The Dissertation Committee for Mark Peter Rothlisberger
certifies that this is the approved version of the following dissertation:

An Analogue of the Korkin-Zolotarev Lattice Reduction for Vector Spaces Over Number Fields

Committee:

Jeffrey D. Vaaler, Supervisor

David Helm

Fernando Rodriguez-Villegas

Felipe Voloch

Lenny Fukshansky

An Analogue of the Korkin-Zolotarev Lattice Reduction for Vector Spaces Over Number Fields

by

Mark Peter Rothlisberger, B.A.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

August 2010

Dedicated to Jenny and Elena.

Acknowledgments

There would not be enough space or time to thank all of the mentors, colleagues, friends, and even students who have accompanied me in life and in my studies. I thank you all for your support of and belief in me, because so often I was in great need of both.

I express my gratitude more specifically for those who have assisted me in formulating this dissertation. First and foremost, I thank my dissertation advisor, Dr. Jeffrey D. Vaaler. From my earliest days in graduate school, he showed me what it meant to be a mathematician. He introduced me to the problems that I address in this dissertation. Whenever my research lagged, he was available for healthy discussion and almost always offered a fresh insight that helped me to press forward.

I also thank the members of my dissertation committee: David Helm, Fernando Rodriguez-Villegas, Felipe Voloch, and Lenny Fukshansky for reading, commenting, and helping me to improve my work.

Finally, I owe a deep debt of gratitude to my beloved wife Jenny, without whom I would never have completed this dissertation. Whether it was making my lunches, encouraging me to work late into the evening, or listening to my mostly nonsensical explanations of abstract mathematics, she has sacrificed dearly on my behalf.

An Analogue of the Korkin-Zolotarev Lattice Reduction for Vector Spaces Over Number Fields

Publication No. _____

Mark Peter Rothlisberger, Ph.D.
The University of Texas at Austin, 2010

Supervisor: Jeffrey D. Vaaler

We show the existence of a basis for a vector space over a number field with two key properties. First, the n-th basis vector has a small twisted height which is bounded above by a quantity involving the n-th successive minima associated with the twisted height. Second, at each place v of the number field, the images of the basis vectors under the automorphism associated with the twisted height satisfy near-orthogonality conditions analagous to those introduced by Korkin and Zolotarev in the classical Geometry of Numbers.

Using this basis, we bound the Mahler product associated with the twisted height. This is the product of a successive minimum of a twisted height with the corresponding successive minimum of its dual twisted height. Previous work by Roy and Thunder in [12] showed that the Mahler product was bounded above by a quantity which grows exponentially as the dimension of the vector space increases. In this work, we demonstrate an upper bound that exhibits polynomial growth as the dimension of the vector space increases.

Table of Contents

Chapter 1

Introduction

1.1 Historical Background

In the classical Geometry of Numbers, Minkowski's successive minima theorem is a foundational result which, for any lattice, guarantees the existence of a set of linearly independent lattice vectors that are all short with respect to a symmetric, convex distance function. Let $f : \mathbb{R}^N \to \mathbb{R}$ be a symmetric, convex distance function and $B_f(\tau) = \{\boldsymbol{x} \in \mathbb{R}^N : f(\boldsymbol{x}) \leq \tau\}$ be the ball with respect to f of radius τ, centered at the origin. Let V_f denote the volume of the unit ball $B_f(1)$. Let $L \subseteq \mathbb{R}^N$ be a full-rank lattice with determinant $d(L)$. The successive minima $\lambda_1, \lambda_2, \ldots, \lambda_N$ of L with respect to f are given by

$$\lambda_n = \min\{\tau > 0 : L \cap B_f(\tau) \text{ contains } n \text{ linearly independent points.}\} \quad (1.1)$$

Theorem 1.1 (Minkowski's Successive Minima Theorem)**.** *Given f, V_f, and L as above, the successive minima $\lambda_1, \lambda_2, \ldots, \lambda_N$ of L with respect to f satisfy the bounds*

$$\frac{2^N}{N!} d(L) \leq \left(\prod_{n=1}^{N} \lambda_n \right) V_f \leq 2^N d(L).$$

Proofs of this theorem can be found in [7] and [4], while a more recent approach is given in [5]. Usually the proofs are complicated and technical, and

although the version given in [5] is shorter, it is based on the same principles that underly the original proof given by Minkowski. In special cases, such as when f is the Euclidean distance function, better bounds can be achieved, as in Theorem I in VIII.2 of [4].

Although it is true that for $N \leq 4$, some set of vectors at which the successive minima of a lattice in $\mathbb{R}^N$ are achieved forms a basis for the lattice, this is not necessarily true in higher dimensions. A particularly simple example is well-known even for $\mathbb{R}^5$. However, for applications it is frequently useful to have a set of short basis vectors for L, although the length condition will be weaker. The search for such a basis is called a reduction problem. By imposing different reduction conditions, it is possible to find different bases. The most obvious choice for reduction conditions is inspired by the successive minima theorem. A *Minkowski-reduced basis* $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_N\}$ of a lattice L with respect to a distance function f is one that satisfies the following conditions:

(i) $f(\boldsymbol{y}_1) = \lambda_1$,

(ii) for $1 \leq n \leq N$, let

$$\mathscr{Y}_n = \mathrm{span}_{\mathbb{R}}\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots \boldsymbol{y}_n\},$$

(iii) then $\boldsymbol{y}_n \in L \backslash \mathscr{Y}_{n-1}$ is chosen so that that $f(\boldsymbol{y}_n)$ is minimal among all vectors $\boldsymbol{y}$ in $L \backslash \mathscr{Y}_{n-1}$ such that $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots \boldsymbol{y}\}$ can be extended to a basis for L.

There is an analogue due to Mahler and, independently, H. Weyl, to the Successive Minima theorem which holds for the Minkowski-reduced basis.

Theorem 1.2. *For any symmetric, convex distance function f and lattice L there exists a basis $\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_N$ of L such that*

$$f(\boldsymbol{y}_n) \leq \left(\frac{3}{2}\right)^{n-1} \lambda_n$$

and therefore also

$$V_f \prod_{n=1}^{N} f(\boldsymbol{y}_n) \leq 2^N \left(\frac{3}{2}\right)^{N(N-1)/2} d(L).$$

Proofs of this theorem can be found in Section 10 of Chapter 2 in [7] and Section 6 of Lecture X in [13].

In recent years, techniques from the classical Geometry of Numbers have been adapted to the study of adele rings of number fields, with applications to the heights of algebraic vectors. In this context, the result corresponding to the Successive Minima theorem leads immediately to Siegel's Lemma. This approach was used in [2], [12], and [17]. However, there is one significant difference between the classical and the number field cases, connected to the fact that any collection of linearly independent elements in a vector space automatically forms a basis. In particular, a linearly independent collection of vectors over a number field at which the successive minima with respect to the height are achieved represents a basis for the vector space over the number field. In [3], Burger and Vaaler proved a *primitive basis version* of Siegel's

lemma, which is related to the classical Theorem 1.2. The primitive basis which they used to prove their main results can be considered an analogue of the Minkowski-reduced basis.

Minkowski reduction is not the only approach to lattice basis reduction; there are other methods that are useful for certain problems. In the present dissertation, we take the reduction conditions first employed by Korkin and Zolotarev, and adapt them to the number field case. In the classical case, Korkin-Zolotarev reduction applies only to the Euclidean distance function. Unlike Minkowski reduction, Korkin-Zolotarev reduction is nontrivial in the adelic Geometry of Numbers. In particular Korkin-Zolotarev reduction ensures that the basis vectors found are as close as possible to being orthogonal at each place. There is no such condition on the successive minima, so by imposing it we potentially find a different basis.

We will prove that with respect to a twisted height there exist vectors which satisfy criteria analagous to those of Korkin-Zolotarev, and then show that the set of vectors obtained in this manner satisfies numerous desirable inequalities, similar to the classical case. In particular, the heights of the Korkin-Zolotarev basis elements are bounded with respect to the successive minima. Furthermore, because of the additional orthogonality conditions, the Korkin-Zolotarev basis is particularly useful in problems where an automorphism of the adeles and its dual automorphism are both required.

For dual lattices L and L^* in $\mathbb{R}^N$, the *Mahler product* is defined to be

$$\lambda_n(L)\lambda_{N-n+1}(L^*),$$

for $1 \leq n \leq N$. Mahler was the first to study it and gave an upper bound which can be easily derived from the successive minima theorem. A more refined result can be found in Chapter VIII, Section 5 of [4]. Using Korkin-Zolotarev basis reduction, Lagarias, Lenstra, and Schnorr made significant improvements to this bound in [6]. More recently, in [1], Banaszczyk introduced an extremely novel method that yields an improved upper bound that is likely to be the best possible, at least up to some constant multiple. In the adelic setting, this question has not yet been studied in depth. A bound analogous to Mahler's was given by Roy and Thunder in [12]. Informed by the work in [6], in the present dissertation we improve the upper bound. It is possible that further improvements might be made by studying the strategy employed in [1]; in principle, this approach could be abstracted and modified to work in the adelic setting.

1.2 Main Results

The remainder of this dissertation is structured as follows: in Section 1.3, we will introduce the relevant content and technical details that contribute to the main object of study, the twisted height functions H_A defined for a vector space over a number field. Chapter 2 establishes many of the foundational results regarding orthogonality and orthogonal projection over local fields. A

general theme of this chapter is first to establish a local result, then deduce the corresponding adelic result by applying the local result at each place.

Chapter 3 is devoted to showing the existence of what we will call the Korkin-Zolotarev matrix, which is designed to have certain properties. In Chapter 4, these analytical properties are exploited to bound various quantities; along with the main results described here, there are also some auxiliary results contained in Section 4.3. Our first main result is that the column vectors of the Korkin-Zolotarev matrix, which will be defined in Chapter 3, must have small twisted height, bounded by the successive minima $\Lambda_n(A)$ associated with an automorphism A of the N-fold product of adeles over a number field. In particular, we prove:

Theorem 4.1. *For A belonging to $\mathrm{Aut}(k_{\mathbb{A}}^N)$, let X in $\mathrm{GL}(N,k)$ be the Korkin-Zolotarev matrix for A, and let $\boldsymbol{\xi}_n$ be the n-th column vector of X. Then*

$$H_A(\boldsymbol{\xi}_n) \leq d_3(k)(1+(n-1)\tau_k^2)^{1/2}\Lambda_n(A).$$

Using this as a foundation, several intermediate results build the necessary machinery to bound the Mahler product of corresponding successive minima of a twisted height and dual twisted height as follows:

Theorem 4.6. *Let A belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ and have dual automorphism A^*. For every integer pair $1 \leq n, m \leq N$ such that $m+n = N+1$ we have*

$$\Lambda_n(A)\Lambda_m(A^*) \leq d_3(k)\left(1+\frac{(N-1)}{2}\tau_k^2\right)\gamma_k^*(N) \tag{1.2}$$

The constants τ_k and $d_3(k)$ are defined in Chapter 3 and Section 4.1, respectively, and depend only on the field k. The constant $\gamma_k^*(N)$ is closely related to the Hermite constant, and is defined in (1.10). As the dimension N grows, $\gamma_k^*(N)$ is known to be bounded above by a linear function of N, so the right hand side of (1.2) grows quadratically in N. The bound for the Mahler product with respect to twisted heights proved in Theorem 7.1 of [12] is

$$\Lambda_n(A)\Lambda_m(A^*) \leq 2^{N(N-1)}, \tag{1.3}$$

which has the advantage that it is *absolute*, which means that it is also true in any field extension K of k. Using the same type of argument, along with Theorem 1 of [17], it is possible to show that

$$\Lambda_n(A)\Lambda_m(A^*) \leq \gamma_k(N)^N. \tag{1.4}$$

As (1.2) is not an absolute result, (1.4) is a better comparison. However, since both (1.3) and (1.4) grow exponentially as N increases, (1.2) represents a substantial improvement.

1.3 Absolute Values, Norms and Heights

Our goal in this section is to define the twisted height of a vector in a vector space over an algebraic number field. In order to do so, we select a norm at each place of the number field and assemble them in an infinite product. Because of the construction, we never need to consider matters of convergence. We briefly introduce all the definitions and constructs necessary to understand the twisted height. Our notation follows standard conventions.

An absolute value on a field F is a map $|\ |\ : F \to \mathbb{R}_{\geq 0}$ with the properties that for all x, y in F,

$$|x| = 0 \text{ if and only if } x = 0$$

$$|xy| = |x||y|$$

$$|x + y| \leq |x| + |y|.$$

The final property is called the *triangle inequality*. For some absolute values, an even stronger inequality is true, namely

$$|x + y| \leq \max\{|x|, |y|\},$$

which is called the *strong triangle inequality*. If an absolute value satisfies the strong triangle inequality it is called *non-Archimedean* or *ultrametric*; otherwise it is called *Archimedean*.

Every field has at least one absolute value, which is called the *trivial absolute value* and defined to be

$$|x| = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0, \end{cases}$$

but in the context of this thesis this absolute value will never be used. In fact, the fields that we consider have an abundance of absolute values, and we require a way of classifying them. Two absolute values $|\ |_1$ and $|\ |_2$ on F are said to be equivalent if there is some positive real constant θ such that for all x in F,

$$|x|_1^\theta = |x|_2.$$

This is the case if and only if $|\ |_1$ and $|\ |_2$ induce the same metric topology on F with respect to the metric induced by the function on $F \times F$ given by

$(x, y) \mapsto |x - y|$; it is also equivalent to the statement that the unit balls with respect to the topologies induced by $|\ |_1$ and $|\ |_2$ are the same. An equivalence class of nontrivial absolute values is called a *place* of the field F.

The places of $\mathbb{Q}$ are particularly simple to classify. First, the place containing the usual absolute value is called the *infinite place*, and the usual absolute value will be denoted $|\ |_\infty$. Beyond that, for any rational number β, if we use the unique prime factorization property to write

$$\beta = \pm 2^{w_2(\beta)} 3^{w_3(\beta)} 5^{w_5(\beta)} \cdots,$$

where $w_p(\beta)$ is a positive or negative integer, and $w_p(\beta) = 0$ for almost all p. For every prime p we define a function $|\ |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ by

$$|\beta|_p = p^{-w_p(\beta)}.$$

It is easy to check that these functions are all distinct non-Archimedean absolute values, which we will call *p-adic absolute values*. It is a theorem of Ostrowski that every nontrivial absolute value on $\mathbb{Q}$ is equivalent to either the usual absolute value or one of the p-adic absolute values, so we may index all the non-infinite places of $\mathbb{Q}$ by the prime numbers. We will call these places the *finite places*. We will denote by $\mathbb{Q}_p$ the complete field found by taking the completion of $\mathbb{Q}$ with respect to the metric topology induced by an absolute value from place p. This is called the *field of p-adic numbers*. In the case of the usual absolute value, we have $\mathbb{Q}_\infty = \mathbb{R}$.

We now turn our attention to algebraic number fields, which are finite extensions of $\mathbb{Q}$. Throughout this dissertation, we will let k denote such a

field, and let $d = [k : \mathbb{Q}]$ be the degree of k over $\mathbb{Q}$. If v is a place of k, and $|\ |_v$ is an absolute value in that place, then by restricting to the subfield $\mathbb{Q}$ of k we find that $|\ |_v$ determines a place p of $\mathbb{Q}$. In this case, we say that the place v *lies over* p and write $v|p$. Let k_v be the completion of k with respect to this absolute value. Then $d_v = [k_v : \mathbb{Q}_p]$ is called the *local degree of* k_v. Given a prime p, there are only finitely many places v lying over p, and their local degrees are related by the identity

$$d = \sum_{v|p} d_v.$$

When $v|\infty$, it must be that $d_v = 1$ or 2. In this case, when $d_v = 1$, k_v is isomorphic to $\mathbb{R}$, and when $d_v = 2$, it follows that k_v is isomorphic to $\mathbb{C}$.

We select from each place v of k two absolute values, normalized to satisfy different properties. The first, which we will denote $\|\ \|_v$, extends the usual absolute value on $\mathbb{Q}$ whenever v is an infinite place. When v is a finite place lying over a rational prime p, we let $\|\ \|_v$ extend the p-adic absolute value on $\mathbb{Q}$.

The second absolute value, denoted $|\ |_v$, is defined by $|x|_v = \|x\|_v^{d_v/d}$. This normalization is chosen in order to satisfy the *product formula*: for any $x \in k^\times$,

$$\prod_v |x|_v = 1. \tag{1.5}$$

In the trivial situation where $k = \mathbb{Q}$, we have $\|\ \|_p = |\ |_p$, but this is not necessarily true when $d > 1$.

For each finite place v, we define several interesting subsets of k_v. First, let $\mathcal{O}_v = \{x \in k_v : \|x\|_v \leq 1\}$, and call $\mathcal{O}_v$ the *ring of v-adic integers* in k. The ring $\mathcal{O}_v$ is a local ring with unique maximal ideal $\mathcal{M}_v = \{x \in k_v : \|x\|_v < 1\}$. Furthermore, we note that $\bigcap_{v \nmid \infty} \mathcal{O}_v = \mathcal{O}_k$ is the *ring of integers* of k, which is the integral closure of $\mathbb{Z}$ in k.

The *adele ring* of k, which we will denote by $k_{\mathbb{A}}$, is a space that allows the consideration of all the places of k at once. That is,

$$k_{\mathbb{A}} \subseteq \prod_v k_v,$$

subject to the condition that an element $x = (x_v)$ of this product belongs to $k_{\mathbb{A}}$ if and only if $\|x_v\|_v \leq 1$ for almost all places v. An in-depth exposition of $k_{\mathbb{A}}$ is given in Section 1 of Chapter IV of [20], including a thorough construction of $k_{\mathbb{A}}$ as a locally compact topological ring, using the restricted direct product topology. We will also let $k_{\mathbb{A}}^L$ signify the L-fold product of the adeles of k.

We will call the subgroup of invertible elements of $k_{\mathbb{A}}$ the *idele group* of k, denoted $k_{\mathbb{A}}^\times$. For any $x = (x_v)$ belonging to $k_{\mathbb{A}}^\times$, it must be that at each place v, $x_v \neq 0$, and furthermore $|x_v|_v = 1$ at almost all places v. The idele group is a locally compact topological group, further details of which are given in Sections 3 and 4 of Chapter IV of [20]. We note that although $k_{\mathbb{A}}^\times$ is contained in $k_{\mathbb{A}}$, the induced topology from $k_{\mathbb{A}}$ on $k_{\mathbb{A}}^\times$ is not the same as the restricted direct product topology on $k_{\mathbb{A}}^\times$.

An important characteristic of any idele $x = (x_v)$ is its *volume* $|x|_{\mathbb{A}}$,

which is defined by the product

$$|x|_{\mathbb{A}} = \prod_v |x_v|_v. \tag{1.6}$$

The volume is well-defined, because $|x_v|_v \neq 1$ at only finitely many places, so there is no question of convergence in (1.6).

If $\alpha \in k$, then for all v it is also true that α is in k_v. Therefore we may embed k in $k_{\mathbb{A}}$ by setting $\alpha_v = \alpha$ at each place v; this is called the principal (or diagonal) embedding. We frequently identify k with this embedding in $k_{\mathbb{A}}$. In light of the product formula (1.5), which is the statement that $|\alpha|_{\mathbb{A}} = 1$ for any $\alpha \in k\backslash\{0\}$, it is clear that $k^\times \subseteq k_{\mathbb{A}}^\times$. In fact, even more is true. The ideles of volume 1 form a subgroup of $k_{\mathbb{A}}^\times$, which we will denote by $k_{\mathbb{A}}^1$. By the product formula, $k^\times \subset k_{\mathbb{A}}^1$. Furthermore, it is the case that $k_{\mathbb{A}}^1/k$ is compact.

For any positive integer L, we may use these absolute values to construct a norm on the L-dimensional vector space k_v^L. Given a vector

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_L \end{pmatrix} \in k_v^L,$$

we define $\| \ \|_v : k_v^L \to [0, \infty)$ by:

$$\|\boldsymbol{x}\|_v = \begin{cases} \max_{l=1,2,\ldots,L} \|x_l\|_v & \text{if } v \nmid \infty \\ \left(\sum_{l=1}^L \|x_l\|^2\right)^{1/2} & \text{if } v \mid \infty. \end{cases}$$

In addition, we define a second norm $| \ |_v : k_v^L \to \infty$ by

$$|\boldsymbol{x}|_v = \|\boldsymbol{x}\|_v^{d_v/d}.$$

A nonzero vector $\boldsymbol{x} \in k^L$ has only finitely many places v such that $|\boldsymbol{x}|_v \neq 1$, and we may define a *height* $H : k^L \backslash \{\mathbf{0}\} \to [0, \infty)$:

$$H(\boldsymbol{x}) = \prod_v |\boldsymbol{x}|_v$$

This is often called the *global height* or *absolute Weil height*. Moreover, the height is well defined on the projective space $\mathbb{P}^{L-1}(k)$ because of the product formula. If $\alpha \in k$, $\alpha \neq 0$, then

$$\begin{aligned} H(\alpha\boldsymbol{x}) &= \prod_v |\alpha\boldsymbol{x}|_v \\ &= \prod_v |\alpha|_v \prod_v |\boldsymbol{x}|_v \\ &= \prod_v |\boldsymbol{x}|_v \\ &= H(\boldsymbol{x}) \end{aligned}$$

From the above equation it is also clear that since any nonzero $\boldsymbol{x} \in k^L$ has at least one non-zero coordinate, there is some α such that $\alpha\boldsymbol{x}$ has at least one coordinate equal to 1, and therefore $H : \mathbb{P}^{L-1}(k) \to [1, \infty)$.

Let A be an automorphism, which we will always understand to be continuous, of $k_{\mathbb{A}}^L$. The automorphisms form a group which we will call $\mathrm{Aut}(k_{\mathbb{A}}^L)$. It follows that A can be realized as a vector of matrices A_v indexed by the places of k, where the entries of each A_v are taken from the corresponding k_v. In order to avoid issues of convergence, it is necessary to require that $(\det A_v)$ be an idele. We extend several of the preceding definitions to apply to the automorphism A. In particular, we define the *volume* of the automorphism to be

$$|A|_{\mathbb{A}} = |(\det A_v)|_{\mathbb{A}} = \prod_v |\det A_v|_v.$$

As a result, the map $A \to |A|_{\mathbb{A}}$ is a continuous homomorphism from $\mathrm{Aut}(k_{\mathbb{A}}^L)$ to the multiplicative group of positive real numbers.

Associated to each automorphism $A = (A_v)$ is a *twisted height*

$$H_A : \mathbb{P}^{L-1}(k) \to [1, \infty)$$

defined by

$$H_A(\boldsymbol{x}) = \prod_v |A_v \boldsymbol{x}|_v.$$

If we let $I = (I_v)$ be the identity matrix at each place v, then $H_I(\boldsymbol{x}) = H(\boldsymbol{x})$. The twisted height was first studied by Thunder in [14], and further developed in [15], in the context of the *Hermite's constant* associated with a number field. He defined $\gamma_k(L)$, the Hermite's constant associated to k^L, to be the smallest number such that, for all A belonging to $\mathrm{Aut}(k_{\mathbb{A}}^L)$, there exists an $\boldsymbol{x}$ in $\mathbb{P}^{L-1}(k)$ such that

$$H_A(\boldsymbol{x}) \leq \gamma_k(L)^{1/2} |A|_{\mathbb{A}}^{1/L} \tag{1.7}$$

In the case $k = \mathbb{Q}$, the classical Hermite's constant is recovered. Vaaler has shown in [17] that this constant is the best possible for Siegel's Lemma. However, even in the classical case, Hermite's constant is still somewhat mysterious. For instance, its exact value is known only for $L \leq 8$, and it is not known in general whether, when $m < n$, it is true that

$$\gamma_{\mathbb{Q}}(m) \leq \gamma_{\mathbb{Q}}(n).$$

It is known that $\gamma_{\mathbb{Q}}(L)$ is bounded above by a linear function of L; in particular for every $L \geq 2$ it is possible to show, as in Section 7 of Chapter IX in [4], that

$$\gamma_{\mathbb{Q}}(L) \leq 2L/3.$$

In the case of other number fields k, even less is known about $\gamma_k(L)$. Estimates have been given by Ohno and Watanabe in [10], and the best known result was proved by Thunder in Corollary 2 of [15], which is given as an asymptotic limit. As $L \to \infty$,

$$\log(\gamma_k(L)) = \log L + O_k(1) \tag{1.8}$$

which implies that

$$\gamma_k(L) \leq c(k)L, \tag{1.9}$$

for some constant $c(k)$ depending on the field k.

Because of our limited knowledge about Hermite's constant, we adopt a convention used for the classical case in [6]. For any positive integer L we define

$$\gamma_k^*(L) = \max_{1 \leq l \leq L} \{\gamma_k(l)\}, \tag{1.10}$$

because we will be required to provide upper bounds for estimates involving the product of Hermite's constant for several different choices of L at once. It follows immediately from (1.9) that

$$\gamma_k^*(L) \leq c(k)L,$$

so that we will still be able to provide estimates involving only the number field k and vector space dimension L, and not be limited by the relative lack of knowledge about Hermite's constant.

Further generalizations of Hermite's constant, along with applications, have been studied by Watanabe in [18] and [19], and more recently by Meyer in [9] and [8]. It is possible that the techniques and results of the present dissertation could also be useful in the contexts of those generalizations.

Chapter 2

Preliminary Lemmas

2.1 Duality of Automorphisms

In the classical Geometry of Numbers, given a lattice Λ of rank N in $\mathbb{R}^N$, its *dual lattice*, also known as its *polar* or *reciprocal lattice* Λ^* is defined as

$$\Lambda^* = \{\boldsymbol{y} \in \mathbb{R}^N : \boldsymbol{x}^T\boldsymbol{y} \in \mathbb{Z} \text{ for all } \boldsymbol{x} \in \Lambda\}$$

Of note, the matrix product used here is the same as the usual inner product on $\mathbb{R}^N$. If $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N\}$ is a basis for Λ, then a dual basis of Λ^* is a set $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_N\}$ defined for $1 \leq i, j \leq N$ by the equations

$$\boldsymbol{x}_i^T\boldsymbol{y}_j = \delta_{ij}.$$

Here δ_{ij} is the Kronecker delta, specifically

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Since any lattice in $\mathbb{R}^N$ can be realized as $A\mathbb{Z}^N$ for $A \in \mathrm{GL}(N, \mathbb{R})$, it is not hard to see that if $\Lambda = A\mathbb{Z}^N$, then $\Lambda^* = A^{-T}\mathbb{Z}^N$. We do not give the proof of this here, but the argument used to prove the main results of this section is essentially the same.

In the context of automorphisms of adeles, the interpretation in terms of matrices is useful. We define the dual automorphism $A^* = (A_v^*)$ of $A = (A_v)$ to be $A^* = (A^{-1})^T = ((A_v^{-1})^T)$. We now show that this definition of duality agrees with the classical one.

Proposition 2.1.1. *Suppose A and A^* belonging to $\mathrm{Aut}(k_{\mathbb{A}}^L)$ are dual automorphisms. Then for any $\boldsymbol{\xi} \in k^L$ and $\boldsymbol{\eta} \in k_{\mathbb{A}}^L$, we have*

$$(A\boldsymbol{\xi})^T \boldsymbol{\eta} \in k \tag{2.1}$$

if and only if $\boldsymbol{\eta} = A^* \boldsymbol{\nu}$ for some $\boldsymbol{\nu} \in k^L$.

Proof. First, assume that $\boldsymbol{\eta} = A^* \boldsymbol{\nu}$ for some $\boldsymbol{\nu} \in k^L$. At each place v we have

$$\begin{aligned}(A_v\boldsymbol{\xi})^T A_v^* \boldsymbol{\nu} &= \boldsymbol{\xi}^T A_v^T (A_v^{-1})^T \boldsymbol{\nu} \\ &= \boldsymbol{\xi}^T (A_v A_v^{-1})^T \boldsymbol{\nu} \\ &= \boldsymbol{\xi}^T \boldsymbol{\nu} = x \in k\end{aligned}$$

and notice that there is no longer a dependence on the place v, so x is the same at each place, which is to say that it is in the principal embedding of k into $k_{\mathbb{A}}$.

Next suppose that $(A\boldsymbol{\xi})^T \boldsymbol{\eta} = x \in k$ for any $\boldsymbol{\xi} \in k^L$, which means that at each place $(A_v\boldsymbol{\xi})^T \boldsymbol{\eta} = x$. Let $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_L$ be the standard basis vectors, and apply the hypothesis to each one, so that $(A_v \boldsymbol{e}_l)^T \boldsymbol{\eta} = x_l \in k$. But $A_v \boldsymbol{e}_l$ is just the l-th column of the matrix A_v, so by assembling the coordinates x_l into the vector

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_L \end{pmatrix} \in k^L,$$

we discover that

$$A_v^T \boldsymbol{\eta} = \boldsymbol{x}$$

$$\boldsymbol{\eta} = (A_v^T)^{-1}\boldsymbol{x} = A^*\boldsymbol{x},$$

so $\boldsymbol{\eta}$ has the desired form. □

It is also useful to observe that

$$|A^*|_{\mathbb{A}} = |A|_{\mathbb{A}}^{-1}. \tag{2.2}$$

2.2 Orthogonality in Local Fields

In the classical Korkin-Zolotarev lattice reduction, a basis is found for which the basis vectors are short and also nearly orthogonal. However, in non-Archimedean local fields the properties of orthogonality are somewhat different than in the Archimedean setting. The basic theory of orthogonality in such circumstances is described in [20], Chapter II, Sections 1 and 2, as well as [16] with further elaborations in [3]. Here we cite some of the technical lemmas in order to use them in constructions that follow.

Suppose that $\mathscr{X}$ and $\mathscr{Y}$ are subspaces of k_v^L. We define $\mathscr{X}$ and $\mathscr{Y}$ to be *orthogonal* if the usual Pythagorean identity

$$\|\boldsymbol{x} + \boldsymbol{y}\|_v^2 = \|\boldsymbol{x}\|_v^2 + \|\boldsymbol{y}\|_v^2 \tag{2.3}$$

holds true for all $\boldsymbol{x} \in \mathscr{X}$ and $\boldsymbol{y} \in \mathscr{Y}$ whenever $v|\infty$. If $v \nmid \infty$, then we require that a non-Archimedean analogue holds, specifically that for all $\boldsymbol{x} \in \mathscr{X}, \boldsymbol{y} \in \mathscr{Y}$ we have

$$\|\boldsymbol{x} + \boldsymbol{y}\|_v = \max\{\|\boldsymbol{x}\|_v, \|\boldsymbol{y}\|_v\}. \tag{2.4}$$

In both cases, we may define an orthogonal projection operator. Let $\mathscr{X}$ have dimension $K \leq L$, and let $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_K\}$ be a basis for $\mathscr{X}$. Consider these basis vectors as column vectors of the $L \times K$ matrix

$$X = (\boldsymbol{x}_1 \ \boldsymbol{x}_2 \ \cdots \ \boldsymbol{x}_K),$$

and for $v|\infty$ define the projection operator $P_v(X)$ to be

$$P_v(X) = X(X^*X)^{-1}X^*.$$

If $v \nmid \infty$, we first introduce some necessary notation. Let I be a subset of $1, 2, \ldots, L$ such that $|I| = K$, and let ${}_IX$ be the $K \times K$ matrix which has as its rows the rows of X indexed by elements of I. From all possible subsets I, let J be one such that

$$|\det {}_JX|_v = \max_{\substack{I \subseteq \{1,2,\ldots,L\} \\ |I|=K}} |\det {}_IX|_v. \tag{2.5}$$

If there are multiple choices ${}_IX$ satisfying (2.5), we must impose a further condition in order to specify ${}_JX$ uniquely and consistently. In this case we will choose J from the candidates to be the K-element subset which occurs first in the lexicographic ordering. It is now possible, for $v \nmid \infty$, to define $P_v(X)$ as

$$P_v(X) = X({}_JX)^{-1}{}_J(\mathbf{1}_L).$$

In both the Archimedean and non-Archimedean cases, this projection operator has many desirable properties.

Lemma 2.1. *Given the orthogonal projection $P_v(\mathscr{X})$ defined above, the following are true:*

(i) $P_v(\mathscr{X})\boldsymbol{z} \in \mathscr{X}$ *for any* $\boldsymbol{z} \in k_v^L$,

(ii) $P_v(\mathscr{X})\boldsymbol{x} = \boldsymbol{x}$ *for* $\boldsymbol{x} \in \mathscr{X}$,

(iii) $P_v(\mathscr{X})$ *is idempotent, i.e.* $P_v^2(\mathscr{X}) = P_v(\mathscr{X})$,

(iv) if $v|\infty$, *then*

$$\|\boldsymbol{z}\|_v^2 = \|P_v(\mathscr{X})\boldsymbol{z}\|_v^2 + \|(\mathbf{1}_L - P_v(\mathscr{X}))\boldsymbol{z}\|_v^2,$$

(v) if $v \nmid \infty$, *then*

$$\|\boldsymbol{z}\|_v = \max\{\|P_v(\mathscr{X})\boldsymbol{z}\|_v, \|(\mathbf{1}_L - P_v(\mathscr{X}))\boldsymbol{z}\|_v\}.$$

We omit the proof, which can be found in [16]. Orthogonal projection allows us to use a Gram-Schmidt orthogonalization process to decompose any nonsingular matrix over a local field.

Lemma 2.2 (Lemma 1 of [17])**.** *Let* $A \in GL(L, k_v)$ *be a nonsingular* $L \times L$ *matrix. Then there exist matrices* Ψ, U, *and* W *such that*

$$A = \Psi U W,$$

where

(i) $W = (w_{ij})$ *is upper triangular and* $w_{ll} = 1$ *for* $l = 1, 2, \ldots, L$,

(ii) $U = [u_l]$ *is diagonal,*

(iii) if $\boldsymbol{\psi}_l$ *denotes the* l*-th column of* Ψ*, then*

$$\|\boldsymbol{\psi}_1\|_v = \|\boldsymbol{\psi}_2\|_v = \cdots = \|\boldsymbol{\psi}_L\|_v = 1$$

and for $i,\ j = 1, 2, \ldots, L$*, with* $i \neq j$*,*

$$\textit{span}\{\boldsymbol{\psi}_i\} \textit{ is orthogonal to } \textit{span}\{\boldsymbol{\psi}_j\}.$$

Proof. Let $\boldsymbol{a}_l$ be the l-th column vector of A. We proceed by induction on l. If $l = 1$, then we define $u_1 = \|\boldsymbol{a}_1\|_v$, $w_{11} = 1$, $w_{i1} = 0$ for $1 < i \leq L$, and $\boldsymbol{\psi}_1 = u_1^{-1}\boldsymbol{a}_1$. Now assume that $l \geq 1$, so that $\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_{l-1}$ have been defined. We define the subspace $\mathscr{X}$ to be

$$\begin{aligned}\mathscr{X} &= \text{span}_{k_v}\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{l-1}\} \\ &= \text{span}_{k_v}\{\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_{l-1}\}\end{aligned}$$

We apply the projection $P_v(\mathscr{X})$ to $\boldsymbol{a}_l$, and because the resulting vector is in $\mathscr{X}$ we may write

$$P_v(\mathscr{X})\boldsymbol{a}_l = \sum_{i=1}^{l-1} \alpha_i \boldsymbol{\psi}_i \tag{2.6}$$

$$\boldsymbol{a}_l = \sum_{i=1}^{l-1} \alpha_i \boldsymbol{\psi}_i + (\mathbf{1}_L - P_v(\mathscr{X}))\boldsymbol{a}_l \tag{2.7}$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_{l-1} \in k_v$. Define $u_l = \|(\mathbf{1}_L - P_v(\mathscr{X}))\boldsymbol{a}_l\|_v$. Since A_v is nonsingular, its column vectors must be linearly independent, so $\boldsymbol{a}_l \notin \mathscr{X}$ and therefore $u_l \neq 0$. Also let $\boldsymbol{\psi_l} = u_l^{-1}(\mathbf{1}_L - P_v(\mathscr{X}))\boldsymbol{a}_l$. Finally, let

$$w_{il} = \begin{cases} \alpha_i/u_i & 1 \leq i < l \\ 1 & i = l \\ 0 & l < i \leq L. \end{cases}.$$

The matrices defined by

$$\Psi_v = (\boldsymbol{\psi}_1\ \boldsymbol{\psi}_2\ \ldots\ \boldsymbol{\psi}_L)$$

$$U = [u_l]$$

$$W = (w_{ij})$$

satisfy the requirements given in the statement of the lemma. □

If $A = (A_v)$ is an automorphism of the adeles of k, then we may apply Lemma 2.2 at each place and achieve a global result.

Lemma 2.3 (Lemma 2 of [17]). *Let $A = (A_v) \in \mathrm{Aut}(k_{\mathbb{A}}^L)$. Then there are $\Psi = (\Psi_v)$, $U = (U_v)$ and $W = (W_v)$ all belonging to $\mathrm{Aut}(k_{\mathbb{A}}^L)$, with the following properties:*

(i) $A = \Psi U W$,

(ii) at each place v of k, U_v is a diagonal matrix,

(iii) at each place v of k, W_v is an upper-triangular matrix with 1's along the diagonal,

(iv) at each place v of k, $\|\Psi_v \boldsymbol{x}\|_v = \|\boldsymbol{x}\|_v$ for all $\boldsymbol{x}$ in k_v^L.

Furthermore, if $u_l = (u_l^{(v)})$ is a diagonal entry of U, then u_l is an idele.

Proof. Because A is in $\mathrm{Aut}(k_{\mathbb{A}}^L)$, A_v is nonsingular at each place v and we may apply Lemma 2.2 at each, yielding the equation

$$A_v = \Psi_v U_v W_v.$$

Set $\Psi = (\Psi_v), U = (U_v), W = (W_v)$, then it is clear that the matrices satisfy (ii), (iii), and (iv). From (iv) it is clear that $\|\det \Psi_v\|_v = 1$ at each place v, so Ψ belongs to $\mathrm{Aut}(k_{\mathbb{A}}^L)$. Likewise, from (iii) it follows that $\det W_v = 1$ at each place, so W belongs to $\mathrm{Aut}(k_{\mathbb{A}}^L)$, and therefore $U = \Psi^{-1}AW^{-1}$ is also in $\mathrm{Aut}(k_{\mathbb{A}}^L)$.

As U_v is a diagonal matrix, we can calculate its determinant:

$$|\det U_v|_v = \prod_{l=1}^{L} |u_l^{(v)}|_v.$$

Since each u_l is an adele, we have that $\|u_l^{(v)}\|_v \leq 1$ for almost all v. But U is in $\mathrm{Aut}(k_{\mathbb{A}}^L)$, so $|\det U_v|_v = 1$ for almost all places. Assume that for some l, $\|u_l^{(v)}\|_v < 1$ at infinitely many places v. Then there must be some $j \neq l$ such that $\|u_j^{(v)}\|_v > 1$ at infinitely many places, which is a contradiction. Therefore $u_l \in k_{\mathbb{A}}^{\times}$ for $l = 1, 2, \ldots, L$, which is the last conclusion of the theorem. □

2.3 Orthogonal Projection of Automorphisms

In order to prove our main results, we must understand the relationship between vector space automorphisms and orthogonal projections. In the most general terms, given a matrix $A \in \mathrm{GL}(N, k_v)$ and an n-dimensional subspace $\mathscr{X} \subseteq k_v^N$, we would like to understand the linear transformations $P_v(\mathscr{X})A$ and $(\mathbf{1}_N - P_v(\mathscr{X}))A$. In particular, we would like to determine the structure of the sets

$$\{P_v(\mathscr{X})A\boldsymbol{x} : \boldsymbol{x} \in k^N\}$$

$$\{(\mathbf{1}_N - P_v(\mathscr{X}))A\boldsymbol{x} : \boldsymbol{x} \in k^N\}$$

However, this will vary depending on the relationship between $\mathscr{X}$ and A. For our purposes, it is enough to understand the situation when

$$\mathscr{X} = \mathrm{span}_{k_v}\{A\boldsymbol{x}_1, A\boldsymbol{x}_2, \ldots, A\boldsymbol{x}_n\},$$

where $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n \in k^N$. In fact, we may simplify the situation even more. If X is in $\mathrm{GL}(N, k)$, then AX still belongs to $\mathrm{GL}(N, k_v)$, and can be used for our purposes instead of A. Therefore it suffices to consider only

$$\mathscr{A} = \mathrm{span}_{k_v}\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n\},$$

where $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ are the first n column vectors of A. Because of this, the results from the previous section, in particular Lemma 2.2, can be applied to the problem at hand.

It will be helpful to define a family of restriction functions

$$\phi_{M,L} : k^M \to k^L, \qquad \text{where } 1 \leq L \leq M.$$

Most often, we will use k^N as the domain of one of these functions. When it is clear that this is the case, we will omit the first subscript and write merely ϕ_L instead of $\phi_{N,L}$. The functions are defined as follows. For $\boldsymbol{x} \in k^M$, we write $\boldsymbol{x}$ coordinate-wise in terms of the standard basis vectors,

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_M \end{pmatrix},$$

Then

$$\phi_{M,L}(\boldsymbol{x}) = \begin{pmatrix} x_{M-L+1} \\ x_{M-L+2} \\ \vdots \\ x_M \end{pmatrix}.$$

Composition of these restriction functions is particularly simple. When $1 \leq L' \leq L \leq M$,

$$\phi_{L,L'} \circ \phi_{M,L}(\boldsymbol{x}) = \phi_{M,L'}(\boldsymbol{x}).$$

For any nonsingular A belonging to $\mathrm{GL}(N, k_v)$, let $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_N$ be the linearly independent column vectors of A. We define a sequence of subspaces $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_N$ of k_v^N by

$$\mathscr{A}_n = \mathrm{span}_{k_v}\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n\}.$$

We are now in position to associate with any A belonging to $\mathrm{GL}(N, k_v)$ a sequence $A^{(1)}, A^{(2)}, \ldots, A^{(N)} = A$. In this sequence, $A^{(L)}$ is an element of $\mathrm{GL}(L, k_v)$, and the relationship between A and $A^{(L)}$ will be made precise in the following lemma.

Lemma 2.4. *Let A belong to $\mathrm{GL}(N, k_v)$, and for $1 \leq L < N$ let $\mathscr{A} = \mathscr{A}_{N-L}$ be the subspace of k_v^N spanned by the first $N - L$ column vectors of A. Then there is a matrix $A^{(L)} \in \mathrm{GL}(L, k_v)$ such that for any $\boldsymbol{x} \in k^N$,*

$$\|(\mathbf{1}_N - P_v(\mathscr{A}))A\boldsymbol{x}\|_v = \|A^{(L)}\phi_L(\boldsymbol{x})\|_v$$

Proof. Apply Lemma 2.2 to the matrix A, yielding the decomposition

$$A = \Psi U W.$$

For convenience, we will let $Z = UW$, so $Z = (z_{mn})$ is upper triangular. Because

$$\mathscr{A} = \mathrm{span}_{k_v}\{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{N-L}\},$$

it follows from the decomposition that

$$\mathscr{A} = \mathrm{span}_{k_v}\{\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_{N-L}\},$$

where $\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_N$ are the column vectors of Ψ. Let

$$\mathscr{B} = \mathrm{span}_{k_v}\{\boldsymbol{\psi}_{N-L+1}, \boldsymbol{\psi}_{N-L+2}, \ldots, \boldsymbol{\psi}_N\}$$

so that $\mathscr{A}$ and $\mathscr{B}$ are orthogonal, and $k_v^N = \mathscr{A} \oplus \mathscr{B}$. Let $\mathscr{B}'$ be the L-dimensional subspace determined as the image of the operator $(\mathbf{1}_N - P_v(\mathscr{A}))$. If v is a non-Archimedean place, then it may be that $\mathscr{B} \neq \mathscr{B}'$. However, because $\mathscr{B}$ is orthogonal to $\mathscr{A}$, it is true that for any $\boldsymbol{y} \in \mathscr{B}$,

$$\|\boldsymbol{y}\|_v = \|(\mathbf{1}_N - P_v(\mathscr{A}))\boldsymbol{y}\|_v. \tag{2.8}$$

Now let

$$\boldsymbol{\xi} = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_N \end{pmatrix}$$

be any nonzero vector in k^N and consider

$$\begin{aligned} A\boldsymbol{\xi} &= \sum_{n=1}^{N} \boldsymbol{a}_n \xi_n \\ &= \sum_{n=1}^{N} \sum_{m=1}^{n} (z_{mn}\boldsymbol{\psi}_m)\xi_n \\ &= \sum_{n=1}^{N} \sum_{m=n}^{N} (z_{nm}\xi_m)\boldsymbol{\psi}_n. \end{aligned}$$

When expanded in terms of the $\boldsymbol{\psi}_n$, we can calculate the projection

$$\begin{aligned}(\mathbf{1}_N - P_v(\mathscr{A}))A\boldsymbol{\xi} &= (\mathbf{1}_N - P_v(\mathscr{A}))\left(\sum_{n=1}^{N}\sum_{m=n}^{N}(z_{nm}\xi_m)\boldsymbol{\psi}_n\right)\\ &= (\mathbf{1}_N - P_v(\mathscr{A}))\left(\sum_{n=1}^{N-L}\sum_{m=n}^{N}(z_{nm}\xi_m)\boldsymbol{\psi}_n\right.\\ &\qquad\left.+\sum_{n=N-L+1}^{N}\sum_{m=n}^{N}(z_{nm}\xi_m)\boldsymbol{\psi}_n\right)\\ &= (\mathbf{1}_N - P_v(\mathscr{A}))\left(\sum_{n=N-L+1}^{N}\sum_{m=n}^{N}(z_{nm}\xi_m)\boldsymbol{\psi}_n\right)\\ &= \sum_{n=N-L+1}^{N}\sum_{m=n}^{N}(z_{nm}\xi_m)(\mathbf{1}_N - P_v(\mathscr{A}))\boldsymbol{\psi}_n\end{aligned}$$

Upon appealing to (2.8) and the fact that $\boldsymbol{\psi}_n$ is orthogonal to $\mathscr{A}$ for $N-L+1 \leq n \leq N$ we find that

$$\|(\mathbf{1}_N - P_v(\mathscr{A}))A\boldsymbol{\xi}\|_v = \left\|\sum_{n=N-L+1}^{N}\sum_{m=n}^{N}(z_{nm}\xi_m)\boldsymbol{\psi}_n\right\|_v.$$

Furthermore, $\|\boldsymbol{\psi}_n\|_v = 1$ for all $n = 1, 2, \ldots N$ so in fact we see that

$$\|(\mathbf{1}_N - P_v(\mathscr{A}))A\boldsymbol{\xi}\|_v = \left\|\sum_{n=N-L+1}^{N}\sum_{m=n}^{N}(z_{nm}\xi_m)\right\|_v.$$

Let

$$\boldsymbol{\xi}' = \phi_L(\boldsymbol{\xi}),$$

and let ${}^{L}Z = (z_{mn})$, where $N-L+1 \leq m \leq N$ and $N-L+1 \leq n \leq N$ be the matrix formed by excerpting the lower right-hand $L \times L$ corner of the matrix Z. Because Z is upper triangular, ${}^{L}Z$ is also upper-triangular. Its diagonal

entries are a subset of those in W, so it is in $\mathrm{GL}(L, k_v)$. Matrix multiplication shows that

$$ {}^{L}Z\boldsymbol{\xi}' = \sum_{n=N-L+1}^{N} \sum_{m=n}^{N} (z_{nm}\xi_m), $$

so that in fact

$$ \|(\mathbf{1}_N - P_v(\mathscr{A}))A\boldsymbol{\xi}\|_v = \left\| {}^{L}Z\phi_L(\boldsymbol{\xi}) \right\|_v . $$

We set $A^{(L)} = {}^{L}W$, so that $A^{(L)}$ satisfies the conclusion of the lemma. □

In fact, if Φ is any isometry of k_v^L, then we could let $A^{(L)} = \Phi({}^{L}Z)$. We implicitly used $\Phi = I$ to construct $A^{(L)}$ in the proof of the lemma.

Much as Lemma 2.2 led to Lemma 2.3, for an automorphism $A = (A_v)$ of $k_{\mathbb{A}}^N$, we apply Lemma 2.4 to each A_v and achieve a global result. In essence, we will show that, for $L \leq N$, there is an automorphism $A^{(L)}$ of $k_{\mathbb{A}}^L$ such that the twisted heights $H_{A^{(L)}}(\boldsymbol{x})$ of points $\boldsymbol{x}$ in k^L capture information about the norms of the images of points $A\boldsymbol{y}$ in $k_{\mathbb{A}}^N$ under orthogonal projection onto a particular L-dimensional subspace of k_v at each place v. This is similar to a result in the classical Geometry of Numbers, used in [6] to describe the construction of the Korkin-Zolotarev basis. There, the result states that the projection of a lattice onto the orthogonal complement of a subspace spanned by some of its vectors is still a lattice, of maximal rank in the subspace onto which it was projected.

Lemma 2.5. *Given an automorphism $A = (A_v)$ belonging to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ and a positive integer $L < N$, at each place let $\mathscr{A}^{(v)} = \mathscr{A}_{N-L}^{(v)}$ denote the subspace of*

k_v^N spanned by the first $N-L$ columns of the matrix A_v. Then there is an automorphism $A^{(L)} = (A_v^{(L)})$ of $k_{\mathbb{A}}^L$ such that for any $\boldsymbol{x}$ in k^N,

$$H_{A^{(L)}}(\phi_L(\boldsymbol{x})) = \prod_v \left|(\mathbf{1}_N - P_v(\mathscr{A}^{(v)}))A_v\boldsymbol{x}\right|_v .$$

Proof. Given $A = (A_v)$, at each place v let $A_v^{(L)}$ be chosen as prescribed by Lemma 2.4. Applying the lemma at each place

$$\left\|A_v^{(L)}\phi_L(\boldsymbol{x})\right\|_v = \left\|(\mathbf{1}_N - P_v(\mathscr{A}^{(v)}))A_v\boldsymbol{x}\right\|_v ,$$

and by raising both sides to the power d_v/d, we see that also

$$\left|A_v^{(L)}\phi_L(\boldsymbol{x})\right|_v = \left|(\mathbf{1}_N - P_v(\mathscr{A}^{(v)}))A_v\boldsymbol{x}\right|_v . \tag{2.9}$$

Because ϕ_L is a function on k^N that is independent of the place chosen, we may use this equation at each place v, and since

$$H_{A^{(L)}}(\phi_L(\boldsymbol{x})) = \prod_v \left|A_v^{(L)}\phi_L(\boldsymbol{x})\right|_v , \tag{2.10}$$

the desired conclusion follows from combining (2.9) and (2.10). □

2.4 Orthogonality and Duality

Having developed some results on orthogonal decomposition of matrices, we now turn to an investigation of the effects of that decomposition on the dual matrix. In particular we will find that the Gram-Schmidt decomposition of A gives us useful information about A^*. Moreover, we can use that information to understand $A^{(L)*}$, for the $A^{(L)}$ defined in Lemma 2.4.

Lemma 2.6. *Let A belong to $\mathrm{GL}(N, k_v)$, and let $A^* = (A^{-1})^T$ be the dual matrix, which also belongs to $\mathrm{GL}(N, k_v)$. If we write, as in Lemma 2.2,*

$$A = \Psi U W,$$

then we have

$$A^* = \Psi U^{-1} W^*.$$

Of note, W^* is a lower-triangular, not upper triangular, so this is not a Gram-Schmidt decomposition of A^*, although that fact will make it even more useful to us.

Proof. The argument is straightforward calculation from linear algebra. Note first that since Ψ is orthogonal, $\Psi^{-1} = \Psi^T$. Also, because U is diagonal, $U^T = U$. Therefore,

$$\begin{aligned} A^* &= (A^{-1})^T \\ &= (W^{-1}U^{-1}\Psi^{-1})^T \\ &= (\Psi^{-1})^T (U^{-1})^T (W^{-1})^T \\ &= \Psi U^{-1} W^*. \end{aligned}$$

□

In Lemma 2.4, the matrix $A^{(L)}$ is chosen to be ${}^L Z$. We would similarly like to understand $A^{(L)*}$ in relation to $Z^* = U^{-1}W^*$, and thus also A^*. In particular, we will show that there is an L-dimensional subspace $\mathscr{Y}$ of k^N that contains precisely one complete set of preimages for the function $\phi_L : k^N \to k^L$, and has the property that for any $\boldsymbol{y} \in \mathscr{Y}$, it is true that $\|A^* \boldsymbol{y}\|_v = \left\|A^{(L)*} \phi_L(\boldsymbol{y})\right\|_v$.

Lemma 2.7. *Let A, A^* belonging to $\mathrm{GL}(N, k_v)$ be dual automorphisms, and $A^{(L)} \in \mathrm{GL}(L, k_v)$ as indicated in Lemma 2.4, with the associated dual automorphism $A^{(L)*}$. Let the subspace $\mathscr{Y} \subseteq k^N$ be defined by*

$$\mathscr{Y} = \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ y_1 \\ \vdots \\ y_L \end{pmatrix} : y_1, y_2, \ldots, y_L \in k \right\},$$

so that the restriction of ϕ_L is a bijective function between $\mathscr{Y}$ and k^L. Then for any $\boldsymbol{y} \in \mathscr{Y}$,

$$\|A^*\boldsymbol{y}\|_v = \left\|A^{(L)*}\phi(\boldsymbol{y})\right\|_v.$$

Proof. For $\boldsymbol{y} \in \mathscr{Y}$, consider

$$A^*\boldsymbol{y} = \Psi U^{-1} W^* \boldsymbol{y}.$$

Because the first $N-L$ entries of $\boldsymbol{y}$ are all equal to 0 and W^* is lower triangular, it is true that with the matrix written in block diagonal form,

$$W^*\boldsymbol{y} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & {}^L(W^*) \end{pmatrix} \boldsymbol{y},$$

and following this same effect from right to left, because U^{-1} is diagonal,

$$U^{-1}W^*\boldsymbol{y} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & {}^L(U^{-1}) \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & {}^L(W^*) \end{pmatrix} \boldsymbol{y}.$$

Because $\|\Psi\boldsymbol{x}\|_v = \|\boldsymbol{x}\|_v$ for all $\boldsymbol{x} \in k_v^N$,

$$\begin{aligned} \|A^*\boldsymbol{y}\|_v &= \|\Psi U^{-1} W^* \boldsymbol{y}\|_v \\ &= \|U^{-1}W^*\boldsymbol{y}\|_v \\ &= \left\| \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & {}^L(U^{-1}) \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & {}^L(W^*) \end{pmatrix} \boldsymbol{y} \right\|_v. \end{aligned}$$

But now it is clear that this is the same as

$$\left\| {}^{L}(U^{-1})^{L}(W^{*})\phi(\boldsymbol{y}) \right\|_{v} = \left\| A^{(L)*}\phi(\boldsymbol{y}) \right\|_{v}. \qquad \square$$

Note that in the proof, the function ϕ_L does not depend on the place v. Therefore, we can apply the lemma at each place and achieve a result involving the height.

Lemma 2.8. *Let $A = (A_v)$ belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$, and let $A^{(L)} = (A_v^{(L)})$ be the automorphism of $k_{\mathbb{A}}^L$, where the relationship at each place v between A_v and $A_v^{(L)}$ is given in Lemma 2.7. As usual, let $A^* \in \mathrm{Aut}(k_{\mathbb{A}}^N)$ and $A^{(L)*} \in \mathrm{Aut}(k_{\mathbb{A}}^L)$ denote the automorphisms dual to A and $A^{(L)}$. Then for any $\boldsymbol{x}$ in k^L, there exists some $\boldsymbol{x}'$ belonging to k^N such that*

$$H_{A^*}(\boldsymbol{x}') = H_{A^{(L)*}}(\boldsymbol{x})$$

Before proving the lemma, we will use it to extract a key corollary.

Corollary 2.9. *For any A^* belonging to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ and associated $A^{(L)*}$ belonging to $\mathrm{Aut}(k_{\mathbb{A}}^L)$,*

$$\Lambda_M(A^*) \leq \Lambda_M(A^{(L)*}),$$

for $M = 1, 2, \ldots, L$.

Proof. Let $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_M$ belonging to k^L be such that

$$H_{A^{(L)*}}(\boldsymbol{\xi}_m) = \Lambda_m(A^{(L)*}).$$

From Lemma 2.8, there are vectors $\boldsymbol{\xi}'_1, \boldsymbol{\xi}'_2, \ldots, \boldsymbol{\xi}'_M$ in k^N such that

$$H_{A^*}(\boldsymbol{\xi}'_m) = H_{A^{(L)*}}(\boldsymbol{\xi}_m) = \Lambda_m(A^{(L)*}), \tag{2.11}$$

and furthermore for at least one of them

$$H_{A^*}(\boldsymbol{\xi}'_m) \geq \Lambda_M(A^*). \tag{2.12}$$

Therefore, by combining (2.11) and (2.12), we have that for some $m \leq M$,

$$\Lambda_M(A^*) \leq \Lambda_m(A^{(L)*}),$$

and the desired result is achieved because $\Lambda_m(A^{(L)*}) \leq \Lambda_M(A^{(L)*})$. □

We now proceed with the proof of Lemma 2.8.

Proof. For any

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_L \end{pmatrix} \in k^L,$$

let

$$\boldsymbol{x}' = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_1 \\ \vdots \\ x_L \end{pmatrix} \in k^N.$$

In the notation of Lemma 2.7, we may say that $\boldsymbol{x}'$ is the unique vector in $\mathscr{Y} \subseteq k^N$ such that $\phi_L(\boldsymbol{x}') = \boldsymbol{x}$. Because the vector $\boldsymbol{x}'$ depends only on $\boldsymbol{x} \in k^L$

and not on the place v, we may apply Lemma 2.7 at each place, yielding

$$\|A_v^* \boldsymbol{x}'\|_v = \left\|A_v^{(L)*} \boldsymbol{x}\right\|_v$$
$$|A_v^* \boldsymbol{x}'|_v = \left|A_v^{(L)*} \boldsymbol{x}\right|_v .$$

Therefore, because the equality holds at each place, we also have

$$\begin{aligned} H_{A^*}(\boldsymbol{x}') &= \prod_v |A_v^* \boldsymbol{x}'|_v \\ &= \prod_v \left|A_v^{(L)*} \boldsymbol{x}\right|_v = H_{A^{(L)*}}(\boldsymbol{x}), \end{aligned}$$

and the lemma is proved. □

2.5 Taming the Places

The twisted height is a function defined on $\mathbb{P}^{N-1}(k)$, which means that we may think of it as a function on k^N, with the additional property that if $\boldsymbol{\xi} \in k^N$ and $\alpha \in k^\times$, then $H_A(\boldsymbol{\xi}) = H_A(\alpha\boldsymbol{\xi})$. For our purposes, it is useful to find a particular α so that $\alpha\boldsymbol{\xi}$ has desirable properties. In particular, we hope that we can control or at least understand $\|A_v \alpha\boldsymbol{\xi}\|_v$ at each place.

This is necessary because if $\boldsymbol{\xi} \in k^N$, and $H_A(\boldsymbol{\xi}) = \mu$, we know very little about the contribution of each individual place in the global height. We only know that $\|A_v \boldsymbol{x}\|_v = 1$ except on some finite set of places. However, it might be that at some place v_1, $\|A_{v_1}\boldsymbol{\xi}\|_{v_1}$ is extremely small, while at some other place v_2, $\|A_{v_2}\boldsymbol{\xi}\|_{v_2}$ is tremendously large. Moreover, let $S_1 = \{v : \|A_v \boldsymbol{x}_1\|_v \neq 1\}$ and $S_2 = \{v : \|A_v \boldsymbol{x}_2\|_v \neq 1\}$. It may be that S_1 and S_2 are very different sets, which is not desirable. In this section we show that by carefully choosing the scalar multiple α for each $\boldsymbol{\xi}$, we can avoid both of these concerns.

Although we are concerned with this result primarily for the purpose of applying it to the twisted height, we will state and prove it in the slightly more general setting of the idele group. As long as $\boldsymbol{\xi} \in k^N \backslash \{\mathbf{0}\}$ and $A \in \mathrm{Aut}(k_{\mathbb{A}}^N)$, then there is some $x = (x_v) \in k_{\mathbb{A}}^\times$ so that $\|x_v\|_v = \|A_v \boldsymbol{\xi}\|_v$ at each place, and hence $H_A(\boldsymbol{\xi}) = |x|_{\mathbb{A}}$. Therefore, any result we prove for elements of the idele group can then be applied to H_A over k^N.

Lemma 2.10. *Let k be a number field of degree d over $\mathbb{Q}$, and $k_{\mathbb{A}}^\times$ the idele group associated to k. There exists a finite set of places $S(k)$, which includes all of the infinite places, so that for every x in $k_{\mathbb{A}}^\times$ there exists some α belonging to $k^\times$ such that*

(i) for $v \notin S(k)$, $|\alpha x_v|_v = 1$,

(ii) for $v \in S(k)$, $v \nmid \infty$,

$$|\alpha x_v|_v \in \mathscr{S}(v), \tag{2.13}$$

(iii) for $v|\infty$,

$$|\alpha x_v|_v \leq d_1(k)(\eta(k)|x|_{\mathbb{A}})^{d_v/d}. \tag{2.14}$$

Here $\mathscr{S}(v) = \mathscr{S}_k(v)$ is a finite set that is defined for each of the finite places v contained in $S(k)$, and $d_1(k)$ and $\eta(k)$ are constants that depend only on the number field k.

Lemma 2.10 bears some resemblance to the weak and strong approximation principles for adele rings. However, those theorems apply to the additive

structure on $k_{\mathbb{A}}$, while Lemma 2.10 is for the idele group $k_{\mathbb{A}}^{\times}$, so it applies to the multiplicative structure of $k_{\mathbb{A}}$. We will require a slightly different form of (2.14), using the $\| \ \|_v$ absolute value instead of $| \ |_v$. For convenience, we record the details here:

$$\begin{aligned} \|\alpha x_v\|_v &= |\alpha x_v|_v^{d/d_v} \\ &\leq (d_1(k)(\eta(k)|x|_{\mathbb{A}})^{d_v/d})^{d/d_v} \\ &= d_1(k)^{d/d_v}\eta(k)|x|_{\mathbb{A}}. \end{aligned} \tag{2.15}$$

In order to prove the lemma, we need to introduce some notation and summarize the relevant information from section 4 of chapter 5 in [20]. For notation that is unique to this section, we closely follow the notation used in that work. For concepts that are used elsewhere in this dissertation, we prefer the previously introduced notation for the sake of consistency.

We will let $\mathcal{O}_v^{\times}$ denote the invertible elements of $\mathcal{O}_v$, which is to say $\mathcal{O}_v^{\times} = \{x \in k_v : |x|_v = 1\}$. Let

$$\begin{aligned} \Omega_{\infty} &= \prod_{v|\infty} k_v^{\times} \times \prod_{v\nmid\infty} \mathcal{O}_v^{\times} \\ &= \{x \in k_{\mathbb{A}}^{\times} : |x_v|_v = 1 \text{ if } v \nmid \infty\}. \end{aligned}$$

Then $k^{\times}\Omega_{\infty}$ is a finite-index subgroup of $k_{\mathbb{A}}^{\times}$, and the index $h = [k_{\mathbb{A}}^{\times} : k^{\times}\Omega_{\infty}]$ is called the *class number* of k.

Let $w_0, w_1, \ldots, w_r$ be the infinite places of k. Define functions

$$\begin{aligned} l : \Omega_{\infty} &\to \mathbb{R}^{r+1} \\ (x_v) &\mapsto (\log|x_{w_0}|_{w_0}, \log|x_{w_1}|_{w_1}, \ldots, \log|x_{w_r}|_{w_r}) \end{aligned}$$

and

$$\begin{aligned} T : \mathbb{R}^{r+1} &\to \mathbb{R} \\ \boldsymbol{x} &\mapsto \sum_{i=0}^{r} x_i. \end{aligned}$$

The function l is a homomorphism from the multiplicative group Ω_∞ to the additive group $\mathbb{R}^{r+1}$. Consider the hyperplane $P = \{\boldsymbol{x} \in \mathbb{R}^{r+1} : T(\boldsymbol{x}) = 0\}$, it then follows that l defines a homomorphism from $\Omega_1 = \Omega_\infty \cap k_{\mathbb{A}}^1$ to P with kernel $U = \{x \in \Omega_\infty : |x_v|_v = 1 \text{ for all } v\}$. Let E be the torsion subgroup of k, i.e. the cyclic group of roots of unity in k; then $l(E) \subseteq U$. For any x in Ω_∞, it is possible to recover the volume of x from the formula

$$T(l(x)) = \log |x|_{\mathbb{A}}. \tag{2.16}$$

Let $\mathcal{O}_k^\times$ be the group of units of k. Then $\mathcal{O}_k^\times \subseteq \Omega_\infty$; by Dirichlet's Unit theorem, $\mathcal{O}_k^\times$ modulo torsion is generated by a set of size r. Furthermore, $\mathcal{O}_k^\times$ is a discrete subgroup of Ω_1 and $\Gamma = l(\mathcal{O}_k^\times)$ is a discrete subgroup of P such that P/Γ is compact, so Γ is a full-rank lattice in the vector space P. Let $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\}$ be a set of free generators for $\mathcal{O}_k^\times / E$; then $\{l(\epsilon_1), l(\epsilon_2), \ldots, l(\epsilon_r)\}$ form an $\mathbb{R}$-basis for P and generate Γ.

A basis for $\mathbb{R}^{r+1}$ can be found by using this basis for P, along with one vector not in P. For this last basis vector, it will be convenient to use $\boldsymbol{\delta} = (d_{w_0}, d_{w_1}, \ldots, d_{w_r})^T$, where as usual d_v is the local degree at the place v. Because the places $w_0, w_1, \ldots, w_r$ are all infinite, the entries of $\boldsymbol{\delta}$ are all 1 or

2, and

$$T(\boldsymbol{\delta}) = \sum_{i=0}^{r} d_{w_i} = d.$$

For reasons that will soon become clear, it is useful to have a normalized form of this vector. Let $\boldsymbol{\delta}' = \boldsymbol{\delta}/d$, therefore $T(\boldsymbol{\delta}') = 1$.

Now that we have chosen $r+1$ linearly independent vectors in $\mathbb{R}^{r+1}$, we form a $(r+1) \times (r+1)$ matrix F using these vectors as its columns, i.e.

$$F = (\boldsymbol{\delta}' \; l(\epsilon_1) \; l(\epsilon_2) \; \cdots \; l(\epsilon_r)),$$

so that $F \in \mathrm{GL}(r+1, \mathbb{R})$. For any $\boldsymbol{t} = (t_0, t_1, \ldots, t_r)^T \in \mathbb{R}^{r+1}$, we have

$$T(F\boldsymbol{t}) = t_0. \tag{2.17}$$

We require one more definition before stating the main proposition. A *fundamental domain of order e* is an idellic subset $\mathscr{D} \subseteq k_{\mathbb{A}}^{\times}$ such that every element α belonging to $k_{\mathbb{A}}^{\times}/k$ has exactly e coset representatives inside of $\mathscr{D}$.

Proposition 2.11. *Let $\{a_1, a_2, \ldots, a_h\}$ be a full set of coset representatives for $k^{\times}\Omega_{\infty}$ in $k_{\mathbb{A}}^{\times}$. Let E be the torsion of k, i.e. the group of roots of unity contained in k, and suppose it has order e. Let $I = [0, 1) \subseteq \mathbb{R}$. With l and F as defined in this section,*

$$\mathscr{D} = \bigcup_{i=1}^{h} a_i l^{-1}(F(\mathbb{R} \times I^r))$$

is a fundamental domain of order e for $k_{\mathbb{A}}^{\times}$ modulo $k^{\times}$.

In this case, the e distinct coset representatives in $\mathscr{D}$ of an element α in $k_{\mathbb{A}}^{\times}/k$ differ only by roots of unity, so at each place the absolute values of all the different coset representatives are the same. The proof of this proposition can be found in Chapter 5 of [20], and we do not reproduce it here because we will not require any of its arguments. Instead, we will use the proposition to prove Lemma 2.10.

Proof of Lemma 2.10. As in Proposition 2.11, let $\{a_1, a_2, \ldots, a_h\}$ be a full set of coset representatives for $k^{\times}\Omega_{\infty}$ in $k_{\mathbb{A}}^{\times}$. As before, let $w_0, w_1, \ldots, w_r$ be the infinite places of k. For each $i = 1, 2, \ldots, h$, let $b_i = (b_i^{(v)}) \in \Omega_{\infty}$ be chosen so that $b_i^{(w_j)} = (a_i^{(w_j)})^{-1}$. Replace each a_i with $a_i b_i$, which is a representative for the same coset, and now $a_i^{(w_j)} = 1$ at all the infinite places.

Because $\mathscr{D}$ is a fundamental domain for $k_{\mathbb{A}}^{\times}/k^{\times}$, for every $x \in k_{\mathbb{A}}^{\times}$ and precisely one of the a_i, there exists an α, unique up to torsion, in $k^{\times}$, as well as some $z = (z_v) \in \mathscr{D}$ such that

$$x = \alpha^{-1} a_i z$$

$$\alpha x = a_i z.$$

By construction,

$$|\alpha x_v|_v = \begin{cases} |z_v|_v & \text{if } v|\infty \\ |a_h^{(v)}|_v & \text{if } v \nmid \infty \end{cases}$$

To simplify notation, let $\mu = |x|_{\mathbb{A}}$ and $\eta_i = |a_i|_{\mathbb{A}}$; then it must be that $|z|_{\mathbb{A}} = \eta_i^{-1}\mu$, and furthermore $T(l(z)) = \log(\eta_i^{-1}\mu)$. If $\boldsymbol{t}$ is chosen so that $F(\boldsymbol{t}) = l(z)$, then $t_0 = \log(\gamma_i^{-1}\mu)$, and we have $0 \leq t_s \leq 1$ whenever $1 \leq s \leq r$.

Because z is in $\mathscr{D}$, we can bound $|z_{w_j}|_{w_j}$ at each infinite place. For $j = 1, 2, \ldots, r$, let $d_j = d_{w_j}$ denote the local degree, and from the definition of l and F we have

$$\log |z_{w_j}|_{w_j} \leq d^{-1} \log(\eta_i^{-1}\mu) d_j + \sum_{s=1}^{r} \log |\epsilon_s^{(w_j)}|_{w_j} \tag{2.18}$$

$$|z_{w_j}|_{w_j} \leq (\eta_i^{-1}\mu)^{d_j/d} \prod_{s=1}^{r} |\epsilon_s^{(w_j)}|_{w_j}. \tag{2.19}$$

The right hand side of the second inequality depends on the coset representatives a_i and the choice of generators for $\mathcal{O}_k^{\times}/E$. There should be some optimal choice of generators, the analytical properties of which can be determined by appealing to the classical Minkowski's Successive Minima theorem.

Even without an optimal choice of generators for the unit group mod torsion, by using any set of generators and choosing maximum absolute values we arrive at a version of (2.19) so that, up to constants determined by the field k, the right hand side depends only on $\mu = |x|_{\mathbb{A}}$. Set

$$d_1(k) = \prod_{s=1}^{r} \max_{0 \leq j \leq r} \{|\epsilon_s^{(w_j)}|_{w_j}\}$$
$$\eta(k) = \max_{1 \leq i \leq h} \{\eta_i^{-1}\}$$

then (2.19) can be simplified as

$$|z_{w_j}|_{w_j} \leq d_1(k)(\eta(k)\mu)^{d_j/d}, \tag{2.20}$$

which is the same as (2.14). □

It would be desirable to find estimates in terms of k for the constants

$d_1(k)$ and $\eta(k)$. For the second, it would be helpful also to know the minimum size of the set $S(k)$. However, this is beyond the scope of the present work.

Chapter 3

The Korkin-Zolotarev Matrix

In this chapter, we describe for each $A = (A_v)$ belonging to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ the choice of a linearly independent set of vectors $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_N$ in k^N that correspond to the classical Korkin-Zolotarev basis vectors. The correspondence is realized in two main properties of the Gram-Schmidt orthogonalization of AX. If we write

$$X = (\boldsymbol{\xi}_1 \ \boldsymbol{\xi}_2 \ \cdots \ \boldsymbol{\xi}_N)$$

for the matrix in $\mathrm{GL}(N, k)$ having $\boldsymbol{\xi}_n$ as its n-th column, then in the Gram-Schmidt decomposition

$$AX = \Psi UW,$$

(i) the diagonal entries u_n of U must have small volume, and

(ii) for $1 < m < n < N$, the entries w_{mn} of W are contained in a simple fundamental domain $\mathcal{F}$ for $k_{\mathbb{A}}/k$, which will be described later.

Along with the careful application of Lemma 2.10, these properties will allow us to bound the twisted heights $H_A(\boldsymbol{\xi}_n)$ in terms of the successive minima $\Lambda_n(A)$.

In constructing the vectors $\boldsymbol{\xi}_n$, we will use Lemma 6 from [17], which states that for any A belonging to $\mathrm{Aut}(k_{\mathbb{A}}^n)$, there exists a point $\boldsymbol{x}_n$ in $\mathbb{P}^{n-1}(k)$ such that

$$H_A(\boldsymbol{x}_n) = \Lambda_n(A).$$

Theorem 3.1. *Let A belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$. Then there exist linearly independent vectors $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_N$ in k^N such that*

(i) $H_A(\boldsymbol{\xi}_1) = \Lambda_1(A)$,

(ii) if $\mathscr{A}_{N-n}^{(v)} = span\{A_v\boldsymbol{\xi}_1, A_v\boldsymbol{\xi}_2, \ldots, A_v\boldsymbol{\xi}_{N-n}\}$, *and* $(AX)^{(n)} = \left((A_vX)^{(n)}\right)$ *is the automorphism of* $k_{\mathbb{A}}^n$ *given by Lemma 2.4, then*

$$H_{(AX)^{(n)}}\left(\phi_n(\boldsymbol{e}_{N-n+1})\right) = \Lambda_1\left((AX)^{(n)}\right), \tag{3.1}$$

where $\boldsymbol{e}_n$ is the n-th standard basis vector.

Before proceeding to the proof, let us note that for each $m = 1, 2, \ldots N$, there are many choices of $\boldsymbol{x}$ such that $\phi_m(\boldsymbol{x}) = \phi_m(\boldsymbol{\xi}_{m+1})$. We may choose any of these, and the results of the theorem will still hold true. Later, when we examine the Gram-Schmidt orthogonalization of AX, we will impose further conditions on $\boldsymbol{\xi}_n$ that afford greater control of the entries in the matrices involved in that decomposition.

Proof. The proof will follow by induction on n. According to Lemma 6 of [17], there exists $\boldsymbol{\xi}_1$ in k^N so that $H_A(\boldsymbol{\xi}_1) = \Lambda_1(A)$. Now, for any $1 < n \leq N$

assume that $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_n$ have been found. Let X_n be any matrix in $\mathrm{GL}(N, k)$ having these vectors as its first n columns.

Apply Lemma 2.5 to the automorphism AX_n, and let B be the automorphism of $k_{\mathbb{A}}^{N-n}$ determined as a result. Again appealing to Lemma 6 of [17], let $\boldsymbol{\xi}'$ be a vector in k^{N-n} such that $H_B(\boldsymbol{\xi}') = \Lambda_1(B)$. Because $\boldsymbol{\xi}'$ is non-zero, any vector $\boldsymbol{x}$ in k^N such that $\phi_{N-n}(\boldsymbol{x}) = \boldsymbol{\xi}'$ has a non-zero component for some m such that $N - n < m \leq N$, so $X^{(n)}\boldsymbol{x}$ is linearly independent of $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_n$. We now select

$$\boldsymbol{\xi}_{n+1} = X_n \boldsymbol{x},$$

because by construction this vector satisfies the conditions of the theorem. □

Although we have established the existence of the vectors $\boldsymbol{\xi}_n$ satisfying Theorem 3.1, there are many possible choices for each vector, not all of which are amenable to our goals. We seek to impose further conditions on the choice, which can be expressed in terms of the Gram-Schmidt orthogonalization of the automorphism AX.

Before proceeding, we require a technical detail regarding $k_{\mathbb{A}}/k$. There is a positive real number τ_k such that the adelic subset

$$\prod_{v|\infty} \{x \in k_v : \|x\|_v \leq \tau_k\} \times \prod_{v \nmid \infty} \mathcal{O}_v$$

contains a fundamental domain for $k_{\mathbb{A}}/k$. We will call this fundamental domain $\mathcal{F}$. When $k = \mathbb{Q}$, we have $\tau_{\mathbb{Q}} = 1/2$, and estimates on τ_k for other number fields can be found in Theorem 6 of [11].

Lemma 3.2. *Let $W = (W_v)$ belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ such that at each place v, W_v is upper triangular, and, furthermore at each place all the diagonal entries $w_{nn}^{(v)}$ are equal to 1, for $n = 1, 2, \ldots, N$. Then there is an upper triangular matrix Y belonging to $\mathrm{GL}(N, k)$ with all diagonal entries equal to 1, and all the off-diagonal entries of $Z = WY$ are contained in $\mathcal{F}$.*

Proof. This proof is due to Vaaler, and its principles are valid in a more general context including many locally compact groups. For $1 < l < n < N$, we have

$$\begin{aligned} z_{ln}^{(v)} &= \sum_{m=l}^{n} w_{lm}^{(v)} y_{mn} \\ &= y_{ln} + \sum_{m=l+1}^{n-1} w_{lm}^{(v)} y_{mn} + w_{ln}^{(v)}. \end{aligned} \tag{3.2}$$

We now induct on the quantity $j = n - l$. For $j = 1$, we have $n = l + 1$, and so equation 3.2 simplifies to

$$z_{l(l+1)}^{(v)} = y_{l(l+1)} + w_{l(l+1)}^{(v)}.$$

Because $\mathcal{F}$ is a fundamental domain for $k_{\mathbb{A}}/k$, it is clear that we may choose $y_{l(l+1)}$ so that $(z_{l(l+1)}^{(v)})$ lies in $\mathcal{F}$. For $j > 1$, we may assume that y_{ln} have been chosen whenever $1 \leq n < l + j$, so in the equation

$$z_{ln}^{(v)} = y_{l(l+j)} + \sum_{m=l+1}^{l+j-1} w_{lm}^{(v)} y_{mn} + w_{l(l+j)}^{(v)}$$

everything is already determined except for the term $y_{l(l+j)}$, and here again we may choose $y_{l(l+j)}$ so that $(z_{l(l+j)}^{(v)})$ falls within $\mathcal{F}$. □

Theorem 3.3. *Let A belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$, and X the matrix determined by Theorem 3.1, which belongs to $\mathrm{GL}(N,k)$. There exists some $B = (B_v)$ also belonging to $\mathrm{Aut}(k_{\mathbb{A}}^N)$, which may be decomposed using Lemma 2.3 as*

$$B = \Psi UW,$$

and has the properties that

(i) for $1 \le n \le N$, $\Lambda_n(B) = \Lambda_n(A)$ and $\Lambda_n(B^*) = \Lambda_n(A^*)$,

(ii) for $1 \le n \le N$, $H_B(\boldsymbol{e}_n) = H_A(\boldsymbol{\xi}_n)$,

(iii) for $1 \le n \le N$, $|u_n|_{\mathbb{A}} = \Lambda_1(B^{(N-n+1)})$,

(iv) for all places v of k and $1 \le n \le N$,

$$|u_n^{(v)}|_v \le d_1(k)(\eta(k)|u|_{\mathbb{A}})^{d_v/d} \text{ if } v|\infty$$
$$|u_n^{(v)}|_v \in \mathscr{S}(v) \text{ if } v \in S(k),\ v \nmid \infty$$
$$|u_n^{(v)}|_v = 1 \quad \text{if } v \notin S(k),$$

(v) for $1 < m < n \le N$, w_{mn} belongs to $\mathcal{F}$.

In the statement of the theorem, $d_1(k), \eta(k), S(k)$, and $\mathscr{S}(v)$ are all the same as those defined in Lemma 2.10.

Proof. This theorem is a combination of Theorem 3.1, Lemma 2.10, and Lemma 3.2.

We start with the matrix AX. Since the twisted height is a function on projective space, for any β in k, we have

$$H_{A^{(n)}}(\phi_n(\beta\boldsymbol{\xi}_{N-n+1})) = H_{A^{(n)}}(\beta\phi_n(\boldsymbol{\xi}_{N-n+1})) = \Lambda_1(A^{(n)}).$$

Now let $\eta = (\eta_v) \in k_{\mathbb{A}}^{\times}$ be such that $\|\eta_v\|_v = \|A_v^{(n)}\phi_n(\boldsymbol{\xi}_{N-n+1})\|_v$. For every η there is an α such that $\alpha\eta$ satisfies the conditions of Lemma 2.10. Let $\boldsymbol{\xi}'_{N-n+1} = \alpha\boldsymbol{\xi}_{N-n+1}$ for each $n = 1, 2, \ldots, N$, and let X' be the matrix with these vectors as its columns. It is clear that AX' still satisfies (3.1).

Now write

$$AX' = \Psi U' W'$$

and apply Lemma 3.2 to W'. The result is that there is an upper-triangular matrix Y in $\mathrm{GL}(N, K)$ and an upper-triangular automorphism Z belonging to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ such that

$$Z = W'Y$$

Let $B = AX'Y$, which has Gram-Schmidt orthogonalization

$$B = AX'Y = \Psi U' Z,$$

and we will show that the matrix B satisfies the conditions of the theorem. Because X' and Y are both in $\mathrm{GL}(N, k)$, we must have $\Lambda_n(B) = \Lambda_n(A)$ for $n = 1, 2, \ldots, N$. Likewise, $B^* = A^*(X'Y)^*$, and $(X'Y)^*$ is in $\mathrm{GL}(N, k)$, so $\Lambda_n(B^*) = \Lambda_n(A^*)$. Furthermore, since Y is upper-triangular and has ones along the diagonal, the n-th column of $B - AX'Y$ is a linear combination of

the first n columns of AX'. Therefore,

$$H_{B^{(n)}}(\phi_n(\boldsymbol{e}_{N-n+1})) = H_{(AX)^{(n)}}(\phi_n(\boldsymbol{e}_{N-n+1})) = \Lambda_1((AX)^{(n)}),$$

because in constructing $(AX)^{(n)}$ we project onto an orthogonal complement of

$$\text{span}\{A\boldsymbol{\xi}_1, A\boldsymbol{\xi}_2, \ldots, A\boldsymbol{\xi}_{N-n}\},$$

so adding a linear combination of these vectors to $A\boldsymbol{\xi}_{N-n+1}$ does not change the projection. □

Chapter 4

The Main Inequalities

In this chapter, we establish the main results of the thesis. Having done the work of showing that a Korkin-Zolotarev matrix exists in the previous chapter, we exploit the analytical properties that it was designed to have. This work is inspired by [6], in particular Theorems 2.1-2.4, along with Propositions 4.1 and 4.2, which prove the classical analogues to the results that we present here.

4.1 Bounds in Terms of Successive Minima

The vectors $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_N$ used in the previous chapter were chosen primarily so that $H_{(AX)^{(n)}}(\phi_n(\boldsymbol{e}_{N-n+1}))$ would be as small as possible. It is our goal now to show that in fact $H_A(\boldsymbol{\xi}_n)$ is small, in particular that $H_A(\boldsymbol{\xi}_n)$ is comparable to $\Lambda_n(A)$.

Theorem 4.1. *For A belonging to $\mathrm{Aut}(k_{\mathbb{A}}^N)$, let X in $\mathrm{GL}(N,k)$ be the matrix defined by Lemma 3.3, and let $\boldsymbol{\xi}_n$ be the n-th column vector of X. Then*

$$H_A(\boldsymbol{\xi}_n) \leq d_3(k)(1+(n-1)\tau_k^2)^{1/2}\Lambda_n(A),$$

where

$$d_3(k) = d_2(k)d_1(k)^r\eta(k)$$

and r is the number of infinite places of k.

The constants $d_1(k), d_2(k), \eta(k)$, and τ_k were all defined in Chapter 3.

Proof. Because $H_A(\boldsymbol{\xi}_n) = H_B(\boldsymbol{e}_n)$, we will work in terms of the latter. Also, since $B = AX$ for some X belonging to $\mathrm{GL}(N, k)$, it must be that for $n = 1, 2, \ldots, N$, $\Lambda_n(A) = \Lambda_n(B)$, so the successive minima are interchangeable. Write

$$B = \Psi U W$$

for the Gram-Schmidt orthogonalization of B. Therefore

$$\begin{aligned} H_A(\boldsymbol{\xi}_n) &= \prod_v |\Psi_v U_v W_v \boldsymbol{e}_n|_v \\ &= \prod_{v|\infty} \left(\|u_n^{(v)}\|_v^2 + \sum_{m=1}^{n-1} \|w_{mn}^{(v)} u_m^{(v)}\|_v^2 \right)^{\frac{d_v}{2d}} \\ &\quad \times \prod_{v\nmid\infty} \max_{1\le m\le n} |u_m^{(v)} w_{mn}^{(v)}|_v. \end{aligned} \tag{4.1}$$

We can refine and simplify this estimate. At non-Archimedean places v that are not in $S(k)$,

$$|u_m^{(v)} w_{mn}^{(v)}|_v \le 1, \quad \text{for } 1 \le m \le n,$$

while for any non-Archimedean place v which is part of $S(k)$,

$$|u_m^{(v)} w_{mn}^{(v)}|_v \le \max_{z\in\mathscr{S}(v)} z, \quad \text{for } 1 \le m \le n.$$

Hence the product over the non-Archimedean places can be estimated as

$$\prod_{v\nmid\infty} \max_{1\le m\le n} |u_m^{(v)} w_{mn}^{(v)}|_v \le \prod_{\substack{v\in S(k)\\ v\nmid\infty}} \max_{z\in\mathscr{S}(v)} z = d_2(k). \tag{4.2}$$

By using (4.2) at the non-Archimedean places and (2.15) in conjunction with Theorem 3.3 at the Archimedean places, (4.1) becomes

$$H_A(\boldsymbol{\xi}_n) \leq d_2(k) \prod_{v|\infty} \left(\left(d_1(k)^{d/d_v} \eta(k) \Lambda_1(B^{(N-n+1)})\right)^2 + \sum_{m=1}^{n-1} \left(\tau_k d_1(k)^{d/d_v} \eta(k) \Lambda_1(B^{(N-m+1)})\right)^2 \right)^{\frac{d_v}{2d}}$$

$$H_A(\boldsymbol{\xi}_n) \leq d_3(k) \prod_{v|\infty} \left(\Lambda_1(B^{(N-n+1)})^2 + \sum_{m=1}^{n-1} \left(\tau_k \Lambda_1(B^{(N-m+1)})\right)^2 \right)^{\frac{d_v}{2d}} \tag{4.3}$$

It suffices now to compare $\Lambda_1(B^{(N-n+1)})$ to $\Lambda_n(A)$, for $1 \leq n \leq N$. At each place v, for all $\boldsymbol{x}$ belonging to k^N we have

$$\left\| B^{(N-n+1)} \phi_{N-n+1}(\boldsymbol{x}) \right\|_v = \left\| (\mathbf{1}_N - P_v(\mathscr{B}_n^{(v)})) B_v \boldsymbol{x} \right\|_v .$$

By the definition of successive minima, there are at least n linearly independent vectors $\boldsymbol{x}$ in k^N such that $H_A(X\boldsymbol{x}) \leq \Lambda_n(B) = \Lambda_n(A)$, and at least one of them, say $\boldsymbol{y} = (y_1, y_2, \ldots, y_N)$, is such that $y_m \neq 0$ for some $N - n + 1 \leq m \leq N$.

At each place v it is true that

$$0 < \left\| B_v^{(N-n+1)} \phi_n(\boldsymbol{y}) \right\|_v \leq \left\| B_v \boldsymbol{y} \right\|_v ,$$

where the right hand side is obvious and the left hand side is implied by the previous assertion, which is equivalent to the statement that $\phi_n(\boldsymbol{y})$ is nonzero. It now follows that

$$\begin{aligned} \Lambda_1(B^{(N-n+1)}) &\leq H_{B^{(N-n+1)}}(\phi_n(\boldsymbol{y})) \\ &\leq H_B(\boldsymbol{y}) \\ &\leq \Lambda_n(B). \end{aligned} \tag{4.4}$$

By applying (4.4) for each $\Lambda_1(B^{(N-n+1)})$ in (4.3) we find

$$H_A(\boldsymbol{\xi}_n) \leq d_3(k) \prod_{v|\infty} \left(\Lambda_n(B)^2 + \sum_{m=1}^{n-1} \left(\tau_k \Lambda_m(B)\right)^2 \right)^{\frac{d_v}{2d}} \tag{4.5}$$

Now, appealing to the trivial fact that for $1 \leq m < n \leq N$ we have $\Lambda_m(A) \leq \Lambda_n(A)$ we simplify the estimate even further.

$$H_A(\boldsymbol{\xi}_n) \leq d_3(k) \prod_{v|\infty} \left(\Lambda_n(B)^2 + \sum_{m=1}^{n-1} \left(\tau_k \Lambda_n(B)\right)^2 \right)^{\frac{d_v}{2d}} \tag{4.6}$$

$$\leq d_3(k)(1 + (n-1)\tau_k^2)^{1/2} \Lambda_n(B), \tag{4.7}$$

which is the desired bound. □

With the twisted height of each $\boldsymbol{\xi}_n$ bounded, it is now possible to produce a theorem bounding the product of these heights in terms that depend only on the field k. The best possible result of this type, using vectors $\boldsymbol{\xi}'_n$ chosen specifically for this purpose, is the version of Siegel's Lemma given by Vaaler in Theorem 1 of [17]. Because we have chosen the vectors $\boldsymbol{\xi}_n$ not only to have small height, but also to satisfy other properties, we may think of the following theorem as a measure of the compromise necessary to have those additonal properties. This is similar to how Theorem 1.2 measures the difference between the original Minkowski's Successive Minima theorem and a basis form of the same.

Theorem 4.2. *Let A belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$, and let $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_N$ be a set of Korkin-Zolotarev vectors with respect to A. Then*

$$\prod_{n=1}^{N} H_A(\boldsymbol{\xi}_n) \leq d_3(k)^N \left(\prod_{n=1}^{N} \left(1 + (n-1)\tau_k^2\right) \right)^{1/2} \gamma_k(N)^{N/2} |A|_{\mathbb{A}}.$$

Proof. For each $n = 1, 2, \ldots, N$, Theorem 4.1 provides a bound for $H_A(\boldsymbol{\xi}_n)$. Taking the product we find

$$\begin{aligned}\prod_{n=1}^{N} H_A(\boldsymbol{\xi}_n) &\leq \prod_{n=1}^{N} \left(d_3(k)(1+(n-1)\tau_k^2)^{1/2}\Lambda_n(A)\right) \\ &= d_3(k)^N \left(\prod_{n=1}^{N}\left(1+(n-1)\tau_k^2\right)\right)^{1/2} \times \prod_{n=1}^{N}\Lambda_n(A).\end{aligned} \tag{4.8}$$

According to the proof of Theorem 1 from [17],

$$\prod_{n=1}^{N}\Lambda_n(A) \leq \gamma_k(N)^{N/2}|A|_{\mathbb{A}}, \tag{4.9}$$

and by combining (4.8) and (4.9) the theorem is proved. □

4.2 Mahler Products

We now seek to bound products of the type

$$\Lambda_n(A)\Lambda_m(A^*),$$

where $m + n = N + 1$. We do this by building up several related theorems first, allowing us to connect the Korkin-Zolotarev estimates with the successive minima.

Proposition 4.3. *Let A belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ and let A^* be its dual automorphism. Let X be the Korkin-Zolotarev matrix for A, with column vectors $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_N$. Then*

$$H_A(\boldsymbol{\xi}_n)\Lambda_1(A^*) \leq d_3(k)\left(1+(n-1)\tau_k^2\right)^{1/2}\gamma_k^*(N).$$

Proof. As in Theorem 4.1, we start with the estimate (4.3) for the height of one of the Korkin-Zolotarev vectors, along with the identity $\Lambda_1(A^*) = \Lambda_1(B^*)$.

$$H_A(\boldsymbol{\xi}_n)\Lambda_1(A^*) \leq d_3(k) \prod_{v|\infty} \left(\Lambda_1(B^{(N-n+1)})^2 + \sum_{m=1}^{n-1} \left(\tau_k \Lambda_1(B^{(N-m+1)})\right)^2 \right)^{\frac{d_v}{2d}} \Lambda_1(B^*) \tag{4.10}$$

We distribute $\Lambda_1(B^*)$ into the product and over the sum, yielding

$$H_A(\boldsymbol{\xi}_n)\Lambda_1(A^*) \leq d_3(k) \prod_{v|\infty} \left(\left(\Lambda_1(B^{(N-n+1)})\Lambda_1(B^*)\right)^2 + \sum_{m=1}^{n-1} \left(\tau_k \Lambda_1(B^{(N-m+1)})\Lambda_1(B^*)\right)^2 \right)^{\frac{d_v}{2d}} \tag{4.11}$$

Using Corollary 2.9 with $l = 1$ we replace $\Lambda_1(B^*)$ with $\Lambda_1(B^{(N-m+1)*})$:

$$H_A(\boldsymbol{\xi}_n)\Lambda_1(A^*) \leq d_3(k) \prod_{v|\infty} \left(\left(\Lambda_1(B^{(N-n+1)})\Lambda_1(B^{(N-n+1)*})\right)^2 + \sum_{m=1}^{n-1} \left(\tau_k \Lambda_1(B^{(N-m+1)})\Lambda_1(B^{(N-m+1)*})\right)^2 \right)^{\frac{d_v}{2d}} \tag{4.12}$$

and by the definition of Hermite's constant, we know that for any C belonging to $\mathrm{Aut}(k_{\mathbb{A}}^n)$

$$\begin{aligned} \Lambda_1(C)\Lambda_1(C^*) &\leq \gamma_k(n)^{1/2} |C|_{\mathbb{A}}^{1/n} \gamma_k(n)^{1/2} |C^*|_{\mathbb{A}}^{1/n} \\ &= \gamma_k(n), \end{aligned}$$

because $|C^*|_{\mathbb{A}} = |C|_{\mathbb{A}}^{-1}$. Using this in each term of the summand on the right

hand side of (4.12) we find

$$H_A(\boldsymbol{\xi}_n)\Lambda_1(A^*) \leq d_3(k)\prod_{v|\infty}\Bigg(\gamma_k(N-n+1)^2 + \sum_{m=1}^{n-1}\tau_k^2\gamma_k(N-m+1)^2\Bigg)^{\frac{d_v}{2d}}.$$

Replacing each occurrence of $\gamma_k(n)$ with $\gamma_k^*(N)$, we carry out an analysis identical to the one performed between (4.6) and (4.7), and the result follows. $\square$

Because $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_n$ are linearly independent, we must have

$$\Lambda_n(A) \leq \max_{1\leq m\leq n} H_A(\boldsymbol{\xi}_m),$$

which directly gives a corollary to Proposition 4.3.

Corollary 4.4. *If A and A^* are dual members of $\mathrm{Aut}(k_{\mathbb{A}}^N)$, then for $n = 1, 2, \ldots, N$, we have*

$$\Lambda_n(A)\Lambda_1(A^*) \leq d_3(k)(1+(n-1)\tau_k^2)^{1/2}\gamma_k^*(N).$$

Theorem 4.5. *Let A and A^* belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ and be dual to each other. Let X be the Korkin-Zolotarev matrix for A with columns $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots \boldsymbol{\xi}_N$. Given n such that $1 \leq n \leq N$, let m be the integer such that $m + n = N + 1$. Then*

$$H_A(\boldsymbol{\xi}_n)\Lambda_m(A^*) \leq d_3(k)(1+(N-1)\tau_k^2+(nm-N)\tau_k^4)^{1/2}\gamma_k^*(N).$$

Proof. We again start with the estimate (4.3) for $H_A(\boldsymbol{\xi}_n)$ in terms of entries

in the Gram-Schmidt decomposition of B.

$$H_A(\boldsymbol{\xi}_n)\Lambda_m(A^*) \le d_3(k)\prod_{v|\infty}\Bigg(\Lambda_1(B^{(m)})^2 + \sum_{i=m+1}^{N}\left(\tau_k\Lambda_1(B^{(i)})\right)^2\Bigg)^{\frac{d_v}{2d}}\Lambda_m(B^*) \tag{4.13}$$

$$\le d_3(k)\prod_{v|\infty}\Bigg(\left(\Lambda_1(B^{(m)})\Lambda_m(B^*)\right)^2 + \sum_{i=m+1}^{N}\left(\tau_k\Lambda_1(B^{(i)})\Lambda_m(B^*)\right)^2\Bigg)^{\frac{d_v}{2d}} \tag{4.14}$$

Now we appeal to Lemma 2.9, but this time using $l = m$, which is valid because $m \le i \le N$

$$H_A(\boldsymbol{\xi}_n)\Lambda_m(A^*) \le d_3(k)\prod_{v|\infty}\Bigg(\left(\Lambda_1(B^{(m)})\Lambda_m(B^{(m)*})\right)^2 + \sum_{i=m+1}^{N}\left(\tau_k\Lambda_1(B^{(i)})\Lambda_m(B^{(i)*})\right)^2\Bigg)^{\frac{d_v}{2d}}, \tag{4.15}$$

and are in a position to use Lemma 4.4, with the roles of B and B^* reversed, resulting in

$$H_A(\boldsymbol{\xi}_n)\Lambda_m(A^*) \le d_3(k)\prod_{v|\infty}\Bigg(\left((1+(m-1)\tau_k)\gamma_k^*(m)\right)^2 + \sum_{i=m+1}^{N}\left(\tau_k(1+(m-1)\tau_k)\gamma_k^*(i)\right)^2\Bigg)^{\frac{d_v}{2d}}. \tag{4.16}$$

Noting that $\gamma_k^*(m) \le \gamma_k^*(i) \le \gamma_k^*(N)$, we replace all the instances on the right

hand side with $\gamma_k^*(N)$ and factor that term out, leaving

$$\begin{aligned} H_A(\boldsymbol{\xi}_n)\Lambda_m(A^*) &\leq d_3(k)\prod_{v|\infty}\Bigg(((1+(m-1)\tau_k)^2)^2 \\ &\qquad + \sum_{i=m+1}^{N}(\tau_k(1+(m-1)\tau_k^2))^2\Bigg)^{\frac{d_v}{2d}}\gamma_k^*(N) \\ &\leq d_3(k)((1+(m-1)\tau_k^2)(1+(n-1)\tau_k^2))^{1/2}\gamma_k^*(N). \end{aligned} \tag{4.17}$$

To arrive at the conclusion of the theorem requires only rearranging the terms involving τ_k. □

We are now ready to bound the Mahler product.

Theorem 4.6. *Let A belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ and have dual automorphism A^*. For every integer pair $1 \leq n, m \leq N$ such that $m+n = N+1$ we have*

$$\Lambda_n(A)\Lambda_m(A^*) \leq d_3(k)\left(1+\frac{(N-1)}{2}\tau_k^2\right)\gamma_k^*(N) \tag{4.18}$$

Proof. From the definition of successive minima, it must be that

$$\Lambda_n(A) \leq \max_{1\leq i\leq n} H_A(\boldsymbol{\xi}_i),$$

so multiplying both sides by $\Lambda_m(A^*)$ yields

$$\begin{aligned} \Lambda_n(A)\Lambda_m(A^*) &\leq \max_{1\leq i\leq n}\{H_A(\boldsymbol{\xi}_i)\}\Lambda_m(A^*) \\ &\leq \max_{1\leq i\leq n}\{H_A(\boldsymbol{\xi}_i)\Lambda_j(A^*)\}, \end{aligned} \tag{4.19}$$

where $M \leq j \leq N$ is such that $i+j = N+1$. Applying Theorem 4.5 to each product, we find

$$\Lambda_n(A)\Lambda_m(A^*) \leq \max_{1\leq i\leq n}\{d_3(k)((1+(i-1)\tau_k^2)(1+(j-1)\tau_k^2))^{1/2}\gamma_k^*(N)\} \tag{4.20}$$

For $i + j = N + 1$, because of the symmetry (or as a simple calculus exercise) this quantity is maximized when $i = j = (N + 1)/2$. Substituting $(N + 1)/2$ for i and j in (4.20) to realize this maximum, we arrive at (4.18). □

4.3 Diagonal Entries

The idelic volumes of entries of the diagonal matrix U are not necessarily monotone increasing, but using Siegel's Lemma, it is possible to report some details that allow comparisons between them.

Lemma 4.7. *Let A belong to $\mathrm{Aut}(k_{\mathbb{A}}^N)$ and let X be the Korkin-Zolotarev matrix for A defined in Theorem 3.3. In the Gram-Schmidt decomposition*

$$AX = \Psi UW,$$

we have, for $1 \leq m < n \leq N$,

$$|u_m|_{\mathbb{A}} \leq \gamma_k(n - m + 1)^{1/2} \left(\prod_{i=2}^{n-m} \gamma_k(i)^{\frac{1}{2i}} \right) |u_n|_{\mathbb{A}}. \tag{4.21}$$

Proof. Let $B = AX$, so that we can refer, as in Theorem 3.1, to the projections $B^{(i)}$, which are the same as the lower $n \times n$ right hand corner of UW. Furthermore, for $j \leq i$, let $B_j^{(i)}$ denote the span at each place of the first j columns of $B^{(i)}$; then as an automorphism of $k_{\mathbb{A}}^j$, it is true that $\Lambda_1(B_j^{(i)}) = \Lambda_1(B^{(i)})$.

By the definition of Hermite's constant and the construction of the Korkin-Zolotarev matrix X, we have

$$|u_m|_{\mathbb{A}} = \Lambda_1(B_j^{(N-m+1)}) \leq \gamma_k(j)^{1/2} |B_j^{(N-m+1)}|_{\mathbb{A}}^{1/j},$$

where now $j = n - m + 1$. The Gram-Schmidt decomposition allows us to expand the last term in a simple way

$$|u_m|_{\mathbb{A}} \leq \gamma_k(j)^{1/2} \left(\prod_{l=0}^{j} |u_{m+l}|_{\mathbb{A}} \right)^{1/j+1}$$

which after algebraic manipulation becomes

$$|u_m|_{\mathbb{A}} \leq \gamma_k(j)^{(j+1)/2j} \left(\prod_{l=1}^{j} |u_{m+l}|_{\mathbb{A}} \right)^{1/j}. \tag{4.22}$$

We proceed with an induction on j. Since $\gamma_k(1) = 1$, the base case is trivial. Now, assume that for $i < j$ it is the case that

$$|u_{m+i}|_{\mathbb{A}} \leq \gamma_k(i)^{1/2} \left(\prod_{l=2}^{i} \gamma_k(l)^{1/2(l-1)} \right) |u_n|_{\mathbb{A}}, \tag{4.23}$$

and substitute (4.23) for each $|u_{m+l}|_{\mathbb{A}}$ on the right hand side of (4.22), yielding

$$\begin{aligned} |u_m|_{\mathbb{A}} &\leq \gamma_k(j)^{(j+1)/2j} \left(\prod_{i=1}^{j} \gamma_k(i)^{1/2} \left(\prod_{l=2}^{i} \gamma_k(l)^{1/2(l-1)} \right) |u_n|_{\mathbb{A}} \right)^{1/j} \\ &= \gamma_k(j)^{(j+1)/2j} \left(\prod_{i=1}^{j} \left(\prod_{l=2}^{i} \gamma_k(l)^{1/2(l-1)} \right) \right)^{1/j} |u_n|_{\mathbb{A}}. \end{aligned} \tag{4.24}$$

By expanding the double product in (4.24) and grouping like terms, we see that the result is true for $j = n - m + 1$ also. □

By again using γ_k^*, we can simplify the estimate

Corollary 4.8. *For A and X as defined in Lemma 4.7, written using the decomposition of Lemma 2.3 as*

$$AX = \Psi UW,$$

and for every m, n such that $1 \leq m < n \leq N$, we have

$$|u_m|_{\mathbb{A}} \leq \gamma_k^*(n-m+1)^{(1+\log(n-m+1))/2}|u_n|_{\mathbb{A}}.$$

Proof. In (4.21), replace each $\gamma_k(i)$ with $\gamma_k^*(n-m+1)$ and apply the elementary bound

$$\sum_{i=2}^{n-m+1} \frac{1}{i-1} \leq \log(n-m+1)$$

on the exponent of the resulting product. □

Bibliography

[1] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Math. Ann.*, 296(4):625–635, 1993.

[2] E. Bombieri and J. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[3] Edward B. Burger and Jeffrey D. Vaaler. On the decomposition of vectors over number fields. *J. Reine Angew. Math.*, 435:197–219, 1993.

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

[5] Martin Henk. Successive minima and lattice points. *Rend. Circ. Mat. Palermo (2) Suppl.*, (70, part I):377–384, 2002. IV International Conference in "Stochastic Geometry, Convex Bodies, Empirical Measures & Applications to Engineering Science", Vol. I (Tropea, 2001).

[6] J. C. Lagarias, H. W. Lenstra, Jr., and C.-P. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

[7] C. G. Lekkerkerker. *Geometry of numbers.* Bibliotheca Mathematica, Vol. VIII. Wolters-Noordhoff Publishing, Groningen, 1969.

[8] Bertrand Meyer. Extreme lattices and vexillar designs. *J. Algebra*, 322(12):4368–4381, 2009.

[9] Bertrand Meyer. Generalised Hermite constants, Voronoi theory and heights on flag varieties. *Bull. Soc. Math. France*, 137(1):127–158, 2009.

[10] Shin Ohno and Takao Watanabe. Estimates of Hermite constants for algebraic number fields. *Comment. Math. Univ. St. Paul.*, 50(1):53–63, 2001.

[11] Robbin O'Leary and Jeffrey D. Vaaler. Small solutions to inhomogeneous linear equations over number fields. *Trans. Amer. Math. Soc.*, 336(2):915–931, 1993.

[12] Damien Roy and Jeffrey Lin Thunder. An absolute Siegel's lemma. *J. Reine Angew. Math.*, 476:1–26, 1996.

[13] Carl Ludwig 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.

[14] Jeffrey Lin Thunder. An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma. *J. Reine Angew. Math.*, 475:167–185, 1996.

[15] Jeffrey Lin Thunder. Higher-dimensional analogs of Hermite's constant. *Michigan Math. J.*, 45(2):301–314, 1998.

[16] Jeffrey D. Vaaler. Small zeros of quadratic forms over number fields. *Trans. Amer. Math. Soc.*, 302(1):281–296, 1987.

[17] Jeffrey D. Vaaler. The best constant in Siegel's lemma. *Monatsh. Math.*, 140(1):71–89, 2003.

[18] Takao Watanabe. On an analog of Hermite's constant. *J. Lie Theory*, 10(1):33–52, 2000.

[19] Takao Watanabe. Hermite constants of division algebras. *Monatsh. Math.*, 135(2):157–166, 2002.

[20] André Weil. *Basic number theory.* Springer-Verlag, New York, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

Vita

Mark Peter Rothlisberger was born in Tucson, Arizona and grew up in Maryland. He studied theater in High School at the Carver Center for Arts and Technology in Towson, Maryland. Afterwards, he studied Mathematics and Russian Literature at Williams College in Williamstown, Massachusetts, graduating with a BA in 2003. He spent one year as a Computer Lab Instructor and Assistant Network Administrator at Williamstown Elementary School. He began graduate studies at the University of Texas at Austin in 2004.

Permanent address: 5001 Convict Hill Road, Apt. 709
Austin, Texas 78749

This dissertation was typeset with LaTeX[†] by the author.

[†]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.