropy and Lemma 4.2.1.
iii. We know that $A[D]/A \subseteq \left(\overline{A}/A\right)_{\mathfrak{p}}$ by i. Notice that

$$\mathrm{rr}(B) \subseteq A[D]/A \subseteq (A[D]/A)^{\perp} \subseteq \mathrm{rr}(B)^{\perp}.$$

Hence $\mathfrak{p}\,(A[D]/A)^{\perp} \subseteq A[D]/A$. As $A[D]$ is an order which is tame at $\mathfrak{p}$, we can apply Theorem 2.3.1 to see that $\left(\overline{A}/A\right)_{\mathfrak{p}} = A[D]/A$. □

This theorem motivates us to 'find' $\mathrm{rr}(B)$ and to give easy descriptions of anisotropy. When can we can apply iii? Is the D above always a ring? These questions will be (partially) answered in later chapters.

Combining the above theorem for all primes, we obtain the following result.

Theorem 4.2.3. *Let A be an order over a Dedekind domain R. Let $\mathrm{Ann}_R(A^{\dagger}/A) = I$. Suppose that $\overline{A}$ is tame at all nonzero primes of R. Suppose that $\langle\ ,\ \rangle : A^{\dagger}/A \times A^{\dagger}/A \to I^{-1}/R$ is anisotropic. Then $\overline{A}/A = \mathrm{lr}(A^{\dagger}/A)$.*

PROOF. Notice that $\overline{A}/A$ is a module of finite length over R/I. Theorem 2.13 from [**3**], Theorem 4.2.2 and Remark 3.5.2 now give

$$\begin{aligned} \overline{A}/A &= \bigoplus_{\mathfrak{p}\in \mathrm{spec}(R/I)} (\overline{A}/A)_{\mathfrak{p}} \\ &= \bigoplus_{\mathfrak{p}\in \mathrm{spec}(R/I)} \mathrm{lr}((A^{\dagger}/A)_{\mathfrak{p}}) \\ &= \mathrm{lr}(A^{\dagger}/A). \end{aligned}$$

□

Remark that from Lemma 2.4.1 we see that tameness is guaranteed for primes not dividing I in the above theorem. Actually, a stronger statement holds. Suppose that $\mathfrak{p} \nmid I$ for $\mathfrak{p} \in \mathrm{Spec}(R)$. We claim that $A/\mathfrak{p} \supseteq R/\mathfrak{p}R$ is étale. Indeed, one sees that $A_{\mathfrak{p}}^{\dagger} = A_{\mathfrak{p}}$. Hence $\mathrm{Tr} : A_{\mathfrak{p}} \times A_{\mathfrak{p}} \to R_{\mathfrak{p}}$ is non-degenerate. If we tensor with $R/\mathfrak{p}R$ we see that $A/\mathfrak{p}A \times A/\mathfrak{p}A \to R/\mathfrak{p}R$ is non-degenerate. This means that $A/\mathfrak{p}A \supseteq R/\mathfrak{p}R$ is étale.

CHAPTER 5

Anisotropy

In this chapter we will study anisotropy and give some equivalent definitions of anisotropy.

In this chapter we will fix a uniserial ring R of length n with maximal ideal $\mathfrak{m} = (\pi)$. We also fix a finitely generated R-module M with $\mathrm{Ann}_R(M) = \mathfrak{m}^r$ $(0 \leq r \leq n)$. We finally fix a free R-module N of rank 1. We will use the convention that any ideal of R is written as $\mathfrak{m}^i$ where $0 \leq i \leq n$.

1. Shaving

Definition 5.1.1. Suppose that $r \geq 2$. Then we define

$$\mathrm{Sh}(M) = M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M.$$

We will call this 'technique' *shaving*.

Remark 5.1.2. Assume that $r \geq 2$. Write $M \cong (R/\mathfrak{m}^r)^s \times M'$ where $\mathrm{Ann}_R(M') \supsetneq \mathfrak{m}^r$. Then $\mathrm{Sh}(M) \cong (\mathfrak{m}/\mathfrak{m}^{r-1})^s \times M'$. Also notice that $\mathrm{Ann}_R(\mathrm{Sh}(M)) \supsetneq \mathrm{Ann}_R(M)$. This shaving is often used in an inductive manner.

Remark 5.1.3. Suppose that $r \geq 2$ and let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Then we have $\langle M[\mathfrak{m}^{r-1}], \mathfrak{m}^{r-1}m\rangle = 0$ and hence we obtain a symmetric R-bilinear form $\langle\ ,\ \rangle : \mathrm{Sh}(M) \times \mathrm{Sh}(M) \to N$. We endow $\mathrm{Sh}(M)$ with this form if such a $\langle\ ,\ \rangle$ is given.

Lemma 5.1.4. *Suppose that $r \geq 2$. Let $\varphi : M[\mathfrak{m}^{r-1}] \to \mathrm{Sh}(M)$ be the canonical map. Then:*

$$\begin{aligned} \mathrm{lr}(M) &= \varphi^{-1}\left(\mathrm{lr}(\mathrm{Sh}(M))\right) \\ \mathrm{ur}(M) &= \varphi^{-1}\left(\mathrm{ur}(\mathrm{Sh}(M))\right). \end{aligned}$$

Proof. This is an easy calculation and left to the reader. □

There is a more intuitive way to see that the above lemma is true. The idea is that the lower root and upper root live somewhere in the middle of a module. By shaving, we remove parts of the module in a symmetric way, so it shouldn't change the lower and upper root.

Lemma 5.1.5. *Let $r \geq 2$ and let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Then we have natural isomorphisms for $i \geq 1$ which respect the inner products given by Definition 3.4.14*

$$\rho_i(\mathrm{Sh}(M)) \cong \begin{cases} 0 & i \geq r \\ \rho_{r-2}(M) \perp \rho_r(M) & i = r-2 \\ \rho_i(M) & i = r-1, i < r-2 \end{cases}$$

PROOF. For the proof, one chooses a decomposition of M into homogeneous modules. Then use Remark 5.1.2 and Lemma 3.4.13. □

Lemma 5.1.6. *Suppose that $r \geq 2$. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Then we have an induced symmetric bilinear form $\langle\ ,\ \rangle' : \mathrm{Sh}(M) \times \mathrm{Sh}(M) \to N$. If $\langle\ ,\ \rangle$ is non-degenerate, then so is $\langle\ ,\ \rangle'$. The converse holds if $r \geq 3$.*

PROOF. The first result follows since $\langle M[\mathfrak{m}^{r-1}], \mathfrak{m}^{r-1}M\rangle = 0$. If $\langle\ ,\ \rangle$ is non-degenerate, then apply Lemma 3.4.7 (and Theorem 3.4.1) to see that $\langle\ ,\ \rangle'$ is non-degenerate. Now suppose that $\langle\ ,\ \rangle'$ is non-degenerate and $r \geq 3$. We now use Lemma 5.1.5, Lemma 3.4.13 and Theorem 3.4.17 (here we need that $r - 2 \geq 1$, otherwise we lose information). □

2. Shaving and the radical root

In this section we fix a non-degenerate symmetric R-bilinear form $\langle\ ,\ \rangle : M \times M \to N$. Assume that $r \geq 2$.

Lemma 5.2.1. *Let $\varphi : M[\mathfrak{m}^{r-1}] \to M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M$ be the natural map. Let*

$$\begin{aligned} \mathfrak{S}_1 &= \{L \subseteq M : \mathfrak{m}L^\perp \subseteq L \subseteq L^\perp, L \subseteq M[\mathfrak{m}^{r-1}]\} \\ \mathfrak{S}_2 &= \{L' \subseteq \mathrm{Sh}(M) : \mathfrak{m}L'^\perp \subseteq L' \subseteq L'^\perp\} \end{aligned}$$

Then we have the following surjection

$$\begin{aligned} \psi : \mathfrak{S}_1 &\to \mathfrak{S}_2 \\ L &\mapsto \varphi(L). \end{aligned}$$

If we restrict the domain to the set of all $L \subset M$ which also satisfy $\mathfrak{m}^{r-1}M \subseteq L$, then the map is a bijection.

PROOF. To see that the map is well defined, we need to show that if $L \in \mathfrak{S}_1$, then $L' = L + \mathfrak{m}^{r-1}M$ satisfies $\mathfrak{m}L'^\perp \subseteq L' \subseteq L'^\perp$. This is an easy calculation. Now suppose that $L' \subseteq \mathrm{Sh}(M)$ satisfies $\mathfrak{m}L'^\perp \subseteq L' \subseteq L'^\perp$. Then let $L = \varphi^{-1}(L')$ and this L satisfies $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$ (here we use that $L^\perp \subseteq M[\mathfrak{m}^{r-1}]$ by non-degeneracy). Also $\mathfrak{m}^{r-1}M \subseteq L$ and $\varphi(L) = L'$ and hence we find a bijection if we restrict our domain. □

Recall the definition of the radical root in this case (we suppress the form $\langle\ ,\ \rangle$ in the definition).

Definition 5.2.2. We define the *radical root* of M as

$$\mathrm{rr}(M) = \bigcap_{L \subseteq M : \mathfrak{m}L^\perp \subseteq L \subseteq L^\perp} L.$$

Corollary 5.2.3. *Let $\varphi : M[\mathfrak{m}^{r-1}] \to M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M$ be the natural map. We have $\mathrm{rr}(M) + \mathfrak{m}^{r-1}M \subseteq \varphi^{-1}(\mathrm{rr}(\mathrm{Sh}(M)))$. If furthermore $\mathfrak{m}^{r-1}M \subseteq \mathrm{rr}(M)$, then $\mathrm{rr}(M) = \varphi^{-1}(\mathrm{rr}(\mathrm{Sh}(M)))$.*

PROOF. $\subseteq$: Let $x \in \mathrm{rr}(M)$ and $y \in \mathfrak{m}^{r-1}M$. Now consider $\varphi(x + y)$. By Lemma 5.2.1 we see that $\varphi(x + y) = \varphi(x) \in \mathrm{rr}(\mathrm{Sh}(M))$.

$\supseteq$ if $\mathfrak{m}^{r-1}M \subseteq \mathrm{rr}(M)$: In Lemma 5.2.1 we now have a bijection. If $\varphi(x) \in \mathrm{rr}(\mathrm{Sh}(M))$, then $x \in \mathrm{rr}(M)$. □

3. Equivalent definitions of anisotropy

In this section we fix a symmetric R-bilinear form $\langle\ ,\ \rangle : M \times M \to N$. Recall the definition of anisotropy.

Definition 5.3.1. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Then $\langle\ ,\ \rangle$ is called *anisotropic* if it is non-degenerate and $\mathrm{lr}(M)$ is the unique submodule $L \subseteq M$ satisfying $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$. If $\langle\ ,\ \rangle$ is not anisotropic, it is called *isotropic*.

Remark 5.3.2. Let k be a field. Let V be a finite dimensional k-vector space and let W be a k-vector space of dimension 1. Let $\langle\ ,\ \rangle : V \times V \to W$ be a symmetric k-bilinear form. Then $\langle\ ,\ \rangle$ is called anisotropic if there is no nonzero vector $x \in V$ with $\langle x, x\rangle = 0$. Notice that an anisotropic space is automatically non-degenerate. There is a unique submodule L satisfying $L \subseteq L^\perp$, namely 0. As $\mathrm{lr}(V) = 0$ it follows that the form is anisotropic with our new definition. On the other hand, suppose that $\langle\ ,\ \rangle$ is anisotropic according to our new definition. As we have $\mathrm{lr}(V) = 0$, it follows that there are no nonzero vectors x with $\langle x, x\rangle = 0$ (consider $L = kx$ for such a vector, then $0 \cdot L \subseteq L \subseteq L^\perp$), hence the space is anisotropic.

We see that both definitions are equivalent in the vector space case.

We want to be able to check if a space is anisotropic by reducing it to the vector space case. We can do this by considering the forms $\langle\ ,\ \rangle_{\mathrm{even}}$ and $\langle\ ,\ \rangle_{\mathrm{odd}}$ of vector spaces. We will first prove some lemmas.

Lemma 5.3.3. *Let $L \subseteq M$ with $L \subseteq L^\perp$. Then any maximal submodule $L' \supseteq L$ with $L' \subseteq L'^\perp$ satisfies $\mathfrak{m}L'^\perp \subseteq L'$.*

Proof. Let L' be such a maximal submodule (which exists since our module is noetherian) and consider the obtained form $\langle\ ,\ \rangle : L'^\perp/L' \times L'^\perp/L' \to N$. If $\mathfrak{m}(L'^\perp/L') \neq 0$, then by Lemma 3.4.6 we can lift the non-trivial lower root to obtain a module $L' \subsetneq L''$ with $L'' \subset L''^\perp$, a contradiction.

There is another proof of this lemma which directly produces such a maximal submodule containing L with the above properties. As $L \subseteq L^\perp$, we have $L^{\perp\perp} \subseteq L^\perp$. Then notice that we obtain a form $L^\perp/L^{\perp\perp} \times L^\perp/L^{\perp\perp} \to N$. Let $L'/L^{\perp\perp} = \mathrm{lr}(L^\perp/L^{\perp\perp})$. We claim that we can take L'. We have

$$L \subseteq L^{\perp\perp} \subseteq L'.$$

Also, $L'^\perp \subset L^\perp$ and by Lemma 3.4.6 we see that L' satisfies $\mathfrak{m}L'^\perp \subseteq L' \subseteq L'^\perp$. □

Lemma 5.3.4. *Let $M' \subseteq M$ be a submodule and let $\mathrm{Ann}_R(M') \supseteq \mathfrak{m}^s$ (where $0 \leq s \leq n$). Let $x_1, \ldots, x_t$ generate M' as R-module and suppose that the matrix $(\langle x_i, x_j\rangle)_{i,j=1}^t$ gives a non-degenerate symmetric bilinear form on $(R/\mathfrak{m}^s)^t$. Then we have an isomorphism $\varphi : (R/\mathfrak{m}^s)^t \to M'$ which maps the i-th standard basis vector to x_i.*

Proof. Let $M'' = (R/\mathfrak{m}^s)^t$. Define a map φ as in the statement which is surjective by definition. Let $\langle\ ,\ \rangle'$ be the non-degenerate symmetric bilinear form on M''. By definition we have for $x, y \in M''$ that $\langle x, y\rangle' = \langle \varphi(x), \varphi(y)\rangle$. Suppose that $\varphi(x) = 0$ for some $x \in M''$. But then $\langle \varphi(x), M'\rangle = 0$ and hence $\langle x, M''\rangle' = 0$. As $\langle\ ,\ \rangle'$ is non-degenerate, we conclude that $x = 0$ and our map is injective. □

Lemma 5.3.5. *Assume that $\langle\ ,\ \rangle : M \times M \to N$ is non-degenerate. Suppose that $\mathrm{Ann}_R(M) = \mathfrak{m}^2$ and suppose that there exists $x \in M \setminus M[\mathfrak{m}]$ with $\pi\langle x, x\rangle = 0$. Then $\langle\ ,\ \rangle$ is isotropic.*

PROOF. We assume that $N = R$. We obtain a non-degenerate symmetric bilinear form $M/M[\mathfrak{m}] \times M/M[\mathfrak{m}] \to R/R[\mathfrak{m}]$ and hence there is $y \in M \setminus M[\mathfrak{m}]$ such that $\pi\langle x, y\rangle \neq 0$. Now consider $H = Rx + Ry$. We first claim that $H \cong R/\mathfrak{m}^2 \oplus R/\mathfrak{m}^2$. Notice that $\mathfrak{m}^2 H = 0$ and consider the following matrix:

$$\begin{pmatrix} \langle x, x\rangle & \langle x, y\rangle \\ \langle y, x\rangle & \langle y, y\rangle \end{pmatrix} = \begin{pmatrix} \pi^{n-2} \cdot \pi r_1 & \pi^{n-2} \cdot r_2 \\ \pi^{n-2} \cdot r_2 & \pi^{n-2} \cdot r_3 \end{pmatrix}$$

where $r_1, r_3 \in R$, $r_2 \in R^*$. Apply the determinant criterion (Theorem 3.4.5) to see that the matrix would give a non-degenerate symmetric bilinear form on $(R/\mathfrak{m}^2)^2$. By Lemma 5.3.4 we see that $H \cong \left(R/\mathfrak{m}^2\right)^2$. Write $M = H \perp H^\perp$ (Theorem 1.1.8). Let $L = R\pi x + \pi H^\perp$. Notice that $L \subseteq L^\perp$. We have that $L^\perp = (R\pi x)^\perp \cap (\pi H^\perp)^\perp \subseteq (R\pi x)^\perp$. We will show that $\mathfrak{m}(R\pi x)^\perp \subseteq L$. Let $z \in (R\pi x)^\perp$. Write $z = z_1 + z_2$ where $z_1 \in H$, $z_2 \in H^\perp$. Then $\pi z_2 \in \pi H^\perp \subseteq L$. We will now show that $\pi z_1 \in R\pi x$. We see that $0 = \langle z_1 + z_2, \pi x\rangle = \langle z_1, \pi x\rangle$. Write $z_1 = r_4 x + r_5 y$ where $r_4, r_5 \in R$. Notice that $0 = \langle z_1, \pi x\rangle = \langle r_4 x + r_5 y, \pi x\rangle = \langle r_5 y, \pi x\rangle$. Hence $r_5 \in (\pi)$ and $\pi z_1 = r_4 \pi x \in R\pi x$. This shows that $\mathfrak{m}L^\perp \subseteq L$.

Finally notice that $\pi y \in \mathrm{lr}(M)$, but $\pi y \notin L$. Indeed, $\langle \pi y, x\rangle \neq 0$, but $x \in L^\perp$. Hence $\mathrm{lr}(M) \neq L$ and our space is isotropic. □

Lemma 5.3.6. *Assume that $\langle\ ,\ \rangle : M \times M \to R$ is non-degenerate. Suppose that $\mathrm{Ann}_R(M) = \mathfrak{m}^r$ where $r \geq 2$. Suppose that $\rho_r(M)$ is anisotropic. Then $\mathfrak{m}^{r-1}M \subseteq \mathrm{rr}(M)$.*

PROOF. Take $L \subseteq M$ with $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$. Suppose $\mathfrak{m}^{r-1}M \not\subseteq L$. Then $L^\perp \not\subseteq M[\mathfrak{m}^{r-1}]$ (by Theorem 3.4.1). Let $x \in L^\perp \setminus M[\mathfrak{m}^{r-1}]$.

First suppose that r is odd. Then take $y = \pi^{\lfloor \frac{r}{2} \rfloor} x$. Then $0 \neq [y] \in \rho_r(M)$. As $\langle x, \pi x\rangle = 0$ (since $\pi x \in L$), it follows that $\langle y, y\rangle = 0$, as $r \geq 2$. This shows that $\rho_r(M)$ is isotropic, a contradiction.

Now suppose that r is even and consider $y = \pi^{\lfloor \frac{r-1}{2} \rfloor} x$ and we find that $\pi\langle y, y\rangle = 0$. Hence $\rho_r(M)$ is isotropic, a contradiction. □

Lemma 5.3.7. *Assume that $\mathrm{char}(R/\mathfrak{m}) \neq 2$. Let $x, y \in M$ such that $(\langle x, x\rangle) = \mathfrak{m}^i$, $(\langle x, y\rangle) = \mathfrak{m}^j$ and $(\langle y, y\rangle) = \mathfrak{m}^k$ where $i + k > 2j$ and $i \geq j$. Then we can find $c \in \mathfrak{m}^{i-j}$ such that the element $z = x + cy$ satisfies $\langle z, z\rangle = 0$ and $(\langle y, z\rangle) = \mathfrak{m}^j$.*

PROOF. For the proof we assume that $N = R$. Let $\langle x, x\rangle = \pi^i r_1$ and let $\langle x, y\rangle = \pi^j r_2$ where $r_1, r_2 \in R^*$. Now let $c = \frac{-\pi^{i-j} r_1}{2r_2}$ and let $z' = x + cy$. We calculate:

$$\begin{aligned} \langle z', z'\rangle &= \langle x + cy, x + cy\rangle \\ &= \langle x, x\rangle + 2c\langle x, y\rangle + c^2\langle y, y\rangle \\ &= \pi^i r_1 + 2\frac{-\pi^{i-j} r_1}{2r_2}\pi^j r_2 + c^2\langle y, y\rangle \\ &= c^2\langle y, y\rangle \end{aligned}$$

Notice that $(c^2\langle y, y\rangle) = \mathfrak{m}^l$ where $l = 2(i-j) + k > i$. We also have:

$$\begin{aligned} (\langle y, z'\rangle) &= (\langle y, x + cy\rangle) \\ &= (\langle x, y\rangle) + (c\langle y, y\rangle) \\ &= \mathfrak{m}^j \end{aligned}$$

(as $i - j + k > j$ by assumption). Now we can continue with z' and y since $l+k > i+k > 2j$ and $l > j$. As $\mathfrak{m}$ is nilpotent we obtain the result by induction. □

Lemma 5.3.8. *Assume that $\langle\ ,\ \rangle : M \times M \to R$ is non-degenerate. Let $x \in M$ with $\mathrm{Ann}_R(x) = \mathfrak{m}^s$. Then for every $r \in \mathfrak{m}^{n-s}$ there is $y \in M$ with $\langle x, y\rangle = r$.*

Proof. First consider the map

$$\begin{array}{rcl} \varphi : Rx & \to & \mathfrak{m}^{n-s} \subseteq R \\ x & \mapsto & r \end{array}$$

which is defined by assumption. As R is an injective R-module (Corollary 3.3.4), we can extend φ to a map $\psi' : M \to R$. Since $\langle\ ,\ \rangle$ is non-degenerate, we see that there is $y \in M$ with $\psi'(z) = \langle z, y\rangle$ for all $z \in M$. Hence we have $r = \psi'(x) = \langle x, y\rangle$. □

Lemma 5.3.9. *Assume that $\langle\ ,\ \rangle$ is anisotropic. Suppose $L \subseteq M$ satisfies $L \subseteq L^\perp$. Then the natural form $L^\perp/L \times L^\perp/L \to R$ is anisotropic, $L \subseteq \mathrm{lr}(M)$ and $\mathrm{lr}(M)/L = \mathrm{lr}(L^\perp/L)$.*

Proof. There is a natural bijection between the set $\mathfrak{S}_1$ of $L''/L \subseteq L^\perp/L$ satisfying $\mathfrak{m}\,(L''/L)^\perp \subseteq L''/L \subseteq (L''/L)^\perp$ and the set $\mathfrak{S}_2$ of $L'' \subseteq M$ satisfying $L \subseteq L''$ and $\mathfrak{m}L''^\perp \subseteq L'' \subseteq L''^\perp$. Notice that $\#\mathfrak{S}_1 = \#\mathfrak{S}_2 \geq 1$ (they contain the 'lower root') and the last set has size at most 1 by anisotropy. We conclude that both sets have size 1 and contain only their lower roots. This means that $L^\perp/L$ is anisotropic. This also shows that $L \subseteq \mathrm{lr}(M)$ and it gives $\mathrm{lr}(M)/L = \mathrm{lr}(L^\perp/L)$. □

Finally we can state and prove the main theorem of this section.

Theorem 5.3.10. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Consider the following statements:*

i. *$\langle\ ,\ \rangle$ is anisotropic;*
ii. *both $\langle\ ,\ \rangle_{\mathrm{even}}$ and $\langle\ ,\ \rangle_{\mathrm{odd}}$ are anisotropic;*
iii. *the form $\langle\ \rangle$ is non-degenerate and for any submodule $L \subseteq M$ with $L \subseteq L^\perp$, we have $L \subseteq \mathrm{lr}(M)$ and $\mathrm{lr}(L^\perp/L) = \mathrm{lr}(M)/L$;*
iv. *the form $\langle\ ,\ \rangle$ is non-degenerate and for any submodule $L \subseteq M$ with $L \subseteq L^\perp$, we have $L \subseteq \mathrm{lr}(M)$;*
v. *the form $\langle\ ,\ \rangle$ is non-degenerate and if $x \in M$ satisfies $\langle x, x\rangle = 0$, then $x \in \mathrm{lr}(M)$.*

Then i $\iff$ ii $\iff$ iii $\implies$ iv $\iff$ v. *If $\mathrm{char}(R/\mathfrak{m}) \neq 2$, then all statements are equivalent.*

Proof. i $\implies$ ii: We will show that not ii implies not i. Suppose that ii doesn't hold. If $\langle\ ,\ \rangle_{\mathrm{odd}}$ is isotropic, then we find $x \notin \mathrm{lr}(M)$ with $\langle x, x\rangle = 0$. Apply Lemma 5.3.3 on $L = Rx$ to find a contradiction with i.

Now suppose that $\langle\ ,\ \rangle_{\mathrm{even}}$ is isotropic. We will show by induction on r that we can find $L \subseteq M$ with $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$, but $L \neq \mathrm{lr}(M)$, hence contradicting anisotropy.

If $\mathrm{Ann}_R(M) = \mathfrak{m}^r$ where $r = 0, 1$, then $M/M[\mathfrak{m}] = 0$ and hence $\langle\ ,\ \rangle_{\mathrm{even}}$ is not isotropic.

Suppose $r = 2$. Then we apply Lemma 5.3.5 to see that M is isotropic.

We now continue with induction. Suppose that $\mathrm{Ann}_R(M) = \mathfrak{m}^r$ where $r \geq 3$. Suppose that x is an isotropic element $\langle\ ,\ \rangle_{\mathrm{even}}$. Then x gives an isotropic element in $\mathrm{Sh}(M)_{\mathrm{even}}$ (Lemma 5.1.5, Lemma 3.4.13 and Definition 3.4.14). As

$\mathrm{Sh}(M)$ has smaller exponent, we apply our induction hypothesis and we find an $L' \subseteq \mathrm{Sh}(M) = M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M$ with $\mathfrak{m}L'^{\perp} \subseteq L' \subseteq L'^{\perp}$ and $L' \neq \mathrm{lr}(\mathrm{Sh}(M))$. Let $\varphi : M[\mathfrak{m}^{r-1}] \to \mathrm{Sh}(M)$ be the canonical map, and let $L = \varphi^{-1}(L')$. We see that $\mathfrak{m}L^{\perp} \subseteq L \subseteq L^{\perp}$ and $L \neq \mathrm{lr}(M)$. This contradicts i.

ii $\implies$ i: We will give a proof by induction on $\mathrm{Ann}_R(M) = \mathfrak{m}^r$. If $r = 0$ the statement follows directly. If $r = 1$ we have $\langle\ ,\ \rangle = \langle\ ,\ \rangle_{\mathrm{odd}}$ which is anisotropic (Remark 5.3.2). Now continue with induction and suppose that $r \geq 2$. By Lemma 5.3.6 it follows that for $L \subseteq M$ with $\mathfrak{m}L^{\perp} \subseteq L \subseteq L^{\perp}$ we have $\mathfrak{m}^{r-1}M \subseteq L$. Let $\varphi : M[\mathfrak{m}^{r-1}] \to \mathrm{Sh}(M)$ be the natural map. Now use Lemma 5.2.1 and the induction hypothesis on $\mathrm{Sh}(M)$ (use Lemma 5.1.5, Lemma 3.4.13 and Definition 3.4.14 to see that ii still holds) to conclude that $L = \varphi^{-1}(\mathrm{lr}(\mathrm{Sh}(M))) = \mathrm{lr}(M)$ (Lemma 5.1.4).

i $\implies$ iii: This is Lemma 5.3.9.

iii $\implies$ i: Suppose that $L \subseteq M$ satisfies $\mathfrak{m}L^{\perp} \subseteq L \subseteq L^{\perp}$. Then iii gives $L \subseteq \mathrm{lr}(M)$ and $\mathrm{lr}(M)/L = \mathrm{lr}(L^{\perp}/L) = L/L$ (as $\mathfrak{m}(L^{\perp}/L) = 0$). It follows that $\mathrm{lr}(M) = L$ and we are done.

iii $\implies$ iv: Obvious.

iv $\iff$ v: This is obvious.

v $\implies$ i if $\mathrm{char}(R/\mathfrak{m}) \neq 2$: We will assume that $N = R$. We will give a proof by induction on the exponent of M using shaving. Assume that $\mathfrak{m}L^{\perp} \subseteq L \subseteq L^{\perp}$. By v we know that $L \subseteq \mathrm{lr}(M)$. We need to prove $L = \mathrm{lr}(M)$.

If $\mathrm{Ann}_R(M) = \mathfrak{m}^r$ where $r = 0, 1$ we see that $L \subseteq \mathrm{lr}(M) = 0$ and we are done.

Now suppose that $\mathrm{Ann}_R(M) = \mathfrak{m}^r$ where $r \geq 2$. As $L \subseteq \mathrm{lr}(M)$ it follows that $\mathrm{Ann}_R(L) = \mathfrak{m}^i$ where $i \leq \lfloor \frac{r}{2} \rfloor < r$. Let $\varphi : M[\mathfrak{m}^{r-1}] \to \mathrm{Sh}(M)$ and consider $L' = \varphi(L)$ which by our induction hypothesis (and Lemma 5.2.1) satisfies $L' = \mathrm{lr}(\mathrm{Sh}(M))$. By Lemma 5.1.4 we conclude that $L + \mathfrak{m}^{r-1}M = \mathrm{lr}(M)$. Hence it is enough to prove that $\mathfrak{m}^{r-1}M \subseteq L$, or equivalently, $L^{\perp} \subseteq M[\mathfrak{m}^{r-1}]$. Let $x \in L^{\perp}$, but $x \notin M[\mathfrak{m}^{r-1}]$. By assumption we know $\pi x \in L$ and hence $0 = \langle x, \pi x\rangle = \pi\langle x, x\rangle$, that is, $\langle x, x\rangle \in R[\mathfrak{m}]$. Write $\langle x, x\rangle = \pi^{n-1}r$ for some $r \in R$. By Lemma 5.3.8 we can find $y \in M$ with $\langle x, y\rangle = \pi^{n-r}$. We can now apply Lemma 5.3.7 (here $i \geq n-1$, $j = n - r$ and $k \geq n - r$, we use that $r > 1$ here) and we see that there is $c \in \mathfrak{m}^{r-1}$ such that $\langle x + cy, x + cy\rangle = 0$. By our assumption in v, $z = x + cy \in \mathrm{lr}(M) \subseteq M[\mathfrak{m}^{r-1}]$. Notice that $\pi cy = 0$, and as $r \geq 2$ we find $cy \in M[\mathfrak{m}^{r-1}]$. Hence we find $x = z - cy \in M[\mathfrak{m}^{r-1}]$ as required. This shows that $\mathrm{lr}(M) = L$ and hence we are done.

□

Example 5.3.11. In this example we will show that v $\implies$ i is in general false.

Let $R = \mathbf{Z}/2^2\mathbf{Z}$. Consider the non-degenerate bilinear form $\langle\ ,\ \rangle$ on $M = \mathbf{Z}/2^2\mathbf{Z} \times \mathbf{Z}/2^2\mathbf{Z}$ given by the following matrix:

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

We first check that v is satisfied. Notice that $\langle (x, y), (x, y)\rangle = 2(x^2 + y^2 + xy)$ for $x, y \in \mathbf{Z}/2^2\mathbf{Z}$. If this is zero, $2 \mid x^2 + y^2 + xy$, and this happens iff both x and y are divisible by 2, that is, if $(x, y) \in \mathrm{lr}(\mathbf{Z}/2^2\mathbf{Z} \times \mathbf{Z}/2^2\mathbf{Z})$.

We claim that i is not satisfied. Let $L = \langle (2, 0)\rangle = 2\mathbf{Z}/2^2\mathbf{Z} \times \{0\}$. A trivial calculation shows that $L^{\perp} = \mathbf{Z}/2^2\mathbf{Z} \times 2\mathbf{Z}/2^2\mathbf{Z}$. Notice that $2L^{\perp} = L$ and $L \subseteq L^{\perp}$. But in this case $\mathrm{lr}(\mathbf{Z}/2^2\mathbf{Z} \times \mathbf{Z}/2^2\mathbf{Z}) = 2\mathbf{Z}/2^2\mathbf{Z} \times 2\mathbf{Z}/2^2\mathbf{Z} \neq 2\mathbf{Z}/2^2\mathbf{Z} \times \{0\}$.

We have the following nice corollary.

Corollary 5.3.12. *Assume that* $\langle\ ,\ \rangle : M \times M \to N$ *is non-degenerate. The following statements hold.*

i. *Suppose that* M *is cyclic. Then* $\langle\ ,\ \rangle$ *is anisotropic.*
ii. *Suppose that* M *is generated by two elements and* $\mathrm{length}_R(M)$ *is odd. Then* $\langle\ ,\ \rangle$ *is anisotropic.*

PROOF. i: This follows from Theorem 5.3.10 since all one-dimensional vector spaces with a non-degenerate form are automatically anisotropic.

ii: This follows from Theorem 5.3.10 since both $\langle\ ,\ \rangle_{\mathrm{odd}}$ and $\langle\ ,\ \rangle_{\mathrm{even}}$ are non-degenerate symmetric bilinear forms on one-dimensional spaces. □

4. Cyclicity

Corollary 5.3.12 has some nice consequences.

Corollary 5.4.1. *Let* R *be a Dedekind domain and* A *an order over* R*. Assume that* $A^\dagger/A$ *is cyclic. Then we have* $\overline{A}/A = \mathrm{lr}(A^\dagger/A)$*.*

PROOF. We apply Theorem 4.2.3, Corollary 5.3.12 and Remark 3.5.9. For this we only need to check that A is tame at certain primes $\mathfrak{p} \subset R$. For this we apply Lemma 2.4.1. If $\mathrm{char}(R/\mathfrak{p}) = 0$, we are automatically done (Lemma 2.4.1). In the other cases, we have $\dim_{R/\mathfrak{p}}\left(\left(A^\dagger/A\right)/\mathfrak{p}\left(A^\dagger/A\right)\right) \leq 1 < \mathrm{char}(R/\mathfrak{p})$. Now apply Lemma 2.4.1. □

Notice that one can also derive local versions of the previous corollary very easily. Unfortunately, we can never apply Lemma 2.4.1 in the case that $\mathrm{char}(R/\mathfrak{p}) = 2$. We will show that $\left(A^\dagger/A\right)_{(\mathfrak{p})}$ is never non-trivially cyclic in that case.

Lemma 5.4.2. *Let* R *be a Dedekind domain and let* A *be an order over* R*. Let* $B = A^\dagger/A$*. Let* $\mathfrak{p} \subset R$ *be prime with* $\mathrm{char}(R/\mathfrak{p}) = 2$*. Then* $\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) \neq 1$*.*

PROOF. Assume that $\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) = 1$. By Lemma 2.4.1 and Lemma 1.3.19 we are in a tame case and we have

$$\begin{aligned} 1 = \dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) &= \dim_{R/\mathfrak{p}}(C^\perp) \\ &= \sum_{\mathfrak{m}\in \mathrm{Spec}(C)} \dim_{R/\mathfrak{p}}(\mathfrak{m}C_{\mathfrak{m}}). \end{aligned}$$

Suppose that $\mathfrak{m}$ is a nonzero prime, with $\dim_{R/\mathfrak{p}}(\mathfrak{m}C_{\mathfrak{m}}) = 1$ (we need such a term). Then $C_{\mathfrak{m}} \supsetneq \mathfrak{m}C_{\mathfrak{m}} \supsetneq 0$ is a composition series for $C_{\mathfrak{m}}$ of length 2, showing that $\mathfrak{m}$ is not tame. Hence we find a contradiction. □

5. Calculating the radical root

In this section we fix a non-degenerate symmetric R-bilinear form $\langle\ ,\ \rangle : M \times M \to N$.

We have the following theorem, of which the proof will be given later in this section.

Theorem 5.5.1. *Assume that* $\mathrm{char}(R/\mathfrak{m}) \neq 2$*. Suppose that* $\rho_r(M)$ *is isotropic. Then* $\mathrm{rr}(M) = 0$*.*

PROOF. We will prove this later in this section (Theorem 5.5.7). □

We will now prove a theorem which gives us $\mathrm{rr}(M)$ if $\mathrm{char}(R/\mathfrak{m}) \neq 2$. It will be a recursive description and if one wants to use it, one needs to be able to test anisotropy for vector spaces over the residue field. In the Appendix, an algorithm is given when $R/\mathfrak{m}$ is a finite field.

Theorem 5.5.2. *Let $\varphi : M[\mathfrak{m}^{r-1}] \to M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M = \mathrm{Sh}(M)$ be the natural map (if $r \geq 1$). Then we have*

$$\mathrm{rr}(M) = \begin{cases} 0 & r \leq 1; \\ 0 & r \geq 2, \rho_r(M) \text{ isotropic and } \mathrm{char}(R/\mathfrak{m}) \neq 2; \\ \varphi^{-1}\left(\mathrm{rr}(\mathrm{Sh}(M))\right) & r \geq 2 \text{ and } \rho_r(M) \text{ anisotropic.} \end{cases}$$

Proof. If $r \leq 1$, then $\mathrm{rr}(M) \subseteq \mathrm{lr}(M) = 0$, hence this proves the first case. The second case is Theorem 5.5.1. If $\rho_r(M)$ is anisotropic, we find by Lemma 5.3.6 and Corollary 5.2.3 that $\mathrm{rr}(M) = \varphi^{-1}(\mathrm{rr}(\mathrm{Sh}(M)))$. This proves the last case. □

Remark 5.5.3. If $\mathrm{char}(R/\mathfrak{m}) = 2$ and we are in the second case of the previous theorem, then it might happen that $\mathrm{rr}(M) \neq 0$. This happens for example in Example 5.5.10. Notice that if one wants to apply the previous theorem, one can determine the ρ_i after shaving by Lemma 5.1.5 (one has to calculate the ρ_i only once).

5.1. The proof. In this subsection we will prove Theorem 5.5.1. It requires some lemmas.

Lemma 5.5.4. *Let k be field with $\mathrm{char}(k) \neq 2$. Let V be a finite dimensional k-vector space and let $\langle\ ,\ \rangle : V \times V \to k$ be a non-degenerate symmetric bilinear form. Assume that V is isotropic. Then $\sum_{x \in k : \langle x,x\rangle = 0} kx = V$. Furthermore, for every nonzero $x \in V$ there exists $y \in V$ with $\langle y, y\rangle = 0$ but $\langle x, y\rangle \neq 0$.*

Proof. Let $W = \sum_{x \in k : \langle x,x\rangle = 0} kx$. Let $x \in V$ such that $\langle x, x\rangle = 0$. Then by non-degeneracy there exists $y' \in V$ with $\langle x, y'\rangle = 1$. Let $y = -\frac{\langle y', y'\rangle}{2}x + y'$. Then notice that $\langle x, x\rangle = 0$, $\langle x, y\rangle = 1$ and $\langle y, y\rangle = 0$. Hence we have found a hyperbolic plane H containing x. Notice that $H \subseteq W$. As H is non-degenerate, we can write $V = H \perp H^{\perp}$. We are done if we can show that $H^{\perp} \subseteq W$. The map

$$\begin{aligned} H &\to k \\ w &\mapsto \langle w, w\rangle \end{aligned}$$

is surjective. Let $v \in H^{\perp}$. There exists $w \in H$ such that $\langle w, w\rangle = -\langle v, v\rangle$. But then $\langle v + w, v + w\rangle = 0$ and $v + w \in W$ and $v \in W$.

Finally let $v \in V$ and suppose that $\langle v, x\rangle = 0$ for all $x \in V$ with $\langle x, x\rangle = 0$. Then $\langle v, W\rangle = \langle v, V\rangle = 0$ and by non-degeneracy we conclude that $v = 0$. □

Lemma 5.5.5. *Assume that $\mathrm{char}(R/\mathfrak{m}) \neq 2$ and that $N = R$. Let M be free over $R/\mathfrak{m}^r$. Suppose that $\rho_r(M)$ is isotropic. Then there are $x, y \in M$ with $\langle x, x\rangle = 0$, $\langle y, y\rangle = 0$ and $\langle x, y\rangle = \pi^{n-r}$. For any $u \in M \setminus \mathfrak{m}M$, there exists $v \in M$ with $(\langle u, v\rangle) = \mathfrak{m}^{n-r}$ and $\langle v, v\rangle = 0$. Furthermore, the map*

$$\begin{aligned} \varphi : M &\to \pi^{n-r} \\ x &\mapsto \langle x, x\rangle \end{aligned}$$

is surjective.

PROOF. By changing our ring to $R/\mathfrak{m}^r$ we may assume $M = R^s$. Then $\langle\ ,\ \rangle$ induces a non-degenerate symmetric bilinear form $\langle\ ,\ \rangle' : M/\mathfrak{m}M \times M/\mathfrak{m}M \to R/\mathfrak{m}$ which is anisotropic (Lemma 3.4.16 and the anisotropy of $\rho_r(M)$). Now let $u \in M\backslash\mathfrak{m}M$. By non-degeneracy and Lemma 5.5.4 there is $v \in M\backslash\mathfrak{m}M$ with $\langle u, v\rangle \in R^*$ and $\langle v, v\rangle \in \mathfrak{m}$. Now use Lemma 5.3.7 (here $i + k \geq 1 > 2j = 0$ and $i \geq j = 0$) and conclude that there exists $y \in M$ such that $\langle y, y\rangle = 0$ and $\langle u, y\rangle \in R^*$. This proves the second statement. Replace u by $\frac{1}{\langle u,y\rangle}u$ to get $\langle y, y\rangle = 0$ and $\langle u, y\rangle = 1$. Let $r = \langle u, u\rangle$ and put $x = u - \frac{r}{2}y$. Then we have

$$\begin{aligned}\langle x, x\rangle &= \langle u, u\rangle - r\langle u, y\rangle + \langle y, y\rangle \\ &= r - r + 0 = 0.\end{aligned}$$

We still have $\langle x, y\rangle = 1$ and this proves the first statement.

For the last statement, let $r' \in R$. Then $\varphi(x + \frac{r'}{2}y) = r'$. □

Lemma 5.5.6. *Assume that* $\mathrm{char}(R/\mathfrak{m}) \neq 2$. *Assume that* $\rho_r(M)$ *is isotropic. Then for every nonzero* $x \in M$ *there is* $y \in M$ *with* $\langle y, y\rangle = 0$ *but* $\langle x, y\rangle \neq 0$.

PROOF. First assume that M is homogeneous. Let $x \in M$ be nonzero. Let i be maximal such that $x \in \mathfrak{m}^i M$ and $x \notin \mathfrak{m}^{i+1}M$, then $i < r$. Write $x = \pi^i x'$ where $x' \in M \setminus \mathfrak{m}M$. Then by Lemma 5.5.5 we can find $y \in M$ with $\langle y, y\rangle = 0$ and $(\langle x', y\rangle) = \mathfrak{m}^{n-r}$. But then $(\langle x, y\rangle) = \mathfrak{m}^{n-r+i} \neq 0$.

Now we will do the general case. Write $M = M_r \perp M'$ where M_r is homogeneous of exponent $\mathfrak{m}^r$ and M' has lower exponent (Corollary 3.4.17). Recall that both M_r and M' are non-degenerate (Theorem 1.1.7). Then let $x \in M$ be nonzero and write $x = x_1 + x_2$ where $x_1 \in M_r$ and $x_2 \in M'$. If $x_1 \neq 0$, then by the homogeneous case there is $y \in M_r$ with $\langle y, y\rangle = 0$ and $\langle x_1, y\rangle \neq 0$. But then $\langle x, y\rangle \neq 0$ as well and we are done. Now assume that $x_1 = 0$. Take $y \in M'$ with $\langle x, y\rangle \neq 0$ (by non-degeneracy). Then let $a = \langle y, y\rangle$. By Lemma 5.5.5 there is $z \in M_r$ with $\langle z, z\rangle = -a$ (this is the essential step where we use that the 'highest part' is isotropic). But then

$$\begin{aligned}\langle y + z, y + z\rangle &= \langle y, y\rangle + 2\langle y, z\rangle + \langle z, z\rangle \\ &= a + 0 - a = 0.\end{aligned}$$

We also have

$$\langle x, y + z\rangle = \langle x, y\rangle \neq 0$$

and hence we are done. □

Theorem 5.5.7. *Assume that* $\mathrm{char}(R/\mathfrak{m}) \neq 2$. *Suppose that* $\rho_r(M)$ *is isotropic. Then* $\mathrm{rr}(M) = 0$.

PROOF. Let $x \in M$ be nonzero. Then there exists $y \in M$ with $\langle y, y\rangle = 0$ and $\langle x, y\rangle \neq 0$ according to Lemma 5.5.6. Then by Lemma 5.3.3 there is a submodule L containing Ry which satisfies $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$. As $\langle x, y\rangle \neq 0$, we conclude that $x \notin L$ and hence $x \notin \mathrm{rr}(M)$. This shows that $\mathrm{rr}(M) = 0$. □

One might wonder how much of these lemmas is true if $\mathrm{char}(R/\mathfrak{m}) = 2$. We will give a few examples below which show that not much is left.

Example 5.5.8. Consider the non-degenerate symmetric bilinear form on $M = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ where $R = \mathbf{Z}/2\mathbf{Z}$ given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

(this form is isomorphic to the form obtained from the identity matrix). Then one can calculate that the vector $(1, 0)$ is perpendicular to all elements $(u, v) \in M$ with $\langle (u, v), (u, v) \rangle = 0$. Indeed, there are just two such elements, $(0, 0)$ and $(1, 0)$ and one easily checks the statement. Hence Lemma 5.5.4 would not be true in this case.

Example 5.5.9. For example consider the non-degenerate symmetric bilinear form on $M = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ where $R = \mathbf{Z}/2\mathbf{Z}$ given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The quadratic form obtained doesn't represent 1, hence Lemma 5.5.5 would be false in this case.

Example 5.5.10. We will now give a counterexample to Theorem 5.5.7 in the case where $\mathrm{char}(R/\mathfrak{m}) = 2$. This example will also contradict Lemma 5.5.6 if we allowed $\mathrm{char}(R/\mathfrak{m}) = 2$. For this consider the non-degenerate symmetric bilinear form on $M = \mathbf{Z}/2^2\mathbf{Z} \times \mathbf{Z}/2^2\mathbf{Z}$ where $R = \mathbf{Z}/2^2\mathbf{Z}$ given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

This form is clearly isotropic. We will show that $\mathrm{rr}(M) \neq 0$. Suppose that $L \subseteq M$ satisfies $\mathfrak{m}L \subseteq L \subseteq L^\perp$. Then $L \cap M[\mathfrak{m}^{r-1}] = L \cap M[\mathfrak{m}] = L \cap \mathrm{lr}(M)$ also satisfies these properties. Hence we need to consider submodules of the lower root. The set of submodules of the lower root is equal to

$$\{0, R(2, 0), R(0, 2), R(2, 2), \mathrm{lr}(M)\}.$$

From these modules only $\mathrm{lr}(M)$ and $R(2, 0)$ satisfy $\mathfrak{m}L \subseteq L^\perp$ and hence $R(2, 0) = \mathrm{rr}(M)$.

CHAPTER 6

Quasi-anisotropy and the integral closure

In this chapter we will study quasi-anisotropy and its applications to the integral closure.

1. Equivalent definitions of quasi-anisotropy

In this section we will fix a uniserial ring R of length n with maximal ideal $\mathfrak{m} = (\pi)$. We also fix a finitely generated R-module M with $\mathrm{Ann}_R(M) = \mathfrak{m}^r$. We finally fix a free R-module N of rank 1. We will use the convention that any ideal of R is written as $\mathfrak{m}^i$ where $0 \leq i \leq n$.

Definition 6.1.1. Let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric R-bilinear form. Then $\langle\ ,\ \rangle$ is called *quasi-anisotropic* if $\langle\ ,\ \rangle$ is non-degenerate and both $\perp_{i \text{ even}} \rho_i(M)$ and $\perp_{i \text{ odd}, i \neq 1} \rho_i(M)$ are anisotropic.

Remark 6.1.2. If $\langle\ ,\ \rangle$ is anisotropic, it is automatically quasi-anisotropic (Theorem 5.3.10)

Corollary 6.1.3. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a non-degenerate symmetric R-bilinear form. Suppose that $\langle\ ,\ \rangle$ is quasi-anisotropic. Then $\mathrm{rr}(M) = \mathrm{lr}(M)$. If $\mathrm{char}(R/\mathfrak{m}) \neq 2$, the converse also holds.*

Proof. $\implies$: We will give a proof by induction. If $r = 0, 1$ it is obvious. Now assume that $r \geq 2$. Let $\varphi : M[\mathfrak{m}^{r-1}] \to M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M = \mathrm{Sh}(M)$ be the natural map. First by Lemma 5.1.5 we see that $\mathrm{Sh}(M)$ is still quasi-anisotropic. Then using Lemma 5.1.4, Theorem 5.5.2 and our induction hypothesis we find

$$\begin{aligned} \mathrm{rr}(M) &= \varphi^{-1}(\mathrm{rr}(\mathrm{Sh}(M))) \\ &= \varphi^{-1}(\mathrm{lr}(\mathrm{Sh}(M))) \\ &= \mathrm{lr}(M). \end{aligned}$$

$\impliedby$ if $\mathrm{char}(R/\mathfrak{m}) \neq 2$: From Theorem 5.5.2 (and Lemma 5.1.4) we have $\mathrm{rr}(M) = \mathrm{lr}(M) \iff r = 0, 1$ or $r \geq 2$, $\rho_r(M)$ is anisotropic and $\mathrm{rr}(\mathrm{Sh}(M)) = \mathrm{lr}(\mathrm{Sh}(M))$. We will now give a proof by induction. If $r = 0, 1$ our form is automatically quasi-anisotropic. If $r = 2$, we conclude that $\rho_2(M)$ is anisotropic and hence our form is quasi-anisotropic. If $r = 3$, we first see that $\rho_3(M)$ is anisotropic and by induction we see that $\mathrm{Sh}(M)$ is quasi-anisotropic. Using Lemma 5.1.5 we see that $\rho_2(M)$ is anisotropic. It follows that our form is quasi-anisotropic. Finally, suppose $r \geq 4$. Then from Lemma 5.1.5 we see that our form is quasi-anisotropic iff $\mathrm{Sh}(M)$ is quasi-anisotropic and by induction we are done.

□

Lemma 6.1.4. *Let $\langle\ ,\ \rangle : M \times M \to N$ be non-degenerate symmetric R-bilinear form. Assume that M is quasi-anisotropic. Let $L \subseteq \mathrm{lr}(M)$ be a submodule. Then we have:*

i. $L \subseteq L^\perp$;
ii. $L^\perp/L$ *is quasi-anisotropic;*
iii. $\mathrm{lr}(L^\perp/L) = \mathrm{lr}(M)/L$.

PROOF. We have $L \subseteq \mathrm{lr}(M) \subseteq \mathrm{ur}(M) \subseteq L^\perp$. Write $M = M_1 \perp M'$ where M_1 is free over $R/\mathfrak{m}$ and $\rho_1(M') = 0$ (Corollary 3.4.17). As $\mathrm{lr}(M_1) = 0$ we can write $L = \{0\} \perp L'$. Then $L^\perp = M_1 \perp L'^\perp$ (where $L'^\perp \subseteq M'$). Notice that by construction M' is anisotropic (Theorem 5.3.10). From Lemma 5.3.9 we see that $L'^\perp/L'$ is anisotropic and $\mathrm{lr}(M')/L' = \mathrm{lr}(L'^\perp/L')$. Hence $L^\perp/L = M_1 \oplus L'^\perp/L'$ is quasi-anisotropic. We then find

$$\begin{aligned} \mathrm{lr}(L^\perp/L) &= \mathrm{lr}(M_1/0) \oplus \mathrm{lr}(L'^\perp/L') \\ &= 0 \oplus \mathrm{lr}(M')/L' \\ &= \mathrm{lr}(M)/L. \end{aligned}$$

□

Theorem 6.1.5. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a non-degenerate symmetric R-bilinear form. Consider the following statements.*

i. *The form $\langle\ ,\ \rangle$ is quasi-anisotropic.*
ii. *The induced form $\langle\ ,\ \rangle' : M/M[\mathfrak{m}] \times M/M[\mathfrak{m}] \to R/R[\mathfrak{m}]$ is anisotropic.*
iii. *For any $L \subseteq \mathrm{lr}(M)$ we have $\mathrm{lr}(L^\perp/L) = \mathrm{lr}(M)/L$.*
iv. $\mathrm{rr}(M) = \mathrm{lr}(M)$.

Then i $\iff$ ii $\iff$ iii $\implies$ iv. *If* $\mathrm{char}(R/\mathfrak{m}) \neq 2$, *all are equivalent.*

PROOF. i $\iff$ ii: This directly follows from the fact that $\rho_i(M/M[\mathfrak{m}]) = \rho_{i+1}(M)$ for $i \geq 1$, and hence we just lose $\rho_1(M)$. Now apply Theorem 5.3.10.

i $\implies$ iii: This is Lemma 6.1.4.

iii $\implies$ i: Let $\mathrm{Ann}_R(M) = \mathfrak{m}^r$. Suppose that $\perp_{i \text{ even}} \rho_i(M)$ or $\perp_{i>1 \text{ odd}} \rho_i(M)$ is isotropic, hence $r \geq 2$. We will find a module $L \subseteq \mathrm{lr}(M)$ with $\mathrm{lr}(L^\perp/L) \neq \mathrm{lr}(M)/L$. First assume that M is homogeneous, say $M \cong (R/\mathfrak{m}^r)^s$. Then there exists $x \in M \setminus \mathfrak{m}M$ with $\langle x, \pi^{r-1}x\rangle = 0$ (see Lemma 3.4.16). Consider the submodule $L = R\pi^{r-1}x \subseteq \mathrm{lr}(M)$ ($r \geq 2$ needed). Then a simple calculation, using Theorem 3.4.1, gives

$$\begin{aligned} \mathrm{length}_R\left(\mathrm{lr}(L^\perp/L)\right) &= 2\lfloor\frac{r-1}{2}\rfloor + (s-2)\lfloor\frac{r}{2}\rfloor \\ \mathrm{length}_R(\mathrm{lr}(M)/L) &= s\lfloor\frac{r}{2}\rfloor - 1. \end{aligned}$$

The difference of these lengths is $2\left(\lfloor\frac{r-1}{2}\rfloor - \lfloor\frac{r}{2}\rfloor\right) + 1 \neq 0$. Hence we are done in the homogeneous case.

Now we will do the general case. Write $M = M_1 \perp \ldots \perp M_n$ as in Corollary 3.4.17. If some $\rho_i(M)$ is isotropic, then again there is $x \in M_i$ with $\langle x, \pi^{i-1}x\rangle = 0$ and we can consider $L = R\pi^{r-1}x$ and as above we contradict iii.

Now we will give a proof by induction on r. If $r = 0, 1$ our spaces can't be isotropic. If $r = 2, 3$ then we know that either $\rho_2(M)$ or $\rho_3(M)$ is isotropic, and we have considered this case. Let $r \geq 4$ and let $\varphi : M[\mathfrak{m}^{r-1}] \to M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M = \mathrm{Sh}(M)$ be the natural surjection. By our induction hypothesis, in combination with Lemma 5.1.5, we know that there is $L \subseteq \mathrm{lr}(\mathrm{Sh}(M))$ with $\mathrm{lr}(L^\perp/L) \neq \mathrm{lr}(\mathrm{Sh}(M))/L$. By Lemma 5.1.4 we have $\varphi^{-1}(\mathrm{lr}(\mathrm{Sh}(M))) = \mathrm{lr}(M)$. Hence $\varphi^{-1}(L) \subseteq \mathrm{lr}(M)$. Now

let $f : A \to B$ be a surjection of R-modules. Then for any R-submodules $C \subseteq D \subseteq B$ we have $f^{-1}(C)/f^{-1}(D) \cong C/D$ by the natural map. In our case we find

$$\begin{aligned} \mathrm{lr}(L^\perp/L) &\cong \mathrm{lr}(\varphi^{-1}(L^\perp)/\varphi^{-1}(L)) \\ &= \mathrm{lr}(\varphi^{-1}(L)^\perp/\varphi^{-1}(L)) \end{aligned}$$

and

$$\begin{aligned} \mathrm{lr}(\mathrm{Sh}(M))/L &\cong \varphi^{-1}(\mathrm{lr}(\mathrm{Sh}(M)))/\varphi^{-1}(L) \\ &= \mathrm{lr}(M)/\varphi^{-1}(L). \end{aligned}$$

As these maps are all natural, $\mathrm{lr}(\varphi^{-1}(L^\perp)/\varphi^{-1}(L)) \neq \mathrm{lr}(M)/\varphi^{-1}(L)$ and this finishes our proof.

i $\implies$ iv: Follows from Corollary 6.1.3.

iv $\implies$ i if $\mathrm{char}(R/\mathfrak{m}) \neq 2$: Follows from Corollary 6.1.3.

□

Example 6.1.6. We will now give a counterexample to the converse of Lemma 5.3.6 if $\mathrm{char}(R/\mathfrak{m}) = 2$. This is also a counterexample to iv $\implies$ i if $\mathrm{char}(R/\mathfrak{m}) = 2$ in our previous theorem. Let $R = \mathbf{Z}/2^3\mathbf{Z}$ and let $M = \mathbf{Z}/2^3\mathbf{Z} \times \mathbf{Z}/2^3\mathbf{Z}$. In this case we have $r = 3$, $\pi = 2$ and $\mathfrak{m} = (2)$. Consider the form given by

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

We directly see that $\rho_3(M)$ is isotropic, hence M is not quasi-anisotropic. We will show that $\mathfrak{m}^2 M = \mathrm{lr}(M) = \mathrm{rr}(M)$. So we start calculating $\mathrm{rr}(M)$.

Let $L \subseteq M$ with $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$. As $L \cap M[\mathfrak{m}^{r-1}]$ also satisfies these properties, we may assume that $L \subseteq M[\mathfrak{m}^{r-1}]$. Suppose that L doesn't contain $\mathrm{lr}(M) = \mathfrak{m}^{r-1}M$. Then L is cyclic. First notice that $\mathrm{length}(L^\perp) = 6 - \mathrm{length}(L)$ (by non-degeneracy). As $L \subseteq L^\perp$, we obtain $\mathrm{length}(L) \leq 3$. If $\mathrm{length}(L) \in \{0, 1\}$, we see that $\mathfrak{m}L^\perp \subseteq L$ can never be satisfied by similar length arguments. Hence $2 \leq \mathrm{length}(L) \leq 3$. As there is no $x \in M \setminus \mathfrak{m}M$ with $\langle x, x\rangle = 0$, we conclude that $\mathrm{length}(L) = 2$. So let $L = R\pi x$ for $x \notin \mathfrak{m}M$. As $\mathrm{length}(L^\perp) = 4$ and $\mathfrak{m}L^\perp \subseteq L$, we conclude that this is only possible if $x \in L^\perp$. This means that $2\langle x, x\rangle = 0$. Write $x = (x_1, x_2)$, then $0 = \langle 2(x_1, x_2), (x_1, x_2)\rangle = 4(x_1^2 + x_2^2 + x_1x_2)$. But $2 \mid x_1^2 + x_2^2 + x_1x_2$ iff $2 \mid x_1$ and $2 \mid x_2$. This would imply $x \in \mathfrak{m}M$, a contradiction. We see that $\mathrm{lr}(M) = \mathfrak{m}^{r-1}M = \mathrm{rr}(M)$.

2. The integral closure

Theorem 6.2.1. *Let R be a complete local discrete valuation ring with maximal ideal $\mathfrak{p} = (\pi)$. Let $(A, \mathfrak{m})$ be a local R-order. Let $I = \mathrm{Ann}_R(A^\dagger/A)$. Assume that the form $\langle\ ,\ \rangle : A^\dagger/A \times A^\dagger/A \to I^{-1}/R$ (as in Lemma 4.1.3) is quasi-anisotropic. Also assume that all R-orders A' with $A \subseteq A' \subseteq A^\dagger$ are tame at $\mathfrak{p}$. Then $\overline{A}/A = \mathrm{lr}(A^\dagger/A)$.*

Proof. Let $B = A^\dagger/A$. We will give a proof by induction on $s = \mathrm{length}_R(\mathrm{lr}(B))$. If $s = 0$, $\mathfrak{p}B = 0$ and by Theorem 2.2.5 we find $\overline{A}/A = A/A = \mathrm{lr}(B)$. Now continue by induction and assume that $s \geq 1$. We know $\mathrm{lr}(B) \subseteq \overline{A}/A \subseteq A^\dagger/A$ (Theorem 6.1.5 and Theorem 4.2.2). As $s \geq 1$, this means $A \subsetneq \overline{A}$. Now consider the order $\mathfrak{m} : \mathfrak{m}$, which satisfies $A \subsetneq \mathfrak{m} : \mathfrak{m} \subseteq \overline{A} \subseteq A^\dagger$ (Lemma 2.2.2 and Theorem 2.2.4). By

Corollary 2.2.6 we have $(\mathfrak{m}:\mathfrak{m})/A = (\mathfrak{p}B)[\mathfrak{m}] = \mathfrak{p}B \cap B[\mathfrak{m}]$. As $\mathfrak{p} \subseteq \mathfrak{m}$ (since the extensions are integral), this gives $\mathfrak{p}B \cap B[\mathfrak{m}] \subseteq \mathfrak{p}B \cap B[\mathfrak{p}] \subseteq \mathrm{lr}(B)$ (by definition). Now use Lemma 6.1.4 to see that $\left((\mathfrak{m}:\mathfrak{m})^\dagger/A\right)/\left((\mathfrak{m}:\mathfrak{m})/A\right)$ is still quasi-anisotropic. This lemma also gives that $\mathrm{lr}(\left((\mathfrak{m}:\mathfrak{m})^\dagger/A\right)/\left((\mathfrak{m}:\mathfrak{m})/A\right)) = \mathrm{lr}(B)/\left((\mathfrak{m}:\mathfrak{m})/A\right)$, which has smaller length than $\mathrm{lr}(B)$ (as $A \subsetneq (\mathfrak{m}:\mathfrak{m})$). By our induction hypothesis we have

$$\begin{aligned}
\mathrm{lr}(B)/\left((\mathfrak{m}:\mathfrak{m})/A\right) &= \mathrm{lr}(\left((\mathfrak{m}:\mathfrak{m})^\dagger/A\right)/\left((\mathfrak{m}:\mathfrak{m})/A\right) \\
&\cong \mathrm{lr}((\mathfrak{m}:\mathfrak{m})^\dagger/(\mathfrak{m}:\mathfrak{m})) \\
&= \overline{\mathfrak{m}:\mathfrak{m}}/(\mathfrak{m}:\mathfrak{m}) \\
&= \overline{A}/(\mathfrak{m}:\mathfrak{m}) \\
&\cong \left(\overline{A}/A\right)/\left((\mathfrak{m}:\mathfrak{m})/A\right)
\end{aligned}$$

This gives $\mathrm{lr}(B) = \overline{A}/A$ and hence we are done. □

In the above theorem, we didn't use the full assumption that all orders between A and $A^\dagger$ are tame, so there might be an improvement here.

Theorem 6.2.2. *Let A be an order over a Dedekind domain R and let $\mathfrak{p} \subset R$ be a nonzero prime. Let $I = \mathrm{Ann}_R(A^\dagger/A)$. Suppose that all $R_\mathfrak{p}$-orders A' with $A_\mathfrak{p} \subseteq A' \subseteq \overline{A_\mathfrak{p}}$ are tame at $\mathfrak{p}$. Let $B = \left(A^\dagger/A\right)_\mathfrak{p}$. Let $\langle\ ,\ \rangle : B \times B \to \left(I^{-1}/R\right)_\mathfrak{p}$ be the induced form (Corollary 4.1.4). Suppose that $\langle\ ,\ \rangle$ is quasi-anisotropic. Then $\left(\overline{A}/A\right)_\mathfrak{p} = \mathrm{lr}(B)$.*

Proof. Consider $A'' = A_\mathfrak{p} \otimes \hat{R}_\mathfrak{p}$. We can write this as $A'' = \prod_{\mathfrak{m} \in \mathrm{MaxSpec}(A'')} A''_\mathfrak{m}$ where the $A''_\mathfrak{m}$ are local orders over $\hat{R}_\mathfrak{p}$ (Theorem 2.2.1). We obviously have

$$A''^\dagger/A'' = \bigoplus_{\mathfrak{m} \in \mathrm{MaxSpec}(A'')} \left(A''_\mathfrak{m}\right)^\dagger/A''_\mathfrak{m}$$

and a similar statement holds for the integral closure. Then we do the following calculation:

$$\begin{aligned}
\mathrm{lr}(\left(A^\dagger/A\right)_\mathfrak{p}) &\cong \mathrm{lr}((A_\mathfrak{p})^\dagger/A_\mathfrak{p}) && \text{exactness of localization and 2.1.1} \\
&\cong \mathrm{lr}(\left((A_\mathfrak{p})^\dagger \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right)/\left(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}\right)) && \text{flatness of } \hat{R}_\mathfrak{p} \text{ and 2.1.6} \\
&= \mathrm{lr}(A''^\dagger/A'') && 2.1.9 \\
&= \textstyle\bigoplus_{\mathfrak{m} \in \mathrm{MaxSpec}(A'')} \mathrm{lr}((A''_\mathfrak{m})^\dagger/A''_\mathfrak{m}) \\
&= \textstyle\bigoplus_{\mathfrak{m} \in \mathrm{MaxSpec}(A'')} \overline{A''_\mathfrak{m}}/A''_\mathfrak{m} && 6.2.1 \\
&= \overline{A''}/A'' \\
&= \overline{A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p}}/A_\mathfrak{p} \otimes_{R_\mathfrak{p}} \hat{R}_\mathfrak{p} \\
&\cong \left(\overline{A}/A\right)_\mathfrak{p} && 2.1.8\ .
\end{aligned}$$

In the proof we have used Theorem 6.2.1 for the orders $A''_\mathfrak{m}$. We still need to check that all orders between $A''_\mathfrak{m}$ and $\overline{A''_\mathfrak{m}}$ are indeed tame at $\mathfrak{p}$. From Remark 1.3.18 it is enough to show that all orders between A'' and $\overline{A''}$ are tame. Using Theorem 2.1.8 and the fact that tameness behaves well under taking tensor products, shows that we only need to check that all orders between $A_\mathfrak{p}$ and $\overline{A_\mathfrak{p}}$ are tame at $\mathfrak{p}$. But this is actually in the assumption of the theorem. □

We will now give a more explicit version of our theorem.

Theorem 6.2.3. *Let A be an order over a Dedekind domain R and let $\mathfrak{p} \subset R$ be a nonzero prime. Let $B = \left(A^\dagger/A\right)_\mathfrak{p}$ and let $I = \mathrm{Ann}_R(A^\dagger/A)$. Assume that $\dim_{R/\mathfrak{p}}(B/\mathfrak{p}B) < \mathrm{char}(R/\mathfrak{p})$ or $\mathrm{char}(R/\mathfrak{p}) = 0$. Let $\langle\ ,\ \rangle : B \times B \to \left(I^{-1}/R\right)_\mathfrak{p}$ be the induced form (Corollary 4.1.4). Suppose that $\langle\ ,\ \rangle$ is quasi-anisotropic. Then $\left(\overline{A}/A\right)_\mathfrak{p} = \mathrm{lr}(B)$.*

Proof. We apply Theorem 6.2.2, and we only need to check the tameness. For this notice that $(A_\mathfrak{p})^\dagger/A_\mathfrak{p} = \left(A^\dagger\right)_\mathfrak{p}/A_\mathfrak{p} = \left(A^\dagger/A\right)_\mathfrak{p} = B$ by Lemma 2.1.1 and exactness of localization. Now apply Lemma 2.4.1. □

These last two theorems, Theorem 6.2.2 and Theorem 6.2.3, are probably the most interesting results in this thesis. First compare these results with Theorem 4.2.2 ii. We have replaced the word anisotropy by quasi-anisotropy. This quasi-anisotropy is weaker than anisotropy. If we let $R = \mathbf{Z}$ and $p \in \mathbf{Z}$ prime, then one can show that if $\dim_{\mathbf{Z}/p\mathbf{Z}}(B/pB) \geq 5$, that our form is isotropic (Theorem 5.3.10 and the fact that 3 dimensional vector spaces over a finite field with inner product are automatically isotropic (Lemma 1) from the Appendix). In the quasi-anisotropic case, we don't have this bound directly. If one compares our two theorems with Theorem 4.2.2 iii, one also sees a big difference. We don't have to find a multiplicative closure, which is a rather unexpected result.

CHAPTER 7

Examples

1. Introduction

In this chapter we will give examples where we can apply our theory to find parts of the integral closure. We will pick an irreducible polynomial $f \in \mathbf{Z}[x]$ and let α be a root of this polynomial. Then we let $A = \mathbf{Z}[\alpha]$. We now want to calculate $A^\dagger$. We have the following theorem:

Theorem 7.1.1. *Suppose that α is integral over $\mathbf{Z}$ and let f be the monic minimal polynomial of α over $\mathbf{Q}$. Then $\mathbf{Z}[\alpha]^\dagger = f'(\alpha)^{-1}\mathbf{Z}[\alpha]$.*

Proof. See [**4**], Proposition 5.5 of Chapter 6. □

2. Cyclic examples

Now let $f(x) = x^2 + ax + b \in \mathbf{Z}[x]$ be irreducible. Let α be a zero of f and consider $\mathbf{Z}[\alpha]$. We want to find a condition such that $A^\dagger/A$ is cyclic. First we calculate and obtain

$$\frac{1}{f'(\alpha)} \quad = \quad \frac{1}{a^2 - 4b}\,(2\alpha + a)\,.$$

We know what $A^\dagger$ is and we find:

$$\begin{aligned} A^\dagger/A &\cong \frac{1}{a^2-4b}\begin{pmatrix} 2 & -a \\ a & -2b \end{pmatrix}\mathbf{Z}^2/\mathbf{Z}^2 \\ &\cong \mathbf{Z}^2/\begin{pmatrix} -2b & a \\ -a & 2 \end{pmatrix}\mathbf{Z}^2 \end{aligned}$$

This group is cyclic iff a is odd. So assume from now that a is odd. We apply Lemma 5.4.1 to see that we need to pull back the lower root to find the integral closure. In the last description we see that the element $(1,0)^t$ is a generator of $A^\dagger/A$. We lift it to obtain the element $\frac{1}{\Delta(f)}\,(2\alpha + a)$.

Now define the lower root of an integer n as the maximal integer of which the square divides n. Then we obtain:

$$\overline{A} \quad = \quad \mathbf{Z}\cdot 1 + \mathbf{Z}\cdot\alpha + \mathbf{Z}\cdot\frac{1}{\mathrm{lr}(\Delta(f))}\,(2\alpha + a)$$

Actually, remark that our calculation for $A^\dagger/A$ is also correct if we just ask that $\Delta(f) \neq 0$.

There are also some cyclic examples of higher degree. We have the following theorem.

Theorem 7.2.1. *Suppose $f(x) = x^n + ax^l + b \in \mathbf{Z}[x]$, with $n > l > 0$, $n \geq 3$ and $ab \neq 0$. Then the Abelian group $\mathbf{Z}[x]/(f, f')$ is cyclic iff the following statements hold:*

i. $|b| = 1$ *or* $l \leq 2$*;*
ii. $\gcd(al(n-l), nb) = 1$.

PROOF. This is exactly Theorem 0.5 from [**5**]. □

Assume that f is irreducible. As $A^\dagger/A \cong \mathbf{Z}[x]/(f, f')$ by Theorem 7.1.1, we can again apply Lemma 5.4.1. Using Lemma 5.4.2 one can also partially prove Theorem 0.3 from [**5**].

3. Non-cyclic examples

We will now consider orders $A = \mathbf{Z}[\alpha]$ where α is a zero in $\mathbf{C}$ of a monic irreducible polynomial over $\mathbf{Z}$. We have selected a few polynomials which show nice examples where we can apply our theorems. We have done most calculations using our computer program. One can find this Sage program on `http://www.math.leidenuniv.nl/~mkosters/Lectures/closure.sage`.

Example 7.3.1. Let $f(x) = x^4 - 20x^3 - 18x^2 + 5x + 6$. Then $\Delta(f) = 5^5 \cdot 8431$. One has $A^\dagger/A \cong \mathbf{Z}/5^2\mathbf{Z} \times \mathbf{Z}/(5^3 \cdot 8431)\mathbf{Z}$. We see that we only need to check the prime 5 which is automatically tame (Lemma 2.4.1). Now apply Corollary 5.3.12 to see that we are in an anisotropic case. One can now lift the lower root and one gets

$$\begin{aligned} \overline{A} &= A + \frac{3\alpha^2+3}{5}\mathbf{Z} + \frac{3\alpha^3+4\alpha^2+3\alpha+4}{5}\mathbf{Z} \\ &= \frac{\alpha^2+1}{5}\mathbf{Z} + \frac{\alpha^3+1}{5}\mathbf{Z} + \alpha^2\mathbf{Z} + \alpha^3\mathbf{Z}. \end{aligned}$$

Example 7.3.2. Let $f(x) = x^4 - 20x^3 - 20x^2 + 17x + 2$. Then $\Delta(f) = 7^4 \cdot 13 \cdot 11897$ and $A^\dagger/A \cong \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/(7^3 \cdot 13 \cdot 11897)\mathbf{Z}$. There is only one prime to check, namely 7. It turns out the obtained space is quasi-anisotropic. By Theorem 6.2.3 we have

$$\begin{aligned} \overline{A} &= A + \frac{3\alpha^3+\alpha^2+2}{7}\mathbf{Z} \\ &= \frac{5\alpha^3+4}{7}\mathbf{Z} + \alpha\mathbf{Z} + \alpha^2\mathbf{Z} + \alpha^3\mathbf{Z}. \end{aligned}$$

Example 7.3.3. Let $f(x) = x^4 + 25x^3 + 92x^2 + 89x + 34$. Then $\Delta(f) = 3^4 \cdot 2311 \cdot 6841$. One has $A^\dagger/A \cong \mathbf{Z}/3^2\mathbf{Z} \times \mathbf{Z}/\left(3^2 \cdot 2311 \cdot 6841\right)\mathbf{Z}$. Only the prime 3 might be a problem (Lemma 2.4.1), but as it turns out we have an anisotropic space and we can directly find the closure. If one does the calculation one obtains

$$\begin{aligned} \overline{A} &= A + \frac{\alpha^3+2\alpha^2+2\alpha}{3}\mathbf{Z} + \frac{\alpha^3+\alpha+2}{3}\mathbf{Z} \\ &= \frac{\alpha^3+\alpha^2+1}{3}\mathbf{Z} + \frac{2\alpha^3+\alpha^2+\alpha}{3}\mathbf{Z} + \alpha^2\mathbf{Z} + \alpha^3\mathbf{Z}. \end{aligned}$$

Example 7.3.4. Let $f(x) = x^4 + 39x^3 + 55x^2 + 60x + 25$. One finds that $\Delta(f) = 3^4 \cdot 5^3 \cdot 883483$ and $A^\dagger/A \cong \mathbf{Z}/\left(3^2 \cdot 5\right)\mathbf{Z} \times \mathbf{Z}/\left(3^2 \cdot 5^2 \cdot 883483\right)\mathbf{Z}$. Hence there are two primes to consider, and both are tame (Lemma 2.4.1). After a calculation one sees that the space is in fact anisotropic, and hence we can lift the lower root. We

obtain

$$\begin{aligned}\overline{A} &= A + \frac{2\alpha^3+2\alpha^2+\alpha+1}{3}\mathbf{Z} + \frac{6\alpha^3+14\alpha^2+10}{15}\mathbf{Z} \\ &= \frac{9\alpha^3+\alpha^2+5}{15}\mathbf{Z} + \frac{2\alpha^3+\alpha}{3}\mathbf{Z} + \frac{4\alpha^3+\alpha^2}{5}\mathbf{Z} + \alpha^3\mathbf{Z}.\end{aligned}$$

Example 7.3.5. Let $f(x) = x^3 + 2$. Then $\Delta(f) = 2^2 \cdot 3^3$ and $A^\dagger/A \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/(2\cdot 3)\,\mathbf{Z} \times \mathbf{Z}/(2\cdot 3)\,\mathbf{Z}$. In this case f itself is wild at 3, but tame at 2. At 2 we can apply Theorem 2.3.1, to see that we are done at this prime. At the prime 3, our theory doesn't help and it doesn't tell us if we are done at 3 or not.

Example 7.3.6. Let $f(x) = x^3 - 4x^2 + 38x + 92$. Then $A^\dagger/A \cong \mathbf{Z}/2^2 \cdot 7^2\mathbf{Z} \times \mathbf{Z}/2^2 \cdot 7^2 \cdot 17\mathbf{Z}$. By Theorem 2.2.5 we know that A is not closed at the primes 2 and 7 (it is tame). At the prime 2 we can't do anything, and unfortunately at 7 we have an isotropic form.

4. More serious examples

In the previous section, we gave a few example where the polynomials had small coefficients and where the exponents of the prime factorization of the discriminant are quite small. In this section we will give a few examples where this is not the case. The trick to construct such polynomials is to take a monic polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ with nonzero discriminant such that where the valuation of a_i for $0 \leq i \leq n$ is large at a fixed prime p. Then consider the order $A = \mathbf{Z}[\alpha]$ where α is a zero of f.

Example 7.4.1. Let $f(x) = x^4 - 625x^3 - 125x^2 - 15625x - 15625$. Then $\Delta(f) = 5^{20} \cdot 13 \cdot 457 \cdot 8111$. In this case $A^\dagger/A \cong \mathbf{Z}/5^3\mathbf{Z} \times \mathbf{Z}/5^7\mathbf{Z} \times \mathbf{Z}/5^{10} \cdot 13 \cdot 457 \cdot 8111\mathbf{Z}$. In fact, we can find the integral closure using our theory (it is anisotropic), and we obtain

$$\overline{A} = \mathbf{Z} + \left(\frac{3}{3125}\alpha^3 + \frac{1}{25}\alpha\right)\mathbf{Z} + \frac{1}{125}\alpha^2\mathbf{Z} + \frac{1}{625}\alpha^3\mathbf{Z}.$$

If one changes certain signs of the coefficients of f, one also obtains such nice results. The polynomial $f(x) = x^4 - 75x^3 + 125x^2 + 3125x - 15625$ gives a nice example as well.

Example 7.4.2. Let $f(x) = x^4+7x^3+343x^2+343x+2401$. Then $\Delta(f) = 7^{13}\cdot 11\cdot 19^2$ and $A^\dagger/A \cong \mathbf{Z}/7^2\mathbf{Z} \times \mathbf{Z}/7^4 \cdot 19\mathbf{Z} \times \mathbf{Z}/7^7 \cdot 11 \cdot 19\mathbf{Z}$. We can use Theorem 2.2.5 to see that we are finished at the prime 19. We are in an isotropic case and we can find the integral closure. We have

$$\overline{A} = \mathbf{Z} + \frac{\alpha}{7}\mathbf{Z} + \frac{\alpha^2}{49}\mathbf{Z} + \frac{\alpha^3}{343}\mathbf{Z}.$$

5. Heuristics

In this section we will check how often one can find the integral closure directly by using the theory developed in this thesis. This means that we only use the theory derived from Theorem 2.3.1. The Sage program which we used can be found on `http://www.math.leidenuniv.nl/~mkosters/Lectures/closure.sage`. This computer program has as input a monic polynomial $f \in \mathbf{Z}[x]$ with $\Delta(f) \neq 0$. The program will try to calculate the integral closure as follows. We look at the different

primes and apply Theorem 6.2.3. If we can apply it, we know that we have found the integral closure at this prime. In many occasions, Theorem 6.2.3 doesn't apply, but we can still test if our starting order is tame. We can then use Theorem 2.3.1 to see that if our starting order is already integrally closed.

We have done the following experiment. First pick a prime $p \in \mathbf{Z}_{\geq 2}$. Then pick $n \in \mathbf{Z}_{\geq 2}$ and a coefficient bound c. Finally pick a random monic polynomial f in $\mathbf{Z}[x]$ of degree n with $\Delta(f) \neq 0$, $p^2 \mid \Delta(f)$ with coefficients bounded in absolute value by c. Then we want to know how often our program can find the integral closure of $A = \mathbf{Z}[x]/(f) \subset \mathbf{Q}[x]/(f)$ at a certain prime. This means that we find an order $A \subseteq A' \subseteq Q(A)$ such that $p \nmid (\overline{A} : A')$.

In practice we first fix a degree. Then we pick a random monic polynomial f with $\Delta(f) \neq 0$ with coefficients bounded in absolute value by c and consider the primes p with $p^2 \mid \Delta(f)$. We do this a total of m times and select only the primes where $p^2 \mid \Delta(f)$ at least t times. We let $m = 10^4$, $c = 100$ and $t = 50$. We round percentages to one decimal. We obtain the following results.

First let $n = 2$. Then we obtain:

Prime	Number of times $p^2 \mid \Delta(f)$	Found closure (%)
2	4942	0.0
3	1121	100.0
5	361	100.0
7	202	100.0
11	66	100.0
13	52	100.0.

The zero in the above table for $p = 2$ can be explained as follows. We can't really check if $\overline{A}$ is tame (Lemma 2.4.1 and Lemma 5.4.2). We would only be able to find the closure if $\mathbf{Z}[x]/(f)$ is tame at 2 and if $\left(A^\dagger/A\right)_{(2)} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. A simple calculation shows that this never happens. If $p > 2$ we are always in a tame and cyclic case and hence we can find the closure (Corollary 5.4.1).

Now let $n = 3$. We then find:

Prime	Number of times $p^2 \mid \Delta(f)$	Found closure (%)
2	5022	24.7
3	1835	39.6
5	698	98.4
7	375	98.9
11	140	100.0
13	108	99.1
19	53	100.

One sees that the chances for success for $p = 2, 3$ are small. This is due to the fact that we can't check tameness in these cases in general (Lemma 2.4.1). For larger primes, our theory in general will apparently give the integral closure.

Now let $n = 4$. We then find:

Prime	Number of times $p^2 \mid \Delta(f)$	Found closure (%)
2	4959	11.9
3	2336	62.0
5	980	97.8
7	512	98.2
11	214	99.1
13	167	100.0
17	87	100.0
19	84	100.0
23	62	100.0.

Finally, let $n = 5$. We obtain:

Prime	Number of times $p^2 \mid \Delta(f)$	Found closure (%)
2	4975	11.5
3	2197	39.5
5	920	96.2
7	530	98.9
11	215	100.0
13	147	100.0
17	95	99.0
19	81	100.0
23	54	100.0

Remark 7.5.1. The probability that $p^2 \mid \Delta(f)$ where $f \in \mathbf{Z}_p[x]$ is monic and has degree n is given by the following table, obtained from [**2**] (page 29):

	$p = 2$	$p \neq 2$
$n = 2$	$\frac{1}{2}$	$\frac{1}{p^2}$
$n = 3$	$\frac{1}{2}$	$\frac{2}{p^2} - \frac{1}{p^3}$
$n \geq 4$	$\frac{1}{2}$	$\frac{1}{p} - \frac{(p-1)^2(1-(-p)^{-n+2})}{p^2(p+1)}$.

Remark 7.5.2. The results which we obtained seem to be promising. One directly sees that one of the main improvements is a better test for tameness. Remark that we have only checked polynomials with 'small' coefficients, which means that the discriminant will be small. This means that the power in which a prime occurs in the factorization of the discriminant is rather small. As we kept n small, we didn't 'notice' the fact that 3-dimensional vector spaces over finite fields are automatically isotropic (Lemma 1 from the Appendix).

CHAPTER 8

Further research

In this thesis we have tried to get as much as possible out of Theorem 2.3.1. It probably isn't a surprise to the reader that not all questions are properly answered. In this chapter we will discuss some open problems and suggestions for further research.

Question 1. Let A be an order over a Dedekind domain R. One of the main problems we have is that we require $\overline{A}$, which we don't have, to be tame at certain primes. How can we check it? Currently, our best option is Lemma 2.4.1. A suggestion by Hendrik Lenstra is that we replace our Dedekind ring R by a better ring (a ring between R/I and A/IA where $I = \mathrm{Ann}_R(A^\dagger/A)$), and that tameness then is more often satisfied. The idea is that the fields $R/\mathfrak{p}$ will be replaced by bigger fields, and as a consequence the dimensions appearing in Lemma 2.4.1 will go down. This will also help in another way if $R = \mathbf{Z}$ for example. Notice that a 3-dimensional vector space over a finite field together with an inner product is automatically isotropic. Hence this 'problem' will occur less often.

Another correlated problem, is that our theory has a lot of trouble with the primes of R with $\mathrm{char}(R/\mathfrak{p}) = 2$. In this thesis, only Theorem 2.3.1 seems to work fine.

Question 2. How well does this thesis in practice help for finding the integral closure? We have not compared our tricks with those already in practice. Our methods don't need that many data to work. As most algorithms probably already collect these data, it seems to be reasonable to try our tricks which shouldn't give much computation, and so to speak obtain part of the integral closure for free.

We have to remark here that the biggest problem for finding the integral closure of an order over $\mathbf{Z}$ is to factor the discriminant of the order, and we didn't work on this problem here.

Question 3. Let M be a finitely generated module over a uniserial ring R together with a non-degenerate symmetric R-bilinear form $\langle\ ,\ \rangle : M \times M \to R$. In Theorem 5.5.2 we show how to find $\mathrm{rr}(M)$ if $\mathrm{char}(R/\mathfrak{m}) \neq 2$. Can one find a (quick) algorithm to do this if $\mathrm{char}(R/\mathfrak{m}) = 2$?

Question 4. An order gives rise to finitely generated modules over certain uniserial rings together with a symmetric non-degenerate bilinear form. But which pairs do we obtain? In Corollary 5.4.2 we have shown that certain cyclic modules will never occur. Are there more restrictions on the modules? Are there restrictions on the inner products?

Question 5. In Theorem 6.2.1 we have shown that the lower root somehow corresponds to a ring. In the proof we use Lemma 5.3.6 and in the 'last step' we obtain a ring. The question is, do we obtain a ring after every application of Lemma 5.3.6

locally at every prime? We will make this problem more clear in the following example. Consider the polynomial $f(x) = x^2+59x+89 \in \mathbf{Z}[x]$ which has discriminant 5^5 (so we are in a local case already) and consider $A = \mathbf{Z}[x]/(f)$. A simple closure shows that the lift of the lower root is given by $A + \frac{9\alpha+3}{25}$ (where α is a zero of f). In the first step of the application of Lemma 5.3.6, we find $A + \frac{9\alpha+3}{5}$, which is in fact a ring already. One can easily show that this happens in all cases where we can apply the formula in Example 2. Does this always happen in the more general case? We didn't find a counterexample to this statement and if the statement would be true, it would lead to a much quicker proof of Theorem 6.2.1. If this statement is false, one can wonder if the radical root always gives a ring back. For the latter question, we have done many tests using a computer program, but we didn't find a counterexample.

Appendix

1. Forms on vector spaces over finite fields

Let $\mathbf{F}_q$ be a finite field and suppose we are given a finite dimensional $\mathbf{F}_q$-vector space V together with a symmetric bilinear form $\langle\ ,\ \rangle : V \times V \to \mathbf{F}_p$. We want to see if this vector space is anisotropic or not.

Lemma 1. *Let $\langle\ ,\ \rangle : V \times V \to \mathbf{F}_q$ be a symmetric bilinear form where V is a finite dimensional $\mathbf{F}_q$-vector space and $q = p^n$ ($n \in \mathbf{Z}_{\geq 1}$ and $p \in \mathbf{Z}_{\geq 2}$ prime). Then V is isotropic if $p = 2$ and $\dim_{\mathbf{F}_q}(V) \geq 2$ or $p > 2$ and $\dim_{\mathbf{F}_q}(V) \geq 3$.*

Proof. If $p = 2$, the map

$$\begin{array}{rcl} \varphi : V & \to & \mathbf{F}_q \\ x & \mapsto & \langle x, x\rangle \end{array}$$

is a morphism of groups. Hence this map is not injective if $\#V > \mathbf{F}_q$, that is, if $\dim_{\mathbf{F}_q}(V) \geq 2$.

If $p > 2$, we apply Chevalley-Warning ([**8**], Page 5, Theorem 3) to find a nonzero $x \in V$ with $\langle x, x\rangle = 0$. □

Lemma 2. *Let $\langle\ ,\ \rangle : V \times V \to \mathbf{F}_q$ be a symmetric bilinear form where V is a finite dimensional $\mathbf{F}_q$-vector space and $q = p^n$. Then $\langle\ ,\ \rangle$ is anisotropic iff one of the following hold:*

i. $\dim_{\mathbf{F}_q}(V) = 0$;
ii. $\dim_{\mathbf{F}_q}(V) = 1$ *and* $\langle\ ,\ \rangle \neq 0$;
iii. $\dim_{\mathbf{F}_q}(V) = 2$, *$q$ is odd and* $\left(-\det\left((\langle e_i, e_j\rangle)_{i,j=0}^{1}\right)\right)^{\frac{q-1}{2}} = -1$ *for a basis* $\{e_0, e_1\}$ *of V over $\mathbf{F}_q$.*

Proof. We use Lemma 1 to see that anisotropic spaces have dimension at most 2. If the space has dimension 0 and 1, our statement is obviously correct. Now suppose that $\dim_{\mathbf{F}_q}(V) = 2$. Then notice that anisotropic spaces are non-degenerate and that q is odd (by Lemma 1). Now apply Proposition 5 on page 35 of [**8**] to see that the form is isomorphic to a form given by the symmetric bilinear form $x_1^2 + \Delta x_2^2$, where Δ is the discriminant of the form (defined up to squares of units and $\Delta = \det\left((\langle e_i, e_j\rangle)_{i,j=0}^{1}\right)$ for any basis $\{e_0, e_1\}$ of V over $\mathbf{F}_q$). This form represents 0 iff $-\Delta$ is a square. This is equivalent to the statement in the theorem. □

2. Forms on uniserial rings

Suppose we are given a uniserial ring R of length n with maximal ideal $\mathfrak{m}$ and a finitely-generated module M together with a symmetric bilinear form $\langle\ ,\ \rangle$:

$M \times M \to R$. Then we want to check if it non-degenerate and moreover if it is anisotropic or quasi-anisotropic.

We propose the following solution to this problem. First pick a decomposition $M = \bigoplus_{i=1}^{n} M_i$ where M_i is free over $R/\mathfrak{m}^i$ $(0 \leq i \leq n)$. Suppose that $M_i \cong \left(R/\mathfrak{m}^i\right)^{m_i}$. Let $e_{i1}, \ldots, e_{im_i}$ form a basis of M_i. Write $\langle e_{ij}, e_{ik} \rangle = \pi^{n-i} r_{ijk}$. Then for $i = 1, \ldots, n$ consider the matrix over $R/\mathfrak{m}$:

$$B_i = (r_{ijk} + \mathfrak{m}\rangle)_{j,k=1}^{m_i}.$$

Lemma 3. *The matrix B_i represents the form on $\rho_i(M)$.*

Proof. This follows from Lemma 3.4.16 and Definition 3.4.14 after splitting into homogeneous parts. □

Lemma 4. *The following statements hold:*

i. *The form $\langle\ ,\ \rangle$ above is non-degenerate iff $\det(B_i) \neq 0$ for $i = 1, \ldots, n$.*
ii. *The form $\langle\ ,\ \rangle$ is anisotropic iff both $\perp_{i \text{ even}} B_i$ and $\perp_{i \text{ odd}} B_i$ are anisotropic.*
iii. *The form $\langle\ ,\ \rangle$ is quasi-anisotropic iff both $\perp_{i \text{ even}} B_i$ and $\perp_{i \text{ odd}, i \neq 1} B_i$ are anisotropic.*

Proof. Use Lemma 3. By Lemma 3.4.15 and Definition 3.4.14 we see that

$$M_{\text{odd}} = \text{ur}(M)/\text{lr}(M) \cong \perp_{i \text{ odd}} \rho_i(M).$$

Similarly,

$$M_{\text{even}} = \text{ur}(M/M[\mathfrak{m}])/\text{lr}(M/M[\mathfrak{m}]) \cong \perp_{i \text{ even}} \rho_i(M).$$

By Theorem 3.4.17 the form $\langle\ ,\ \rangle$ is non-degenerate iff M_{odd} and M_{even} are non-degenerate. By Theorem 5.3.10 the form is anisotropic iff M_{even} and M_{odd} are anisotropic. The last statement follows by definition. □

3. Implementation

An implementation in Sage of the ideas in this thesis can be found at `http://www.math.leidenuniv.nl/~mkosters/Lectures/closure.sage`.

Bibliography

[1] M. F Atiyah, I.G. MacDonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Company, 1969

[2] J. Brakenhoff, Counting problems for number rings, 2009, http://www.math.leidenuniv.nl/scripties/proefschrift-brakenhoff.pdf

[3] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer, 1995

[4] S. Lang, Algebra, Revised third edition, Springer-Verlag, 2002

[5] S. Liu, Trinomials and Exponential Diophantine Equations, Universiteit Leiden, 2008, http://www.math.leidenuniv.nl/scripties/Liu2Master.pdf

[6] T. Y. Lam, Lectures on Modules and Rings, Springer-Verlag, 1999

[7] J. P. May, Notes on Dedekind Rings, http://www.math.uchicago.edu/~may/MISC/Dedekind.pdf

[8] J.-P. Serre, A Course in Arithmetic, Verlag, 1973

[9] P. Stevenhagen, Number Rings, Universiteit Leiden, 2008, http://websites.math.leidenuniv.nl/algebra/ant.pdf

[10] O. Zariski, P. Samuel, Commutative Algebra Volume I, D. Van Nostrand Company, Princeton, 1958

Index