Singular Alternating Matrices over Rings of Integers

by

Kristina Nelson

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Melanie Wood, Co-chair
Professor Kenneth Ribet, Co-chair
Professor Sug Woo Shin

Summer 2023

Singular Alternating Matrices over Rings of Integers

Abstract

Singular Alternating Matrices over Rings of Integers

by

Kristina Nelson

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Melanie Wood, Co-chair

Professor Kenneth Ribet, Co-chair

Let K be a number field with ring of integers $\mathcal{O}_K$. Consider the set of $n \times n$ alternating matrices with fixed rank, $r < n$, norm bounded by X, and entries in O_K. We give an asymptotic formula for the number of such matrices as X varies, where n, r and K are treated as constants. Our work extends previous results by Eskin and Katznelson [EK95], who considered an analogous problem about symmetric integer matrices; as well as by Park, Poonen, Voight, and Wood [PPVW19], who counted alternating integer matrices.

The principal ideas behind the proof were first introduced by Katznelson in [Kat93]. There, the problem of counting matrices is reduced to one of counting lattice points. Because our matrices have entries in $\mathcal{O}_K$ rather than $\mathbb{Z}$, the lattices of Katznelson are replaced in the present work with $\mathcal{O}_K$-modules. The generalization from $\mathbb{Q}$ to K renders the standard tools of lattice-theory less directly applicable, and we rely on the Minkowski map and novel arguments to, at various turns, reduce to the lattice case, or abstract results from lattices to $\mathcal{O}_K$-modules. Ancillary results in our work include a new formula for the discriminant of a torsion-free $\mathcal{O}_K$-module in terms of its *pseudo-basis* and a novel structure theorem about the set of alternating matrices whose rows lie in a specified $\mathcal{O}_K$-module.

Contents

Acknowledgments

I am endlessly grateful to my long distance advisor Melanie Wood. I began working with Melanie during a challenging part of my PhD, and despite everything going on in her own life, including several cross country moves, she went completely above and beyond to support me. Melanie is incredibly generous with her knowledge and her time and I feel extremely lucky to have met her when I did.

My Berkeley advisor, Ken Ribet, was remarkably encouraging and flexible as I ping ponged between focuses and advisors. Ken has always been happy to hear about whatever I was working on, and to share his wisdom. I can't thank him enough for all the advice and support over the years.

Warmest thanks to Sug Woo Shin for serving on my committee and his kind guidance as I prepared to retake the qual.

Much love to Lauren, David, and Anya. The times we've spend just hanging around are my best memories of Berkeley. Anya singlehandedly turned several otherwise impossible classes into adventures.

Thanks to everyone else in my cohort, and on the soccer team. I don't think I've ever met a group of people so friendly and funny and kind before.

Thanks to my mom, who I think is still expecting me to move back home after this PhD, and my dad who was so excited about Science One at UBC. Thanks to my brother for being just incorrigibly positive about everything I do.

Finally, Edward, thank you for your loving patience and willingness have me explain my math problems to you solely so I can complain about them. I couldn't wish for a more loyal and supportive partner.

Chapter 1

Introduction

Understanding the distribution of the bounded integer points of a variety is a major problem in arithmetic geometry. Consider, for example, the affine case: let $f_1, \dots f_a \in \mathbb{Z}[x_1, \dots, x_b]$ be a set of irreducible polynomials and define

$$\mathcal{V}(\mathbb{Z}, X) := \left\{ \boldsymbol{x} \in \mathbb{Z}^b : ||\boldsymbol{x}|| < X \text{ and } f_i(\boldsymbol{x}) = 0, \ \forall\, i = 1, \dots, a \right\}.$$

Here, we are interested in the growth of $\#\mathcal{V}(\mathbb{Z}, X)$ as X tends to infinity. See also the discussion of Duke, Rudnick and Sarnak in [DRS93] for a more extensive background. Though resolving the above problem for varieties in complete generality is “hopeless” [DRS93], progress is underway in a number of cases where additional structure exists.

Take the set of matrices $A \in M_{n\times m}(\mathbb{R})$ of specified rank, $\operatorname{rk}(A) = r$. This is a quasi-affine set, defined as the zero set of the $(r+1)$-dimensional minors intersected with the open set where at least one r-dimensional minor is nonzero. Katznelson tackles the integer point problem in this case in [Kat93] and [Kat94]. In the former, he estimates the number of singular $A \in M_n(\mathbb{Z})$ contained in a bounded open set, and in the latter, the number of $A \in M_{n\times m}(\mathbb{Z})$ with $\operatorname{rk}(A) = r$ and $||A|| < X$.

Expanding on the same techniques, Eskin and Katznelson bound the number of symmetric $A \in M_n(\mathbb{Z})$ with $\operatorname{rk}(A) = r$ and $||A|| < X$ in [EK95]. Park, Poonen, Voight, and Wood adapt their argument to estimate the number of *alternating* $A \in M_n(\mathbb{Z})$ with $\operatorname{rk}(A) = r$ and $||A|| < X$ [PPVW19]. Their paper proposes a probabilistic model based on random alternating matrices to predict the arithmetic behaviour of elliptic curves over $\mathbb{Q}$. In particular, the distribution of $\operatorname{rk}(A)$ over alternating $A \in M_n(\mathbb{Z})$ with $||A|| < X$, as X goes to infinity, is used to make heuristic predictions about the boundedness of ranks of elliptic curves.

Let K be a number field and $\mathcal{O}_K$ its ring of integers. In the current work we investigate the number of alternating $A \in M_n(\mathcal{O}_K)$ with $\operatorname{rk}(A) = r$ and norm bounded by X. One motivation of this work is a potential future analog of [PPVW19]'s model, extended to elliptic curves defined over K and ranks considered over certain finite extensions L/K.

1.1 Main result

As above, let K be a number field with ring of integers $\mathcal{O}_K$. For a matrix, $A \in M_n(K)$, we define the *Minkowski norm* of A to be

$$||A||_\mu := \left(\sum_{1 \leq i,j \leq n} \sum_{\tau : K \to \mathbb{C}} |\tau(A_{ij})|^2 \right)^{1/2},$$

where the inner sum varies over all complex embeddings of K. We say $A \in M_n(K)$ is alternating if $A^t = -A$ and we denote the collection of alternating matrices by $M_n(K)_{\text{alt}}$. Let $\mathcal{A}^K_{n,r}(X)$ be the set of rank r matrices $A \in M_n(\mathcal{O}_K)_{\text{alt}}$ with norm bounded by X, that is,

$$\mathcal{A}^K_{n,r}(X) := \{A \in M_n(\mathcal{O}_K)_{\text{alt}} : \text{rk}(A) = r \text{ and } ||A||_\mu < X\}. \tag{1.1}$$

We consider $\#\mathcal{A}^K_{n,r}(X)$ as a function of X and investigate its behaviour as X grows. Using Notation 2.1.2, our main result is as follows.

Theorem 1.1.1. *Let $0 \leq r < n$, with r even, and $s = [K : \mathbb{Q}]$. Then $\#\mathcal{A}^K_{n,r}(X) \ll_{K,n} X^{nrs/2}$. For X sufficiently large, $\#\mathcal{A}^K_{n,r}(X) \gg_{K,n} X^{nrs/2}$ as well.*

Proof. The theorem is proven in two parts, the upper bound in Proposition 6.0.14, and the lower bound in Proposition 7.0.5 □

Remark 1.1.2. *We let r be even in Theorem 1.1.1, as otherwise the number of alternating matrices of rank r is zero [Lan02, Chapter XV, Theorem 8.1]. The nonsingular case follows from Theorem 1.1.1. Indeed, in Corollary 6.0.15 we show when $r = n$ is even, $\mathcal{A}^K_{n,n}(X) \ll_{K,n} X^{sn(n-1)/2}$ and for X sufficiently large $\mathcal{A}^K_{n,n}(X) \gg_{K,n} X^{sn(n-1)/2}$.*

1.2 Methods

For $\boldsymbol{v} \in \mathbb{Z}^n$, define the lattice $\Sigma_{\boldsymbol{v}} := \{\boldsymbol{u} \in \mathbb{Z}^n : \boldsymbol{u} \perp \boldsymbol{v}\}$ and let $\mathcal{M}(\Sigma_{\boldsymbol{v}})$ be the set of matrices $A \in M_n(\mathbb{Z})$ whose rows lie in $\Sigma_{\boldsymbol{v}}$, or equivalently, the set of $A \in M_n(\mathbb{Z})$ with $\boldsymbol{v} \in \ker(A)$. Then $\mathcal{M}(\Sigma_{\boldsymbol{v}})$ is itself a lattice. Our key idea comes from Katznelson's paper [Kat93] counting singular matrices $A \in M_n(\mathbb{Z})$ with $||A|| < X$: since every such matrix has some short integer vector, $\boldsymbol{v} \in \mathbb{Z}^n$ in its kernel, the problem can be split into counting the small matrices of $\mathcal{M}(\Sigma_{\boldsymbol{v}})$ for finitely many vectors $\boldsymbol{v} \in \mathbb{Z}^n$.

The present work follows previous adaptions of Katznelson's argument to symmetric [EK95] and alternating [PPVW19] matrices of rank $r < n$. We are interested in matrices over $\mathcal{O}_K$ rather than $\mathbb{Z}$. Thus, instead of lattices, $\Sigma_{\boldsymbol{v}} \subset \mathbb{Z}^n$, spanning codimension 1 subspaces of $\mathbb{R}^n$, we consider $\mathcal{O}_K$-modules, $\Lambda \subset \mathcal{O}_K^n$, spanning r-dimensional subspaces of K^n. We restrict our count to alternating matrices by replacing $\mathcal{M}(\Sigma_{\boldsymbol{v}})$ with $\mathcal{A}(\Lambda)$, the $\mathcal{O}_K$-module of alternating matrices $A \in M_n(\mathcal{O}_K)_{\text{alt}}$ whose rows lie in Λ. Then $\#\mathcal{A}^K_{n,r}(X)$ is estimated by counting the number of matrices each $\mathcal{A}(\Lambda)$ contributes.

In practice, $\mathcal{A}(\Lambda)$ is much nicer to work with when Λ is *primitive*, i.e. when $\Lambda = \mathcal{O}_K^n \cap \mathrm{Span}_K(\Lambda)$. We prove results about the structure and discriminant of a more technical $\mathcal{O}_K$-module of matrices, $\mathcal{B}(\Lambda)$, and then show in Lemma 4.0.6 that $\mathcal{A}(\Lambda) = \mathcal{B}(\Lambda)$ whenever Λ is primitive. This lemma generalizes [EK95, Proposition 3.3]. Some additional work is needed in the proof, as the lattice bases have to be replaced by more complex *pseudo-bases* for Λ and $\mathcal{B}(\Lambda)$.

The upper bound involves two broad steps: first, we need to choose the set, $\mathcal{P}$, of $\mathcal{O}_K$-modules Λ which we will consider $\mathcal{A}(\Lambda)$ of; secondly, we need a count of the small matrices contributed by each $\mathcal{A}(\Lambda)$.

Eskin and Katznelson showed that for their counting problem it suffices to consider primitive, rank r, lattices of bounded discriminant. Analogously, we show in Proposition 3.2.6 and Lemma 6.0.8 that $\mathcal{P}$ can be taken to be the set of *primitive*, *module-rank* r, $\mathcal{O}_K$-modules with bounded *module-discriminant*. Specifically, Proposition 3.2.6 shows that if $\mathcal{B}(\Lambda)$ contains a small, rank r, matrix then the module-discriminant of Λ is small as well. This generalizes Corollary 4.2 of [EK95], however their proof uses *reduced lattice bases*, which do not translate in quite the way we need to $\mathcal{O}_K$-modules [FS10]. Instead, we develop a novel proof in Chapter 3.2 that exploits the structure of $\mathcal{B}(\Lambda)$ and works with any pseudo-basis of Λ.

An extended version of the Minkowski embedding $\mu : K^n \to K_{\mathbb{R}}^n$ (Definition 2.5.3) allows us to turn $\mathcal{O}_K$-modules, Λ, into lattices, $\mu(\Lambda)$. We define the module-discriminant, $\mathfrak{D}(\Lambda)$, of an $\mathcal{O}_K$-module Λ as the lattice-discriminant of $\mu(\Lambda)$ (see Chapter 2.5). This agrees with other authors [Thu92, FS10]. However, we also give a novel expression for $\mathfrak{D}(\Lambda)$ in terms of the *pseudo-basis* of Λ[1] (Proposition 2.5.17), which is critical to the proof of the above-mentioned Proposition 3.2.6 as well as Proposition 3.1.8 and other results.

Proposition 3.1.8 shows $\mathfrak{D}(\mathcal{B}(\Lambda)) \asymp \mathfrak{D}(\Lambda)^{r-1}$ and generalizes [EK95, Lemma 3.5]. A new method of reducing to the $r = n$ case is used[2].

We rely on Thunder [Thu92] for a bound on the number of modules in $\mathcal{P}$. Thunder's work generalizes that of Schmidt [Sch68] to an arbitrary number field. Schmidt's result, a count of the number of primitive lattices of fixed rank and bounded discriminant, is used analogously by Eskin and Katznelson.

Having figured out $\mathcal{P}$, the second step is to bound the size of the set

$$\mathcal{A}(\Lambda)_{<X} := \{A \in \mathcal{A}(\Lambda) : ||A||_\mu < X\}.$$

In Lemma 5.0.10 we generalize a standard formula for the number of lattice points in a ball [EK95, Lemma 2.4] to $\mathcal{O}_K$-modules. We replace the reduced basis used there with *(successive) minima*, as the latter generalize more usefully to $\mathcal{O}_K$-modules. Lemma 6.0.5 relates the minima of $\mathcal{A}(\Lambda)$ to those of Λ. This lemma is functionally equivalent to [EK95, Lemma 3.2], but requires a new proof using the relation $\mathfrak{D}(\mathcal{A}(\Lambda)) \asymp \mathfrak{D}(\Lambda)^{r-1}$ since we no

[1] Or equivalently, the *Steinitz class* and a *basis matrix* of Λ.

[2] This allowed us to avoid the use of orthonormal vectors, which was desirable as our norm $|| \cdot ||_\mu$ does not play as naturally with the module-discriminant as the L^2-norm on $\mathbb{R}^n$ does with lattice-discriminants.

longer have all the features of a nice reduced lattice basis. The above results in hand, Lemma 6.0.6 then bounds $\mathcal{A}(\Lambda)_{<X}$ in terms of the minima of Λ – or more precisely the *truncated modules*, $\mathrm{trnc}_q(\Lambda)$, of Λ, which are constructed using the minima.

Truncated modules are new to our version of the matrix-counting argument, though they also appear in Thunder [Thu92]. Using $\mathrm{trnc}_q(\Lambda)$ in our expression for $\#\mathcal{A}(\Lambda)_{<X}$ standardizes all terms appearing in the upper bound on $\#\mathcal{A}^K_{n,r}(X)$ (Proposition 6.0.14). This leaves us with a single formula to bound and no error terms needing to be handled separately [EK95, Theorem 4.1, Sections 6 and 7].

Finally, the proof of the lower bound on $\#\mathcal{A}^K_{n,r}(X)$ (Proposition 7.0.5) follows that of [PPVW19] and relies on the notion of a *c-regular* $\mathcal{O}_K$-module, i.e. one whose the smallest minima vector is *short*. We show a large number of $\mathcal{O}_K$-modules in $\mathcal{P}$ are c-regular (Lemma 7.0.4) and that each c-regular $\mathcal{O}_K$-module contributes at least one matrix to $\mathcal{A}^K_{n,r}(X)$. Lemma 7.0.4 is a generalization of [EK95, Proposition 2.6] and uses a new argument: instead of inductively constructing c-regular modules, we use [Thu92, Lemma 15] to show there cannot be too many non-c-regular modules in $\mathcal{P}$.

1.3 Roadmap

We begin in Chapter 2 with background material on lattices and $\mathcal{O}_K$-modules that will be used throughout the article. In Chapter 3 we introduce the $\mathcal{O}_K$-module of matrices, $\mathcal{B}(\Lambda) \subset M_n(K)_{\mathrm{alt}}$, which is constructed from another $\mathcal{O}_K$-module, $\Lambda \subset K^n$. We relate the module-discriminant of $\mathcal{B}(\Lambda)$ to that of Λ. Chapter 4 discusses primitive modules, a generalization of primitive lattices. We show that when Λ is primitive, $\mathcal{B}(\Lambda)$ consists of exactly the alternating matrices whose rows lie in Λ, that is, $\mathcal{B}(\Lambda) = \mathcal{A}(\Lambda)$. Chapter 5 generalizes the notion of successive minima from lattices to $\mathcal{O}_K$-modules and shows how to count module-points of small norm using the minima. In Chapter 6, we bound $\#\mathcal{A}^K_{n,r}(X)$ above by summing $\mathcal{A}(\Lambda)_{<X}$ over a finite set of primitive $\Lambda \subset K^n$, $\mathcal{P}$. Chapter 7 bounds $\#\mathcal{A}^K_{n,r}(X)$ below by showing a large number of modules in $\mathcal{P}$ each contribute at least one matrix to $\mathcal{A}^K_{n,r}(X)$.

Chapter 2

Background, lattices and modules

2.1 Notation

Notation 2.1.1. *Throughout this note K will be a number field of degree $s = [K : \mathbb{Q}]$ with ring of integers $\mathcal{O}_K$.*

We use the following asymptotic notation.

Notation 2.1.2. *Let $\mathcal{X}$ be a set of allowed function inputs and $\mathfrak{P}$ a second set of inputs, which are thought of as parameters. Let $f, g : \mathcal{X} \times \mathfrak{P} \to \mathbb{R}_{\geq 0}$ be a pair of nonnegative functions. Then we write*

$$f(x, a) \ll_a g(x, a)$$

(or, for the reverse bound, $f(x, a) \gg_a g(x, a)$) to mean that there exists a positive function $C : \mathfrak{P} \to \mathbb{R}_{>0}$ such that $f(x, a) \leq C(a)g(x, a)$ ($f(x, a) \geq C(a)g(x, a)$, respectively) for all values of $(x, a) \in \mathcal{X} \times \mathfrak{P}$ that are under consideration.

The expression

$$f(x, a) \asymp_a g(x, a)$$

indicates that both $f(x, a) \ll_a g(x, a)$ and $f(x, a) \gg_a g(x, a)$ hold for all $(x, a) \in \mathcal{X} \times \mathfrak{P}$ under consideration.

Most often, we have $\mathcal{X} = \mathbb{R}_{>0}$. In this case, we write

$$f(x, a) \gg_a g(x, a) \text{ for } x \text{ sufficiently large,}$$

when there exist functions $C : \mathfrak{P} \to \mathbb{R}_{>0}$ and $x_0 : \mathfrak{P} \to \mathcal{X}$ such that $f(x, a) \geq C(a)g(x, a)$ for all $(x, a) \in \mathcal{X} \times \mathfrak{P}$ with $x \geq x_0(a)$. This is necessary in situations where $g(x, a)$ can be zero for small values of x.

Remark 2.1.3. *To simplify the asymptotic notation, when possible we will replace pairs of parameters with a single value. For instance, let $\mathfrak{P} = \{(a, b) \in \mathbb{N}^2 : a \leq b\}$ and consider* *functions $f, g : \mathcal{X} \times \mathfrak{P} \to \mathbb{R}_{\geq 0}$. If there exists some nonnegative function $C : \mathfrak{P} \to \mathbb{R}_{\geq 0}$ such that $f(x, a, b) \leq C(a, b)g(x, a, b)$ for all $x \in \mathcal{X}$ and integers $1 \leq a \leq b$, then*

$$\begin{aligned} f(x, a, b) &\leq C(a, b)g(x, a, b) \\ &\leq (C(1, b) + C(2, b) + \cdots C(b, b))g(x, a, b) \\ &= \left(\sum_{i=1}^{b} C(i, b)\right) g(x, a, b) = C'(b)g(x, a, b). \end{aligned} \tag{2.1}$$

Thus we can shorten $f(x, a, b) \ll_{a,b} g(x, a, b)$ to $f(x, a, b) \ll_b g(x, a, b)$.

In practice this means our asymptotic bounds will depend on the ambient number field K, and the dimension n, but not the rank r, since $r < n$.

Notation 2.1.4. *Let L be a field. The following symbols will aid our matrix manipulations.*

- *Throughout this thesis, bold letters will denote column vectors. Let $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_a \in L^b$. Then by $[\boldsymbol{u}_1 \cdots \boldsymbol{u}_a]$ we mean the matrix in $M_{b \times a}(L)$ whose i^{th} column is $\boldsymbol{u}_i$.*
- *$\boldsymbol{e}_1, \ldots, \boldsymbol{e}_b \in L^b$ denote the standard basis vectors and $I_b = [\boldsymbol{e}_1 \ldots \boldsymbol{e}_b]$ denote the $m \times m$ identity matrix.*
- *If A is a matrix, A_{ij} refers to the entry of A in row i column j.*
- *For any ring R, $M_b(R)_{alt}$ denotes the set of alternating $b \times b$ matrices with entries in R. In all cases we consider $char(R) \neq 2$, so $M_b(R)_{alt} = \{A \in M_b(R) : A^t = -A\}$.*
- *Fix $b > 0$. For any $1 \leq i < j \leq b$, we write E^{ij} to mean the alternating $b \times b$ matrix that is zero everywhere except at $(E^{ij})_{ij} = 1$ and $(E^{ij})_{ji} = -1$.*
- *We let $\mathcal{E}^b := \{E^{ij} : 1 \leq i < j \leq b\}$ be the standard basis of alternating matrices.*
- *If $F : X \to Y$ is a linear map and $\mathcal{X}, \mathcal{Y}$ are bases of vector spaces X, Y respectively, then $[F]_{\mathcal{X}}^{\mathcal{Y}}$ denotes the matrix of F with respect to those bases. When the exponents are clear from context, we simplify $[F]_{\mathcal{E}^b}^{\mathcal{E}^a}$ to $[F]_{\mathcal{E}}$.*
- *All vector spaces in this work are assumed finite.*

Checking the following fact is a fun exercise for one's working memory.

Fact 2.1.5. *Let R be a ring and let $A = [\boldsymbol{a}_1 \cdots \boldsymbol{a}_b] \in M_{a \times b}(R)$ and $B = [\boldsymbol{b}_1 \cdots \boldsymbol{b}_b] \in M_{c \times b}(R)$. Then we have*

$$AB^t = \sum_{i=1}^{b} \boldsymbol{a}_i \boldsymbol{b}_i^t.$$

Definition 2.1.6. *On the complex vector space $\mathbb{C}^b$, by the **standard complex inner product** we mean the map $\langle\ ,\ \rangle : \mathbb{C}^b \times \mathbb{C}^b \to \mathbb{C}$ given by*

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle := \sum_{i=1}^{b} \overline{\boldsymbol{x}_i} \boldsymbol{y}_i = \boldsymbol{x}^* \boldsymbol{y}.$$

Note that the conjugation is on the first input. We denote the induced norm by

$$||\boldsymbol{x}|| := \langle \boldsymbol{x}, \boldsymbol{x} \rangle^{1/2} = (\sum_{i=1}^{b} |x_i|^2)^{1/2}.$$

The inner product and norm are extended to matrices $A, B \in M_{b\times a}(\mathbb{C})$ via

$$\langle A, B \rangle := \sum_{1\leq i,j\leq a,b} \overline{A_{ij}} B_{ij}, \text{ and } ||A|| := \langle A, A \rangle^{1/2}.$$

2.2 Lattices

This thesis contains many lattice-inspired arguments about $\mathcal{O}_K$-modules. Because the following definitions will soon be generalized to such modules, we emphasize when we are speaking about the *lattice*-rank versus the *module*-rank.

Definition 2.2.1. *Let $\mathcal{V}$ be a real vector space with inner product $\langle\ ,\ \rangle_{\mathcal{V}} : \mathcal{V} \times \mathcal{V} \to \mathbb{R}$. A **lattice** is a subgroup $\Sigma \subset \mathcal{V}$ of the form $\Sigma = \mathbb{Z}\boldsymbol{x}_1 + \cdots + \mathbb{Z}\boldsymbol{x}_a$ for some $\mathbb{R}$-linearly independent vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_a$. The set of $\boldsymbol{x}_i$ form a **lattice-basis** of Σ. The number of basis vectors is a constant associated to Σ and called the **(lattice-)rank** of Σ. The value $\mathfrak{d}(\Sigma) := |\det(\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle_{ij})|^{1/2}$ is Σ's **(lattice-)discriminant**. One can check $\mathfrak{d}(\Sigma)$ is independent of the choice of basis.*

A standard result shows lattices are automatically discrete (that is, every point of the lattice is an isolated point) [Neu99, Prop 4.2].

Warning 2.2.2. *The requirement that the basis vectors $\boldsymbol{x}_i$ be linearly independent over $\mathbb{R}$ is strictly stronger than requiring $\mathbb{Z}\boldsymbol{x}_1 + \cdots + \mathbb{Z}\boldsymbol{x}_a$ be a direct sum. This stronger condition is necessary for "discreteness" of the lattice. For a non-example of a lattice: consider the $\mathbb{Z}$-module $\Gamma = \mathbb{Z}[\sqrt{2}](2, 0, 1) + \mathbb{Z}[\sqrt{2}](0, 0, 1) \subset \mathbb{R}^3$. Indeed, the sum*

$$\Gamma = \mathbb{Z}(2, 0, 0) + \mathbb{Z}(2\sqrt{2}, 0, 0) + \mathbb{Z}(0, 0, 1) + \mathbb{Z}(0, 0, \sqrt{2})$$

is direct, but, as one can check, Γ does not have a generating set of $\mathbb{R}$-independent vectors.

2.3 Finitely generated $\mathcal{O}_K$-modules

This work adapts the matrix-counting arguments of [EK95] and [PPVW19] from $M_n(\mathbb{Z})_{\text{alt}}$ to $M_n(\mathcal{O}_K)_{\text{alt}}$. Because our matrices have entries in $\mathcal{O}_K$ rather than $\mathbb{Z}$, we use $\mathcal{O}_K$-modules in place of their lattices. Specifically, we consider finitely generated $\mathcal{O}_K$-modules in a finite dimensional K-vector space, $\mathcal{W}$. Let $\Gamma \subset \mathcal{W}$ be one such module. Note that Γ is automatically torsion free via its containment in $\mathcal{W}$[1].

Traditional lattices come equipped with a basis because they are modules over the principal ideal domain (PID) $\mathbb{Z}$. As we noted above, $\mathcal{O}_K$-modules in $\mathcal{W}$ are automatically torsion free. Thus, when $\mathcal{O}_K$ is a PID, any finitely generated $\mathcal{O}_K$-module $\Gamma \subset \mathcal{W}$ is in fact free and armed with a basis.

In general though, $\mathcal{O}_K$ is only a Dedekind domain and Γ may well have no basis. Remarkably, there is an alternative notion of "basis" for finitely generated torsion-free modules over Dedekind domains (such as Γ) that allows many arguments to run analogously to their form in the free case.

Proposition 2.3.1. *Let R be a Dedekind domain with fraction field L, $\mathcal{W}$ an L-vector space and $\Gamma \subset \mathcal{W}$ a finitely generated, torsion-free R-module. Then there exist vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_a \in \mathcal{W}$, and fractional ideals $\mathfrak{U}_1, \ldots, \mathfrak{U}_a \subset L$ of R such that*

$$\Gamma = \mathfrak{U}_1 \boldsymbol{u}_1 + \cdots + \mathfrak{U}_a \boldsymbol{u}_a,$$

*with the sum being direct. The $\mathfrak{U}_i$ are called **coefficient ideals** of Γ and we call the set of pairs $(\mathfrak{U}_1, \boldsymbol{u}_1), \ldots, (\mathfrak{U}_a, \boldsymbol{u}_a)$ a **pseudo-basis** for Γ. The number of vectors in any pseudo-basis of Γ is a constant and called the **(module-)rank** of Γ [Coh00, Cor 1.2.25 and Def 1.4.1].*

Fact 2.3.2. *Let Γ, $\mathcal{W}$, $\{(\mathfrak{U}_i, \boldsymbol{u}_i)\}_{i=1}^{a}$ be as in Proposition 2.3.1.*

1. *For each $i \in \{1, \ldots, a\}$, $1 \in \mathfrak{U}_i$ if and only if $\boldsymbol{u}_i \in \Gamma$. By scaling, one can ensure that all the vectors $\boldsymbol{u}_i$ lie in Γ. Alternatively, one can scale the other way to ensure the ideals $\mathfrak{U}_i$ are contained in R.*

2. *The rank of Γ (i.e. the number of pseudo-basis vectors) agrees with the dimension of $Span_L(\Gamma)$.*

2.4 $\mathcal{O}_K$-modules in $M_n(K)$

This thesis includes both $\mathcal{O}_K$-modules lying in K^n, as well as $\mathcal{O}_K$-modules of matrices contained in $M_n(K)$. Throughout our arguments we will (often implicitly) interpret these matrices as vectors in K^{n^2}. It will be useful to allow such vectors to be indexed by a pair.

[1] Whenever we say $\Gamma \subset \mathcal{W}$ is an $\mathcal{O}_K$-module, we mean that the action of $\mathcal{O}_K$ on Γ is the restriction of the action of K on $\mathcal{W}$.

Notation 2.4.1. *Let the pairs $\{(a,b) : 1 \le a, b \le n\}$ be ordered lexicographically, so $(1,1) \le (1,2) \le \cdots \le (1,n) \le \cdots \le (n,n)$.*

Using this ordering, we will speak of the (a,b) entry of a vector $\boldsymbol{v} \in K^{n^2}$.

Definition 2.4.2. *For $1 \le a, b \le n$, let $\boldsymbol{e}_{ab} \in K^{n^2}$ be the standard basis vector with value 1 in position (a,b) and zeros elsewhere.*

Definition 2.4.3. *Let $\iota : M_n(K) \to K^{n^2}$ be the isomorphism given by $\iota(A) = \sum_{ab} A_{ab}\boldsymbol{e}_{ab}$ for any $A \in M_n(K)$.*

Typically, we will define a given property for finitely generated $\mathcal{O}_K$-modules in K^b, and then extend this definition to $\mathcal{O}_K$-modules of matrices, $\Gamma \subset M_n(K)$, by viewing Γ as the vector module $\iota(\Gamma) \subset K^{n^2}$.

2.5 The Minkowski Embedding

This section is dedicated to defining several maps, in particular several variations of the traditional Minkowski embedding of a number field. These will allow us to embed any $\mathcal{O}_K$-module living in K^b into a real vector space, where we will be able to view the module's image as a lattice and make use of norms and discriminants.

Definition 2.5.1. *Recall $s = [K : \mathbb{Q}]$. Let $K_{\mathbb{C}} := \mathbb{C}^s$. We index the components of $\mathbb{C}^s$ by some ordering of the s complex embeddings $\tau : K \to \mathbb{C}$. E.g. $\boldsymbol{x}_\tau$ is one component of the vector $\boldsymbol{x} \in K_{\mathbb{C}}$. Then the **Minkowski space** of K is the subset $K_{\mathbb{R}} := \{\boldsymbol{x} \in K_{\mathbb{C}} : \overline{\boldsymbol{x}_\tau} = \boldsymbol{x}_{\overline{\tau}}\}$. One can check that $K_{\mathbb{R}}$ is a real vector space, and that the complex inner product $\langle \boldsymbol{x}, \boldsymbol{y}\rangle := \sum_\tau \overline{\boldsymbol{x}_\tau}\boldsymbol{y}_\tau$ and norm $||\boldsymbol{x}|| = \langle \boldsymbol{x}, \boldsymbol{x}\rangle^{1/2}$ on $K_{\mathbb{C}}$ restrict to a real inner product and norm (respectively) on $K_{\mathbb{R}}$.*

More generally, for any $b \in \mathbb{Z}_{\ge 0}$, we will refer to $K_{\mathbb{R}}^b \subset \mathbb{C}^{sb}$ as the Minkowski space of K^b. The complex inner product and norm again restrict to a real inner product and norm on $K_{\mathbb{R}}^b$ and will again be denoted by $\langle\ ,\ \rangle$ and $||\cdot||$, respectively.

Definition 2.5.2. *Let $\tau_1, \ldots, \tau_s : K \to \mathbb{C}$ be the complex embeddings of K. For vectors $\boldsymbol{u} = (u_1, \ldots, u_b)^t \in K^b$ and matrices $A \in M_{a\times b}(K)$, τ_z is applied element-wise. Thus*

$$\tau_z(\boldsymbol{u}) = (\tau_z(u_1), \ldots, \tau_z(u_b))^t \in \mathbb{C}^b,$$

and

$$\tau_z(A) \in M_{a\times b}(\mathbb{C}) \text{ with } (\tau_z(A))_{ij} = \tau_z(A_{ij}) \text{ for all } ij.$$

Definition 2.5.3. *For $\boldsymbol{u} = (u_1, \ldots, u_b)^t \in K^b$, let $\mu : K^b \to \mathbb{C}^{bs}$ be given by*

$$\mu(\boldsymbol{u}) := \begin{pmatrix} \tau_1(\boldsymbol{u}) \\ \vdots \\ \tau_s(\boldsymbol{u}) \end{pmatrix} = (\tau_1(u_1), \ldots, \tau_1(u_n), \ldots, \tau_s(u_1), \ldots, \tau_s(u_b))^t \in \mathbb{C}^{bs}.$$

We call μ the ***Minkowski embedding*** *(or map) of K^b into $K_{\mathbb{R}}^b \subset \mathbb{C}^{bs}$.*

When $b = 1$ we will simply write $\mu(u)$ for $u \in K$. If $A \in M_{a\times b}(K)$ then $\mu(A)$ denotes the block matrix

$$\mu(A) := \begin{pmatrix} \tau_1(A) \\ \vdots \\ \tau_s(A) \end{pmatrix} \in M_{as\times b}(\mathbb{C}).$$

The Minkowski embedding allows us to pull the complex norm (Definition 2.5.1) back from $K_{\mathbb{R}}^b$ to K^b.

Definition 2.5.4. *For $\boldsymbol{u} = (u_1, \dots, u_b)^t \in K^b$ we let*

$$||\boldsymbol{u}||_\mu := ||\mu(\boldsymbol{u})|| = \left(\sum_{i=1}^{b} \sum_{z=1}^{s} |\tau_z(u_i)|^2 \right)^{1/2}.$$

Likewise, for any matrix $A \in M_{a\times b}(K)$, the Minkowski norm *of A is*

$$||A||_\mu := ||\mu(A)|| = \left(\sum_{\substack{1\le i\le a \\ 1\le j\le b}} \sum_{\tau:K\to\mathbb{C}} |\tau(A_{ij})|^2 \right)^{1/2}.$$

Remark 2.5.5. *Because the non-real embeddings $\tau : K \to \mathbb{C}$ come in conjugate pairs, and because $|\overline{\tau(x)}| = |\tau(x)|$ for all $x \in K$, the inner sum in Definition 2.5.4 will include these values twice. One could consider a modified version of $||\cdot||$ where factors of $\frac{1}{2}$ are added to the components corresponding to non-real embeddings (see Neukirch's discussion after Proposition 5.1 in [Neu99, Chapter 1]). However, once Theorem 1.1.1 has been proven for one choice of complex norm $||\cdot||$ it holds for all. One can see this by viewing Theorem 1.1.1 as an asymptotic count of the complex "vectors"*

$$\{\mu(A) \in M_{ns\times n}(\mathbb{C}) : A \in M_n(\mathcal{O}_K)_{alt}, rk(A) = r\}$$

with $||\mu(A)|| < X$. By the equivalence of norms on finite dimensional complex vector spaces, given any other norm, $||\cdot||_2$, there exists constants $C_1, C_2 > 0$ such that $C_1||\cdot||_2 < ||\cdot|| < C_2||\cdot||_2$. Thus the matrices A with $||\mu(A)||_2 < X$ satisfy $||\mu(A)|| < C_2X$ and there are asymptotically at most $(C_2X)^{nrs/2}$ of them by Theorem 1.1.1. Similarly, the theorem implies there are at least $(C_1X)^{nrs/2}$ matrices $\mu(A) \in M_{ns\times n}(\mathbb{C})$ with $||\mu(A)||_2 < X$, because all matrices with $||\mu(A)|| < C_1X$ satisfy $||\mu(A)||_2 < \frac{1}{C_1}||\mu(A)|| < X$.

Remark 2.5.6. *Note that for any $A \in M_{a\times b}(K)$, $||A||_\mu = ||\iota(A)||_\mu$. Thus when $\Gamma \subset M_n(K)$ is an $\mathcal{O}_K$-module of matrices, the norms of its elements as matrices in $M_n(K)$ and as vectors in K^{n^2} agree.*

The Minkowski map also has the interesting ability to embed the $\mathbb{Q}$-vector space K^b into $\mathbb{C}^{bs}$ in such a way that $\mathbb{Q}$-linearly independent vectors become $\mathbb{C}$-linearly independent.

Lemma 2.5.7. *Let $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_a \in K^b$ be $\mathbb{Q}$-linearly independent. Then $\mu(\boldsymbol{u}_1), \ldots, \mu(\boldsymbol{u}_a) \in \mathbb{C}^{sb}$ are $\mathbb{C}$-linearly independent (and thus in particular $\mathbb{R}$-linearly independent, when viewed in $K^b_{\mathbb{R}}$).*

Proof. By extending the set if necessary, we may assume $a = sb$ so the $\boldsymbol{u}_i$ form a basis for K^b over $\mathbb{Q}$.

Let $\theta \in \overline{\mathbb{Q}}$ be a primitive element for K, i.e. $K = \mathbb{Q}(\theta)$. Consider the following $\mathbb{Q}$-basis of K^b: $\boldsymbol{v}_{i,j} := \theta^i \boldsymbol{e}_j$ for $i = 0, \ldots, s-1$ and $j = 1, \ldots, b$. Our goal is to show the $\mu(\boldsymbol{v}_{ij})$ form a $\mathbb{C}$-basis of $\mathbb{C}^{sb}$. Then, because the $\boldsymbol{u}_i$ span the $\boldsymbol{v}_{ij}$ over $\mathbb{Q}$, and μ is $\mathbb{Q}$-linear, it follows that the $\mu(\boldsymbol{u}_i)$ are a $\mathbb{C}$-basis as well. Thus it suffices to show the claim for the $\boldsymbol{v}_{ij}$.

Consider the matrix $A = [\mu(\boldsymbol{v}_{0,1})\ \mu(\boldsymbol{v}_{1,1}) \cdots \mu(\boldsymbol{v}_{s-1,b})] \in M_{sb}(\mathbb{C})$. After rearranging the rows, one sees it is row equivalent to a block-diagonal matrix A', where each of the b diagonal blocks is of the form

$$\begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{s-1} \\ 1 & \theta_2 & \cdots & \theta_2^{s-1} \\ & & \vdots & \\ 1 & \theta_{s-1} & \cdots & \theta_{s-1}^{s-1} \end{pmatrix} \in M_s(\mathbb{C}),$$

where $\theta = \theta_1$ and $\theta_2, \ldots, \theta_{s-1}$ are the roots of θ's minimal polynomial over $\mathbb{Q}$. This is a Vandermonde matrix, and its determinant is $\prod_{0 \leq i < j \leq s-1} (\theta_i - \theta_j) \neq 0$. It follows that $\det(A) \neq 0$, and thus the $\mu(\boldsymbol{v}_{ij})$ are linearly independent. Since there are sb of them, they form a basis for $\mathbb{C}^{sb}$, as desired. □

Lemma 2.5.7 allows us to investigate $\mu(\Gamma)$ using tools from lattice theory.

Fact 2.5.8. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module. Then $\mu(\Gamma) \subset K^b_{\mathbb{R}}$ is a lattice.*

Proof. Indeed, Γ is a torsion-free $\mathbb{Z}$-module, and therefore has a basis over $\mathbb{Z}$. Since the elements of this $\mathbb{Z}$-basis must be $\mathbb{Q}$-linearly independent, their images under μ will form an $\mathbb{R}$-linearly independent basis of $\mu(\Gamma)$ by Lemma 2.5.7. Note that if a is the module-rank of Γ then the lattice-rank is sa. □

We can now extend the definition of the discriminant from lattices to $\mathcal{O}_K$-modules, admittedly in a fairly naive way. This discriminant will get a nicer expression later on in the section.

Definition 2.5.9. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module. Then the **(module-)discriminant**, $\mathfrak{D}(\Gamma)$ of Γ is defined to be the lattice-discriminant of the lattice $\mu(\Gamma)$. That is, letting $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_a \in K^b_{\mathbb{R}}$ be a lattice-basis for $\mu(\Gamma)$, we have*

$$\mathfrak{D}(\Gamma) := \mathfrak{d}(\mu(\Gamma)) = |\det((\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle)_{ij})|^{1/2}.$$

Notation 2.5.10. *If $\Gamma \subset M_n(K)$ is a finitely generated $\mathcal{O}_K$-module of matrices we also use $\mathfrak{D}(\Gamma)$ to denote what is technically the module-discriminant of $\iota(\Gamma) \subset K^{n^2}$, $\mathfrak{D}(\iota(\Gamma))$.*

Definition 2.5.11. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module. Let $(\mathfrak{U}_1, \boldsymbol{u}_1), \dots, (\mathfrak{U}_a, \boldsymbol{u}_a)$ be a pseudo-basis for Γ. We will refer to the matrix $U = [\boldsymbol{u}_1 \cdots \boldsymbol{u}_a] \subset M_{b\times a}(K)$ as the* ***basis matrix of*** *Γ associated to the given pseudo-basis.*

Notation 2.5.12. *If $\Gamma \subset M_n(K)$ is a finitely generated $\mathcal{O}_K$-module of matrices with pseudo-basis $(\mathfrak{U}_1, U^1), \dots, (\mathfrak{U}_a, U^a)$ (i.e. $U^i \in M_n(K)$) then when we speak of the associated* ***basis matrix*** *we mean the $n^2 \times a$ matrix $U = [\iota(U^1) \cdots \iota(U^a)]$.*

Definition 2.5.13. *For $A \in M_{a\times b}(K)$, let $\varphi(A) \in M_{as\times bs}(\mathbb{C})$ be the block diagonal matrix*

$$\varphi(A) := \begin{pmatrix} \tau_1(A) & & \\ & \ddots & \\ & & \tau_s(A) \end{pmatrix} \in M_{as\times bs}(\mathbb{C}).$$

When $a = b = 1$ we will simply write $\varphi(u) := \varphi([u])$ for $u \in K$.

We recall the field norm and discriminant of K.

Definition 2.5.14. *Let $\alpha_1, \dots, \alpha_s$ be a $\mathbb{Z}$-module basis of the ring of integers $\mathcal{O}_K$. Then the discriminant of K is*

$$d_K := \det((\tau_i(\alpha_j))_{ij})^2 \in \mathbb{Z}.$$

Definition 2.5.15. *The (field) norm of an element $u \in K$ is*

$$N_{K/\mathbb{Q}}(u) := \prod_{z=1}^{s} \tau_z(u) = \det(\varphi(u)) \in \mathbb{Q}.$$

The norm of an ideal $\mathfrak{V} \subset \mathcal{O}_K$ is

$$N_{K/\mathbb{Q}}(\mathfrak{V}) := [\mathcal{O}_K : \mathfrak{V}] \text{ or } 0, \text{ if } \mathfrak{V} = \{0\}.$$

In either case the norm is multiplicative (e.g. $N_{K/\mathbb{Q}}(\mathfrak{V}_1\mathfrak{V}_2) = N_{K/\mathbb{Q}}(\mathfrak{V}_1)N_{K/\mathbb{Q}}(\mathfrak{V}_2)$). The ideal-norm can be uniquely extended to a multiplicative norm on fractional ideals. On principal ideals the two norms "agree" with $N_{K/\mathbb{Q}}((u)) = |N_{K/\mathbb{Q}}(u)|$ for all $u \in K$. Finally, if $u_1, \dots, u_s \in K$ form a $\mathbb{Z}$-basis for $\mathfrak{V}$, then

$$d_K \cdot N_{K/\mathbb{Q}}(\mathfrak{V})^2 = \det([\mu(u_1) \cdots \mu(u_s)])^2. \tag{2.2}$$

[Neu99, Chapter1, Prop 2.12]

It turns out that τ, μ and φ play nicely with matrix multiplication. Indeed, one can check we have the following results.

Fact 2.5.16. *Let $\tau : K \to \mathbb{C}$ be a complex embedding. Then for compatibly-sized matrices A, B and vector $\boldsymbol{u}$, all with entries in K, we have*

1. *$\tau(AB) = \tau(A)\tau(B)$, which implies $\varphi(AB) = \varphi(A)\varphi(B)$.*

2. *$\tau(A)\tau(\boldsymbol{u}) = \tau(A\boldsymbol{u})$, which implies $\varphi(A)\mu(\boldsymbol{u}) = \mu(A\boldsymbol{u})$ and in turn $\varphi(A)\mu(B) = \mu(AB)$.*

3. *$\varphi(A^t) = \varphi(A)^t$.*

4. *$\det(\tau(A)) = \tau(\det(A))$, when A is a square matrix, and it follows that $N_{K/\mathbb{Q}}(\det(A)) = \det(\varphi(A))$.*

Proposition 2.5.17. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module with pseudo-basis $(\mathfrak{U}_1, \boldsymbol{u}_1), \dots, (\mathfrak{U}_a, \boldsymbol{u}_a)$. Let $U = [\boldsymbol{u}_1 \dots \boldsymbol{u}_a] \in M_{b\times a}(K)$ be the associated basis matrix and let $\mathfrak{U} = \prod_{i=1}^a \mathfrak{U}_i$ be the product[2]. Then the module-discriminant of Γ satisfies*

$$\mathfrak{D}(\Gamma) = |d_K|^{a/2} |\det(\varphi(U)^*\varphi(U))|^{1/2} |N_{K/\mathbb{Q}}(\mathfrak{U})|. \tag{2.3}$$

Proof. Let $w_{i,1}, \dots, w_{i,s} \in K$ be a $\mathbb{Z}$-basis of $\mathfrak{U}_i$, i.e. $\mathfrak{U}_i = \mathbb{Z}w_{i,1} + \cdots + \mathbb{Z}w_{i,s}$ for all i. By Lemma 2.5.7, $\mu(\Gamma)$ is a lattice and the set

$$\{\boldsymbol{x}_{ij} := \mu(w_{ij}\boldsymbol{u}_i) : 1 \le i \le a,\ 1 \le j \le s\}$$

is a lattice-basis of $\mu(\Gamma)$. Let $X = [\boldsymbol{x}_{1,1}\boldsymbol{x}_{1,2} \cdots \boldsymbol{x}_{a,s}] \in M_{sb\times sa}(\mathbb{C})$. Then Definition 2.5.9 becomes

$$\mathfrak{D}(\Gamma) = \mathfrak{d}(\mu(\Gamma)) = |\det(\langle \boldsymbol{x}_{ij}, \boldsymbol{x}_{xy}\rangle_{ij,xy})|^{1/2} = |\det(X^*X)|^{1/2},$$

where X^* is the conjugate of X.

Let $M = [(w_{1,1}\boldsymbol{u}_1)(w_{1,2}\boldsymbol{u}_1) \cdots (w_{a,s}\boldsymbol{u}_a)] \in M_{b\times sa}(K)$. We have $X = \mu(M)$ so

$$\mathfrak{D}(\Gamma) = |\det(\mu(M)^*\mu(M))|^{1/2}. \tag{2.4}$$

Let $U = [\boldsymbol{u}_1 \cdots \boldsymbol{u}_a] \in M_{b\times a}(K)$ and

$$W = \begin{pmatrix} w_{1,1}\dots w_{1,s} & & & \\ & w_{2,1}\dots w_{2,s} & & \\ & & \ddots & \\ & & & w_{a,1}\dots w_{a,s} \end{pmatrix} \in M_{a\times sa}(K).$$

Then $M = UW$, so by Fact 2.5.16, $\mu(M) = \varphi(U)\mu(W)$. Also, by exchanging rows, one sees $\mu(W)$ shares its determinant with an equivalent block diagonal matrix $\widetilde{\mu(W)}$ where block (i,i) of $\widetilde{\mu(W)}$ is

$$\begin{pmatrix} \tau_1(w_{i,1}) & \cdots & \tau_1(w_{i,s}) \\ \vdots & & \vdots \\ \tau_s(w_{i,1}) & \cdots & \tau_s(w_{i,s}) \end{pmatrix} = ([\mu(w_{i,1}) \cdots \mu(w_{i,s})]).$$

Thus

$$\begin{aligned} \det(\mu(W))^2 = \det(\widetilde{\mu(W)})^2 &= \prod_{i=1}^a \det([\mu(w_{i,1}) \cdots \mu(w_{i,s})])^2 \\ &= \prod_{i=1}^a d_K \cdot N_{K/\mathbb{Q}}(\mathfrak{U}_i)^2, \end{aligned} \tag{2.5}$$

[2] This is the Steinitz class of Γ.

where we've used equation 2.2 for the last equality.

Finally, combining equations 2.4 and 2.5, and using that $\mu(M) = \varphi(U)\mu(W)$, we have

$$\begin{aligned}\mathfrak{D}(\Gamma)^2 &= |\det(\mu(M)^*\mu(M))| \\ &= |\det(\varphi(U)^*\varphi(U))||\det(\mu(W))|^2 \\ &= |\det(\varphi(U)^*\varphi(U))||d_K|^a|\prod_{i=1}^{a} N_{K/\mathbb{Q}}(\mathfrak{U}_i)^2|.\end{aligned}$$

The claim follows. □

Any nonzero lattice has nonzero discriminant. Combining this with Proposition 2.5.17 implies that the matrix used to compute $\mathfrak{D}(\Gamma)$ has nonzero determinant.

Corollary 2.5.18. *Let $\Gamma \subset K^b$ be a finitely generated, nonzero, $\mathcal{O}_K$-module with basis matrix $U = [\boldsymbol{u}_1 \dots \boldsymbol{u}_a] \in M_{b\times a}(K)$. Then $\varphi(U)^*\varphi(U)$ is non-singular, as are its block-diagonal blocks, $\tau(U)^*\tau(U)$, for all $\tau : K \to \mathbb{C}$.*

To review, given a finitely-generated $\mathcal{O}_K$-module $\Gamma \subset K^b$, we previously defined the module-discriminant of Γ only in terms of μ and the standard inner product on $K^b_{\mathbb{R}}$. Specifically, we had $\mathfrak{D}(\Gamma) := \mathfrak{d}(\mu(\Gamma)) = |\det(\langle \boldsymbol{x}_i, \boldsymbol{x}_j\rangle_{ij})|^{1/2}$, where the $\boldsymbol{x}_i$ were a lattice basis for $\mu(\Gamma)$. We have just shown that this module-discriminant also equals

$$\mathfrak{D}(\Gamma) = |d_K|^{a/2}|\det(\varphi(U)^*\varphi(U))|^{1/2}|N_{K/\mathbb{Q}}(\mathfrak{U})|, \tag{2.6}$$

where U and $\mathfrak{U}$ are as defined in Proposition 2.5.17. Note that, information-theoretically, the embedding μ is appearing in equation 2.6 as φ.

Applying Proposition 2.5.17 in the case of a module of matrices gives the following.

Corollary 2.5.19. *Let $\Gamma \subset M_n(K)$ be a finitely generated $\mathcal{O}_K$-module of matrices with pseudo-basis $(\mathfrak{U}_1, U^1), \dots, (\mathfrak{U}_a, U^a)$, for $U^i \in M_n(K)$. Then the module-discriminant of Γ satisfies*

$$\mathfrak{D}(\Gamma) = \mathfrak{D}(\iota(\Gamma)) = |d_K|^{a/2}|\det(\varphi(U)^*\varphi(U))|^{1/2}|N_{K/\mathbb{Q}}(\mathfrak{U})|,$$

where $U = [\iota(U^1) \dots \iota(U^a)] \in M_{n^2\times a}(K)$ is the associated basis matrix and $\mathfrak{U} = \prod_{i=1}^{a} \mathfrak{U}_i$.

Remark 2.5.20. *The form of the module-discriminant appearing in Proposition 2.5.17 agrees up to a constant factor with the definitions of Thunder [Thu92] (see Remark 6.0.10 for details) and Fieker-Stehlé [FS10].*

Warning 2.5.21. *The ring of integers $\mathcal{O}_K$ is itself an example of an $\mathcal{O}_K$-module contained in K. In this case our module-discriminant, $\mathfrak{D}(\cdot)$, differs from the usual number field discriminant of K (which is sometimes also described as a discriminant of $\mathcal{O}_K$) by an absolute value and a power of $1/2$, i.e. $\mathfrak{D}(\mathcal{O}_K) = |d_K|^{1/2}$.*

As in the free case, a finitely generated $\mathcal{O}_K$-module can have multiple equivalent pseudo-bases.

Proposition 2.5.22. *Let $((\mathfrak{U}_i, \boldsymbol{u}_i))_{i=1}^a$ and $((\mathfrak{U}'_i, \boldsymbol{u}'_i))_{i=1}^a$ be two pseudo-bases for an $\mathcal{O}_K$-module $\Gamma \subset K^b$. Let $C \in GL_a(K)$ be such that $[\boldsymbol{u}_1 \cdots \boldsymbol{u}_a]C = [\boldsymbol{u}'_1 \cdots \boldsymbol{u}'_a]$. Then it follows that*

1. $C_{ij} \in \mathfrak{U}_i \mathfrak{U}'^{-1}_j$.
2. $\prod_{i=1}^a \mathfrak{U}'_i \det(C) = \prod_{i=1}^a \mathfrak{U}_i$.

Conversely, if $((\mathfrak{U}_i, \boldsymbol{u}_i))_{i=1}^a$ is a pseudo-basis for $\mathcal{O}_K$-module $\Gamma \subset K^b$ and there exists $C \in GL_a(K)$ and ideals $\mathfrak{U}'_1, \ldots, \mathfrak{U}'_a$ such that items 1 and 2 above are satisfied, then $((\mathfrak{U}'_i, \boldsymbol{u}_i C))_{i=1}^a$ forms a pseudo-basis for Γ [Coh00, Prop 1.4.2].

Though Proposition 2.5.17 showed $\mathfrak{D}(\Gamma)$ can be written in terms of a pseudo-basis, the original definition of the module-discriminant, $\mathfrak{D}(\Gamma) = \mathfrak{d}(\mu(\Gamma))$, reassures us that $\mathfrak{D}(\Gamma)$ is independent of the specific pseudo-basis chosen.

Chapter 3

The module of matrices, $\mathcal{B}(\Lambda)$

Our first goal in this chapter is to construct an $\mathcal{O}_K$-module of matrices, $\mathcal{B}(\Lambda) \subset M_n(K)_{\text{alt}}$ from a module of vectors $\Lambda \subset K^n$. Later, we will show that in all cases we care about $\mathcal{B}(\Lambda) = \mathcal{A}(\Lambda)$, where $\mathcal{A}(\Lambda)$ is the module of matrices whose rows all lie in Λ. Thus, the results we prove here using the simpler structure of $\mathcal{B}(\Lambda)$ will apply to $\mathcal{A}(\Lambda)$ as well, and can help us estimate the number of matrices contributed to $\mathcal{A}_{n,r}^K(X)$ by each $\mathcal{A}(\Lambda)$.

The first section relates $\mathfrak{D}(\mathcal{B}(\Lambda))$ to $\mathfrak{D}(\Lambda)$. In the second we show that $\mathfrak{D}(\Lambda)$ cannot be too large if there exists $A \in \mathcal{B}(\Lambda)$ with $||A||_\mu$ small.

3.1 The discriminants of $\mathcal{B}(\Lambda)$ and Λ

We will need a specialized formula for $\mathfrak{D}(\mathcal{B}(\Lambda))$. The following notation will keep our subscripts from exploding too much in complexity.

Notation 3.1.1. *In this chapter we will encounter several "large" matrices whose rows and columns are naturally indexed into by a pair rather than a single integer. For example, in Definition 3.1.3 we introduce the $\binom{n}{2} \times \binom{r}{2}$ matrix B and will speak about the (xy, ij) entry of B, where $1 \le x < y \le n$ and $1 \le i < j \le r$.*

Similarly, "large" vectors in K^{n^2} will be indexed by a pair and we will speak of the (a, b) entry of a vector $\boldsymbol{v} \in K^{n^2}$ (see also, Notation 2.4.1).

In order for matrix multiplication to work, we fix a consistent lexicographical ordering for each set of pairs we consider. For example, the set of pairs $\{(a, b) : 1 \le a, b \le n\}$ are ordered $(1, 1), (1, 2), \ldots, (1, n), \ldots, (n, n)$.

Definition 3.1.2. *Let $J^{ij} \in M_n(K)$ be the standard basis matrix with 1 in position (i, j) and zeros elsewhere. Let $\mathcal{J}^n := \{J^{ij} : 1 \le i, j \le n\}$.*

Definition 3.1.3. *Let $\Lambda \subset K^n$ be an $\mathcal{O}_K$-module with pseudo-basis $\{(\mathfrak{V}_i, \boldsymbol{\nu}_i)\}_{i=1}^r$ and basis matrix $V = [\boldsymbol{\nu}_1 \cdots \boldsymbol{\nu}_r] \subset M_{n\times r}(K)$. Define*

$$\mathcal{B}(\Lambda) := \{VZV^t : Z \in M_r(K)_{alt}, Z_{ij} \in \mathfrak{V}_i\mathfrak{V}_j\}.$$

One can check $\mathcal{B}(\Lambda) \subset M_n(K)_{alt}$ is itself a rank $r(r-1)/2$ $\mathcal{O}_K$-module with pseudo-basis

$$\{B^{ij} := (\mathfrak{V}_i\mathfrak{V}_j, VE^{ij}V^t) : E^{ij} \in \mathcal{E}^r\}.$$

We think of $\mathcal{B}(\Lambda)$ as the $\mathcal{O}_K$-module $\iota(\mathcal{B}(\Lambda)) \subset K^{n^2}$ with module-discriminant $\mathfrak{D}(\mathcal{B}(\Lambda)) = \mathfrak{D}(\iota(\mathcal{B}(\Lambda)))$.

The pseudo-basis in Definition 3.1.3 involves multiplying the matrices of $\mathcal{E}^r$ by V and V^t. It will be useful to give a name to this action.

Definition 3.1.4. *Let L be a field and $G \in M_{a\times b}(L)$. Then we define $F_G : M_b(L)_{alt} \to M_a(L)_{alt}$ to be the map $F_G(A) = GAG^t$.*

Recall, as described in Notation 2.1.4, that $[F]^{\mathcal{Y}}_{\mathcal{X}}$ denotes the matrix of a linear map $F : X \to Y$ with respect to bases $\mathcal{X}, \mathcal{Y}$ of vector spaces X, Y.

Fact 3.1.5. *Let L be a field and $G \in M_{a\times b}(L)$ be a matrix. Then for all $E^{xy} \in \mathcal{E}^b$*

$$GE^{xy}G^t = \sum_{E^{ij}\in\mathcal{E}^a} G_{ix}G_{jy}E^{ij}. \tag{3.1}$$

In particular, with F_G as in Definition 3.1.4, the (ij, xy) entry of $[F_G]_{\mathcal{E}} := [F_G]^{\mathcal{E}^a}_{\mathcal{E}^b}$ is $G_{ix}G_{jy}$.

Lemma 3.1.6. *Let $\Lambda \subset K^n$ be an $\mathcal{O}_K$-module with pseudo-basis $\{(\mathfrak{V}_i, \boldsymbol{\nu}_i)\}_{i=1}^r$ and basis matrix $V = [\boldsymbol{\nu}_1 \cdots \boldsymbol{\nu}_r] \subset M_{n\times r}(K)$. Let $B := [F_V]^{\mathcal{E}^n}_{\mathcal{E}^r} \in M_{\binom{n}{2}\times\binom{r}{2}}(K)$. Then $\mathcal{B}(\Lambda)$ has module-discriminant*

$$\mathfrak{D}(\mathcal{B}(\Lambda)) = |d_K|^{r(r-1)/4}2^{sr(r-1)/4}|\det(\varphi(B)^*\varphi(B))|^{1/2}|N_{K/\mathbb{Q}}(\mathfrak{V})|^{r-1}, \tag{3.2}$$

where $\mathfrak{V} := \prod_{i=1}^r \mathfrak{V}_i$.

Proof. Let $E = [I]^{\mathcal{J}^n}_{\mathcal{E}^n}$, where I is the identity embedding $M_n(K)_{\text{alt}} \to M_n(K)$. Then $EB = [F_V]^{\mathcal{J}^n}_{\mathcal{E}^r}$, and in particular the ij^{th} column of EB is $\iota(VE^{ij}V^t) = \iota(B^{ij})$. Thus EB is the basis matrix of $\iota(\mathcal{B}(\Lambda))$.

Because the entries of E are all ±1, we have $\varphi(E)^* = \varphi(E^*)$. One can also check that $E^*E = 2I$, where I is the $\binom{n}{2} \times \binom{n}{2}$ identity matrix. Thus

$$\begin{aligned}\varphi(EB)^*\varphi(EB) &= \varphi(B)^*\varphi(E)^*\varphi(E)\varphi(B)\\ &= \varphi(B)^*\varphi(E^*E)\varphi(B) = 2\varphi(B)^*\varphi(B).\end{aligned} \tag{3.3}$$

Inserting equation (3.3) into the module-discriminant formula from Proposition 2.5.17,

$$\mathfrak{D}(\mathcal{B}(\Lambda)) = |d_K|^{r(r-1)/4}|\det(\varphi(EB)^*\varphi(EB))|^{1/2}|N_{K/\mathbb{Q}}(\mathfrak{V}^{r-1})|,$$

then proves the claim. □

Our goal in this chapter is to show $\mathfrak{D}(\mathcal{B}(\Lambda)) \asymp \mathfrak{D}(\Lambda)^{r-1}$. The following lemma will form a core step of the proof.

Lemma 3.1.7. *Let $G \in GL_r(\mathbb{C})$ and $F_G : M_r(\mathbb{C})_{alt} \to M_r(\mathbb{C})_{alt}$ be as in Definition 3.1.4. Then* $\det(F_G) = \det(G)^{r-1}$.

Proof. Let $f : GL_r(\mathbb{C}) \to \mathbb{C}^*$ be the group homomorphism sending $G \in GL_r(\mathbb{C})$ to $\det(F_G)$. Note that the determinant, $\det : GL_r(\mathbb{C}) \to \mathbb{C}^*$, is also a group homomorphism.

By [Lan02, Chapter XIII Theorem 8.3]

$$SL_r(\mathbb{C}) = [GL_r(\mathbb{C}), GL_r(\mathbb{C})] := \{ABA^{-1}B^{-1} : A, B \in GL_r(\mathbb{C})\}.$$

Because its target is abelian, f sends $[GL_r(\mathbb{C}), GL_r(\mathbb{C})]$ to zero. Thus $\ker(f)$ contains $SL_r(\mathbb{C}) = \ker(\det)$ and it follows that $f = g \circ \det$ for some $g \in \mathrm{Hom}(\mathbb{C}^*)$.

Let $x \in \mathbb{C}^*$ and $x^{1/r} \in \mathbb{C}^*$ be any root. Let I_r be the $r \times r$ identity matrix. Then $f(x^{1/r}I_r) = \det([A \mapsto x^{2/r}A]_{\mathcal{E}}) = \det(x^{2/r}I_{r(r-1)/2}) = x^{r-1}$. Thus for all $x \in \mathbb{C}^*$, since $x = \det(x^{1/r}I_r)$, we have

$$g(x) = g(\det(x^{1/r}I_r)) = f(x^{1/r}I_r) = x^{r-1}.$$

This proves the claim. □

We are now prepared to prove the main result of this chapter.

Proposition 3.1.8. *Let $\Lambda \subset K^n$ be a finitely generated, rank r, $\mathcal{O}_K$-module. Then*

$$\mathfrak{D}(\mathcal{B}(\Lambda)) = \left(\frac{2^s}{|d_K|}\right)^{r(r-1)/4} \mathfrak{D}(\Lambda)^{r-1}.$$

Proof. Let $\{(\mathfrak{V}_i, \boldsymbol{\nu}_i)\}_{i=1}^r$ be Λ's pseudo-basis and $V = [\boldsymbol{\nu}_1 \cdots \boldsymbol{\nu}_r] \in M_{n\times r}(K)$ be the associated basis matrix. As in Lemma 3.1.6, let $B = [F_V]_{\mathcal{E}^r}^{\mathcal{E}^n}$, or $[F_V]_{\mathcal{E}}$, for short.

By Lemma 3.1.6,

$$\mathfrak{D}(\mathcal{B}(\Lambda)) = |d_K|^{r(r-1)/4} 2^{sr(r-1)/4} |\det(\varphi(B)^*\varphi(B))|^{1/2} |N_{K/\mathbb{Q}}(\mathfrak{V})|^{r-1},$$

while

$$\mathfrak{D}(\Lambda) = |d_K|^{r/2} |\det(\varphi(V)^*\varphi(V))|^{1/2} |N_{K/\mathbb{Q}}(\mathfrak{V})|.$$

Thus it suffices to prove $\det(\varphi(B)^*\varphi(B)) = \det(\varphi(V)^*\varphi(V))^{r-1}$. Thanks to the block-diagonal structure of the matrices on either side, this is in turn equivalent to showing

$$\det(\tau(B)^*\tau(B)) = \det(\tau(V)^*\tau(V))^{r-1}, \tag{3.4}$$

for all embeddings $\tau : K \to \mathbb{C}$.

Consider first the rational square case, i.e. when $K = \mathbb{Q}$ and $n = r$. Because V is then in $GL_r(\mathbb{Q})$, Lemma 3.1.7 implies $\det([F_V]_{\mathcal{E}}) = \det(V)^{r-1}$. Since $B = [F_V]_{\mathcal{E}}$, in this case $\det(B) = \det(V)^{r-1}$, which implies (3.4).

In order to apply Lemma 3.1.7 in the general case, we need to massage $\tau(B)^*\tau(B)$ into a more useful form. Specifically, we will show $\tau(B)^*\tau(B)$ is itself of the form $[F_G]_{\mathcal{E}}$ so Lemma 3.1.7 can be applied to the entire thing.

We proceed in several steps.

Claim 3.1.9. $[F_{\tau(V)}]_{\mathcal{E}} = \tau([F_V]_{\mathcal{E}})$.

Recall by $[F_{\tau(V)}]_{\mathcal{E}}$ we mean $[F_{\tau(V)}]_{\mathcal{E}^r}^{\mathcal{E}^n}$. By Fact 3.1.5, the (ij, xy) entry of $\tau([F_V]_{\mathcal{E}})$ is $\tau(V_{ix}V_{jy})$ and the (ij, xy) entry of $[F_{\tau(V)}]_{\mathcal{E}}$ is $(\tau V)_{ix}(\tau V)_{jy} = \tau(V_{ix}V_{jy})$.

Claim 3.1.10. $[F_{\tau(V)^*}]_{\mathcal{E}} = [F_{\tau(V)}]_{\mathcal{E}}^*$.

Indeed, Fact 3.1.5 implies the (xy, ij) entry of $[F_{\tau(V)}]_{\mathcal{E}}^*$ is $\overline{\tau(V)_{ix}\tau(V)_{jy}}$ and that the (xy, ij) entry of $[F_{\tau(V)^*}]_{\mathcal{E}}$ is $\tau(V)^*_{xi}\tau(V)^*_{yj} = \overline{\tau(V)_{ix}\tau(V)_{jy}}$.

Claim 3.1.11. *For any embedding $\tau : K \to \mathbb{C}$, $\tau(B)^*\tau(B) = [F_{\tau(V)^*\tau(V)}]_{\mathcal{E}}$.*

For all $A \in M_r(\mathbb{C})_{\text{alt}}$ we have

$$F_{\tau(V)^*\tau(V)}(A) = (\tau(V)^*\tau(V))A(\tau(V)^*\tau(V))^t = F_{\tau(V)^*}(F_{\tau(V)}(A)).$$

So $F_{\tau(V)^*\tau(V)} = F_{\tau(V)^*} \circ F_{\tau(V)}$. Combining this fact with claims 3.1.10 and 3.1.9 we have

$$\begin{aligned}[F_{\tau(V)^*\tau(V)}]_{\mathcal{E}} &= [F_{\tau(V)^*}]_{\mathcal{E}}[F_{\tau(V)}]_{\mathcal{E}} \\ &= [F_{\tau(V)}]_{\mathcal{E}}^*[F_{\tau(V)}]_{\mathcal{E}} = \tau([F_V]_{\mathcal{E}})^*\tau([F_V]_{\mathcal{E}}) = \tau(B)^*\tau(B),\end{aligned}$$

proving Claim 3.1.11.

We can at last show equation (3.4) (and thus the entire proposition) for general $r \leq n$ and K. Indeed,

$$\det(\tau(B)^*\tau(B)) = \det([F_{\tau(V)^*\tau(V)}]_{\mathcal{E}}) = \det(\tau(V)^*\tau(V))^{r-1},$$

with the first equality from Claim 3.1.11 and the second by Lemma 3.1.7 (using that $\tau(V)^*\tau(V) \in GL_r(\mathbb{C})$ by Corollary 2.5.18). □

3.2 $\mathfrak{D}(\Lambda)$ is small when $\mathcal{B}(\Lambda)$ contains small matrices

Let $\Lambda \subset K^n$ be a finitely generated $\mathcal{O}_K$-module. In this section we show that if $\mathcal{B}(\Lambda)$ contains at least one rank r matrix of small norm then $\mathfrak{D}(\Lambda)$ must be small as well. They key idea is that any matrix $VZV^t \in \mathcal{B}(\Lambda)$ (with V and Z as in Definition 3.1.3) contains the necessary components for calculating $\mathfrak{D}(\Lambda)$ – namely Λ's basis matrix V, and information about Λ's coefficient ideals in the matrix Z. Indeed, it turns out that a bound on the norm of VZV^t can be turned into a bound on the determinants of the relevant matrices used to compute $\mathfrak{D}(\Lambda)$.

Expressing $||\cdot||_\mu$ in terms of φ will simplify our calculations because, unlike the Minkowski embedding, φ is multiplicative on matrices.

Fact 3.2.1. *Let $A \in M_{a\times b}(K)$. Then $||A||_\mu = ||\varphi(A)||$ because $\varphi(A) \in M_{sa\times sb}(\mathbb{C})$ only differs from $\mu(A) \in M_{sa\times b}$ by additional matrix entries of value zero.*

Proving the main claim of this section is easier when $\Lambda \subset K^n$ is full (i.e. when Λ's rank r equals n). Rotation matrices will allow us to simulate this situation.

Fact 3.2.2. *Let $R \in M_b(\mathbb{C})$. We say R is a (complex) rotation matrix if for all $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{C}^b$, $\langle R\boldsymbol{u}, R\boldsymbol{v}\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$. The following are equivalent*

1. $\langle R\boldsymbol{u}, R\boldsymbol{v}\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$ *for all* $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{C}^b$.
2. $R^*R = RR^* = I_b$.
3. $\langle R^t\boldsymbol{u}, R^t\boldsymbol{v}\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle$ *for all* $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{C}^b$.
4. *For any* $\boldsymbol{u} \in \mathbb{C}^b$, $||R\boldsymbol{u}|| = ||\boldsymbol{u}||$.
5. *For any* $C \in M_{b\times a}(\mathbb{C})$, $||RC|| = ||CR|| = ||C||$.

The next two lemmas allow us to turn a bound on the norm of a matrix into a bound on its determinant.

Lemma 3.2.3. *Let $C \in GL_b(\mathbb{C})$ satisfy $||C|| < X$. Then $|\det(C)| < b!X^b$.*

Proof. We have $|C_{ij}|^2 \leq \sum_{i,j} |C_{ij}|^2 = ||C||^2 < X^2$. Thus, letting S_b denote the symmetric group,

$$|\det(C)| = \left| \sum_{\sigma\in S_b} \left(\operatorname{sgn}(\sigma) \prod_{i=1}^{b} C_{i\sigma(i)} \right) \right| < \sum_{\sigma\in S_b} X^b = b!X^b.$$

□

Lemma 3.2.4. *Let $a \leq b$. Let $C \in M_{b\times a}(\mathbb{C})$ have rank a and let $D \in M_a(\mathbb{C})$. Define $T \in M_{a\times b}(\mathbb{C})$ to be the"truncation matrix" $T = [\boldsymbol{e}_1 \cdots \boldsymbol{e}_a\ \boldsymbol{0} \cdots \boldsymbol{0}] = \left(\begin{smallmatrix} I_a & \boldsymbol{0} \end{smallmatrix} \right)$. Then there exists rotation matrix $R \in M_b(\mathbb{C})$ such that*

$$||TR(CDC^t)R^tT^t|| = ||CDC^t||$$

and

$$|\det(TR(CDC^t)R^tT^t)| = |\det(C^*C)||\det(D)|.$$

In other words, conjugation by TR leaves the norm of CDC^t unchanged, but allows us to compute something like a "determinant" of CDC^t. This will be particularly useful in the case where $\det(CDC^t) = 0$ (which occurs whenever $b > a$) yet $\det(D) \neq 0$.

Proof. Let R be any rotation matrix sending the column space of C onto $\mathrm{Span}_{\mathbb{C}}(\boldsymbol{e}_1, \dots, \boldsymbol{e}_a)$[1]. In other words, $(RC)_{ij} = 0$ when $i > a$. It follows that $A := RCDC^tR^t$ is of the form

$$A = \left(\begin{smallmatrix} A' & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{smallmatrix}\right) \in M_b(\mathbb{C}),$$

for some $A' \in M_a(\mathbb{C})$ and three all-zero matrices, $\mathbf{0}$, of the appropriate sizes. Note that $||A|| = ||A'||$. We also have

$$TAT^t = \left(\begin{smallmatrix} I_a & \mathbf{0} \end{smallmatrix}\right) \left(\begin{smallmatrix} A' & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{smallmatrix}\right) \left(\begin{smallmatrix} I_a \\ \mathbf{0} \end{smallmatrix}\right) = A'.$$

Thus $||TAT^t|| = ||A'|| = ||A||$. Meanwhile, Lemma 3.2.2(5) implies $||A|| = ||CDC^t||$. All together $||TR(CDC^t)R^tT^t|| = ||TAT^t|| = ||A|| = ||CDC^t||$, proving the first claim.

We turn to the second result. Suppose B is a matrix of the form $B = \left(\begin{smallmatrix} B' \\ \mathbf{0} \end{smallmatrix}\right) \in M_{b\times a}(\mathbb{C})$ where $B' \in M_a(\mathbb{C})$. Then $(TB)^*TB = (B')^*B' = B^*B$. Applying this with $B = RC$, and using that $R^*R = I_b$ yields

$$\det((TRC)^*TRC) = \det(C^*C). \tag{3.5}$$

Now, since $TRC \in M_b(\mathbb{C})$ is square, we can split up the following determinant

$$|\det(TRCDC^tR^tT^t)| = |\det(TRC)||\det(D)||\det(C^tR^tT^t)|$$

then conjugate one factor and apply equation 3.5 to obtain

$$|\det(TRCDC^tR^tT^t)| = |\det((TRC)^*TRC)||\det(D)| = |\det(C^*C)||\det(D)|.$$

□

Let $\Lambda \subset K^n$ be an $\mathcal{O}_K$-module with pseudo-basis $\{(\boldsymbol{\nu}_i, \mathfrak{B}_i)\}_{i=1}^r$, V be the associated basis matrix, and VZV with $Z_{ij} \in \mathfrak{B}_i\mathfrak{B}_j$ be a matrix in $\mathcal{B}(\Lambda)$. The next lemma will help us relate $N_{K/\mathbb{Q}}(\mathfrak{B})$ where $\mathfrak{B} := \prod_{i=1}^r \mathfrak{B}_i$ is the product of Λ's coefficient ideals, to $|\det(\varphi(Z)|$.

Lemma 3.2.5. *Let $\mathfrak{B} \subset K$ be a fractional ideal and let $u \in \mathfrak{B}$. Then $|N_{K/\mathbb{Q}}(\mathfrak{B})| \leq |N_{K/\mathbb{Q}}(u)|$.*

Proof. Suppose first that $\mathfrak{B} \subset \mathcal{O}_K$ is integral. Then, as $\mathcal{O}_K$ is a Dedekind Domain, $(u) \subset \mathfrak{B}$ implies $(u) = \mathfrak{B}\mathfrak{Q}$, for some ideal $\mathfrak{Q} \subset \mathcal{O}_K$. Thus

$$N_{K/\mathbb{Q}}(u) = N_{K/\mathbb{Q}}((u)) = N_{K/\mathbb{Q}}(\mathfrak{B})N_{K/\mathbb{Q}}(\mathfrak{Q}) \geq N_{K/\mathbb{Q}}(\mathfrak{B}),$$

because $N_{K/\mathbb{Q}}(\mathfrak{Q}) = [\mathcal{O}_K : \mathfrak{Q}] \in \mathbb{Z}$.

Now, for any fractional ideal $\mathfrak{B} \subset K$, there exists $m \in \mathbb{Z}$ such that $m\mathfrak{B} \subset \mathcal{O}_K$ is an integral ideal. Then $mu \in m\mathfrak{B}$ and by the previous paragraph

$$m^sN_{K/\mathbb{Q}}(u) = N_{K/\mathbb{Q}}(mu) = N_{K/\mathbb{Q}}((mu)) \geq N_{K/\mathbb{Q}}(m\mathfrak{B}) = m^sN_{K/\mathbb{Q}}(\mathfrak{B}).$$

□

[1] For instance, R^{-1} can be constructed by applying Gram-Schmidt to the columns of $[\boldsymbol{c}_1 \cdots \boldsymbol{c}_a\boldsymbol{c}_{a+1} \cdots \boldsymbol{c}_b] \in M_b(\mathbb{C})$, where $\boldsymbol{c}_1, \dots, \boldsymbol{c}_a$ are the columns of C and $\boldsymbol{c}_{a+1}, \dots, \boldsymbol{c}_b$ are any $b - a$ vectors making the whole set linearly independent. Then invert to obtain R.

We are now ready to prove the main result of this section.

Proposition 3.2.6. *Let $0 \leq r \leq n$, with r even and let $X > 0$. Let $\Lambda \subset K^n$ be a finitely generated $\mathcal{O}_K$-module of rank r. Suppose there exists a matrix $A \in \mathcal{B}(\Lambda)$ satisfying $||A||_\mu < X$ and $rk_K(A) = r$. Then*

$$\mathfrak{D}(\Lambda)^2 < |d_K|^r (rs)! X^{rs}.$$

Proof. We may assume $r > 0$, else the result is trivial. Let $((\mathfrak{V}_1, \boldsymbol{\nu}_1), \ldots, (\mathfrak{V}_r, \boldsymbol{\nu}_r))$ be a pseudo-basis of Λ and let $V = [\boldsymbol{\nu}_1 \cdots \boldsymbol{\nu}_r] \in M_{n\times r}(K)$ be the associated basis matrix. Set $\mathfrak{V} := \prod_{i=1}^r \mathfrak{V}_i$.

Because $A \in \mathcal{B}(\Lambda)$, we have $A = VZV^t$ for some $Z \in M_r(K)_{\text{alt}}$ satisfying $Z_{ij} \in \mathfrak{V}_i\mathfrak{V}_j$. In the $r = n$ case, $\varphi(VZV^t)$ is square and non-singular and one could show $\mathfrak{D}(\Lambda)^2 \leq |\det(\varphi(VZV^t))|$ (the reader need not try this now). Lemma 3.2.3 implies that $|\det(\varphi(VZV^t))| < (rs)!X^{rs}$ and so one could obtain $\mathfrak{D}(\Lambda) < \sqrt{(rs)!}X^{rs/2}$.

Unfortunately, when $r < n$, $\varphi(VZV^t)$ is singular and its determinant no longer bounds $\mathfrak{D}(\Lambda)^2$. Instead, we can handle the general $r \leq n$ case by applying an argument like the one above to the matrix $TR\varphi(VZV^t)R^tT^t$, where the truncation matrix $T = \begin{pmatrix} I_{rs} & \mathbf{0} \end{pmatrix} \in M_{rs\times ns}(K)$ and rotation matrix $R \in GL_{ns}(\mathbb{C})$ are as in Lemma 3.2.4.

First, because $\det(Z) \in \mathfrak{V}^2$, Lemma 3.2.5 and Fact 2.5.16(4) imply $|N_{K/\mathbb{Q}}(\mathfrak{V})|^2 \leq |N_{K/\mathbb{Q}}(\det(Z))| = |\det(\varphi(Z))|$. It follows from Proposition 2.5.17 that

$$\begin{aligned}\mathfrak{D}(\Lambda)^2 &= |d_K|^r |\det(\varphi(V)^*\varphi(V))||N_{K/\mathbb{Q}}(\mathfrak{V})|^2 \\ &\leq |d_K|^r |\det(\varphi(V)^*\varphi(V))||\det(\varphi(Z))|.\end{aligned}$$

From Lemma 3.2.4, we have that

$$\mathfrak{D}(\Lambda)^2 \leq |d_K|^r |\det(TR\varphi(VZV^t)R^tT^t)|. \tag{3.6}$$

Lemma 3.2.4 also implies $||TR\varphi(VZV^t)R^tT^t|| = ||\varphi(VZV^t)|| < X$. Thus, by Lemma 3.2.3,

$$|\det(TR\varphi(VZV^t)R^tT^t)| < (rs)!X^{rs}. \tag{3.7}$$

Combining equations (3.6) and (3.7) gives the desired bound on $\mathfrak{D}(\Lambda)$. □

Chapter 4

Primitive $\mathcal{O}_K$-modules and $\mathcal{A}(\Lambda)$

A primitive lattice $\Sigma \subset \mathbb{R}^b$ is one satisfying $\Sigma = \mathrm{Span}_{\mathbb{R}}(\Sigma) \cap \mathbb{Z}^b$ [EK95, Definition 1.1]. In this chapter we translate this definition to $\mathcal{O}_K$-modules in K^b, and show that when Λ is primitive, $\mathcal{B}(\Lambda)$ is the set of alternating matrices whose rows all lie in Λ.

Definition 4.0.1. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module. Then we say Γ is **primitive** if $\Gamma = Span_K(\Gamma) \cap \mathcal{O}_K^b$.*

Note that any primitive module $\Gamma \subset \mathcal{O}_K^b$ is automatically finitely generated because $\mathcal{O}_K$ is noetherian. One can check that the set of primitive, rank a, $\mathcal{O}_K$-modules in K^b are in one to one correspondence with the a-dimensional subspaces of K^b.

A defining characteristic of primitive lattices $\Gamma \subset \mathbb{Z}^b$ is that they are exactly those lattices whose bases can be extended to a basis of $\mathbb{Z}^b$. Indeed, the quotient $\mathbb{Z}^b/\Gamma$ is torsion free (and thus free) if and only if Γ is primitive. Equivalently, there exists a basis of $\mathbb{Z}^b/\Gamma$, to lift and combine with $\Gamma's$ basis into a basis of $\mathbb{Z}^b$, if and only if Γ is primitive.

As the next lemma shows, primitive $\mathcal{O}_K$-modules in K^b share this property of being precisely those modules which have pseudo-bases extending to $\mathcal{O}_K^b$. We will make use of the following notation.

Notation 4.0.2. *Let $\mathcal{W}$ be a K-vector space, $\Gamma \subset \mathcal{W}$ be an $\mathcal{O}_K$-module, and $\mathfrak{U} \subset K$ a fractional ideal. We define their product to be*

$$\mathfrak{U}\Gamma := \left\{ \sum_{i=1}^{n} w_i \boldsymbol{u}_i : n \in \mathbb{N}, w_i \in \mathfrak{U}, \boldsymbol{u}_i \in \Gamma \right\},$$

and note $\mathfrak{U}\Gamma$ is again an $\mathcal{O}_K$-module. Note that if $\mathfrak{U}_1, \mathfrak{U}_2 \subset K$ are two fractional ideals, then $\mathfrak{U}_1(\mathfrak{U}_2\Gamma) = (\mathfrak{U}_1\mathfrak{U}_2)\Gamma$. In particular, $\mathfrak{U}\mathfrak{U}^{-1}\Gamma = \mathcal{O}_K\Gamma = \Gamma$. Furthermore, if $g : \mathcal{W}_1 \to \mathcal{W}_2$ is any K-linear map, and $\Gamma \subset \mathcal{W}_1$ is an $\mathcal{O}_K$-module, then

$$\mathfrak{U}g(\Gamma) = g(\mathfrak{U}\Gamma).$$

Lemma 4.0.3. *Let $\Gamma \subset K^b$ be a primitive $\mathcal{O}_K$-module. Let $(\mathfrak{U}_1, \boldsymbol{u}_1), \ldots, (\mathfrak{U}_a, \boldsymbol{u}_a)$ be a pseudo-basis of Γ. Then there exist $\mathfrak{U}_{a+1}, \ldots, \mathfrak{U}_b \subset K$ and $\boldsymbol{u}_{a+1}, \ldots, \boldsymbol{u}_b \in K^b$ such that $(\mathfrak{U}_1, \boldsymbol{u}_1), \ldots, (\mathfrak{U}_b, \boldsymbol{u}_b)$ forms a pseudo-basis for $\mathcal{O}_K^b$.*

Proof. Let $S = \mathrm{Span}_K(\Gamma)$ and let $\pi : K^b \to K^b/S$ be the quotient map. Then $\pi(\mathcal{O}_K^b)$ is a finitely generated $\mathcal{O}_K$-module whose span has dimension $b-a$. Proposition 2.3.1 and Fact 2.3.2 then imply $\pi(\mathcal{O}_K^b)$ has a pseudo-basis of length $b-a$. Thus there exist fractional ideals $\mathfrak{U}_{a+1}, \ldots, \mathfrak{U}_b \subset K$ and vectors $\boldsymbol{p}_{a+1}, \ldots, \boldsymbol{p}_b \in \pi(K^b)$ such that $\pi(\mathcal{O}_K^b) = \mathfrak{U}_{a+1}\boldsymbol{p}_{a+1} + \cdots + \mathfrak{U}_b\boldsymbol{p}$ and the sum is direct.

Let $i \in \{a+1, \ldots, b\}$. Multiplying $\mathfrak{U}_i\boldsymbol{p}_i \subset \pi(\mathcal{O}_K^b)$ by $\mathfrak{U}_i^{-1}$ shows that $\boldsymbol{p}_i \in \mathfrak{U}_i^{-1}\pi(\mathcal{O}_K^b) = \pi(\mathfrak{U}_i^{-1}\mathcal{O}_K^b)$. Writing $\boldsymbol{p}_i = \pi(\boldsymbol{u}_i)$ for some $\boldsymbol{u}_i \in \mathfrak{U}_i^{-1}\mathcal{O}_K^b$, we have $\mathfrak{U}_i\boldsymbol{p}_i = \mathfrak{U}_i\pi(\boldsymbol{u}_i) = \pi(\mathfrak{U}_i\boldsymbol{u}_i)$. By construction, $\mathfrak{U}_{a+1}\boldsymbol{u}_{a+1}, \ldots, \mathfrak{U}_b\boldsymbol{u}_b$ all lie in $\mathcal{O}_K^b$.

To prove the $\{(\mathfrak{U}_i, \boldsymbol{p}_i)\}_{i=a+1}^b$ extend Γ's pseudo-basis to $\mathcal{O}_K^b$, we show

$$\mathfrak{U}_1\boldsymbol{u}_1 + \cdots + \mathfrak{U}_b\boldsymbol{u}_b = \mathcal{O}_K^b, \tag{4.1}$$

and that the sum on the left is direct.

Let $\boldsymbol{v} \in \mathcal{O}_K^b$. We have $\pi(\boldsymbol{v}) = \sum_{i=a+1}^b w_i\pi(\boldsymbol{u}_i)$ for some $w_i \in \mathfrak{U}_i$. Equivalently, $\boldsymbol{v} - \sum_{i=a+1}^b w_i\boldsymbol{u}_i \in \ker(\pi) = S$, and since $w_i\boldsymbol{u}_i \in \mathcal{O}_K^b$,

$$\boldsymbol{v} - \sum_{i=a+1}^{b} w_i\boldsymbol{u}_i \in \mathcal{O}_K^b \cap S = \Gamma.$$

Thus $\boldsymbol{v}$ has expansion $\boldsymbol{v} = \sum_{i=1}^a w_i\boldsymbol{u}_i + \sum_{i=a+1}^b w_i\boldsymbol{u}_i$ for some $\sum_{i=1}^a w_i\boldsymbol{u}_i \in \Gamma$ and equation (4.1) follows. The $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_b$ span $\mathcal{O}_K^b$ over $\mathcal{O}_K$ and thus also span K^b over K. It follows the $\{\boldsymbol{v}_i\}_{i=1}^b$ must be K-independent and the sum in (4.1) is direct. □

The next lemma will be key in proving the main result of this chapter, Lemma 4.0.6.

Lemma 4.0.4. *Let $a \le b$. Let $\Gamma \subset K^b$ be a primitive $\mathcal{O}_K$-module with pseudo-basis $(\mathfrak{U}_1, \boldsymbol{u}_1), \ldots, (\mathfrak{U}_a, \boldsymbol{u}_a)$ and associated basis matrix $U = [\boldsymbol{u}_1 \cdots \boldsymbol{u}_a] \in M_{b\times a}(K)$. Then there exists a left inverse, $U^{-1} \in M_{a\times b}(K)$, of U satisfying $U^{-1}U = I_a$ and $(U^{-1})_{ij} \in \mathfrak{U}_i$ for all i, j.*

Proof. By Lemma 4.0.3, there exist $\boldsymbol{u}_{a+1}, \ldots, \boldsymbol{u}_b \in K^b$ and $\mathfrak{U}_{a+1}, \ldots, \mathfrak{U}_b \subset K$ extending Γ's pseudo-basis to one of $\mathcal{O}_K^b$. Let $\overline{U} = [\boldsymbol{u}_1 \cdots \boldsymbol{u}_b] \in M_{b\times b}(K)$ be the associated basis matrix. Note that $\mathcal{O}_K\boldsymbol{e}_1 + \cdots \mathcal{O}_K\boldsymbol{e}_b = \mathcal{O}_K^b$ is another pseudo-basis for $\mathcal{O}_K^b$ and the basis matrix in that case is simply I_b. It follows from Proposition 2.5.22 that $\overline{U}$ has an inverse $\overline{U}^{-1} \in GL_b(K)$ with $(\overline{U}^{-1})_{ij} \in \mathfrak{U}_i\mathcal{O}_K^{-1} = \mathfrak{U}_i$ for all i, j.

Set $U^{-1} \in M_{a\times b}(K)$ to be the first a rows of $\overline{U}^{-1}$ to obtain the claim. □

Definition 4.0.5. *Let $\Lambda \subset K^n$ be a finitely generated $\mathcal{O}_K$-module. Define*

$$\mathcal{A}(\Lambda) := \{A \in M_n(K)_{alt} : \text{ every row of } A \text{ lies in } \Lambda\}.$$

Since $\mathcal{O}_K$ is Noetherian, $\mathcal{A}(\Lambda)$ is a finitely generated $\mathcal{O}_K$-module.

As we'll see, for every alternating matrix A of $M_n(K)_{\text{alt}}$ there is some primitive $\Lambda \subset K^n$ such that $A \in \mathcal{A}(\Lambda)$. This allows us to break the problem of counting alternating matrices down into counting matrices of $\mathcal{A}(\Lambda)$. The following result shows that, for primitive Λ, the set $\mathcal{A}(\Lambda)$ agrees with a friendly object which we already know a lot about.

Lemma 4.0.6. *Let $\Lambda \subset K^n$ be a primitive $\mathcal{O}_K$-module. Then $\mathcal{A}(\Lambda) = \mathcal{B}(\Lambda)$.*

Proof. Because Λ is primitive, we know it is a finitely generated $\mathcal{O}_K$-module in $\mathcal{O}_K^b$. Let $(\mathfrak{V}_1, \boldsymbol{\nu}_1), \ldots, (\mathfrak{V}_r, \boldsymbol{\nu}_r)$ be a pseudo-basis for Λ and let $V = [\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_r] \in M_{n\times r}(K)$ be the associated basis matrix of Λ.

We first show $\mathcal{B}(\Lambda) \subset \mathcal{A}(\Lambda)$. Let VZV^t be an arbitrary element of $\mathcal{B}(\Lambda)$ (with $Z \in M_r(K)_{\text{alt}}$ and $Z_{ij} \in \mathfrak{V}_i\mathfrak{V}_j \ \forall i, j$). Since $VE^{xy}V^t = V(\boldsymbol{e}_x\boldsymbol{e}_y^t - \boldsymbol{e}_y\boldsymbol{e}_x^t)V^t = \boldsymbol{\nu}_x\boldsymbol{\nu}_y^t - \boldsymbol{\nu}_y\boldsymbol{\nu}_x^t$, we have

$$VZV^t = \sum_{E^{xy}\in\mathcal{E}^r} Z_{xy}(VE^{xy}V^t) = \sum_{E^{xy}\in\mathcal{E}^r} Z_{xy}(\boldsymbol{\nu}_x\boldsymbol{\nu}_y^t - \boldsymbol{\nu}_y\boldsymbol{\nu}_x^t). \tag{4.2}$$

Write $Z_{xy} = uv$ for some $u \in \mathfrak{V}_x$, $v \in \mathfrak{V}_y$. Then we have $u\boldsymbol{\nu}_x \in \Lambda \subset \mathcal{O}_K^n$ and $v\boldsymbol{\nu}_y \in \Lambda$ and it follows that each row of the matrix $Z_{xy}(\boldsymbol{\nu}_x\boldsymbol{\nu}_y^t) = (u\boldsymbol{\nu}_x)(v\boldsymbol{\nu}_y)^t$ lies in Λ. Repeating this analysis on $Z_{xy}(\boldsymbol{\nu}_y\boldsymbol{\nu}_x^t)$, we conclude all rows of VZV^t lie in Λ. By construction, VZV^t is alternating and so the matrix lies in $\mathcal{A}(\Lambda)$, as desired.

For the converse containment, let $A \in \mathcal{A}(\Lambda)$ be arbitrary. Since A's rows lie in Λ, we have that $A = BV^t$ for some $B \in M_{n\times r}(K)$ (see Fact 2.1.5). Let $(V^t)^{-1}$ denote the right inverse. Since A is alternating, its columns also lie in Λ. It follows that the columns of $A(V^t)^{-1} = B$ lie in $\text{Span}_K(\Lambda)$. Thus we can also decompose B to obtain $A = BV^t = (VZ)V^t$ for some $Z \in M_r(K)$ (see Fact 2.1.5).

By Lemma 4.0.4, V has a left inverse $V^{-1} \in M_{n\times r}$ satisfying $(V^{-1})_{ij} \in \mathfrak{V}_i$. Note

$$V^{-1}A(V^{-1})^t = V^{-1}(VZV^t)(V^{-1})^t = Z.$$

Thus $Z \in M_r(K)_{\text{alt}}$. Because $\Lambda \subset \mathcal{O}_K^b$, we have $A \in M_n(\mathcal{O}_K)_{\text{alt}}$. Since the i^{th} row of V^{-1} lies in $\mathfrak{V}_i^n \subset K^n$ and likewise the j^{th} column of $(V^{-1})^t$ in $\mathfrak{V}_j^n$, it follows that $\forall i, j$

$$Z_{ij} = (V^{-1}A(V^{-1})^t)_{ij} \in \mathfrak{V}_i\mathfrak{V}_j.$$

Thus $A = VZV^t \in \mathcal{B}(\Lambda)$, as desired. □

Chapter 5

Minima and truncated modules

This chapter generalizes the notions of successive minima [Cas97, Chapter VIII, Section 1] and truncation[1] [Sch68, Section 5] from lattices to finitely generated $\mathcal{O}_K$-modules in K^b. We translate several standard results using successive minima, including Minkowski's Second Theorem, and finish by bounding the number of module points in a ball. These tools will be applied in the next chapter to our module of matrices, $\mathcal{A}(\Lambda)$.

We now review lattice successive minima, and expand the concept to $\mathcal{O}_K$-modules in Definition 5.0.2.

Definition 5.0.1. *Let $\mathcal{V}$ be a real vector space with norm $||\cdot||_{\mathcal{V}}$ and let $\Sigma \subset \mathcal{V}$ be a lattice of lattice-rank a. Set $\boldsymbol{z}_0 = \boldsymbol{0} \in \Sigma$. Then, recursively for each $1 \leq i \leq a$, choose some*

$$\boldsymbol{z}_i \in \Sigma \backslash \mathrm{Span}_{\mathbb{R}}(\boldsymbol{z}_0, \ldots, \boldsymbol{z}_{i-1})$$

so that the norm $||\boldsymbol{z}_i||_{\mathcal{V}}$ is minimal. The $\boldsymbol{z}_i$ are a set of ***lattice-(successive) minima vectors*** *for Σ. Their lengths, $||\boldsymbol{z}_i||_{\mathcal{V}}$, are the* ***lattice-(successive) minima*** *of Σ.*

Definition 5.0.2. *Let $\Gamma \subset K^b$ be an $\mathcal{O}_K$-module of rank a. Set $\boldsymbol{w}_0 = \boldsymbol{0} \in \Gamma$. Then, recursively for each $1 \leq i \leq a$, choose some*

$$\boldsymbol{w}_i \in \Gamma \backslash \mathrm{Span}_K(\boldsymbol{w}_0, \ldots, \boldsymbol{w}_{i-1})$$

*so that the norm $||\boldsymbol{w}_i||_\mu$ is minimal (such $\boldsymbol{w}_i$ exists because $\mu(\Gamma)$, which shares its norm with Γ, is a lattice). We refer to the $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_a$ as $\mathcal{O}_K$-**(successive) minima vectors** for Γ. Their lengths, $||\boldsymbol{w}_1||_\mu \leq \cdots \leq ||\boldsymbol{w}_a||_\mu$, are the $\mathcal{O}_K$-**(successive) minima** of Γ.*

Unless otherwise stated, all successive minima vectors of either kind will be given in increasing order. While the minima vectors may not be uniquely defined for Σ or Γ, the next lemma implies that their lengths are.

[1] *Truncation* is our terminology, this concept goes unnamed in Schmidt as well as in [Thu92], where it is also generalized to $\mathcal{O}_K$-modules.

The successive minima are constructed by greedily taking the shortest vector available at each turn. Lemma 5.0.3 reassures us that this results in an ordered set where each vector is the shortest possible vector in that position of the list (even compared to lists where earlier vectors are allowed to be longer).

Lemma 5.0.3. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module. Let $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_a$ be $\mathcal{O}_K$-successive minima vectors for Γ. Let $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_a \in \Gamma$ be any other competing set of K-linearly independent vectors, also written in increasing order with respect to their lengths. Then we have*

$$||\boldsymbol{w}_i||_\mu \leq ||\boldsymbol{w}'_i||_\mu,$$

for all $i \in 1, \ldots, a$.

The analogous result also holds in the lattice case. That is, if $\Sigma \subset K^b$ is a lattice with lattice-minima $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_a$, and $\boldsymbol{z}'_1, \ldots, \boldsymbol{z}'_a \in \Sigma$ are any other set of $\mathbb{R}$-independent vectors, written in increasing order, then we have $||\boldsymbol{z}_i||_\mu \leq ||\boldsymbol{z}'_i||_\mu$ for all $i \in 1, \ldots, a$.

Proof. First, the $\mathcal{O}_K$-module case. By definition, $||\boldsymbol{w}_1||_\mu \leq ||\boldsymbol{w}'_1||_\mu$. Suppose for contradiction that $||\boldsymbol{w}'_c||_\mu < ||\boldsymbol{w}_c||_\mu$ for some $c > 1$. It follows that $||\boldsymbol{w}'_i||_\mu < ||\boldsymbol{w}_c||_\mu$ for $i = 1, \ldots, c$. Then $\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_c$ form a set of K-linearly independent vectors, and cannot all be contained in the $c-1$-dimensional space $\text{Span}_K(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{c-1})$. In other words, there exists some $\boldsymbol{w}'_i \in \Gamma \backslash \text{Span}_K(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{c-1})$ that is shorter than $||\boldsymbol{w}_c||_\mu$ – a contradiction with $||\boldsymbol{w}_c||_\mu$ being the c^{th} successive minima.

The lattice case follows by the same argument with $\text{Span}_K(\cdots)$ replaced by $\text{Span}_{\mathbb{R}}(\cdots)$. □

A finitely generated $\mathcal{O}_K$-module $\Gamma \subset K^b$ now has two kinds of minima associated to it: its own $\mathcal{O}_K$-minima, as well as the lattice-minima of $\mu(\Gamma)$. Any set of K-linearly independent vectors, $\{\boldsymbol{w}_j\}_{j=1}^a$, in Γ can be combined with a $\mathbb{Z}$-basis of $\mathcal{O}_K$, $\{p_i\}_{i=1}^s$, to produce a set of $\mathbb{R}$-linearly independent vectors in $\mu(\Gamma)$, $\{\mu(p_i\boldsymbol{w}_j)\}_{ij}$ (Lemma 2.5.7). Thus, we might wonder if the $\mathcal{O}_K$-minima can be used to construct a set of lattice-minima. Thunder's result in Lemma 5.0.5 below shows that this is true, at least asymptotically.

First, we introduce some notation that will make comparing the $p_i\boldsymbol{w}_j$ and lattice-minima of $\mu(\Gamma)$ a little easier.

Notation 5.0.4. *Given an $\mathcal{O}_K$-module $\Gamma \subset K^b$, we index the lattice-minima of $\mu(\Gamma)$ with a pair, e.g. $\{\sigma_{ij} : 1 \leq i \leq s, 1 \leq j \leq a\}$, ordered first by the j-term then the i-term, i.e.*

$$\begin{aligned} &\sigma_{1,1} \leq \ldots \sigma_{s,1} \\ \leq\ &\sigma_{1,2} \leq \ldots \sigma_{s,2} \\ &\vdots \\ \leq\ &\sigma_{1,a} \leq \cdots \leq \sigma_{s,a}. \end{aligned}$$

Lemma 5.0.5. *[Thu92, Lemma 9] Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module of rank a. Let $\gamma_1 \leq \cdots \leq \gamma_a$ be the $\mathcal{O}_K$-minima of Γ. Let $\sigma_{1,1} \leq \cdots \leq \sigma_{s,a}$ be the lattice-minima of the lattice $\mu(\Gamma)$. Then the $\sigma_{i,j}$ agree with the $\mathcal{O}_K$-minima in chunks of size s. That is, for $j = 1, \dots, a$ we have*

$$\sigma_{1,j}, \dots, \sigma_{s,j} \asymp_K \gamma_j.$$

The following result is a translation of Minkowski's Second Theorem to finitely generated $\mathcal{O}_K$-modules contained in K^b.

Lemma 5.0.6. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module of rank a. Let $\gamma_1, \dots, \gamma_a$ be the $\mathcal{O}_K$-minima of Γ. Then there exist $c_1 > 0$ and $c_2 > 0$ depending only on K and n such that*

$$\mathfrak{D}(\Gamma) \leq c_1 \gamma_1^s \cdots \gamma_a^s \text{ and } \gamma_1^s \cdots \gamma_a^s \leq c_2 \mathfrak{D}(\Gamma).$$

Proof. Let $\sigma_{1,1}, \dots, \sigma_{s,a} \in K_{\mathbb{R}}^b$ be the lattice-minima of the lattice $\mu(\Gamma)$. Then, by Minkowski's Second Theorem [Cas97, Chapter VIII, Theorem V],

$$\mathfrak{d}(\mu(\Gamma)) \asymp_{K,b} \sigma_{1,1} \cdots \sigma_{s,a}.$$

Using $\mathfrak{D}(\Gamma) = \mathfrak{d}(\mu(\Gamma))$ and Lemma 5.0.5, we have

$$\mathfrak{D}(\Gamma) \asymp_{K,b} \sigma_{1,1} \cdots \sigma_{s,a} \asymp_K \gamma_1^s \cdots \gamma_a^s.$$

□

The successive minima vectors of an $\mathcal{O}_K$-module Γ naturally give rise to a sequence of lower rank modules contained in Γ. These lower rank, *truncated* modules will later give us a way of rewriting formulas depending on the $\mathcal{O}_K$-minima to instead be in terms of discriminants.

Definition 5.0.7. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module of rank a. Let $\boldsymbol{w}_1, \dots, \boldsymbol{w}_a$ be a set of $\mathcal{O}_K$-minima vectors for Γ. Then for each $c \in \{1, \dots, a\}$ we define the c-truncated module to be*

$$\operatorname{trnc}_c(\Gamma) := \Gamma \cap \operatorname{Span}_K(\boldsymbol{w}_1, \dots, \boldsymbol{w}_c),$$

and we let $\operatorname{trnc}_0(\Gamma) := \{\mathbf{0}\}$.

One can check $\operatorname{trnc}_c(\Gamma)$ *is a finitely generated $\mathcal{O}_K$-module of rank c. Furthermore, if Γ is primitive then so is* $\operatorname{trnc}_c(\Gamma)$.

Remark 5.0.8. *Though it is suppressed in the notation, the truncation* $\operatorname{trnc}_c(\Gamma)$ *depends on particular set of minima vectors chosen. Later on, when we start truncating modules en masse, we will assign a fixed set of minima to each so that the truncation is well-defined.*

Lemma 5.0.9. *Let $\Gamma \subset K^b$ be a finitely generated $\mathcal{O}_K$-module. Let $\gamma_1 \leq \dots, \leq \gamma_a$ be the $\mathcal{O}_K$-minima of Γ. Let $\boldsymbol{w}_1, \dots, \boldsymbol{w}_a$ be any choice of $\mathcal{O}_K$-minima vectors of Γ, and let* $\operatorname{trnc}_c(\Gamma)$ *be the truncation with respect to $\{\boldsymbol{w}_i\}_{i=1}^c$. Then* $\operatorname{trnc}_c(\Gamma)$ *has $\mathcal{O}_K$-minima $\gamma_1 \leq \cdots \leq \gamma_c$.*

Proof. This follows by noting that $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_c$ are a valid set of successive minima vectors for $\mathrm{trnc}_c(\Gamma)$, that could result from the construction in Definition 5.0.2. □

The following lemma is a natural generalization of a standard result on lattices (see [Kat94, Lemma 1] and [Sch68, Lemma 2] for two versions).

Lemma 5.0.10. *Let $\Gamma \subset K^b$ be a finitely generated, rank a, $\mathcal{O}_K$-module. Let $\gamma_1, \ldots, \gamma_a$ be the $\mathcal{O}_K$-minima of Γ. Then*

$$\#\{\boldsymbol{x} \in \Gamma : ||\boldsymbol{x}||_\mu < X\} \ll_{K,b} \sum_{j=0}^{a} \left(\frac{X^j}{\gamma_1 \cdots \gamma_j}\right)^s .$$

Proof. We first recall the analogous result on lattices. If $\Sigma \subset \mathcal{V}$ is a lattice in a real vector space with norm $|| \cdot ||_{\mathcal{V}}$, then we have

$$\#\{\boldsymbol{x} \in \Sigma : ||\boldsymbol{x}||_{\mathcal{V}} < X\} \ll_a \sum_{i=0}^{a} \frac{X^i}{\sigma_1 \cdots \sigma_i}, \tag{5.1}$$

where $\sigma_1, \ldots, \sigma_a$ are the lattice-minima of Σ. This follows from [Sch68, Lemma 2], which gives a bound in terms of the lattice-discriminant of Γ, and [Cas97, Chapter VIII, Section 1] which relates the lattice-discriminant to the lattice-minima.

Turning to the $\mathcal{O}_K$-module case, note first that $\#\{\boldsymbol{x} \in \Gamma : ||\boldsymbol{x}||_\mu < X\} = \#\{\boldsymbol{y} \in \mu(\Gamma) : ||\boldsymbol{y}|| < X\}$. Let $\sigma_{1,1} \leq \cdots \leq \sigma_{s,1} \leq \cdots \leq \sigma_{s,a}$ be the lattice-minima of $\mu(\Gamma) \subset K^b_{\mathbb{R}}$. By equation 5.1,

$$\#\{\boldsymbol{y} \in \mu(\Gamma) : ||\boldsymbol{y}|| < X\} \ll_{sa} 1 + \sum_{\substack{j=1,\ldots,a \\ i=1,\ldots,s}} \frac{X^{s(j-1)+i}}{\sigma_{1,1}\sigma_{2,1} \cdots \sigma_{i,j}}. \tag{5.2}$$

By Lemma 5.0.5, we have $\sigma_{1,j}, \ldots, \sigma_{s,j} \asymp_K \gamma_j$ for $j = 1, \ldots, a$, and so the right side of equation (5.2) is bounded above

$$\ll_{K,a} 1 + \sum_{\substack{j=1\ldots a \\ i=1\ldots s}} \frac{X^{s(j-1)+i}}{\gamma_1^s \cdots \gamma_{j-1}^s \gamma_j^i}.$$

If $X > \gamma_j$, the summand $\frac{X^{s(j-1)+i}}{\gamma_1^s \cdots \gamma_{j-1}^s \gamma_j^i}$ is bounded above by $\left(\frac{X^j}{\gamma_1 \cdots \gamma_j}\right)^s$. If $X \leq \gamma_j$, then the summand is bounded by $\left(\frac{X^{j-1}}{\gamma_1 \cdots \gamma_{j-1}}\right)^s$. The claim follows. □

Chapter 6

Bounding $\#\mathcal{A}_{n,r}^K(X)$ from above

Notation 6.0.1. *Recall*

$$\mathcal{A}_{n,r}^K(X) = \{A \in M_n(\mathcal{O}_K)_{alt} : rk(A) = r \text{ and } ||A||_\mu < X\}.$$

Whenever we say a matrix is "small", we mean with respect to $||\cdot||_\mu$. We let $\mathcal{A}(\Lambda)_{<X}$ denote the ball $\{A \in \mathcal{A}(\Lambda) : ||A||_\mu < X\}$.

In this chapter we use Lemma 5.0.10 to count the number of small alternating matrices contained in $\mathcal{A}(\Lambda)_{<X}$. There exists a finite set of Λ, such that every matrix in $\mathcal{A}_{n,r}^K(X)$ lives in $\mathcal{A}(\Lambda)$ for some Λ in this set. Thus our count of small matrices in $\mathcal{A}(\Lambda)_{<X}$ gives rise to an overall bound on $\#\mathcal{A}_{n,r}^K(X)$.

Lemma 5.0.10 gives a bound on $\#\mathcal{A}(\Lambda)_{<X}$ in terms of the successive minima of $\mathcal{A}(\Lambda)$. Our next main lemma, Lemma 6.0.5, allows us to put this bound in terms of the minima of Λ instead. That way, when we sum $\#\mathcal{A}(\Lambda)_{<X}$ over Λ to bound $\#\mathcal{A}_{n,r}^K(X)$, the summand can be written in terms of computable values of Λ.

We begin with a fact and a preliminary lemma. Both of these will also be useful when proving the lower bound later on.

Fact 6.0.2. *Let $\mathcal{C}$ be any collection of constants (for example, $\mathcal{C} = \{K, n\}$). Suppose $x_1, \ldots, x_a, y_1, \ldots, y_a \in \mathbb{R}_{\geq 0}$ satisfy $x_1 \cdots x_a \ll_{\mathcal{C}} y_1 \cdots y_a$ and yet $y_i \ll_{\mathcal{C}} x_i$ for each $i = 1 \ldots a$. Then it follows that $x_i \asymp_{\mathcal{C}} y_i$ for all $i = 1 \ldots a$.*

Proof. Indeed, for any $j \in 1 \ldots a$, let $c_j \in \mathbb{R}$ be such that $c_j x_j = y_j$ and note

$$\prod_{i=1}^a x_i \ll_{\mathcal{C}} \prod_{i=1}^a y_i = c_j x_j \prod_{i \neq j} y_i \ll_{\mathcal{C}} c_j \prod_{i=1}^a x_i,$$

so $1 \ll_{\mathcal{C}} c_j$ and thus $x_j \ll_{\mathcal{C}} y_j$. □

Lemma 6.0.3. *Let $\Lambda \subset \mathcal{O}_K^n$ be a primitive, rank r, $\mathcal{O}_K$-module. Let $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r \in \Lambda$ be a set of $\mathcal{O}_K$-minima vectors for Λ and let $W = [\boldsymbol{w}_1 \cdots \boldsymbol{w}_r] \in M_{n\times r}(\mathbb{Z})$. Then $WE^{ij}W^t \in \mathcal{A}(\Lambda)$, for any $E^{ij} \in \mathcal{E}^r$.*

Proof. Let $(\mathfrak{V}_1, \boldsymbol{\nu}_1), \ldots, (\mathfrak{V}_r, \boldsymbol{\nu}_r)$ be a pseudo-basis of Λ and $V = [\boldsymbol{\nu}_1 \cdots \boldsymbol{\nu}_r] \in M_{n\times r}(\mathbb{Z})$ be the associated basis matrix. Because each $\boldsymbol{w}_i$ lies in $\mathfrak{V}_1\boldsymbol{\nu}_1 + \cdots + \mathfrak{V}_r\boldsymbol{\nu}_r$, there exists $C \in M_r(K)$ with $C_{ij} \in \mathfrak{V}_i$ for all i, j such that $W = VC$. It follows that, for each $E^{ij} \in \mathcal{E}^r$,

$$WE^{ij}W^t = VCE^{ij}C^tV^t = VZV,$$

where $Z = CE^{ij}C^t \in M_r(K)_{\text{alt}}$ satisfies $Z_{xy} \in \mathfrak{V}_x\mathfrak{V}_y$. Thus $WE^{ij}W^t \in \mathcal{B}(\Lambda) = \mathcal{A}(\Lambda)$ (using Lemma 4.0.6 for the final equality). □

Notation 6.0.4. *If $\Gamma \subset M_n(K)$ is a finitely generated $\mathcal{O}_K$-module of matrices, then when we say "the $\mathcal{O}_K$-minima of Γ", we technically mean the minima of $\iota(\Gamma) \subset K^{n^2}$. Recall that $||A||_\mu = ||\iota(A)||_\mu$ for any $A \in M_n(K)$, so it is enough to look at norms in $M_n(K)$.*

Lemma 6.0.5. *Let $\Lambda \subset \mathcal{O}_K^n$ be a primitive, rank r, $\mathcal{O}_K$-module. Let $\lambda_1 \leq \cdots \leq \lambda_r$ be the $\mathcal{O}_K$-minima of Λ and $\alpha_1, \ldots, \alpha_{r(r-1)/2}$ the $\mathcal{O}_K$-minima of $\mathcal{A}(\Lambda)$. Then, for each $i < j$, there exists a distinct index $k_{ij} \in \{1, \ldots, r(r-1)/2\}$ such that $\alpha_{k_{ij}} \asymp_{K,n} \lambda_i\lambda_j$.*

Proof. We first show that $\alpha_{k_{ij}} \ll_{K,n} \lambda_i\lambda_j$ by constructing a contender for the successive minima of $\mathcal{A}(\Lambda)$ out of those of Λ.

Let $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r \in \Lambda$ be at set of $\mathcal{O}_K$-minima vectors for Λ and let $W = [\boldsymbol{w}_1 \cdots \boldsymbol{w}_r] \in M_{n\times r}(\mathbb{Z})$. Also let $(\mathfrak{V}_1, \boldsymbol{\nu}_1), \ldots, (\mathfrak{V}_r, \boldsymbol{\nu}_r)$ be a pseudo-basis of Λ and $V = [\boldsymbol{\nu}_1 \cdots \boldsymbol{\nu}_r] \in M_{n\times r}(\mathbb{Z})$ be the associated basis matrix.

By Lemma 6.0.3, $WE^{ij}W^t \in \mathcal{A}(\Lambda)$ for each $E^{ij} \in \mathcal{E}^r$. We have $WE^{ij}W^t = \boldsymbol{w}_i\boldsymbol{w}_j^t - \boldsymbol{w}_j\boldsymbol{w}_i^t$, thus

$$||WE^{ij}W^t||_\mu \leq 2||\boldsymbol{w}_i\boldsymbol{w}_j^t||_\mu \ll_{K,n} ||\boldsymbol{w}_i||_\mu||\boldsymbol{w}_j||_\mu = \lambda_i\lambda_j.$$

The set $\{WE^{ij}W^t : 1 \leq i < j \leq r\}$ is K-linearly independent and contained in $\mathcal{A}(\Lambda)$, and so by Lemma 5.0.3 each α_k is bounded above by some unique $||WE^{ij}W^t||_\mu$. In other words, there exists a labelling of the indices $\{k_{ij} : 1 \leq i < j \leq r\}$ such that

$$\alpha_{k_{ij}} \leq ||WE^{ij}W^t||_\mu \ll_{K,n} \lambda_i\lambda_j, \tag{6.1}$$

for each $i < j$.

For the reverse inequality, we use that $\mathfrak{D}(\mathcal{A}(\Lambda)) \asymp_{K,n} \mathfrak{D}(\Lambda)^{r-1}$ by Proposition 3.1.8. Combining this with Lemma 5.0.6 results in

$$\prod_{1\leq i<j\leq r} \alpha_{k_{ij}}^s \asymp \mathfrak{D}(\mathcal{A}(\Lambda)) \asymp \mathfrak{D}(\Lambda)^{r-1} \asymp \left(\prod_{i=1}^r \lambda_i^s\right)^{r-1} = \prod_{1\leq i<j\leq r} \lambda_i^s\lambda_j^s,$$

where all implied constants depend only on K and n. In particular, we have $\prod \lambda_i\lambda_j \ll_{K,n} \prod \alpha_{k_{ij}}$. On the other hand, we've already shown in equation 6.1 that $\lambda_i\lambda_j \gg_{K,n} \alpha_{k_{ij}}$, for each i, j. Thus, applying the logic of Fact 6.0.2 we can conclude $\lambda_i\lambda_j \asymp_{K,n} \alpha_{k_{ij}}$.

□

Now that we can relate the minima of $\mathcal{A}(\Lambda)$ to those of Λ, we are ready to write down an $\mathcal{A}(\Lambda)$-specific version of Lemma 5.0.10.

Lemma 6.0.6. *Let $\Lambda \subset \mathcal{O}_K^n$ be a primitive, rank r, $\mathcal{O}_K$-module with a choice of $\mathcal{O}_K$-minima vectors. Then*

$$\#\{A \in \mathcal{A}(\Lambda) : ||A||_\mu < X\} \ll_{K,n} \sum_{q=0}^{r} \frac{X^{qs(r-1)/2}}{\mathfrak{D}(\mathrm{trnc}_q(\Lambda))^{r-1}},$$

where $\mathfrak{D}(\mathrm{trnc}_0(\Lambda)) = \mathfrak{D}(\{\mathbf{0}\}) := 1$ and the other truncations are taken with respect to the chosen minima vectors.

Proof. Let $\lambda_1 \le \cdots \le \lambda_r$ be the $\mathcal{O}_K$-minima of Λ. Let $p := r(r-1)/2$ and let $\alpha_1 \le \cdots \le \alpha_p$ be the $\mathcal{O}_K$-minima of $\mathcal{A}(\Lambda)$.

By Lemma 5.0.10,

$$\#\{A \in \mathcal{A}(\Lambda) : ||A||_\mu < X\} \ll_{K,n} \sum_{k=0}^{p} \left(\frac{X^k}{\alpha_1 \cdots \alpha_k}\right)^s. \tag{6.2}$$

Lemma 6.0.5 tells us that each α_i in the above sum can be replaced by some $\lambda_a\lambda_b$. We don't know which $\lambda_a\lambda_b$ will appear where, but we can upper bound each term of the form

$$\left(\frac{X^k}{\alpha_1 \cdots \alpha_k}\right)^s \tag{6.3}$$

by assuming the $\lambda_a\lambda_b$ are as smallest possible. Because Lemma 6.0.5 assigns each of the p α_i a unique pair $\lambda_a\lambda_b$ (with $a < b$), it follows that any given λ_a can appear at most $r-1$ times in (6.3). Thus, letting $q := \lfloor 2k/(r-1) \rfloor$, we have

$$(6.3) \ll_{K,n} \left(\frac{X^k}{\lambda_1^{r-1}\lambda_2^{r-1} \cdots \lambda_q^{r-1}\lambda_{q+1}^{i}}\right)^s, \tag{6.4}$$

where $i \in \{1, \dots, r-1\}$ is such that $q(r-1) + i = 2k$.

We can write the numerator as $X^k = \sqrt{X}^{2k} = \sqrt{X}^{q(r-1)+i}$. Then, depending on if $\left(\frac{\sqrt{X}}{\lambda_{q+1}}\right)^i$ is ≤ 1 or > 1, we can bound (6.4) above by replacing i with 0 or $r-1$. In other words, the right hand side of (6.4) is upper bounded by

$$(6.4) \le \left(\frac{\sqrt{X}^{q'(r-1)}}{\lambda_1^{r-1}\lambda_2^{r-1} \cdots \lambda_{q'}^{r-1}}\right)^s, \tag{6.5}$$

for q' equal to either q or $q+1$. Thus every term in the sum in (6.2) can be upper bounded by one of the form in (6.5) for some $q' \in \{0, \dots, r\}$[1]. Putting this all together we have

[1] We have $q' \le r$. Indeed, when $k = p = r(r-1)/2$ we have $q = \lfloor 2k/(r-1) \rfloor = r$ and $i = 0$, thus $q' = r$. When $k < p$, then $q < r$ and so $q' \le r$.

$$\#\{A \in \mathcal{A}(\Lambda) : ||A||_\mu < X\} \ll_{K,n} \sum_{q'=0}^{r} \left(\frac{\sqrt{X}^{q'(r-1)}}{\lambda_1^{r-1}\lambda_2^{r-1}\cdots\lambda_{q'}^{r-1}} \right)^s .$$

Then applying Lemmas 5.0.9 and 5.0.6 to replace the denominator of each term with $\mathfrak{D}(\mathrm{trnc}_{q'}(\Lambda))^{r-1}$ completes the proof. □

As we show next in Lemma 6.0.8, every matrix of $\mathcal{A}^K_{n,r}(X)$ can be found in some $\mathcal{A}(\Lambda)$, where Λ is a primitive $\mathcal{O}_K$-module of small discriminant. We now give this collection of nice modules a name, and choose a set of minima vectors for each each Λ in the collection, as this will ease notation in the rest of the chapter.

Definition 6.0.7. *For $X > 0$, let $\mathcal{P}_{n,r}(X)$ be the set of primitive, rank r, $\mathcal{O}_K$-modules $\Lambda \subset \mathcal{O}_K^n$ satisfying $\mathfrak{D}(\Lambda) < X$.*

*Assign a fixed set of $\mathcal{O}_K$-minima vectors to each Λ, so that we may speak of **the minima vectors** of $\Lambda \in \mathcal{P}_{n,r}(X)$. From now on, when we say **the truncation**, $\mathrm{trnc}_c(\Lambda)$, of $\Lambda \in \mathcal{P}_{n,r}(X)$, we mean with respect to these minima vectors. (Note that $\#\mathcal{P}_{n,r}(X) < \infty$ by 6.0.11).*

Lemma 6.0.8. *Let $0 \le r \le n$, with r even. Suppose $A \in \mathcal{A}^K_{n,r}(X)$. Let $c_3 := (|d_K|^r(rs)!)^{1/2}$. Then there exists $\Lambda \in \mathcal{P}_{n,r}(c_3X^{rs/2})$ such that $A \in \mathcal{A}(\Lambda)$.*

Proof. We have $A \in M_n(\mathcal{O}_K)_{\mathrm{alt}}$ with rank r and $||A||_\mu < X$. Let Λ be the unique, rank r, primitive $\mathcal{O}_K$-module in K^n that contains the rows of A. In other words, $\Lambda = \mathcal{O}_K^n \cap \mathrm{Row}(A)$, where $\mathrm{Row}(A)$ is the K-span of A's rows. Then $A \in \mathcal{A}(\Lambda) = \mathcal{B}(\Lambda)$ (Lemma 4.0.6) and it follows from Proposition 3.2.6 that $\mathfrak{D}(\Lambda)^2 < |d_K|^r(rs)!X^{rs}$, as desired. □

We've just seen that every matrix $A \in \mathcal{A}^K_{n,r}(X)$ is contained in a module of the form $\mathcal{A}(\Lambda)$ for some $\Lambda \in \mathcal{P} := \mathcal{P}_{n,r}(c_3X^{sr/2})$. Combining this with Lemma 6.0.6 shows that

$$\#\mathcal{A}^K_{n,r}(X) \ll_{K,n} \sum_{q=0}^{r} \sum_{\Lambda \in \mathcal{P}} \frac{X^{qs(r-1)/2}}{\mathfrak{D}(\mathrm{trnc}_q(\Lambda))^{r-1}}. \tag{6.6}$$

We'd like to adjust the inner sum to run over distinct truncations, $\Lambda_q := \mathrm{trnc}_q(\Lambda)$, rather than Λ. Two things are required to do this. First, we need to know the maximum discriminant a truncated module appearing in equation 6.6 can have. Lemma 6.0.9 answers this question. Secondly, we need the number times a given truncation, Λ_q, appears in equation 6.6. We handle this with Lemma 6.0.13, where we adapt a result of Thunder's which counts the number of modules that truncate to another module.

Lemma 6.0.9. *Let $0 \le q \le r \le n$. If $\Lambda \in \mathcal{P}_{n,r}(X)$ then there exists $c_4 > 0$ depending only on K and n, such that the truncation of Λ satisfies $\mathrm{trnc}_q(\Lambda) \in \mathcal{P}_{n,q}(c_4X^{q/r})$.*

Proof. If $q = 0$, then $\mathrm{trnc}_q(\Lambda) = \mathbf{0}$ is trivially contained in $\mathcal{P}_{n,0}(X^0) = \mathcal{P}_{n,0}(1)$.

Assume $q > 0$. Let $\gamma_1 \leq \cdots \leq \gamma_r$ be Λ's $\mathcal{O}_K$-minima, and let $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r$, with $||\boldsymbol{w}_i||_\mu = \gamma_i$, be the $\mathcal{O}_K$-minima vectors. Then, since

$$\Lambda = \mathcal{O}_K^n \cap \mathrm{Span}_K(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r),$$

it follows that the truncation with respect to $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_q$ is

$$\mathrm{trnc}_q(\Lambda) = \mathcal{O}_K^n \cap \mathrm{Span}_K(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_q).$$

Recall $\mathrm{trnc}_q(\Lambda)$ is primitive, rank q, and that the $\gamma_1, \ldots, \gamma_q$ form a set of $\mathcal{O}_K$-minima vectors for $\mathrm{trnc}_q(\Lambda)$ (Lemma 5.0.9). Thus by Lemma 5.0.6,

$$\begin{aligned}\mathfrak{D}(\mathrm{trnc}_q(\Lambda)) &\leq c_1\gamma_1 \cdots \gamma_q \leq c_1(\gamma_1 \cdots \gamma_r)^{q/r} \\ &\leq c_1(c_2\mathfrak{D}(\Lambda))^{q/r} \leq c_1 c_2^{q/r} X^{q/r},\end{aligned}$$

where $c_1 > 0$ and $c_2 > 0$ are as in Lemma 5.0.6 and depend only on K and n. □

The next two results of Thunder together show that there are not too many primitive $\mathcal{O}_K$-modules of bounded discriminant, and in particular not too many which also truncate to a given module.

Remark 6.0.10. *Initially, [Thu92] gives his results in terms of counting subspaces $S \subset K^n$ of bounded height. However, the r-dimensional subspaces of K^n are in one-to-one correspondence with the rank r primitive $\mathcal{O}_K$-modules*[2] *and, as Thunder shows, his height, $H(S)$, of a subspace $S \subset K^n$ agrees with our discriminant of the associated $\mathcal{O}_K$-module, $\mathfrak{D}(\mathcal{O}_K^n \cap S)$ (up to a constant depending only on K and n).*

Specifically, using the notation of this article, Thunder's Theorem 2 says

$$H(\mathit{Span}_K(\Gamma)) = |d_K|^{-d/2}\mathfrak{D}(\Gamma),$$

for any primitive $\mathcal{O}_K$-module $\Gamma \subset \mathcal{O}_K^n$.

Translated into the language of $\mathcal{O}_K$-modules per Remark 6.0.10, Thunder's main theorem is as follows.

Theorem 6.0.11. *[Thu92, Theorems 1 and 2] Let $0 < r < n$. Then*

$$|\#\mathcal{P}_{n,r}(X) - c_5 X^n| \ll_{K,n} X^{n-c_6},$$

where $c_5, c_6 > 0$ are constants depending only on K and n. (If $r = 0$ or n then there is only one such primitive module.)

[2] The module corresponding to a subspace S is $\Gamma_S = \mathcal{O}_K^n \cap S$, and the subspace corresponding to a module Γ is $S_\Gamma = \mathrm{Span}_K(\Gamma)$.

Remark 6.0.12. *Thunder describes truncated modules in his notation immediately before Lemma 9 in [Thu92]. His definition is identical to ours, and depends on a choice of $\mathcal{O}_K$-minima vectors in the same way. Technically, his definition operates on subspaces $S \subset K^n$, and he allows one to fix a fractional ideal $\mathfrak{B} \subset K$ such that the minima vectors must lie in the $\mathcal{O}_K$-module $\mathfrak{B}(\mathcal{O}_K^n \cap S)$. Our definition is equivalent his restricted to the case $\mathfrak{B} = \mathcal{O}_K$.*

The following lemma of Thunder has been translated into our notation per Remarks 6.0.10 and 6.0.12.

Lemma 6.0.13. *[Thu92, Lemma 15] Let $0 \leq q < r < n$ and let $\Lambda_q \subset \mathcal{O}_K^n$ be a primitive, rank q, $\mathcal{O}_K$-module. Let $X \geq \mathfrak{D}(\Lambda_q)$. Then*

$$\#\{\Lambda \in P_{n,r}(X) : \operatorname{trnc}_q(\Lambda) = \Lambda_q\} \ll_{K,n} X^{n-q}\mathfrak{D}(\Lambda_q)^{r-n}.$$

Proposition 6.0.14. *Let $0 \leq r < n$, with r even. Let $\mathcal{A}^K_{n,r}(X)$ denote the set of rank r matrices $A \in M_n(\mathcal{O}_K)_{alt}$ which satisfy $||A||_\mu < X$. Then*

$$\#\mathcal{A}^K_{n,r}(X) \ll_{K,n} X^{nrs/2}.$$

Proof. By Lemma 6.0.8, each $A \in \mathcal{A}^K_{n,r}(X)$ lies in $\mathcal{A}(\Lambda)$ for some $\Lambda \in \mathcal{P}_{n,r}(c_3X^{sr/2})$, where $c_3 > 0$ depends only on K and n. Thus, letting $\mathcal{P} := \mathcal{P}_{n,r}(c_3X^{sr/2})$, we have

$$\#\mathcal{A}^K_{n,r}(X) \leq \sum_{\Lambda \in \mathcal{P}} \#\{A \in \mathcal{A}(\Lambda) : ||A||_\mu < X\}.$$

By lemma 6.0.6, it follows that

$$\#\mathcal{A}^K_{n,r}(X) \ll_{K,n} \sum_{q=0}^{r} \sum_{\Lambda \in \mathcal{P}} \frac{X^{qs(r-1)/2}}{\mathfrak{D}(\operatorname{trnc}_q(\Lambda))^{r-1}}.$$

Because r is a constant, it suffices to bound the inner sum,

$$\sum_{\Lambda \in \mathcal{P}} \frac{X^{qs(r-1)/2}}{\mathfrak{D}(\operatorname{trnc}_q(\Lambda))^{r-1}}, \tag{6.7}$$

for each $q \in \{0, \dots, r\}$.

Case 1: When $q = 0$ we have $\mathfrak{D}(\operatorname{trnc}_0(\Lambda)) = \mathfrak{D}(\{\mathbf{0}\}) = 1$, and the summand of (6.7) equals 1. In this case, (6.7) becomes a count of $\Lambda \in \mathcal{P}_{n,r}(c_3X^{sr/2})$, which is asymptotically bounded by $X^{nrs/2}$ (Theorem 6.0.11).

Case 2: Let $q > 0$. The only part of Λ appearing in (6.7) is $\mathfrak{D}(\operatorname{trnc}_q(\Lambda))$. We will adjust the sum to vary over the possible values of this discriminant, rather than over $\Lambda \in \mathcal{P}$. By Lemma 6.0.9, $\mathfrak{D}(\operatorname{trnc}_q(\Lambda)) < c_4(c_3X^{rs/2})^{q/r} \leq c_7X^{qs/2}$, where $c_7 > 0$ depends only on K and n. Let $\mathcal{I} := \{\frac{c_7X^{qs/2}}{2^i}\}_{i=0}^{\infty}$.

Sub-case 2(a): Suppose $q < r$. For each $Y \in \mathcal{I}$, we have from Theorem 6.0.11 and Lemma 6.0.13 that

$$\#\{\Lambda \in \mathcal{P}_{n,r}(c_3X^{rs/2}) : \mathfrak{D}(\mathrm{trnc}_q(\Lambda)) \in [Y/2, Y)\} \ll_{K,n} (X^{rs/2})^{n-q}Y^r.$$

Putting this together, the inner sum can be rewritten as

$$\begin{aligned}(6.7) &\ll_{K,n} \sum_{Y\in\mathcal{I}} \frac{X^{qs(r-1)/2}}{(Y/2)^{r-1}} \left((X^{rs/2})^{n-q}Y^r\right)\\ &\ll_{K,n} X^{(nrs-qs)/2} \sum_{i=1}^{\infty} \frac{X^{qs/2}}{2^i}\\ &\ll_{K,n} X^{nrs/2}.\end{aligned}$$

Sub-Case 2(b): Finally, if $q = r$, then for each $Y \in \mathcal{I}$, Theorem 6.0.11 implies

$$\#\{\Lambda \in \mathcal{P}_{n,r}(c_3X^{rs/2}) : \mathfrak{D}(\Lambda) \in [Y/2, Y)\} \ll_{K,n} Y^n,$$

and so

$$\begin{aligned}(6.7) &\ll_{K,n} \sum_{Y\in\mathcal{I}} \frac{X^{rs(r-1)/2}}{(Y/2)^{r-1}} Y^n\\ &\ll_{K,n} X^{rs(r-1)/2} \sum_{i=1}^{\infty} \left(\frac{X^{rs/2}}{2^i}\right)^{n-r+1} \ll_{K,n} X^{nrs/2}. \qquad (6.8)\end{aligned}$$

□

Now that we have a bound on $\#\mathcal{A}^K_{n,r}(X)$ for all $r < n$, the $r = n$ case follows without much additional work.

Corollary 6.0.15. *Let $n > 0$ be even. Then we have $\mathcal{A}^K_{n,n}(X) \ll_{K,n} X^{sn(n-1)/2}$ and, for X sufficiently large, $\mathcal{A}^K_{n,n}(X) \gg_{K,n} X^{sn(n-1)/2}$.*

Proof. Let $\mathcal{A}^K_n(X)$ be the set of all alternating matrices $A \in M_n(\mathcal{O}_K)_{\mathrm{alt}}$ with $||A||_\mu < X$. The matrices of $\mathcal{A}^K_n(X)$ are in one to one correspondence with the vectors $\boldsymbol{v} \in \mathcal{O}_K^{n(n-1)/2}$ with $||\boldsymbol{v}||_\mu < X/\sqrt{2}$. The image $\mu(\mathcal{O}_K^{n(n-1)/2})$ is a rank $sn(n-1)/2$ lattice in $K_{\mathbb{R}}^{n(n-1)/2}$ and $\#\mathcal{A}^K_n(X)$ equals the number of points of this lattice with norm less than $X/\sqrt{2}$. Because the lattice $\mu(\mathcal{O}_K^{n(n-1)/2})$ depends only on the constants K and n, it follows from [Sch68, Lemma 2] that $\#\mathcal{A}^K_n(X) \ll_{K,n} X^{sn(n-1)/2}$, and when X is sufficiently large $\#\mathcal{A}^K_n(X) \gg_{K,n} X^{sn(n-1)/2}$.

We have $\#\mathcal{A}^K_n(X) = \sum_{r=0}^n \#\mathcal{A}^K_{n,r}(X)$. There are no alternating matrices of odd rank. Thus, because n is even, $\#\mathcal{A}^K_{n,r}(X) \ll_{K,n} X^{sn(n-2)/2}$ (Proposition 6.0.14) for all $r < n$ and it follows that

$$\#\mathcal{A}^K_{n,n}(X) = \#\mathcal{A}^K_n(X) - \sum_{r=0}^{n-1} \#\mathcal{A}^K_{n,r}(X) \ll_{K,n} X^{sn(n-1)/2},$$

and that $\#\mathcal{A}^K_{n,n}(X) \gg_{K,n} X^{sn(n-1)/2}$ for X sufficiently large. □

Chapter 7

Bounding $\#\mathcal{A}_{n,r}^{K}(X)$ from below

In this chapter we construct a large number of alternating matrices with small norm. To do this, we carve out a special subset of the primitive modules,"c-regular modules", with the helpful property that each module in this subset contributes at least one matrix to $\mathcal{A}_{n,r}^{K}(X)$.

Definition 7.0.1. *Let $\Lambda \subset K^b$ be a finitely generated $\mathcal{O}_K$-module with $\mathcal{O}_K$-minima $\lambda_1 \leq \cdots \leq \lambda_a$. We say Λ is c-regular (for some $c > 0$) if $\lambda_1 \geq c\mathfrak{D}(\Lambda)^{1/as}$.*

Definition 7.0.2. *Let $\mathcal{P}_{b,a}^{c}(X)$ be the set of primitive, rank a, c-regular, $\mathcal{O}_K$-modules $\Lambda \subset \mathcal{O}_K^b$ satisfying $\mathfrak{D}(\Lambda) < X$.*

Fact 7.0.3. *Let $\Lambda \subset \mathcal{O}_K^b$ be a primitive, c-regular $\mathcal{O}_K$-module with $\mathcal{O}_K$-minima $\lambda_1 \leq \cdots \leq \lambda_a$. Then, for all $i = 1, \ldots, a$,*

$$\lambda_i \asymp_{K,n,c} \mathfrak{D}(\Lambda)^{1/as}. \tag{7.1}$$

Proof. Equation 7.1 follows (see Fact 6.0.2 for details) because all minima of a c-regular module satisfy $\lambda_i \geq c\mathfrak{D}(\Lambda)^{1/as}$ and yet $\lambda_1^s \cdots \lambda_a^s \ll_{K,n} \prod_{i=1}^{as} \mathfrak{D}(\Lambda)^{1/as}$ by Lemma 5.0.6. □

Despite defining c-regular modules in terms of having a large first minima, λ_1, the key property we care about is that such a module contains a set of r, relatively short, linearly independent vectors (Fact 7.0.3). As we shall see later, when Λ is c-regular, these vectors can be used to define a rank r matrix in $\mathcal{A}(\Lambda)_{<X}$.

This next lemma shows that a constant fraction of the primitive modules are c-regular.

Lemma 7.0.4. *Let $0 < r < n$, then there exists $c > 0$ depending only on K and n such that*

$$\#\mathcal{P}_{n,r}^{c}(X) \gg_{K,n} X^n$$

for X sufficiently large.

Proof. By Theorem 6.0.11, there exist constants $X_0, c_8 \in \mathbb{R}_{>0}$ depending only on K and n such that for $X \geq X_0$, $\#\mathcal{P}_{n,r}(X) \geq c_8 X^n$. Let $X > X_0$.

Let $c > 0$ be undetermined for now. Consider $\Lambda \in \mathcal{P}_{n,r}(X)$ with successive minima $\lambda_1 \leq \cdots \leq \lambda_r$ and $\lambda_1 < c\mathfrak{D}(\Lambda)^{1/rs}$ (so Λ is not c-regular). Then λ_1 is the first (and only) successive minima of $\mathrm{trnc}_1(\Lambda)$. It follows that with $c_1 > 0$ as in Lemma 5.0.6

$$\mathfrak{D}(\mathrm{trnc}_1(\Lambda)) \leq c_1\lambda_1^s < c_1c^s\mathfrak{D}(\Lambda)^{1/r} < c_1c^sX^{1/r}.$$

Thus we can bound the number of non-c-regular $\Lambda \in \mathcal{P}_{n,r}(X)$, by counting the number of primitive, rank-r, $\mathcal{O}_K$-modules $\Lambda \subset \mathcal{O}_K^n$ with $\mathfrak{D}(\Lambda) < X$ and $\mathfrak{D}(\mathrm{trnc}_1(\Lambda)) < c_1c^sX^{1/r}$.

Let $\Lambda_1 := \mathrm{trnc}_1(\Lambda)$, so $\Lambda_1 \subset \mathcal{O}_K^n$ is a primitive, rank 1, $\mathcal{O}_K$-module with $\mathfrak{D}(\Lambda_1) < c_1c^sX^{1/r}$. By Theorem 6.0.11, the number of distinct Λ_1 that could arise as $\mathrm{trnc}_1(\Lambda)$ is less than

$$c_9(c_1c^sX^{1/r})^n, \tag{7.2}$$

where $c_9 > 0$ depends on K and n.

Meanwhile, the number of $\Lambda \in \mathcal{P}_{n,r}(X)$ truncating to a given Λ_1 is at most

$$c_{10}X^{n-1}\mathfrak{D}(\Lambda_1)^{r-n} < c_{10}X^{n-1}(c_1c^sX^{1/r})^{r-n} \tag{7.3}$$

by Lemma 6.0.13, for some $c_{10} > 0$ depending on K and n.

Combining equations 7.2 and 7.3, we have that the number of non-c-regular $\Lambda \in \mathcal{P}_{n,r}(X)$ is at most

$$\begin{aligned} &c_9(c_1c^sX^{1/r})^n \cdot c_{10}X^{n-1}(c_1c^sX^{1/r})^{r-n} \\ &= c^{rs}c_9c_1^rc_{10}X^n. \end{aligned}$$

All the constants c_i depend only on K and n, so one may choose a value for c, also depending only on K and n, such that $c^{rs}c_9c_1^rc_{10} < \frac{c_8}{10}$. Then the number of c-regular $\Lambda \in \mathcal{P}_{n,r}(X)$ must be at least

$$c_8X^n - \frac{c_8}{10}X^n = \frac{c_89}{10}X^n.$$

□

We now have the tools to prove the main result of this chapter.

Proposition 7.0.5. *Let $0 \leq r < n$, with r even. Let $\mathcal{A}_{n,r}^K(X)$ denote the set of rank r matrices $A \in M_n(\mathcal{O}_K)_{alt}$ which satisfy $||A||_\mu < X$. Then, for X sufficiently large, we have*

$$\#\mathcal{A}_{n,r}^K(X) \gg_{K,n} X^{nrs/2}.$$

Proof. When $r = 0$, we have $\#\mathcal{A}_{n,0}^K(X) = 1 = X^0$, so the proposition is trivial.

Let $r > 0$. Let $c > 0$ be as in Lemma 7.0.4, and note c depends only on K and n. Let $Y_0 > 0$ be the lower bound implied by Lemma 7.0.4 such that when $Y > Y_0$ we have $\#\mathcal{P}_{n,r}^c(Y^{rs/2}) \gg_{K,n} Y^{nrs/2}$. By the lemma, Y_0 depends only on K and n.

Let $Y > Y_0$ be an indeterminant for now – we will ultimately choose Y so that each $\Lambda \in \mathcal{P}_{n,r}^c(Y^{rs/2})$ contributes at least one matrix to $\mathcal{A}_{n,r}^K(X)$. Fix some $\Lambda \in \mathcal{P}_{n,r}^c(Y^{rs/2})$.

Let $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r$ be a set of $\mathcal{O}_K$-minima vectors for Λ and let $W = [\boldsymbol{w}_1 \cdots \boldsymbol{w}_r] \in M_{n\times r}(K)$. Consider the $n \times n$ matrix

$$A_\Lambda := \sum_{i=1}^{r/2} WE^{2i-1,2i}W^t = W\left(\sum_{i=1}^{r/2} E^{2i-1,2i}\right)W^t,$$

where the $E^{2i-1,2i} \in \mathcal{E}^r$ are members of the standard basis of alternating matrices (Notation 2.1.4).

By Lemma 6.0.3, A_Λ lies in $\mathcal{A}(\Lambda)$. The matrix $\sum_{i=1}^{r/2} E^{2i-1,2i}$ is a row permutation of the identity matrix, and it follows that A_Λ is of rank r. Since Λ is c-regular, we have $||\boldsymbol{w}_j||_\mu \ll_{K,n} \mathfrak{D}(\Lambda)^{1/rs}$ for all $j = 1, \ldots, r$ (using Fact 7.0.3 and the fact that c depended only on K and n). By choice of Λ, we have $\mathfrak{D}(\Lambda) < Y^{rs/2}$, so $||\boldsymbol{w}_j||_\mu \ll_{K,n} Y^{1/2}$.

Each summand of A_Λ then has norm

$$||WE^{2i-1,2i}W^t||_\mu = ||\boldsymbol{w}_{2i-1}\boldsymbol{w}_{2i}^t - \boldsymbol{w}_{2i}\boldsymbol{w}_{2i-1}^t||_\mu \ll_{K,n} ||\boldsymbol{w}_{2i-1}||_\mu||\boldsymbol{w}_{2i}||_\mu \ll_{K,n,c} Y.$$

So $||A_\Lambda||_\mu < bY$ for some $b > 0$ depending on K and n. In the case of this lemma, "X sufficiently large" can be taken to mean $X > Y_0 b$. Indeed, we can then set $Y := X/b$ to obtain $A_\Lambda \in \mathcal{A}^K_{n,r}(X)$ and since $Y = X/b > Y_0$, we also have

$$\#\mathcal{P}^c_{n,r}(Y^{rs/2}) \gg_{K,n} Y^{nrs/2} \gg_{K,n} X^{nrs/2}. \tag{7.4}$$

Because A_Λ has rank r, the primitive module Λ is fully specified by A_Λ. Indeed $\Lambda = \mathcal{O}_K^n \cap \mathrm{Row}(A_\Lambda)$, where $\mathrm{Row}(A_\Lambda)$ is the K-span of A_Λ's rows. It follows that if two modules $\Lambda, \Gamma \in \mathcal{P}^c_{n,r}(Y^{rs/2})$ are distinct, then their matrices must be distinct as well, $A_\Lambda \neq A_\Gamma$.

Putting all this together, we have from (7.4) that there exist $X^{nrs/2}$ modules Λ, each contributing a distinct matrix, A_Λ, to $\mathcal{A}^K_{n,r}(X)$. This proves the claim. □

Bibliography

[Cas97] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[Coh00] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[DRS93] W. Duke, Z. Rudnick, and P. Sarnak. Density of integer points on affine homogeneous varieties. *Duke Math. J.*, 71(1):143–179, 1993.

[EK95] A. Eskin and Yonatan R. Katznelson. Singular symmetric matrices. *Duke Math. J.*, 79(2):515–547, 1995.

[FS10] C. Fieker and D. Stehlé. Short bases of lattices over number fields. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 157–173. Springer, Berlin, 2010.

[Kat93] Y. R. Katznelson. Singular matrices and a uniform bound for congruence groups of $\mathrm{S}L_n(\boldsymbol{Z})$. *Duke Math. J.*, 69(1):121–136, 1993.

[Kat94] Y. R. Katznelson. Integral matrices of fixed rank. *Proc. Amer. Math. Soc.*, 120(3):667–675, 1994.

[Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[PPVW19] J. Park, B. Poonen, J. Voight, and M. M. Wood. A heuristic for boundedness of ranks of elliptic curves. *J. Eur. Math. Soc. (JEMS)*, 21(9):2859–2903, 2019.

[Sch68] W. M. Schmidt. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Math. J.*, 35:327–339, 1968.

[Sie89] C. L. Siegel. *Lectures on the geometry of numbers.* Springer-Verlag, Berlin, 1989. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan.

[Thu92] J. L. Thunder. An asymptotic estimate for heights of algebraic subspaces. *Trans. Amer. Math. Soc.*, 331(1):395–424, 1992.