Thijs Vorselen

On Kronecker's Theorem

over the adèles

Master's thesis, defended on April 27, 2010

Thesis advisor: Jan-Hendrik Evertse

Mathematisch Instituut

Universiteit Leiden

Contents

Introduction iv

1 Kronecker's Theorem **1**
1.1 An introduction to the geometry of numbers 1
1.2 Kronecker's approximation theorem 4
1.3 Systems of linear equations over principal ideal domains 7
1.4 A more general Kronecker's Theorem 8

2 Valuations **12**
2.1 Some algebraic preliminaries 12
2.2 An introduction to absolute values 15
2.3 Completions 17
2.4 Absolute values on number fields 19

3 An effective Kronecker's Theorem **24**
3.1 Uniform distribution 24
3.2 An effective Kronecker's Theorem 28
3.3 Subspace Theorem 31

4 Geometry of numbers over the adèles **34**
4.1 Adèles 34
4.2 Strong Approximation Theorem 37
4.3 Fundamental domain 40
4.4 The Haar measure on the adèle space 41
4.5 Minkowski's Theorem for adèle spaces 43

5 Kronecker's Theorem over the adèles **45**
5.1 Kronecker's theorem for adèle spaces 45
5.2 An effective adèlic Kronecker's Theorem 53
5.3 A more general adèlic Kronecker's Theorem 55

Bibliography 61
List of symbols 63
Index 65

Introduction

In this thesis we state and prove "effective" versions and adèlic generalizations of Kronecker's Theorem. Kronecker's Theorem takes an important place in the field of mathematics called Diophantine approximation. This field of mathematics is concerned with approximating real numbers by rational numbers. Kronecker's Theorem deals with inhomogeneous Diophantine inequalities and is published in 1884 by Kronecker in a paper [10] called "Näherungsweise ganzzahlige Auflösung linearer Gleichungen".

Let $L_i(\mathbf{q}) = \alpha_{i1}q_1 + \cdots + \alpha_{in}q_n$ $(i = 1, \ldots, m)$ be m linear forms with real coefficients α_{ij} and let A be the $m \times n$ matrix with elements α_{ij}. The following theorem is a special case of Kronecker's Theorem.

Theorem 1. (Kronecker) *Assume that*

$$\{\mathbf{z} \in \mathbb{Q}^m : A^T\mathbf{z} \in \mathbb{Q}^n\} = \{\mathbf{0}\}. \tag{1}$$

Then for every $\varepsilon > 0$, $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{R}^m$, *there exist* $\mathbf{p} = (p_1, \ldots, p_m) \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ *such that*

$$|L_i(\mathbf{q}) - p_i - b_i| \leq \varepsilon \qquad \text{for } i = 1, \ldots, m.$$

Condition (1) of this theorem is a necessary condition. Another important theorem from Diophantine approximation is Dirichlet's Theorem. This theorem is proven by Dirichlet in 1840 and deals with homogeneous Diophantine inequalities. If we compare Kronecker's Theorem with Dirichlet's Theorem, then we come across an interesting difference.

Theorem 2. (Dirichlet) *For every* ε *with* $0 < \varepsilon < 1$, *there exist* $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ *with* $\mathbf{q} \neq \mathbf{0}$ *such that*

$$|L_i(\mathbf{q}) - \mathbf{p}_i| \leq \varepsilon \text{ for } i = 1, \ldots, m, \quad \|\mathbf{q}\| \leq \varepsilon^{-m/n}.$$

In contrast to Kronecker's Theorem this theorem gives an upper bound for $\|\mathbf{q}\|$ that is easy to calculate in terms of ε. We call such an upper bound an effective upper bound. Motivated by this observation we ask ourselves if there also exists an effective upper bound in the case of Kronecker's Theorem. In this thesis we answer this question in the affirmative for a matrix A with algebraic elements α_{ij}.

In 1966 Mahler [15] published a proof of Kronecker's Theorem with methods from the geometry of numbers. Geometry of numbers is concerned with convex bodies and integer vectors in n-dimensional Euclidean space. In 1988 R. Kannan and L. Lovász

also use geometry of numbers to prove a quantitative version of Theorem 1 for the case $n = 1$, published in [9]. Their theorem gives an ineffective upper bound for $\|\mathbf{q}\|$ and is the starting point of our proof of an effective Kronecker's Theorem.

In the first chapter we give an introduction to geometry of numbers and generalize the proof of R. Kannan and L. Lovász to arbitrary m. We also give a more general quantitative version of Kronecker's Theorem.

In the second chapter we recall some results from algebraic number theory and more specifically the theory of valuations. These results are used in Chapter 3 to prove an effective version of Kronecker's Theorem in the case that the elements of A are algebraic.

In Chapter 4 we introduce the adèle space. This space was introduced by Chevalley in 1940 and is useful to solve number theoretic problems. Many of the concepts and theorems in geometry of numbers have been generalized over the adèles. An important result is the adèlic version of the Second Theorem of Minkowki. This theorem is published by R. McFeat [16] in 1971. Unaware of McFeat's result E. Bombieri and J. Vaaler [3] proved the same theorem in 1983. Motivated by the results in geometry of numbers over the adèles we wondered if it would be possible to generalize a version of Kronecker's Theorem over the adèles.

In Chapter 5 we prove some adèlic versions of Kronecker's Theorem. Again the article by R. Kannan and L. Lovász forms the starting point of our proof. The adèlic Second Theorem of Minkowski also plays a crucial role.

I would like to thank Jan-Hendrik Evertse for the idea of this thesis and for many suggestions and corrections.

Chapter 1
Kronecker's Theorem

In this chapter we give an introduction to the geometry of numbers and prove some versions of Kronecker's Theorem using geometry of numbers.

1.1 An introduction to the geometry of numbers

Let n be an integer with $n \geq 1$. We denote by $\mathbb{R}^n$ the vector space of n-dimensional column vectors. We use shorthand $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ by $(x_1, \ldots, x_n)^T, (y_1, \ldots, y_n)^T \in \mathbb{R}^n$, respectively. A *body* is a closed, bounded, connected subset of $\mathbb{R}^n$ with inner points. A body $\mathcal{C}$ is called *convex* if for all $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ and all $t \in [0, 1]$ the point $(1-t)\mathbf{x} + t\mathbf{y}$ lies in $\mathcal{C}$. A body $\mathcal{C}$ in $\mathbb{R}^n$ is called *symmetric*, if $\mathbf{x} \in \mathcal{C}$ implies that $-\mathbf{x} \in \mathcal{C}$.

Henceforth, let $\mathcal{C}$ be a bounded symmetric convex body in $\mathbb{R}^n$. Such a body $\mathcal{C}$ is Lebesgue measurable, so it has a finite *volume*, which we denote by $V(\mathcal{C})$. For $\lambda \in \mathbb{R}$ we define

$$\lambda\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} = \lambda\mathbf{y},\ \mathbf{y} \in \mathcal{C}\}.$$

Let $\langle\ ,\ \rangle$ denote the standard inner product on $\mathbb{R}^n$, given by

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i \qquad \text{for } \mathbf{x}, \mathbf{y} \in \mathbb{R}^n.$$

The *polar* of $\mathcal{C}$, denoted by $\mathcal{C}^*$, is given by

$$\mathcal{C}^* := \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \leq 1 \text{ for all } \mathbf{y} \in \mathcal{C}\}.$$

This is again a bounded symmetric convex body. See Gruber and Lekkerkerker [7], Chapter 2, Section 14, Theorem 1 for a proof of this fact.

A *lattice* in $\mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$ that spans $\mathbb{R}^n$ as a real vector space. If $\mathcal{L}$ is a lattice and $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ is a basis of $\mathcal{L}$, then $|\det(\mathbf{x}_1, \ldots, \mathbf{x}_n)|$ is called the determinant of $\mathcal{L}$ and is denoted by $\det \mathcal{L}$. Define the $n \times n$ matrix

$$A := [\mathbf{x}_1, \ldots, \mathbf{x}_n],$$

where $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are the columns of A. This matrix A is invertible, because $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are linearly independent. We have

$$\mathcal{L} = \{A\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}.$$

The *dual* of $\mathcal{L}$ is given by

$$\mathcal{L}^* = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{y} \in \mathcal{L}\}.$$

It is a corollary of the next lemma that $\mathcal{L}^*$ is again a lattice in $\mathbb{R}^n$. We use the following notation. Let $\mathrm{GL}_n(R)$ denote the set of invertible $n \times n$ matrices over a ring R.

Lemma 1.1. *Let $A \in \mathrm{GL}_n(\mathbb{R})$ and let $\mathcal{L} = \{A\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}$ be the associated lattice in $\mathbb{R}^n$. Then its dual is given by $\mathcal{L}^* = \{(A^{-1})^T\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}$.*

Proof. We have

$$\langle (A^{-1})^T\mathbf{x}, A\mathbf{y} \rangle = \mathbf{x}^T A^{-1} A\mathbf{y} = \mathbf{x}^T\mathbf{y} = \langle \mathbf{x}, \mathbf{y} \rangle.$$

Hence, $\langle (A^{-1})^T\mathbf{x}, A\mathbf{y} \rangle \in \mathbb{Z}$ if and only if $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$. Further, it is easy to see that

$$\{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{y} \in \mathbb{Z}^n \} = \mathbb{Z}^n.$$

We conclude that

$$\mathcal{L}^* = \{(A^{-1})^T\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}.$$

This proves the lemma. □

We define the *n successive minima $\lambda_1(\mathcal{C}, \mathcal{L}), \ldots, \lambda_n(\mathcal{C}, \mathcal{L})$ of $\mathcal{C}$ with respect to $\mathcal{L}$* by

$$\lambda_i(\mathcal{C}, \mathcal{L}) = \inf\{\lambda \in \mathbb{R}_{>0} : \dim(\lambda\mathcal{C} \cap \mathcal{L}) \geq i\}.$$

If it is not necessary to specify $\mathcal{C}$ and $\mathcal{L}$, we will denote $\lambda_i(\mathcal{C}, \mathcal{L})$ by λ_i. It is easy to see that $0 < \lambda_1 \leq \cdots \leq \lambda_n < \infty$. We defined successive minima as infima, but they are in fact minima, as suggested by their name.

Theorem 1.2. (Second Minkowski's Convex Body Theorem) *Let $\mathcal{C}$ be a bounded symmetric convex body and $\mathcal{L}$ a lattice in $\mathbb{R}^n$. Then the successive minima $\lambda_1, \ldots, \lambda_n$ of $\mathcal{C}$ with respect to $\mathcal{L}$ satisfy*

$$\frac{2^n}{n!} \leq \lambda_1 \ldots \lambda_n \frac{V(\mathcal{C})}{\det \mathcal{L}} \leq 2^n.$$

Proof. See Minkowski [17], Kapitel V, for the original proof. We refer to Gruber and Lekkerkerker [7], Chapter 2, Section 9, Theorem 1 for a shorter proof by Estermann. □

Let $\mathcal{C}$ be a bounded symmetric convex body and $\mathcal{L}$ a lattice in $\mathbb{R}^n$. For any $\mathbf{u} \in \mathcal{L}$ we define the set

$$\lambda\mathcal{C} + \mathbf{u} = \{\mathbf{x} + \mathbf{u} : \mathbf{x} \in \lambda\mathcal{C}\}.$$

Then $\mu(\mathcal{C}, \mathcal{L})$, defined by

$$\mu(\mathcal{C}, \mathcal{L}) = \inf\{\lambda \in \mathbb{R}_{>0} \ : \bigcup_{\mathbf{u}\in\mathcal{L}} (\lambda\mathcal{C} + \mathbf{u}) = \mathbb{R}^n\},$$

is called the *covering radius* or *inhomogeneous minimum* of $\mathcal{C}$ with respect to $\mathcal{L}$.

For many problems in the geometry of numbers, it is useful to have an upper bound for the product of $\mu(\mathcal{C}, \mathcal{L})$ and $\lambda_1(\mathcal{C}^*, \mathcal{L}^*)$.

Lemma 1.3. *Let $\mathcal{C}$ be a symmetric convex body in $\mathbb{R}^n$ and $\mathcal{L}$ a lattice in $\mathbb{R}^n$. Then*

$$\mu(\mathcal{C}, \mathcal{L})\lambda_1(\mathcal{C}^*, \mathcal{L}^*) \leq \tfrac{1}{2}n^2.$$

Proof. See Lagarias, Lenstra, and Schnorr [12], Theorem 2.9. □

Theorem 1.4. *Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Its successive minima $\lambda_1, \ldots, \lambda_n$ and covering radius μ satisfy*

$$\tfrac{1}{2}\lambda_n \leq \mu \leq \tfrac{1}{2}(\lambda_1 + \cdots + \lambda_n).$$

Proof. First we prove the lower bound by contradiction. Let t be the number of linearly independent vectors in $(\mu + \frac{1}{2}\lambda_n)\mathcal{C} \cap \mathcal{L}$. Suppose that $\mu + \frac{1}{2}\lambda_n < \lambda_n$, implying that $t < n$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_t \in (\mu + \frac{1}{2}\lambda_n)\mathcal{C} \cap \mathcal{L}$ be linearly independent. Choose $\mathbf{x} \in \lambda_n\mathcal{C} \cap \mathcal{L}$ such that $\mathbf{x} \notin \mathrm{Span}\{\mathbf{x}_1, \ldots, \mathbf{x}_t\}$. There exists $\mathbf{u} \in \mathcal{L}$ such that $\frac{1}{2}\mathbf{x} - \mathbf{u} \in \mu\mathcal{C}$ by the definition of the covering radius. By symmetry and convexity of $\mathcal{C}$ we find that both $\mathbf{u} = \mathbf{u} - \frac{1}{2}\mathbf{x} + \frac{1}{2}\mathbf{x}$ and $\mathbf{x} - \mathbf{u} = \frac{1}{2}\mathbf{x} - \mathbf{u} + \frac{1}{2}\mathbf{x}$ are in $(\mu + \frac{1}{2}\lambda_n)\mathbf{x}$. Hence, $\mathbf{u}, \mathbf{x} - \mathbf{u} \in \mathrm{Span}\{\mathbf{x}_1, \ldots, \mathbf{x}_t\}$, which contradicts $\mathbf{x} \notin \mathrm{Span}\{\mathbf{x}_1, \ldots, \mathbf{x}_t\}$. This proves the lower bound.

Now, we prove the upper bound. Choose linearly independent $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathcal{L}$ such that $\mathbf{x}_i \in \lambda_i\mathcal{C}$ for $i = 1, \ldots, n$. Let us take an arbitrary $\mathbf{x} \in \mathbb{R}^n$. There exist $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ such that $\mathbf{x} = \alpha_1\mathbf{x}_1 + \cdots + \alpha_n\mathbf{x}_n$, because $\mathbf{x}_1, \ldots, \mathbf{x}_n$ span $\mathbb{R}^n$. Choose $a_1, \ldots, a_n \in \mathbb{Z}$ such that $|\alpha_i - a_i| \leq \frac{1}{2}$ for $i = 1, \ldots, n$. Then $\mathbf{x} - (a_1\mathbf{x}_1 + \cdots + a_n\mathbf{x}_n) \in \frac{1}{2}(\lambda_1 + \cdots + \lambda_n)\mathcal{C}$. This proves the theorem. □

1.2 Kronecker's approximation theorem

The aim of this section is to obtain a quantitative version of Kronecker's approximation theorem for linear forms. The proof of this version is based on geometry of numbers. This idea comes originally from K. Mahler. He published a paper [15] in 1966 in which he applies geometry of numbers to prove Kronecker's Theorem.

Let R be a ring. We denote the space of n-dimensional column vectors by R^n and the ring of $m \times n$ matrices over R by $R^{m,n}$. We define the following two norms on $\mathbb{R}^n$:

1. $\|\mathbf{x}\|_1 := \sum_{i=1}^n |x_i|$ for all $\mathbf{x} \in \mathbb{R}^n$, called the *sum norm*, and
2. $\|\mathbf{x}\|_\infty := \max\{|x_1|, \ldots, |x_n|\}$ for all $\mathbf{x} \in \mathbb{R}^n$ called the *maximum norm.*

Let $L_i(\mathbf{q}) = \alpha_{i1}q_1 + \cdots + \alpha_{in}q_n \ \ (i = 1, \ldots, m)$ be m linear forms with real coefficients and define

$$A := \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}.$$

The following theorem is a special case of Kronecker's approximation theorem for linear forms.

Theorem 1.5. (Kronecker) *Let $A \in \mathbb{R}^{m,n}$ and assume that*

$$\{\mathbf{z} \in \mathbb{Q}^m : A^T\mathbf{z} \in \mathbb{Q}^n\} = \{\mathbf{0}\}. \tag{1.1}$$

Then for every $\varepsilon > 0$, $b_1, \ldots, b_m \in \mathbb{R}$, there exist $p_1, \ldots, p_m \in \mathbb{Z}$, $\mathbf{q} \in \mathbb{Z}^n$ such that

$$|L_i(\mathbf{q}) - p_i - b_i| \leq \varepsilon \qquad \text{for } i = 1, \ldots, m. \tag{1.2}$$

Proof. A proof is given in this section. See [10] for Kronecker's original paper. □

The next lemma states that condition (1.1) is necessary for this theorem.

Lemma 1.6. *If for every $\varepsilon > 0$, $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{R}^m$ there exist $\mathbf{p} = (p_1, \ldots, p_m) \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$, such that $|L_i(\mathbf{q}) - p_i - b_i| < \varepsilon$ then condition (1.1) is satisfied.*

Proof. This is a proof by contradiction. Suppose there exists $\mathbf{z}' \in \mathbb{Q}^m$ such that $A^T\mathbf{z}' \in \mathbb{Q}^n$ and $\mathbf{z}' \neq 0$. Let $\mathbf{z}$ be the vector obtained by multiplying $\mathbf{z}'$ with the lowest common multiple of the denominators of the coordinates in $\mathbf{z}'$ and $A^T\mathbf{z}'$. Note that

$\mathbf{z} \in \mathbb{Z}^m$ and $A^T\mathbf{z} \in \mathbb{Z}^n$. There exists $\mathbf{b} \in \mathbb{R}^m$ with $\langle \mathbf{z}, \mathbf{b}\rangle \notin \mathbb{Z}$ since $\mathbf{z} \neq 0$. For all vectors $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ we have

$$\begin{aligned} |\langle \mathbf{z}, A\mathbf{q} - \mathbf{p} - \mathbf{b}\rangle| &= |(A\mathbf{q})^T\mathbf{z} - \langle \mathbf{z}, \mathbf{p}\rangle - \langle \mathbf{z}, \mathbf{b}\rangle| \\ &= |\mathbf{q}^T A^T\mathbf{z} - \langle \mathbf{z}, \mathbf{p}\rangle - \langle \mathbf{z}, \mathbf{b}\rangle|. \end{aligned}$$

Note that $\mathbf{q}^T A^T\mathbf{z} - \langle \mathbf{z}, \mathbf{p}\rangle \in \mathbb{Z}$ for all $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ and $\langle \mathbf{z}, \mathbf{b}\rangle \notin \mathbb{Z}$. Hence, $|\langle \mathbf{z}, A\mathbf{q} - \mathbf{p} - \mathbf{b}\rangle| \geq \lceil \langle \mathbf{z}, \mathbf{b}\rangle \rfloor > 0$ independent of $\mathbf{p}$ and $\mathbf{q}$. This proves the lemma. □

Theorem 1.5 does not give an upper bound for $\|\mathbf{q}\|_\infty$. The following theorem by Dirichlet proves an effective upper bound for homogeneous linear forms.

Theorem 1.7. (Dirichlet) *For every ε with $0 < \varepsilon < 1$, there exist $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ with $\mathbf{q} \neq \mathbf{0}$ such that*

$$|L_i(\mathbf{q}) - \mathbf{p}_i| \leq \varepsilon \text{ for } i = 1, \ldots, m, \quad \|\mathbf{q}\|_\infty \leq \varepsilon^{-m/n}.$$

Proof. Dirichlet proved this in 1842. See Cassels [5] for a proof. □

We wonder if we can calculate such an effective upper bound for $\|\mathbf{q}\|_\infty$ in the case of a system of inhomogenous linear forms. The following theorem implies a non-effective upper bound. The inequalities in (1.2) can be stated in the following more efficient way

$$\|A\mathbf{q} - \mathbf{p} - \mathbf{b}\|_\infty \leq \varepsilon.$$

We denote the distance from a real number x to the nearest integer by $\lceil x \rfloor$.

Theorem 1.8. *Let Q, ε be positive reals such that for all integers $a_1, \ldots, a_m$, not all zero,*

$$Q \sum_{j=1}^{n} \lceil a_1\alpha_{j1} + \cdots + a_m\alpha_{jm} \rfloor + \varepsilon \sum_{i=1}^{m} |a_i| \geq \tfrac{1}{2}(m+n)^2. \tag{1.3}$$

Then for all $\mathbf{b} \in \mathbb{R}^n$ there exist $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ such that

$$\|A\mathbf{q} - \mathbf{p} - \mathbf{b}\|_\infty \leq \varepsilon, \quad \|\mathbf{q}\|_\infty \leq Q.$$

Kannan and Lovász proved this theorem for $n = 1$. The following proof expands theirs ([9], Theorem 5.5) to arbitrary n.

Proof. Let $\mathcal{C} = \{\mathbf{x} \in \mathbb{R}^{m+n} : \|\mathbf{x}\|_\infty \leq 1\}$ be the unit cube and let $\mathcal{L}$ be the lattice generated by the columns of the matrix

$$B = \begin{pmatrix} I_m & -A \\ 0 & \frac{\varepsilon}{Q} I_n \end{pmatrix},$$

where I_n denotes the $n \times n$ identity matrix. It is easy to see that $\mathcal{C}^* = \{\mathbf{x} \in \mathbb{R}^{m+n} : \|\mathbf{x}\|_1 \leq 1\}$ and that the dual lattice $\mathcal{L}^*$ is generated by the columns of the inverse transpose of B

$$(B^{-1})^T = \begin{pmatrix} I_m & 0 \\ \frac{Q}{\varepsilon} A^T & \frac{Q}{\varepsilon} I_n \end{pmatrix}.$$

That is, lattice points in $\mathcal{L}^*$ are of the form

$$\begin{pmatrix} \mathbf{a} \\ \frac{Q}{\varepsilon} (A^T \mathbf{a} + \mathbf{c}) \end{pmatrix}$$

with $\mathbf{a} \in \mathbb{Z}^m$, $\mathbf{c} \in \mathbb{Z}^n$. Condition (1.3) in Theorem 1.8 implies that for all $(\mathbf{a}, \mathbf{c}) \neq (\mathbf{0}, \mathbf{0})$ one has

$$\left\| \begin{pmatrix} \mathbf{a} \\ \frac{Q}{\varepsilon} (A^T \mathbf{a} + \mathbf{c}) \end{pmatrix} \right\|_1 \geq \tfrac{1}{2}(m+n)^2/\varepsilon.$$

Hence, by definition of $\lambda_1(\mathcal{C}^*, \mathcal{L}^*)$ we have

$$\lambda_1(\mathcal{C}^*, \mathcal{L}^*) \geq \tfrac{1}{2}(m+n)^2/\varepsilon.$$

For all $\mathbf{b} \in \mathbb{R}^m$ there exist vectors $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ such that $\|B\binom{\mathbf{p}}{\mathbf{q}} + \binom{\mathbf{b}}{\mathbf{0}}\|_\infty \leq \mu(\mathcal{C}, \mathcal{L})$ by definition of $\mu(\mathcal{C}, \mathcal{L})$. Since $\mu(\mathcal{C}, \mathcal{L}) \leq \varepsilon$ by Lemma 1.3 we have

$$\begin{aligned} \|\mathbf{p} - A\mathbf{q} + \mathbf{b}\|_\infty &\leq \varepsilon \\ \|\mathbf{q}\|_\infty &\leq Q. \end{aligned}$$

This proves the theorem. □

Lemma 1.9. *Theorem 1.8 implies Theorem 1.5.*

Proof. Choose an arbitrary $\varepsilon > 0$. For every $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ with $\mathbf{a} \neq \mathbf{0}$ we find $\sum_{j=1}^n \lceil a_1\alpha_{1j} + \cdots + a_m\alpha_{mj} \rfloor > 0$, because of condition (1.1). Now take

$$Q = \frac{1}{2}(m+n)^2 \left(\min_{\substack{\|\mathbf{a}\|_1 \leq \frac{1}{2}(m+n)^2/\varepsilon \\ \mathbf{a} \neq \mathbf{0}}} \sum_{j=1}^n \lceil a_1\alpha_{1j} + \cdots + a_n\alpha_{mj} \rfloor \right)^{-1}.$$

With this ε and Q, condition (1.3) is satisfied. The lemma follows. □

1.3 Systems of linear equations over principal ideal domains

In this section we prove a criterion for the solvability of systems of linear equations over principal ideal domains. Recall that a *principal ideal domain* is a domain, of which all ideals are principal. This result is used for the proof of a more general Kronecker's Theorem in the next section.

A *diagonal matrix* is a square matrix in which all elements outside the main diagonal are zero. Let R be a principal ideal domain. For $a, b \in R, a \neq 0$ we denote $a|b$ if a divides b.

Theorem 1.10. *Let $A \in R^{m,n}$. Then there exist $V_1 \in \mathrm{GL}_m(R)$, $V_2 \in \mathrm{GL}_n(R)$ such that A' given by $A' := V_1 A V_2$ is a diagonal matrix*

$$A' = \begin{pmatrix} \delta_1 & & & & & \\ & \ddots & & & & \\ & & \delta_t & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

where $\delta_1, \ldots, \delta_t \in R$ with $\delta_1 | \ldots | \delta_t$ and $t = \mathrm{rank}(A)$.

Proof. See Bourbaki [4], Livre II, Chapitre VII, Section 4.5, Corollaire 1 of Proposition 4. For a proof in the special case that $R = \mathbb{Z}$, see Smith [21]. □

The matrix A' is called the *Smith normal form* of A. Bachem and Kannan, [1], published a polynomial time algorithm to calculate the Smith normal form in the special case that $R = \mathbb{Z}$.

Theorem 1.11. *Let R be a principal ideal domain with field of fractions K and let $A \in R^{m,n}$, $\mathbf{b} \in R^m$. Then the following two assertions are equivalent.*

(i) There exists $\mathbf{x} \in R^n$ such that $A\mathbf{x} = \mathbf{b}$.

(ii) $\{\mathbf{z} \in K^m : A^T\mathbf{z} \in R^n\} \subseteq \{\mathbf{z} \in K^m : \mathbf{b}^T\mathbf{z} \in R\}$.

Proof. First we prove *(i) ⇒ (ii)*. Let $\mathbf{z} \in K^m$, such that $A^T\mathbf{z} \in R^n$. Then

$$\mathbf{b}^T\mathbf{z} = \mathbf{x}^T A^T \mathbf{z} \in \mathbf{x}^T R^n \subset R.$$

This proves *(i) ⇒ (ii)*.

Now, we prove *(ii)* $\Rightarrow$ *(i)*. Let $A \in R^{m,n}$ and $\mathbf{b} \in R^m$ satisfy assertion *(ii)*. Let A' be the Smith normal form of A and let V_1, V_2 be the matrices such that $A' = V_1 A V_2$ as in Theorem 1.10.

If ${A'}^T\mathbf{z} \in R^n$ then we have $V_2^T A^T V_1^T \mathbf{z} \in R^n$ and as $V_2 \in \mathrm{GL}_n(R)$ we get $A^T V_1^T \mathbf{z} \in R^n$. By assertion *(ii)* we see that $(V_1\mathbf{b})^T\mathbf{z} = \mathbf{b}^T V_1^T \mathbf{z} \in R$. We conclude that A' and $\mathbf{b}' := (b'_1, \ldots, b'_m)^T = V_1\mathbf{b}$ also satisfy assertion *(ii)*.

For every $\mathbf{z} = (z_1, \ldots, z_m) \in K^m$ we have

$$ {A'}^T\mathbf{z} = \begin{pmatrix} \delta_1 & & & & & \\ & \ddots & & & & \\ & & \delta_t & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \mathbf{z} = (\delta_1 z_1, \ldots, \delta_t z_t, 0, \ldots, 0)^T. $$

It is easy to see that $\delta_1 | b'_1, \ldots, \delta_t | b'_t$ and that $b'_{t+1} = 0, \ldots, b'_m = 0$. Define

$$ \mathbf{x}' := (b'_1/\delta_1, \ldots, b'_t/\delta_t, 0, \ldots, 0) $$

and note that $\mathbf{x}' \in R^n$ and $A'\mathbf{x}' = \mathbf{b}'$. Define $\mathbf{x} := V_2^{-1}\mathbf{x}'$, then we have $\mathbf{x} \in R^m$ and $A\mathbf{x} = \mathbf{b}$. This proves the theorem. □

1.4 A more general Kronecker's Theorem

We already proved a special case of Kronecker's Theorem for linear forms. In this section we use that result to prove the following more general form of Kronecker's theorem. We use the following notation in this proof. Let again $A \in \mathbb{R}^{r,s}$ be the $r \times s$ matrix

$$ A := \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1s} \\ \vdots & \ddots & \vdots \\ \alpha_{r1} & \cdots & \alpha_{rs} \end{pmatrix}. $$

Define a norm $\|\cdot\|$ on $\mathbb{R}^{r,s}$ by

$$ \|A\| := \max_{1 \le i \le r} \sum_{j=1}^{s} |\alpha_{ij}|. $$

Note that $\|A\mathbf{x}\|_\infty \le \|A\|\|\mathbf{x}\|_\infty$ for all $A \in \mathbb{R}^{r,s}$, $\mathbf{x} \in \mathbb{R}^s$.

Theorem 1.12. *Let $A \in \mathbb{R}^{r,s}$ and $\mathbf{b} \in \mathbb{R}^r$. Then the following two assertions are equivalent.*

(i) For every $\varepsilon > 0$ there exists $\mathbf{x} \in \mathbb{Z}^s$ such that $\|A\mathbf{x} - \mathbf{b}\|_\infty \leq \varepsilon$.

(ii) For all $\mathbf{z} \in \mathbb{R}^r$ with $A^T\mathbf{z} \in \mathbb{Z}^s$ we have $\mathbf{b}^T\mathbf{z} \in \mathbb{Z}$.

In the proof of this theorem we need some lemmas, in which we refer repeatedly to assertions *(i)* and *(ii)*.

Lemma 1.13. *Let $U \in \mathrm{GL}_r(\mathbb{R})$, $V \in \mathrm{GL}_s(\mathbb{Z})$ and put $\tilde{A} := UAV$, $\tilde{\mathbf{b}} := U\mathbf{b}$. Then:*
(i) is equivalent to the assertion that for every $\varepsilon > 0$ there is $\mathbf{x} \in \mathbb{Z}^s$ such that $\|\tilde{A}\mathbf{x} - \tilde{\mathbf{b}}\|_\infty \leq \varepsilon$,
(ii) is equivalent to the assertion that

$$\{\mathbf{z} \in \mathbb{R}^r : \tilde{A}^T\mathbf{z} \in \mathbb{Z}^s\} \subseteq \{\mathbf{z} \in \mathbb{R}^r : \tilde{\mathbf{b}}^T\mathbf{z} \in \mathbb{Z}\}.$$

Proof. Suppose assertion *(i)* holds. Then for every $\varepsilon > 0$ there exists $\mathbf{x} \in \mathbb{Z}^s$ such that

$$\|A\mathbf{x} - \mathbf{b}\|_\infty \leq \frac{\varepsilon}{\|U\|}.$$

Define $\tilde{\mathbf{x}} := V^{-1}\mathbf{x}$. Then

$$\|\tilde{A}\tilde{\mathbf{x}} - \tilde{\mathbf{b}}\|_\infty = \|UA\mathbf{x} - U\mathbf{b}\|_\infty \leq \varepsilon.$$

The proof of the reverse implication is entirely similar.

Suppose assertion *(ii)* holds. If there exists $\mathbf{z} \in \mathbb{R}^r$, $\mathbf{w} \in \mathbb{Z}$ such that $V^TA^T(U^T\mathbf{z}) = \mathbf{w}$ then $A^T(U^T\mathbf{z}) = (V^T)^{-1}\mathbf{w} \in \mathbb{Z}$. By assertion *(ii)* we have $\mathbf{b}^TU^T\mathbf{z} \in \mathbb{Z}$. We conclude that

$$\{\mathbf{z} \in \mathbb{R}^r : \tilde{A}^T\mathbf{z} \in \mathbb{Z}^s\} \subseteq \{\mathbf{z} \in \mathbb{R}^r, \tilde{\mathbf{b}}^T\mathbf{z} \in \mathbb{Z}\}.$$

Again, the reverse implication is proved in the same manner. □

Lemma 1.14. *Assume (ii) holds. Then there exist $U \in \mathrm{GL}_r(\mathbb{R})$, $V \in \mathrm{GL}_s(\mathbb{Z})$ such that*

$$UAV = \begin{pmatrix} I_t & 0 & -A_1 \\ 0 & I_{m-t} & -A_2 \\ 0 & 0 & 0 \end{pmatrix}, \quad U\mathbf{b} = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{0} \end{pmatrix}$$

where $0 \leq t \leq m \leq r$, $A_1 \in \mathbb{Q}^{t,s-m}, A_2 \in \mathbb{R}^{m-t,s-m}$, $\mathbf{b}_1 \in \mathbb{Q}^t$, $\mathbf{b}_2 \in \mathbb{R}^{m-t}$, and

$$\begin{aligned} \{\mathbf{z}_1 \in \mathbb{Z}^t : A_1^T\mathbf{z}_1 \in \mathbb{Z}^{s-m}\} &\subseteq \{\mathbf{z}_1 \in \mathbb{Z}^t : \mathbf{b}_1^T\mathbf{z}_1 \in \mathbb{Z}\}, \\ \{\mathbf{z}_2 \in \mathbb{Z}^{m-t} : A_2^T\mathbf{z}_2 \in \mathbb{Z}^{s-m}\} &= \{\mathbf{0}\}. \end{aligned}$$

Proof. Let $m := \mathrm{rank}(A)$ and suppose without loss of generality that the first m rows of A are linearly independent. Then by elementary linear algebra, there exists $U_1 \in \mathrm{GL}_r(\mathbb{R})$ such that

$$U_1 A = \begin{pmatrix} I_m & -A' \\ 0 & 0 \end{pmatrix} \quad \text{with } A' \in \mathbb{R}^{m,s-m}.$$

By Lemma 1.13, the validity of *(ii)* is unaffected if we replace A by $U_1 A$. That is, *(ii)* is equivalent to the assertion that

$$\{\mathbf{z} \in \mathbb{R}^r : \begin{pmatrix} I_m & -A' \\ 0 & 0 \end{pmatrix} \mathbf{z} \in \mathbb{Z}^s\} \subseteq \{\mathbf{z} \in \mathbb{R}^r : \mathbf{b}^T U^T \mathbf{z} \in \mathbb{Z}\}. \tag{1.4}$$

For this to hold, we must have $U_1 \mathbf{b} = (\mathbf{b}', \mathbf{0})^T$ with $\mathbf{b}' \in \mathbb{R}^m$. Thus, (1.4) becomes

$$\{\mathbf{z}' \in \mathbb{Z}^m : A'^T \mathbf{z}' \in \mathbb{Z}^{s-m}\} \subseteq \{\mathbf{z}' \in \mathbb{Z}^m : \mathbf{b}'^T \mathbf{z}' \in \mathbb{Z}\}. \tag{1.5}$$

The left-hand side is a sub-$\mathbb{Z}$-module M of $\mathbb{Z}^{s-m}$, hence free of rank $t \leq m$. If $t = 0$ we are done. Suppose $t > 0$. Then by Theorem 1.11 there is a basis $\{\mathbf{d}_1, \ldots, \mathbf{d}_m\}$ of $\mathbb{Z}^m$ and there are positive integers $\delta_1, \ldots, \delta_t$, such that $\{\delta_1 \mathbf{d}_1, \ldots, \delta_t \mathbf{d}_t\}$ is a $\mathbb{Z}$-basis of M.

Now, let $D := [\mathbf{d}_1, \ldots, \mathbf{d}_m]$ be the matrix with columns $\mathbf{d}_1, \ldots, \mathbf{d}_m$. Then $D \in \mathrm{GL}_m(\mathbb{Z})$. Define $\hat{A} := D^T A'$, $\hat{\mathbf{b}} := D^T \mathbf{b}'$. Then

$$\begin{pmatrix} D^T & 0 \\ 0 & I_{r-t} \end{pmatrix} \begin{pmatrix} I_m & -A' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} (D^T)^{-1} & 0 \\ 0 & I_{s-m} \end{pmatrix} = \begin{pmatrix} I_m & -\hat{A} \\ 0 & 0 \end{pmatrix}. \tag{1.6}$$

The right-hand side is clearly of the shape UAV with $U \in \mathrm{GL}_r(\mathbb{R})$, $V \in \mathrm{GL}_s(\mathbb{Z})$. Writing $\hat{\mathbf{z}} := D^{-1} \mathbf{z}'$ we see that (1.5) is equivalent to

$$\{\hat{\mathbf{z}} \in \mathbb{Z}^m : \hat{A}^T \hat{\mathbf{z}} \in \mathbb{Z}^{s-m}\} \subseteq \{\hat{\mathbf{z}} \in \mathbb{Z}^m : \hat{\mathbf{b}}^T \hat{\mathbf{z}} \in \mathbb{Z}\}. \tag{1.7}$$

Let A_1 consist of the first t rows of $\hat{A}$ and A_2 of the last $m-t$ rows. Further, let $\mathbf{b}_1$ and $\mathbf{b}_2$ consist of respectively the first t and the last $m-t$ coordinates of $\hat{\mathbf{b}}$. Notice that the left-hand side of (1.7) consists of all vectors of the shape $(\delta_1 x_1, \ldots, \delta_r x_t, 0, \ldots, 0)^T$ with $x_1, \ldots, x_t \in \mathbb{Z}$. Hence, $A_1 \in \mathbb{Q}^{t,s-m}$, $\mathbf{b}_1 \in \mathbb{Q}^t$ and

$$\{\mathbf{z}_1 \in \mathbb{Z}^t : A_1^T \mathbf{z}_1 \in \mathbb{Z}^{s-m}\} \subseteq \{\mathbf{z}_1 \in \mathbb{Z}^t : \mathbf{b}_1^T \mathbf{z}_1 \in \mathbb{Z}\}.$$

Further, by applying (1.7) with vectors $(0, \ldots, 0, z_{t+1}, \ldots, z_m)^T$, we see that

$$\{\mathbf{z}_2 \in \mathbb{Z}^t : A_2^T \mathbf{z}_2 \in \mathbb{Z}^{s-m}\} = \{\mathbf{0}\}.$$

This proves the lemma. □

Proof of Theorem 1.12. The proof of *(i)* ⇒ *(ii)* is very similar to that of *(i)* ⇒ *(ii)* of Theorem 1.11, and is therefore left to the reader.

Now, we prove *(ii)* ⇒ *(i)*. By Lemmas 1.13 and 1.14, we may assume without loss of generality, that

$$A = \begin{pmatrix} I_t & 0 & -A_1 \\ 0 & I_{m-t} & -A_2 \\ 0 & 0 & 0 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{0} \end{pmatrix},$$

with $A_1, A_2, \mathbf{b}_1, \mathbf{b}_2$ as in Lemma 1.14. Writing $\mathbf{x}^T = (\mathbf{q}^T, \mathbf{p}_1^T, \mathbf{p}_2^T)$, We can rewrite *(i)* as

$$\|A_1\mathbf{q} - \mathbf{p}_1 - \mathbf{b}_1\|_\infty \le \varepsilon, \quad \|A_2\mathbf{q} - \mathbf{p}_2 - \mathbf{b}_2\|_\infty \le \varepsilon, \tag{1.8}$$

to be solved in $\mathbf{q} \in \mathbb{Z}^{s-m}, \mathbf{p}_1 \in \mathbb{Z}^t, \mathbf{p}_2 \in \mathbb{Z}^{m-t}$. By Theorem 1.11 there exist $\mathbf{q}' \in \mathbb{Z}^{s-m}, \mathbf{p}_1' \in \mathbb{Z}^t$ such that

$$A_1\mathbf{q}' - \mathbf{p}_1' = \mathbf{b}_1.$$

Recall that $A_1 \in \mathbb{Q}^{t,s-m}$. Let d be a positive integer, such that $dA_1 \in \mathbb{Z}^{t,s-m}$. By Theorem 1.8, there exist $\mathbf{q}'' \in \mathbb{Z}^{s-m}$, $\mathbf{p}_2' \in \mathbb{Z}^t$, such that

$$\|A_2\mathbf{q}'' - \mathbf{p}_2' - \frac{1}{d}(\mathbf{b}_2 - A_2\mathbf{q}')\|_\infty \le \frac{\varepsilon}{d}. \tag{1.9}$$

Hence,

$$\begin{gathered} A_1(\mathbf{q}' + d\mathbf{q}'') - (\mathbf{p}_1' + dA_1\mathbf{q}'') - \mathbf{b}_1 = \mathbf{0}, \\ \|A_2(\mathbf{q}' + d\mathbf{q}'') - d\mathbf{p}_2' - \mathbf{b}_2\|_\infty < \varepsilon, \end{gathered}$$

which implies that (1.8) is satisfied with $\mathbf{q} = \mathbf{q}' + d\mathbf{q}''$, $\mathbf{p}_1 = \mathbf{p}_1' + dA_1\mathbf{q}''$, $\mathbf{p}_2 = d\mathbf{p}_2'$. This proves the theorem. □

Chapter 2
Valuations

In Chapter 3 we give an effective version of Kronecker's Theorem for a matrix $A \in \mathbb{R}^{m,n}$ with algebraic entries. For this we need some algebraic number theory and more specifically, the theory of valuations.

2.1 Some algebraic preliminaries

We refer to "Algebraic Number Theory" by J. Neukirch [18] for algebraic number theory. In this section we have stated some definitions and results.

A *number field* K is a finite extension of $\mathbb{Q}$. Define

$$\mathcal{O}_K = \{x \in K : \exists \text{ monic } f \in \mathbb{Z}[X] \text{ such that } f(x) = 0\}$$

This set is a subring of K and is called the *ring of integers* of K. This ring is a Dedekind domain, which means that it is a noetherian, integrally closed, integral domain in which every non-zero prime ideal is a maximal ideal. Ideals in Dedekind domains can be factorized into prime ideals in a unique way.

Let $K \subset L$ be an extension of number fields and let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Then the set

$$\mathfrak{p}\mathcal{O}_L = \{xy : x \in \mathfrak{p},\ y \in \mathcal{O}_L\}$$

is an ideal of $\mathcal{O}_L$. Using the unique ideal factorization in $\mathcal{O}_L$ we get

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

for certain prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ of $\mathcal{O}_L$ and positive integers $e_1, \ldots, e_g$. We call e_i the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$ and $f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ the *residue class degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Theorem 2.1. (Fundamental identity) *Let $K \subset L$ be an extension of number fields of degree d. Then one has*

$$\sum_{i=1}^{g} e_i f_i = d.$$

Proof. See Neukirch [18], Chapter I, Proposition 8.2. □

A *fractional ideal* of $\mathcal{O}_K$ is a finitely generated non-zero sub-$\mathcal{O}_K$-module $\mathfrak{a} \neq (0)$ of K. Every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be expressed uniquely as a product

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_n^{k_n},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals and $k_1, \ldots, k_n \in \mathbb{Z}$. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we define $\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{a}) := k_i$ for $i = 0, \ldots, n$ and $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) := 0$ if $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. We have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \neq 0$ for only finitely many prime ideals $\mathfrak{p}$. For an element $x \in K$, we define $\mathrm{ord}_{\mathfrak{p}}(x) := \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$, where $\mathfrak{b} = (x)$ is the fractional $\mathcal{O}_K$-ideal generated by x.

The set of fractional ideals of $\mathcal{O}_K$ is a group under multiplication, denoted by $\mathcal{I}_K$. Let $\mathcal{P}_K$ denote the group of *principal fractional ideals* of $\mathcal{O}_K$, i.e., the set of fractional ideals generated by one element of K. The factor group $\mathcal{I}_K/\mathcal{P}_K$ is the *ideal class group* of K and its order is called the *class number* of K.

Theorem 2.2. *The ideal class group $\mathcal{I}_K/\mathcal{P}_K$ is finite.*

Proof. See Janusz [8], Chapter I, Theorem 11.10. □

Note that $\mathcal{O}_K$ is a principal ideal domain if and only if the ideal class group of K is trivial.

Proposition 2.3. *Let K be a number field of degree $d = [K : \mathbb{Q}]$ over $\mathbb{Q}$ and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Then as a $\mathbb{Z}$-module, $\mathfrak{a}$ is free of rank d.*

Proof. This follows directly from Neukirch [18], Chapter I, Proposition 2.10. □

Let $K \subset L$ be an extension of number fields. The map

$$\begin{aligned} \mathrm{Tr}_{L/K} \colon L &\longrightarrow K \\ x &\longmapsto \sum_{\sigma} \sigma(x) \end{aligned}$$

is called the *trace* and the map

$$\begin{aligned} N_{L/K} \colon L &\longrightarrow K \\ x &\longmapsto \prod_{\sigma} \sigma(x) \end{aligned}$$

is called the *norm*. Here the sum and product range over all K-isomorphic embeddings σ of L in $\mathbb{C}$.

We can also define a norm on the group of fractional ideals. Any fractional ideal $\mathfrak{a}$ can be expressed uniquely as $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$, where $\mathfrak{b}, \mathfrak{c}$ are integral ideals such that $\mathfrak{b} + \mathfrak{c} = (1)$. We then define $N(\mathfrak{a})$ by

$$N(\mathfrak{a}) := (\#\mathcal{O}_K/\mathfrak{b}) \cdot (\#\mathcal{O}_K/\mathfrak{c})^{-1}.$$

Let $K \subset L$ an extension of number fields of degree d. We define the *discriminant* of a basis $\{x_1, \ldots, x_d\}$ of L over K by

$$D_{L/K}(x_1, \cdots, x_d) = \left(\det(x_i^{(j)})_{i,j=1}^d\right)^2,$$

where $x_i^{(1)}, \ldots, x_i^{(d)}$ are the d images of x_i under the K-isomorphic embeddings of L in $\mathbb{C}$. By some elementary calculations, we can rewrite this as

$$D_{L/K}(x_1, \cdots, x_d) = \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j)\right)_{i,j=1}^d.$$

We have the following important proposition regarding the discriminant.

Proposition 2.4. *Let $\{x_1, \ldots, x_d\}$ be a $\mathbb{Q}$-basis of K. Then*

$$D_{K/\mathbb{Q}}(x_1, \ldots, x_d) \neq 0.$$

If $\{x_1, \ldots, x_d\}$ and $\{y_1, \ldots, y_d\}$ are $\mathbb{Z}$-bases of the same fractional ideal of $\mathcal{O}_K$, then we have

$$D_{K/\mathbb{Q}}(x_1, \ldots, x_d) = D_{K/\mathbb{Q}}(y_1, \ldots, y_d).$$

Proof. See Lang [13], Chapter I, Section 2, Proposition 8 and Proposition 12. □

Let again K be a number field and $\mathfrak{a}$ a fractional ideal of $\mathcal{O}_K$. By Proposition 2.4, we can define the discriminant $D_{K/\mathbb{Q}}(\mathfrak{a})$ of a fractional ideal $\mathfrak{a}$ by $D_{K/\mathbb{Q}}(\mathfrak{a}) = D_{K/\mathbb{Q}}(x_1, \ldots, x_d)$, where $\{x_1, \ldots, x_d\}$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$ as a $\mathbb{Z}$-module. In particular, we define the *discriminant D_K of a number field K* by

$$D_K = D_{K/\mathbb{Q}}(\mathcal{O}_K).$$

Hence, if we choose a basis $\{\omega_1, \ldots, \omega_d\}$ of $\mathcal{O}_K$, then we get

$$D_K = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j))_{i,j=1}^d.$$

As $\omega_i\omega_j \in \mathcal{O}_K$ for $i, j = 1, \cdots, d$, we find that $\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j) \in \mathbb{Z}$. Now, it follows that $D_K \in \mathbb{Z}$.

Proposition 2.5. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Then*

$$D_{K/\mathbb{Q}}(\mathfrak{a}) = N(\mathfrak{a})^2 D_K.$$

Proof. This follows directly by expressing $\mathfrak{a}$ as a product of two integral ideals $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ and applying Lang [13], Chapter I, Section 2, Proposition 12 to these ideals. □

2.2 An introduction to absolute values

Definition 2.6. An *absolute value* on a field K is a function $|\cdot|_v \colon K \to \mathbb{R}_{\geq 0}$ such that

1. $|x|_v = 0$ if and only if $x = 0$ for all $x \in K$;
2. $|xy|_v = |x|_v |y|_v$ for all $x, y \in K$;
3. there exists $C \in \mathbb{R}_{>0}$, such that $|x+y|_v \leq C \max\{|x|_v, |y|_v\}$ for all $x, y \in K$.

Definition 2.7. A *valuation on a field K* is a function $v \colon K \to \mathbb{R} \cup \{\infty\}$ such that

1. $v(x) = +\infty$ if and only if $x = 0$ for all $x \in K$;
2. $v(xy) = v(x) + v(y)$ for all $x, y \in K$;
3. $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

An example of a valuation on a number field is given by $\mathrm{ord}_{\mathfrak{p}}$. It is easy to see that a valuation v gives rise to an absolute value $|\cdot|_v \colon K \to \mathbb{R}_{\geq 0}$ defined by $|x|_v = c^{-v(x)}$ with $c \in \mathbb{R}_{>1}$. In other literature, sometimes the term valuation is used for absolute value.

Example 2.8. The most trivial example of an absolute value, which can be defined on any field K, is the absolute value that sends all $x \in K$ with $x \neq 0$ to 1. This absolute value is called *trivial*. Henceforth, all absolute values we consider are assumed to be *non-trivial*.

Example 2.9. The *standard absolute value* on $\mathbb{Q}$, $|\cdot|_\infty$, is defined by

$$\begin{array}{rccc} |\cdot|_\infty \colon & \mathbb{Q} & \longrightarrow & \mathbb{R}_{\geq 0} \\ & x & \longmapsto & |x|. \end{array}$$

We call ∞ the *infinite prime*.

Example 2.10. Let $x \in \mathbb{Q}\backslash\{0\}$. We can write x as $x = \frac{b}{c}$ with $b, c \in \mathbb{Z}$. If we subsequently extract the highest possible power of p from b and c, we get

$$x = p^m \frac{b}{c}, \quad \gcd(bc, p) = 1.$$

The *p-adic absolute value* $|x|_p$ of x is then defined by $|x|_p := \frac{1}{p^m}$. Further, we put $|0|_p := 0$.

Definition 2.11. Let K be a field. Two absolute values $|\cdot|_v$ and $|\cdot|_w$ on K are called *equivalent* if and only if there exists a real number $c > 0$ such that

$$|x|_v = |x|_w^c$$

for all $x \in K$. An equivalence class of absolute values on K is called a *place* of K. We denote the collection of all places of K by M_K.

Proposition 2.12. *Let $|\cdot|_v$ and $|\cdot|_w$ be two absolute values on a field K. Then the following two assertions are equivalent:*

(i) $|\cdot|_v$ and $|\cdot|_w$ are equivalent,

(ii) $|x|_v < 1 \Leftrightarrow |x|_w < 1$ for all $x \in K$.

Proof. See Neukirch [18], Chapter II, Proposition 3.3. □

Definition 2.13. An absolute value $|\cdot|_v$ on a field K is called *non-archimedean* if it satisfies the *ultrametric inequality*

$$|x + y|_v \leq \max\{|x|_v, |y|_v\} \text{ for all } x, y \in K.$$

Otherwise it is called *archimedean* .

The p-adic absolute values are non-archimedean and the standard absolute value is archimedean. The following lemma shows that we can define this property for places.

Lemma 2.14. *Equivalent absolute values are either both archimedean or both non-archimedean.*

Proof. Let $|\cdot|_v$ and $|\cdot|_w$ be equivalent absolute values on a field K. Hence, there exists an $c > 0$ such that $|x|_v = |x|_w^c$ for all $x \in K$. Suppose $|\cdot|_v$ is non-archimedean, then

$$|x + y|_w = |x + y|_v^c \leq \max\{|x|_v, |y|_v\}^c = \max\{|x|_v^c, |y|_v^c\} = \max\{|x|_w, |y|_w\}$$

for all $x, y \in K$. Hence, $|\cdot|_w$ is archimedean too. By symmetry we get the other implication. □

For a field K, denote by M_K the set of places of K, by M_K^∞ the set of archimedean places of K, and by M_K^{fin} the set of non-archimedean places of K. By the following theorem we can identify these places in the case that $K = \mathbb{Q}$.

Theorem 2.15. (Ostrowski) *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent either to $|\cdot|_\infty$ or to $|\cdot|_p$ for some prime number p.*

Proof. For a proof see Neukirch [18], Chapter II, Proposition 3.7. □

Hence, we may identify a non-archimedean place of $\mathbb{Q}$ with its corresponding prime number. Thus, we may write $M_\mathbb{Q} = \{\infty\} \cup \{\text{primes}\}$.

Theorem 2.16. (Product formula) *We have*

$$\prod_{p \in M_\mathbb{Q}} |x|_p = 1 \text{ for all } x \in \mathbb{Q}^*.$$

Proof. Take an arbitrary $x \in \mathbb{Q}^*$. The theorem follows directly from writing

$$x = \pm p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$$

and calculating $\prod_{p \in M_\mathbb{Q}} |x|_p$. □

2.3 Completions

We are already familiar with the construction of the real numbers as completion of the rational numbers. This is done with respect to the standard absolute value $|\cdot|_\infty$. We can adjust the same construction to arbitrary fields K with respect to any absolute value $|\cdot|_v$ on this field K.

A field K is called *complete* with respect to an absolute value $|\cdot|_v$, if every *Cauchy sequence* in K converges in K with respect to $|\cdot|_v$. Let R be the ring of Cauchy sequences in K with respect to $|\cdot|_v$. This is a ring under pointwise addition and multiplication of the sequences. The subset of R consisting of all sequences in R converging to 0 with respect to $|\cdot|_v$ form a maximal ideal of R which we denote by $\mathfrak{m}$. The field $K_v := R/\mathfrak{m}$ is called the *completion* of K with respect to $|\cdot|_v$. It is easy to see that K_v contains K. We can extend $|\cdot|_v$ to K_v in the following way. For every

$x \in K_v$ there exists a Cauchy sequence $(x_k)_{k=1}^{\infty}$ in K with $\lim_{k\to\infty} x_k = x$. We define $|\cdot|_v$ on K_v by $|x|_v := \lim_{k\to\infty} |x_k|_v$. The field K_v is complete with respect to this valuation.

The completion K_v of a field K with respect to an archimedean absolute value is equal to $\mathbb{R}$ or $\mathbb{C}$. This follows directly from the following result regarding fields that are complete with respect to an archimedean absolute value.

Theorem 2.17. (Ostrowski) *Every field that is complete with respect to an archimedean absolute value is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.*

Proof. See Neukirch [18], Chapter II, Theorem 4.2. □

The next definition is that of an extension of an absolute value. This is very important in the next section, where we look at absolute values on number fields.

Definition 2.18. Let $K \subset L$ be a field extension and let $|\cdot|_v$ and $|\cdot|_w$ be absolute values on K and L respectively. We say that $|\cdot|_w$ *extends* $|\cdot|_v$ if the restriction of $|\cdot|_w$ to K is equal to $|\cdot|_v$.

Now, it is natural to speak of an extension of a place as in the following definition.

Definition 2.19. Let $K \subset L$ be a field extension and let v, w be places on respectively K and L. A place w *extends* v, denoted $w|v$, if the restriction of a representative of w to K is equivalent to a representative of v. We say that w *lies above* v.

We have the following important theorem regarding extensions of absolute values.

Theorem 2.20. *Let K be a complete field with respect to an absolute value $|\cdot|_v$ and let $K \subset L$ be a field extension of finite degree d. Then there exists an unique extension of $|\cdot|_v$ to L given by*

$$|x|_w := \sqrt[d]{|N_{L/K}(x)|_v} \quad \text{for } x \in L$$

and L is complete with respect to $|\cdot|_w$.

Proof. See Neukirch [18], Chapter II, Theorem 4.8. □

Theorem 2.21. *Let $|\cdot|_v$ be an absolute value on K. There exists a unique extension of $|\cdot|_v$ from K_v to $\overline{K_v}$ also denoted by $|\cdot|_v$, given by*

$$|x|_v := \sqrt[d]{|N_{K_v(x)/K_v}(x)|_v} \quad \text{for } x \in \overline{K_v}.$$

Proof. Let $x \in \overline{K_v}$. Let L_1 and L_2 be any two finite field extions of K_v containing x. There exist two unique absolute values by Theorem 2.20, on respectively L_1 and L_2, given by

$$|x|_{v_1} := \sqrt[d]{|N_{L_1/K_v}(x)|_v} \qquad \text{for } x \in L_1$$
$$|x|_{v_2} := \sqrt[d]{|N_{L_2/K_v}(x)|_v} \qquad \text{for } x \in L_2$$

on respectively L_1 and L_2. These absolute values agree on $L_1 \cap L_2$, because the extension of $|\cdot|_v$ to $L_1 \cap L_2$ is unique by Theorem 2.20. We conclude that there exists an unique extension of $|\cdot|_v$ to $\overline{K_v}$. □

2.4 Absolute values on number fields

In this section we state and prove some results of absolute values in the more specific case of number fields. Henceforth, let K be a number field and let $\overline{K}$ denote the algebraic closure of K.

Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of K, and let $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ be the complex embeddings of K ordered such that $\sigma_{r+s+i} = \overline{\sigma_{r+i}}$ for $i = 1, \ldots, s$. Define $d := [K : \mathbb{Q}]$. Note that $r + 2s = d$.

Let $\sigma \colon K \hookrightarrow \mathbb{C}$ be an embedding of K in $\mathbb{C}$. We define an absolute value $|\cdot|_\sigma$ associated to an embedding σ by

$$|x|_\sigma := |\sigma(x)| \qquad \text{for all } x \in K \text{ if } \sigma \text{ is real,}$$
$$|x|_\sigma := |\sigma(x)|^2 \qquad \text{for all } x \in K \text{ if } \sigma \text{ is complex.}$$

Let σ be a complex embedding. We denote its complex conjugate by $\overline{\sigma}$. Note that we have $|\sigma(x)| = |\overline{\sigma}(x)|$ for all $x \in K$. So, conjugate embeddings give rise to the same absolute value. We call a place associated to a real embedding a *real place* and a place associated to a complex embedding a *complex place*. There are r real places and s complex places of K.

Lemma 2.22. *Every archimedean place on K is induced by an embedding*

$$\sigma \colon K \hookrightarrow \mathbb{C}.$$

Proof. Let $|\cdot|_v$ be an archimedean abolute value on K. The completion K_v of K with respect to $|\cdot|_v$ is either isomorphic to $\mathbb{R}$ or $\mathbb{C}$ as stated in Theorem 2.17. Hence, the

natural embedding composed with this isomorphism is an embedding of K in either $\mathbb{R}$ or $\mathbb{C}$. Every archimedean absolute value on $\mathbb{R}$ or $\mathbb{C}$ is equivalent to the standard absolute value. Hence, $|\cdot|_v$ is equivalent to $|\cdot|_\sigma$. This proves the lemma. $\square$

Henceforth, we identify the embeddings $\{\sigma_1, \ldots, \sigma_{r+s}\}$ with the corresponding archimedean places and we choose $|\cdot|_{\sigma_i}$ as standard representative for the place σ_i. This is possible by Lemma 2.22.

Lemma 2.23. *The ring of integers $\mathcal{O}_K$ of K is equal to*

$$\{x \in K : |x|_v \leq 1 \text{ for all } v \in M_K^{\text{fin}}\}.$$

Proof. First we prove that $\mathcal{O}_K \subset \{x \in K : |x|_v \leq 1 \text{ for all } v \in M_K^{\text{fin}}\}$. Take an arbitrary $x \in \mathcal{O}_K$ and $v \in M_K^{\text{fin}}$. Note that $v|p$ for some prime number p, because v is non-archimedean. As x is integral over $\mathbb{Z}$, we can find a monic polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

There is a $c \in \mathbb{R}_{>0}$ such that $|\cdot|_v = |\cdot|_p^c$ on $\mathbb{Q}$. Hence, $|a_i|_v \leq 1$ for $i = 0, \ldots, n-1$. If we take the absolute value and use the ultrametric inequality we get

$$|x^n|_v = |a_{n-1}x^{n-1} + \cdots + a_1x + a_0|_v \leq \max_{0 \leq i \leq n-1} |a_i x^i|.$$

We get a contradiction if $|x|_v > 1$. We conclude that $|x|_v \leq 1$ for all $v \in M_K^{\text{fin}}$.

We still have to show that $\{x \in K : |x|_v \leq 1 \text{ for all } v \in M_K^{\text{fin}}\} \subset \mathcal{O}_K$. Choose an $x \in K$ such that $|x|_v \leq 1$ for all $v \in M_K^{\text{fin}}$. Let f be the monic minimal polynomial of x over $\mathbb{Q}$. It is given by

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

with $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. We have to prove that $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\overline{K_v}$. Sending x to one of the values $\alpha_1, \ldots, \alpha_n$ induces an embedding of $K(x)$ in $\overline{K_v}$. Let $\sigma_1, \ldots, \sigma_n$ be those embeddings. Extend $|\cdot|_v$ to $\overline{K_v}$ and define an absolute value $|\cdot|_w$ by

$$|y|_w := |\sigma_i(y)|_v \quad \text{for } y \in K(x).$$

The restriction to K of this absolute value is a non-archimedean, hence $|x|_w \leq 1$. It follows that $|\alpha_i|_v \leq 1$ for $i = 1, \ldots, n$. The coefficients $a_0, \ldots, a_{n-1}$ of f are up to sign sums of products of subsets of $\{\alpha_1, \ldots, \alpha_n\}$. We conclude that $|a_1|_v \leq 1, \ \ldots, \ |a_{n-1}|_v \leq 1$ for all $v \in M_K^{\text{fin}}$. Hence, $|a_i|_p \leq 1$ for all $p \in M_{\mathbb{Q}}^{\text{fin}}$ and so $a_i \in \mathbb{Z}$

for $i = 0, \ldots, n-1$. This proves the lemma. $\square$

Every prime ideal $\mathfrak{p} \neq 0$ of $\mathcal{O}_K$ gives rise to a non-archimedean absolute value $|\cdot|_\mathfrak{p}$ by defining

$$|x|_\mathfrak{p} = N(\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p}(x)} \text{ for } x \in K^*, \quad |0|_\mathfrak{p} = 0.$$

Lemma 2.24. *The map f from the set of prime ideals of $\mathcal{O}_K$ to the set of non-archimedean places of K given by*

$$\mathfrak{p} \mapsto \textit{place of } |\cdot|_\mathfrak{p}$$

is a bijection.

Proof. Note that the set $\{x \in \mathcal{O}_K : |x|_\mathfrak{p} < 1\}$ is equal to $\mathfrak{p}$. So, different prime ideals give representatives for different places by Proposition 2.12. This proves the injectivity of f. To prove surjectivity of f take an arbitrary non-archimedean absolute value $|\cdot|_v$ on K. The set $\{x \in \mathcal{O}_K : |x|_v < 1\}$ is an ideal. By Lemma 2.23 and the property $|xy|_v = |x|_v|y|_v$ we get primality of this ideal. The image of this prime ideal under f gives back an absolute value equivalent to $|\cdot|_v$ by Proposition 2.12. $\square$

Henceforth, for an algebraic number field K, we identify every prime ideal of $\mathcal{O}_K$ with the corresponding non-archimedean place. Thus,

$$M_K \;=\; \{\text{prime ideals of } \mathcal{O}_K\} \cup \{\sigma_1, \ldots, \sigma_{r+s}\}.$$

Lemma 2.25. *If $x \in K$ then $|x|_v \leq 1$ for almost all $v \in M_K$.*

Proof. The fractional ideal (x) of $\mathcal{O}_K$ generated by $x \in K$ has a unique prime factorization

$$(x) = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_g^{k_g}.$$

Hence, $|x|_v \leq 1$ for all $v \in M_K^{\mathrm{fin}}$ with $v \neq \mathfrak{p}_1, \ldots, v \neq \mathfrak{p}_n$. $\square$

Lemma 2.26. *Let $K \subset L$ be an extension of number fields and let $v \in M_K$, $w \in M_L$ with $w|v$. Then*

$$|x|_w = |N_{L_w/K_v}(x)|_v^{[L_w:K_v]} \textit{ for all } x \in L.$$

Proof. Note that there exists a $c \in \mathbb{R}_{>0}$ such that

$$|x|_w = |N_{L_w/K_v}(x)|_v^c \text{ for all } x \in L$$

by Theorem 2.20.

Now, we calculate c for v, w non-archimedean. We have $v = \mathfrak{p}$ for a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. The unique prime factorization in $\mathcal{O}_L$ gives

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

As $\{x \in K : |x|_w < 1\} = \mathfrak{p}$ we know that $w = \mathfrak{P}_i$ for some $1 \leq i \leq g$. Expressing $|x|_{\mathfrak{P}_i}$ in terms of $|x|_{\mathfrak{p}}$ for $x \in K$, we get

$$\begin{aligned} |x|_{\mathfrak{P}_i} &= (\#\mathcal{O}_L/\mathfrak{P}_i)^{-\mathrm{ord}_{\mathfrak{P}_i}(x)} &&= (\#\mathcal{O}_L/\mathfrak{P}_i)^{-e_i \mathrm{ord}_{\mathfrak{p}}(x)} \\ &&&= (\#\mathcal{O}_K/\mathfrak{p})^{-e_i f_i \mathrm{ord}_{\mathfrak{p}}(x)} &&= |x|_{\mathfrak{p}}^{e_i f_i}. \end{aligned}$$

By Neukirch [18], Chapter II, Proposition 6.8 (with Remark) and the explanation under Proposition 8.5 we have $[L_w : K_v] = e_i f_i$. We conclude that

$$|x|_w = |N_{L_w/K_v}(x)|_v \text{ for all } x \in L.$$

It is easy to derive the same relation for v, w archimedean. □

Theorem 2.27. *Let $K \subset L$ be an extension of number fields of degree d. Let $v \in M_K$. For the places $w \in M_L$ extending v we have the following formula:*

$$\prod_{w|v} |x|_w = |N_{L/K}(x)|_v \quad \textit{for all } x \in L.$$

Proof. Let $v \in M_K$. We have

$$\prod_{w|v} |x|_w = \prod_{w|v} |N_{L_w/K_v}(x)|_v$$

and by Neukirch [18], Chapter II, Corollary 8.4

$$\prod_{w|v} |N_{L_w/K_v}(x)|_v = |N_{L/K}(x)|_v.$$

This proves the theorem. □

Theorem 2.28. (Product formula) *For a number field K we have the following product formula:*

$$\prod_{v \in M_K} |x|_v = 1 \quad \textit{for all } x \in K^*.$$

Proof. Using Theorem 2.27 for a field extension $\mathbb{Q} \subset K$, we get

$$\prod_{v \in M_K} |x|_v = \prod_{p \in M_\mathbb{Q}} \prod_{v|p} |x|_v = \prod_{p \in M_\mathbb{Q}} |N_{K/\mathbb{Q}}(x)|_p = 1 \quad \text{for all } x \in K^*.$$

This proves the theorem. □

Now, we are able to define the *height* for $\mathbf{x} \in \overline{\mathbb{Q}}^n$.

Definition 2.29. Let $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ with $\mathbf{x} \neq \mathbf{0}$, then

$$H_K(\mathbf{x}) = \prod_{v \in M_K} \max(|x_1|_v, \ldots, |x_n|_v)$$

is called the height of $\mathbf{x}$ with respect to K and denoted by $H_K(\mathbf{x})$.

Let L be a field extension of K and let $\mathbf{x} \in K^n$. Then we have

$$\begin{aligned} H_L(\mathbf{x}) &= \prod_{w \in M_L} \max(|x_1|_w, \ldots, |x_n|_w) \\ &= \prod_{v \in M_K} \prod_{w|v} \max(|x_1|_w, \ldots, |x_n|_w) \\ &= \prod_{v \in M_K} \prod_{w|v} \max(|x_1|_v, \ldots, |x_n|_v)^{[L_w:K_v]} \\ &= \prod_{v \in M_K} \max(|x_1|_v, \ldots, |x_n|_v)^{[L:K]} \\ &= H_K(\mathbf{x})^d. \end{aligned}$$

Now, we define the *absolute height* for $\mathbf{x} \in \overline{\mathbb{Q}}^n$ by choosing a number field K such that $\mathbf{x} \in K^n$, and putting $H(\mathbf{x}) = H_K(\mathbf{x})^{1/[K:\mathbb{Q}]}$. By what we just observed, this is independent of the choice of K.

Chapter 3
An effective Kronecker's Theorem

3.1 Uniform distribution

Let A be $m \times n$ matrix with real coefficients satisfying the condition (1.1) of Kronecker's Theorem. Then by Kronecker's Theorem there exist $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ such that

$$\|A\mathbf{q} - \mathbf{p} - \mathbf{b}\|_\infty \leq \varepsilon. \tag{3.1}$$

In Theorem 1.8 we proved a non-effective upper bound for $\|\mathbf{q}\|_\infty$. In the next sections we also prove an effective upper bound and in this section we will use the theory of uniform distribution to get some heuristics on the order of the upper bound for $\|\mathbf{q}\|_\infty$ in terms of ε.

Define $\lfloor x \rfloor$ as the largest integer not greater than x.

Definition 3.1. Let $(x_k)_{k=1}^\infty$ be a sequence of reals. For $a, b \in \mathbb{R}$ with $0 \leq a < b < 1$ let $T([a,b); K)$ denote the number of x_k with $k \leq K$ such that $x_k - \lfloor x_k \rfloor \in [a,b)$. The sequence $(x_k)_{k=1}^\infty$ is said to be *uniformly distributed (modulo 1)* if

$$\lim_{K \to \infty} \frac{T([a,b); K)}{K} = b - a$$

for all intervals $[a,b)$ in $[0,1)$.

Theorem 3.2. (Weyl's criterion) *A sequence $(x_k)_{k=1}^\infty$ is uniformly distributed if and only if for all integers $h \neq 0$*

$$\lim_{K \to \infty} \frac{1}{K} \sum_{k=1}^{K} e^{2\pi i h x_k} = 0.$$

Proof. See Kuipers and Niederreiter [11], Chapter 1, Theorem 2.1. See Weyl [22] for Weyl's original proof. □

Corollary 3.3. *Let $\alpha \in \mathbb{R} \backslash \mathbb{Q}$. Then the sequence $(x_k)_{k=1}^\infty$ defined by $x_k = k\alpha$ is uniformly distributed.*

Proof. If $x \neq 1$, we have the following identity

$$\sum_{k=0}^{K} x^k = \frac{1 - x^{K+1}}{1 - x}.$$

Since $\alpha \notin \mathbb{Q}$, we have $e^{2\pi i h\alpha} \neq 1$ for all $h \neq 0$. Hence,

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} e^{2\pi i h\alpha k} = \lim_{K\to\infty} \frac{1}{K} \left(\frac{1 - (e^{2\pi i\alpha})^K}{1 - e^{2\pi i\alpha}} - 1 \right) = 0,$$

since the numerator is bounded. Corollary 3.3 follows directly from Weyl's criterion, Theorem 3.2. □

Corollary 3.4. *Let $(\mathbf{q}_k)_{k=1}^{\infty}$ be a sequence in $\mathbb{R}^n$, ordered such that if s, t are any positive integers with $\|\mathbf{q}_s\|_\infty < \|\mathbf{q}_t\|_\infty$ then $s < t$. If $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \notin \mathbb{Q}^n$ then the sequence $(x_k)_{k=1}^{\infty}$ defined by $x_k = \langle \mathbf{q}_k, \boldsymbol{\alpha} \rangle$ is uniformly distributed.*

Proof. By Weyl's criterion, it suffices to prove

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} e^{2\pi i h x_k} = 0 \quad \text{for all integers } h \neq 0.$$

Choose an integer $h \neq 0$. For every $K \in \mathbb{N}$ there is a non-negative integer L such that $(2L+1)^n \leq K < (2L+3)^n$. We split $\frac{1}{K} \sum_{k=1}^{(2L+1)^n} e^{2\pi i h x_k}$ into $S_1 + S_2$, where

$$\begin{aligned} S_1 &:= \frac{1}{K} \sum_{k=1}^{(2L+1)^n} e^{2\pi i h x_k} \quad \text{and} \\ S_2 &:= \frac{1}{K} \sum_{k=(2L+1)^n+1}^{K} e^{2\pi i h x_k}. \end{aligned}$$

Without loss of generality, assume $\alpha_1 \notin \mathbb{Q}$. Then

$$\begin{aligned} S_1 &\leq \frac{1}{(2L+1)^n}\left|\sum_{l_1=-L}^{L}\cdots\sum_{l_n=-L}^{L} e^{2\pi i h(\alpha_1 l_1+\cdots+\alpha_n l_n)}\right| \\ &\leq \frac{1}{(2L+1)^n}\left|\sum_{l_1=-L}^{L} e^{2\pi i h\alpha_1 l_1}\left(\sum_{l_2=-L}^{L}\cdots\sum_{l_n=-L}^{L} e^{2\pi i h(\alpha_2 l_2+\cdots+\alpha_n l_n)}\right)\right| \\ &= \frac{1}{(2L+1)^n}(2L+1)^{n-1}\left|\sum_{l_1=-L}^{L} e^{2\pi i h\alpha_1 l_1}\right| \\ &= \frac{1}{2L+1}\left|\sum_{l_1=-L}^{L} e^{2\pi i h\alpha_1 l_1}\right|. \end{aligned}$$

Further,

$$\begin{aligned} S_2 &\leq \frac{(2L+3)^n-(2L+1)^n}{(2L+1)^n} \\ &= \left(1+\frac{2}{2L+1}\right)^n - 1. \end{aligned}$$

Note that $S_1 \to 0$ as $K \to \infty$ and $S_2 \to 0$ as $K \to \infty$. We conclude

$$\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K} e^{2\pi i h x_k} = 0.$$

Corollary 3.4 follows. □

The theory of uniform distribution can be extended to higher dimensions. But before stating the definition of uniform distribution in n-dimensional space, we need some new notation. Let $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$ be two real vectors in $\mathbb{R}^n$ with $a_i < b_i$ for $i = 1, \ldots, n$. We denote the n-dimensional interval $\prod_{i=1}^{n}[a_i, b_i)$ by $[\mathbf{a}, \mathbf{b})$. For $\mathbf{x} \in \mathbb{R}^n$ we denote the vector $(x_1 - \lfloor x_1 \rfloor, \cdots, x_n - \lfloor x_n \rfloor)$ by $\mathbf{x} - \lfloor \mathbf{x} \rfloor$. By $\mathbf{0}$ and $\mathbf{1}$ we denote the two n-dimensional vectors defined by $\mathbf{0} = (0, \cdots, 0)$ and $\mathbf{1} = (1, \cdots, 1)$.

Definition 3.5. Let $(\mathbf{x}_k)_{k=1}^{\infty}$ be a sequence in $\mathbb{R}^n$. Let $[\mathbf{a}, \mathbf{b})$ be an n-dimensional interval and let $T([\mathbf{a}, \mathbf{b}); K)$ denote the number of $\mathbf{x}_k$ with $k \leq K$ such that $\mathbf{x}_k - \lfloor \mathbf{x}_k \rfloor \in [\mathbf{a}, \mathbf{b})$. A sequence $(\mathbf{x}_k)_{k=1}^{\infty}$ is said to be *uniformly distributed (modulo 1) in* $\mathbb{R}^n$ if

$$\lim_{K\to\infty}\frac{T([\mathbf{a}, \mathbf{b}); K)}{K} = \prod_{j=1}^{n}(b_j - a_j)$$

for all intervals $[\mathbf{a}, \mathbf{b}) \subset [\mathbf{0}, \mathbf{1})$.

Theorem 3.6. (Weyl's criterion) *A sequence $(\mathbf{x}_k)_{k=1}^{\infty}$ in $\mathbb{R}^n$ is uniformly distributed if and only if for every $\mathbf{h} \in \mathbb{Z}^n$, $\mathbf{h} \neq \mathbf{0}$,*

$$\lim_{K \to \infty} \frac{1}{K} \sum_{k=1}^{K} e^{2\pi i \langle \mathbf{h}, \mathbf{x}_k \rangle} = 0.$$

Proof. See Kuipers and Niederreiter [11], Chapter 1, Theorem 6.2. See Weyl [22] for Weyl's original proof. □

Corollary 3.7. *A sequence $(\mathbf{x}_k)_{k=1}^{\infty}$ in $\mathbb{R}^n$ is uniformly distributed if and only if for every $\mathbf{h} \in \mathbb{Z}^n$, $\mathbf{h} \neq \mathbf{0}$, the sequence of real numbers $(\langle \mathbf{h}, \mathbf{x}_k \rangle)_{k=1}^{\infty}$, is uniformly distributed.*

Proof. See Kuipers and Niederreiter [11], Chapter 1, Theorem 6.3. See Weyl [22] for Weyl's original proof. □

Corollary 3.8. *Define $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ with $\alpha_1, \ldots, \alpha_m$ $\mathbb{Q}$-linearly independent. The sequence $(\mathbf{x})_{k=1}^{\infty}$ defined by $\mathbf{x}_k = k\boldsymbol{\alpha}$ is uniformly distributed in $\mathbb{R}^m$.*

Proof. For every $\mathbf{h} \in \mathbb{Z}^n$ with $\mathbf{h} \neq 0$, we have $\langle \mathbf{h}, \boldsymbol{\alpha} \rangle \notin \mathbb{Q}$ by the $\mathbb{Q}$-linear independence of $\alpha_1, \ldots, \alpha_m$. The result follows from Corollary 3.3. □

Lemma 3.9. *Let $(\mathbf{q}_k)_{k=1}^{\infty}$ be a sequence in $\mathbb{Z}^n$, ordered such that if s, t are any positive integers with $\|\mathbf{q}_s\|_{\infty} < \|\mathbf{q}_t\|_{\infty}$ then $s < t$. Further, let A be an $m \times n$-matrix with real entries, that fulfills the condition of Kronecker's theorem,*

$$\{\mathbf{z} \in \mathbb{Q}^m : A^T \mathbf{z} \in \mathbb{Q}^n\} = \{\mathbf{0}\}. \tag{3.2}$$

Finally, let $\mathbf{x}_k = A\mathbf{q}_k$ for $k = 1, \ldots, n$. Then the sequence $(\mathbf{x}_k)_{k=1}^{\infty}$ is uniformly distributed in $\mathbb{R}^m$.

Proof. For any $\mathbf{h} \in \mathbb{Z}^n$ we have

$$\begin{aligned} \langle \mathbf{h}, \mathbf{x}_k \rangle &= \langle \mathbf{h}, A\mathbf{q}_k \rangle \\ &= \langle A^T \mathbf{h}, \mathbf{q}_k \rangle. \end{aligned}$$

As A satisfies equation (3.2) one has $A^T\mathbf{h} \notin \mathbb{Q}^n$ for all $\mathbf{h} \neq \mathbf{0}$. The sequence $(\langle A^T\mathbf{h}, \mathbf{q}_k\rangle)_{k=1}^{\infty}$ is a sequence as in Corollary 3.4. This implies that it is uniformly distributed. Now Theorem 3.6 gives the required result. □

For $\mathbf{x} \in \mathbb{R}^n$ define $\lceil \mathbf{x} \rfloor = \max(\lceil x_1 \rfloor, \ldots, \lceil x_n \rfloor)$. Let A be a matrix as in Lemma 3.9. This lemma implies that for all $\mathbf{b} \in \mathbb{R}^m$ and $0 < \varepsilon < \frac{1}{2}$ we have the limit

$$\lim_{Q\to\infty} \frac{\#\{\mathbf{q} \in \mathbb{Z}^n : \|\mathbf{q}\|_\infty \leq Q, \lceil A\mathbf{q} - \mathbf{b} \rfloor \leq \varepsilon\}}{Q^n} = (2\varepsilon)^m.$$

Note that $\lceil A\mathbf{q} - \mathbf{b} \rfloor < \varepsilon$ if and only if $A\mathbf{q} - \mathbf{b} - \lfloor A\mathbf{q} - \mathbf{b} \rfloor \in [\mathbf{0}, \varepsilon\mathbf{1}) \cup (\mathbf{1} - \varepsilon\mathbf{1}, \mathbf{1})$. This explains the factor 2^m. Kronecker's theorem states that for every ε there exist $\mathbf{q} \in \mathbb{Z}^n$ and $\mathbf{p} \in \mathbb{Z}^m$ such that $\|A\mathbf{q} - \mathbf{p} - \mathbf{b}\| \leq \varepsilon$. This also follows from the limit just stated. For an effective Kronecker's theorem we want to give an upper bound Q for $\|\mathbf{q}\|$ in terms of ε. The limit suggests that for "most" A and $\mathbf{b}$ there should be a solution $\mathbf{q} \in \mathbb{Z}^n$ of $\lceil A\mathbf{q} - \mathbf{b} \rfloor \leq \varepsilon$ with $\|\mathbf{q}\|_\infty$ of the order $\varepsilon^{-m/n}$.

3.2 An effective Kronecker's Theorem

At this point we know enough algebraic number theory to prove an effective version of Kronecker's approximation theorem for linear forms with algebraic coefficients.

Proposition 3.10. *Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subset \mathbb{R}$ be a number field and let $d = [K : \mathbb{Q}]$. Then we have*

$$|q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n| \geq \|\mathbf{q}\|_\infty^{1-d}(n+1)^{1-d}H(1, \alpha_1, \ldots, \alpha_n)^{-d}$$

for every $\mathbf{q} = (q_0, \ldots, q_n) \in \mathbb{Z}^{n+1}$ with $q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n \neq 0$.

Proof. By assumption $K \subset \mathbb{R}$. Denote by v the place represented by $|\cdot|$. As $q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n \neq 0$ we may rewrite the product formula, Theorem 2.28, as

$$\begin{aligned} |q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n| &= \prod_{\substack{w\in M_K \\ w\neq v}} |q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n|_w^{-1} \\ &\geq \|\mathbf{q}\|_\infty^{1-d}(n+1)^{1-d} \prod_{\substack{w\in M_K \\ w\neq v}} \max\{1, |\alpha_1|_w, \ldots, |\alpha_n|_w\}^{-1} \\ &\geq \|\mathbf{q}\|_\infty^{1-d}(n+1)^{1-d}H(1, \alpha_1, \ldots, \alpha_n)^{-d}. \end{aligned}$$

This proves the proposition. □

With this proposition we can make Theorem 1.8 effective for the case that A is an $m \times n$ matrix with real algebraic elements satisfying condition (1.1). Let

$$A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{pmatrix}$$

with real algebraic elements α_{ij}. The extensions $\mathbb{Q}(\alpha_{1j}, \dots, \alpha_{mj})$ over $\mathbb{Q}$ are finite for $j = 1, \dots, n$, because $\alpha_{1j}, \dots, \alpha_{mj}$ are algebraic over $\mathbb{Q}$. Define

$$d_j := [\mathbb{Q}(\alpha_{1j}, \dots, \alpha_{mj}) : \mathbb{Q}] \ \ (j = 1, \dots, n) \quad d := \max(d_1, \dots, d_n). \tag{3.3}$$

We define the height of A as

$$H^*(A) = (n+1)^{d-1} \max_{j=1,\dots,n} H(1, \alpha_{1j}, \dots, \alpha_{mj})^d.$$

This notation is not standard, but it turns out to be very useful in the next theorem.

Theorem 3.11. *Let $A = (\alpha_{ij})$ be an $m \times n$ matrix with real algebraic elements such that*

$$\{\mathbf{z} \in \mathbb{Q}^m : A^T\mathbf{z} \in \mathbb{Q}^n\} = \{\mathbf{0}\}. \tag{3.4}$$

Let d be given by (3.3) and define for $\varepsilon > 0$

$$Q(\varepsilon) := \tfrac{d}{2^{d-1}}(m+n)^{2d} H^*(A) \left(\frac{1}{\varepsilon}\right)^{d-1}.$$

Then for every $\varepsilon > 0$, $\mathbf{b} \in \mathbb{R}^m$, there exist $\mathbf{p} \in \mathbb{Z}^m$, $\mathbf{q} \in \mathbb{Z}^n$ with

$$\|A\mathbf{q} - \mathbf{p} - \mathbf{b}\|_\infty \le \varepsilon, \quad \|\mathbf{q}\|_\infty \le Q(\varepsilon).$$

Proof. Let $\mathbf{a} \in \mathbb{Z}^m$ with $\mathbf{a} \neq \mathbf{0}$. Condition (3.4) implies that there is a $j \in \{1, \dots, m\}$, such that $\alpha_{1j}a_1 + \dots + \alpha_{mj}a_m \neq 0$. Proposition 3.10 gives

$$|\alpha_{1j}a_1 + \dots + \alpha_{mj}a_m| \ge H^*(A)^{-1} \|\mathbf{a}\|_\infty^{1-d_j}.$$

Let $\varepsilon > 0$. If we choose Q such that

$$Q \sum_{j=1}^{n} \lceil a_1\alpha_{1j} + \dots + a_m\alpha_{mj} \rfloor + \varepsilon \sum_{i=1}^{m} |a_i| \ge \tfrac{1}{2}(m+n)^2,$$

then we can apply Theorem 1.8. In view of Proposition 3.10 this inequality is satisfied if

$$QH^*(A)^{-1}\|\mathbf{a}\|_\infty^{1-d} + \varepsilon\|\mathbf{a}\|_\infty \geq \tfrac{1}{2}(m+n)^2.$$

By elementary calculus the minimum of the function f defined by

$$f(x) = QH^*(A)^{-1}x^{1-d} + \varepsilon x$$

is assumed at

$$x_{\min} = \left(\frac{QH^*(A)^{-1}(d-1)}{\varepsilon n}\right)^{\frac{1}{d}}.$$

Hence, we must choose Q such that

$$QH^*(A)^{-1}x_{\min}^{1-d} + \varepsilon x_{\min} \quad \geq \quad \tfrac{1}{2}(m+n)^2.$$

An easy calculation shows that this inequality is satisfied for

$$Q = \tfrac{d}{2^{d-1}}(m+n)^{2d}H^*(A)\varepsilon^{1-d}.$$

Theorem 3.11 now follows by applying Theorem 1.8. □

Recall that the heuristic argument in Section 3.1 suggests that in general Kronecker's Theorem should hold with $\|\mathbf{q}\|_\infty \ll \varepsilon^{-m}$. We only get this expected best result if A is a $m \times 1$ matrix and the extension $\mathbb{Q} \subset \mathbb{Q}(\alpha_{11}, \ldots, \alpha_{m1})$ is of degree m. In Section 3.3 below we derive in the case that A is a $m \times 1$ matrix and any $\delta > 0$ an upper bound for $\|\mathbf{q}\|_\infty$ of order $(\varepsilon^{-1})^{m+\delta}$. This upper bound is independent of the degree of the extension, but is not effectively computable by the method of proof.

It is also possible to apply this result to Kronecker's theorem in the more general form as in Section 1.4. Before stating this theorem we need the following definitions. Let A be a $r \times s$ matrix with real algebraic elements α_{ij}. Define K as the field extension of $\mathbb{Q}$ generated by the elements of A. We define $c(A) := [K : \mathbb{Q}]$.

Theorem 3.12. *Let $A \in \mathbb{R}^{r,s}, \mathbf{b} \in \mathbb{R}^r$ both with algebraic elements, such that for all $\mathbf{z} \in \mathbb{R}^r$ with $A^T\mathbf{z} \in \mathbb{Z}^s$ we have $\mathbf{b}^T\mathbf{z} \in \mathbb{Z}$. Then there exists $C \in \mathbb{R}_{>0}$, effectively computable and depending on A and $\mathbf{b}$, such that for all $\varepsilon > 0$, there exists $\mathbf{x} \in \mathbb{Z}^s$ with*

$$\|A\mathbf{x} - \mathbf{b}\|_\infty \leq \varepsilon, \quad \|\mathbf{x}\|_\infty \leq C\left(\frac{1}{\varepsilon}\right)^{c(A)-1}.$$

Proof. For the proof of this theorem we follow the steps of Theorem 1.12. By Lemma 1.13 and Lemma 1.14 we can find $U \in \mathrm{GL}_r(\mathbb{R})$ such that UA is in the shape as demanded at the start of the proof of Theorem 1.12. Let A_1, A_2, $\mathbf{b}_1$, and $\mathbf{b}_2$ be defined as in Lemma 1.14. These matrices and vectors are effectively computable, as there exists a polynomial time algorithm to calculate the Smith normal form. See Bachem and Kannan, [1], for this. A basis for the module M in the proof of Theorem 1.12 is also effectively computable by expressing the elements of A as $\mathbb{Q}$-linear combinations of a chosen $\mathbb{Q}$-basis of K, and then using linear algebra over $\mathbb{Z}$. By Theorem 1.11 there exists $\mathbf{q}' \in \mathbb{Z}^{s-m}, \mathbf{p}'_1 \in \mathbb{Z}^t$ such that

$$A_1\mathbf{q}' - \mathbf{p}'_1 = \mathbf{b}_1.$$

By Lemma 1.13 and inequality (1.9) of Theorem 1.12 we have

$$\|A_2\mathbf{q}'' - \mathbf{p}'_2 - \frac{1}{d}(\mathbf{b}_2 - A_2\mathbf{q}')\|_\infty \leq \frac{\varepsilon}{d\|U\|}.$$

We want to give an upper bound for $\|\mathbf{q}''\|$ in this inequality. By Theorem 3.11 there exist $\mathbf{q}'' \in \mathbb{Z}^n$, $\mathbf{p}'_2 \in \mathbb{Z}^{m-t}$ such that

$$\|\hat{A}'_2\mathbf{q}'' - \mathbf{p}'_2 - \frac{1}{d}(\mathbf{b}_2 + A_2\mathbf{q}')\|_\infty \leq \|U\|\frac{\varepsilon}{d},$$
$$\|\mathbf{q}''\|_\infty \leq \frac{c(A)}{2^{c(A)+1}}(m+n)^{2c(A)}H^*(A_2)\left(\frac{d}{\varepsilon}\right)^{c(A)-1}.$$

The proof of this theorem follows if we use this result and continue with the proof of Theorem 1.12. □

3.3 Subspace Theorem

In this section we use the Subspace Theorem, see below, to prove an effective version of Kronecker's Theorem for matrix $A \in \mathbb{R}^{m,1}$ with algebraic entries.

First we need the following definition. We say that n linear forms

$$L_i = \alpha_{i1}x_1 + \cdots + \alpha_{in}x_n, \qquad i = 1, \ldots, n,$$

are *linearly independent* if

$$\det(L_1, \ldots, L_n) = \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{vmatrix} \neq 0.$$

Theorem 3.13. (Subspace Theorem) *Let $L_1, \ldots, L_n$ be n linearly independent forms with algebraic coefficients in $\mathbb{C}$ and let $\delta > 0$. Then the set of solutions of the equation*

$$0 \leq |L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leq \|\mathbf{x}\|_\infty^{-\delta}$$

with $\mathbf{x} \in \mathbb{Z}^n$ is contained in the union of finitely many proper linear subspaces of $\mathbb{Q}^n$.

Proof. See Schmidt [20]. □

Corollary 3.14. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be algebraic and linearly independent over $\mathbb{Q}$ and let $\delta > 0$. Then there exist only finitely many $\mathbf{x} \in \mathbb{Z}^n$ with $|\alpha_1 x_1 + \cdots + \alpha_n x_n| \leq \|\mathbf{x}\|_\infty^{1-n-\delta}$.*

Proof. This proof is by induction. If $\alpha_1 \neq 0$ then there exist only finitely many $x \in \mathbb{Z}$ such that $|\alpha_1 x| \leq |x|^{-\delta}$. This proves the theorem for the case $n = 1$.

Assume that the theorem is true for $n-1$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$. Take $L_1(\mathbf{x}) = \alpha_1 x_1 + \cdots + \alpha_n x_n$ and $L_i(\mathbf{x}) = x_i$ for $2 \leq i \leq n$. Note that $L_1, \ldots, L_n$ are chosen such that $\det(L_1, \ldots, L_n) \neq 0$. The set of solutions of $|L_1(\mathbf{x})| \leq \|\mathbf{x}\|_\infty^{1-n-\delta}$ is contained in the set of solutions of $|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leq \|\mathbf{x}\|_\infty^{-\delta}$. By the Subspace theorem we find that the solutions with $\mathbf{x} \in \mathbb{Z}^n$ are contained in the union of finitely many proper linear subspaces of $\mathbb{Q}^n$ of dimension $n-1$. These subspaces are of the form $c_1 x_1 + \cdots + c_n x_n = 0$ with $(c_1, \ldots, c_n) \in \mathbb{Q}^n \backslash \{\mathbf{0}\}$. For such a subspace the solutions of $|L_1(\mathbf{x})| \leq \|\mathbf{x}\|_\infty^{1-n-\delta}$ are also solutions of $|(\alpha_1 - \frac{c_1}{c_n}\alpha_n)x_1 + \cdots + (\alpha_{n-1} - \frac{c_{n-1}}{c_n}\alpha_n)x_{n-1}| \leq \|\mathbf{x}\|_\infty^{1-n-\delta}$. Note that $\alpha_1 - \frac{c_1}{c_n}\alpha_n, \cdots, \alpha_{n-1} - \frac{c_{n-1}}{c_n}\alpha_n$ are linearly independent over $\mathbb{Q}$. Hence, these equations have only finitely many solutions $(x_1, \ldots, x_{n-1}) \in \mathbb{Z}^{n-1}$ by the induction hypothesis. This proves the corollary. □

So, if $1, \alpha_1, \ldots, \alpha_n$ are linearly independent with $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, then there exists a constant $C \in \mathbb{R}_{>0}$ such that all $\mathbf{x} \in \mathbb{Z}^n$ satisfy the inequality

$$\lceil \alpha_1 x_1 + \cdots + \alpha_n x_n \rfloor \geq C \|\mathbf{x}\|_\infty^{-n-\delta}.$$

Hence, we proved a lower bound for the sum $\lceil \alpha_1 x_1 + \cdots + \alpha_n x_n \rfloor$ as in Proposition 3.10. In contrast to Proposition 3.10 we do not have an effective lower bound and we have the stronger condition that $1, \alpha_1, \ldots, \alpha_n$ must be linearly independent. But for this result the lower bound is in many cases much stronger than the one depending on the degree of the field extension. As in Section 3.2 we would now like to formulate a version of Kronecker's Theorem using this result. This can not be done for Kronecker's Theorem for linear forms, because of the stronger condition that $1, \alpha_1, \ldots, \alpha_n$ must be linearly independent. This is why we only consider the problem of inhomogeneous simultaneous approximation of real numbers by rational numbers.

Theorem 3.15. *Let $1, \alpha_1, \ldots, \alpha_m \in \mathbb{R}$ be algebraic numbers that are linearly independent over $\mathbb{Q}$ and let $\delta > 0$. Then there exist a constant $D > 0$ depending on $\alpha_1, \ldots, \alpha_m, \delta$ such that for all $\varepsilon > 0$ and $\mathbf{b} \in \mathbb{R}^m$ there exist $\mathbf{p} \in \mathbb{Z}^m$, $q \in \mathbb{Z}$ with*

$$|q\alpha_i - p_i - b_i| \leq \varepsilon \quad \text{for } i = 1, \ldots, m, \quad q \leq D\left(\frac{1}{\varepsilon}\right)^{m+\delta}.$$

Proof. Let $\delta > 0$. According to Corollary (3.14) there exists a constant C such that

$$\lceil a_1\alpha_1 + \cdots + a_m\alpha_m \rfloor \geq C\|\mathbf{a}\|_\infty^{-m-\delta} \quad \text{for all } \mathbf{a} \in \mathbb{Z}^m.$$

With the same calculation as in the proof of Theorem 3.11 we conclude that there exists a constant D such that with

$$Q(\varepsilon) = D\varepsilon^{-m-\delta}$$

we satisfy

$$Q(\varepsilon)C\|\mathbf{a}\|_\infty^{-m-\delta} + \varepsilon\|\mathbf{a}\|_\infty \geq \tfrac{1}{2}(m+1)^2.$$

for all $\varepsilon > 0$. We conclude that

$$Q(\varepsilon)\lceil a_1\alpha_1 + \cdots + a_m\alpha_m \rfloor + \varepsilon \sum_{i=1}^{m} |a_i| \geq \tfrac{1}{2}(m+1)^2.$$

We can apply Theorem 1.8 with $n = 1$. We conclude that there exist $\mathbf{p} \in \mathbb{Z}^m$, $q \in \mathbb{Z}$ with

$$|q\alpha_i - p_i - b_i| \leq \varepsilon \quad \text{for all } 0 < i \leq m, \quad q \leq D\varepsilon^{-m-\delta}.$$

This proves the theorem. □

Based on the heuristic argument in Section 3.1 the best possible result would be proving that Q grows as ε^{-m}. We proved that Q grows as $\varepsilon^{-m-\delta}$, so we came pretty close.

Chapter 4
Geometry of numbers over the adèles

4.1 Adèles

Let K be a number field. For any finite set P of places on K containing M_K^∞, define

$$\mathbb{A}_K(P) = \prod_{v \in P} K_v \times \prod_{v \notin P} \mathcal{O}_v,$$

where $\mathcal{O}_v$, defined by

$$\mathcal{O}_v := \{x \in K_v : |x|_v \leq 1\},$$

is the *maximal compact subring* of K_v with respect to the topology induced by $|\cdot|_v$. Let $\mathbb{A}_K$ be the union $\mathbb{A}_K = \bigcup_P \mathbb{A}_K(P)$ over all such $P \subset M_K$. This set forms a ring under componentwise addition and multiplication and is called the *adèle ring* over K. Elements of this ring are called *adèles* and denoted by (a_v), with $a_v \in K_v$ for all $v \in M_K$ and $a_v \in \mathcal{O}_v$ for almost all[1] $v \in M_K^{\text{fin}}$. We call $(a_v)_{v \in M_K^\infty}$ the infinite part and $(a_v)_{v \in M_K^{\text{fin}}}$ the finite part of the adèle (a_v). On every completion K_v of K we have a topology induced by the absolute value $|\cdot|_v$ on K_v. These topologies induce a topology on $\mathbb{A}_K$, with a basis of the following shape

$$\prod_{v \in M_K} U_v,$$

where U_v is a non-empty open subset of K_v for all $v \in M_K$, and $U_v = \mathcal{O}_v$ for almost all $v \in M_K^{\text{fin}}$. With this toplogy the adèle ring $\mathbb{A}_K$ is the restricted topological product of K_v with respect to $\mathcal{O}_v$. We can say a bit more about the topological structure of $\mathbb{A}_K$, but first we need to define the notion of a locally compact abelian group.

A *locally compact abelian group* is a locally compact Hausdorff space that is also an abelian group, such that the opposite map

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & -x \end{array}$$

and the group operation

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & x + y \end{array}$$

[1] With almost all places we mean all but finitely many places.

with the product topology on $G \times G$ are continuous.

Lemma 4.1. *With the topology defined above the additive group of $\mathbb{A}_K$ is a locally compact topological group.*

Proof. See Cassels and Fröhlich [6], Chapter 2, Section 14. □

The n-dimensional Cartesian product of $\mathbb{A}_K$ is called the *n-dimensional adèle space* denoted $\mathbb{A}_K^n$. Elements of this space are denoted by $(\mathbf{a}_v)$ with $\mathbf{a}_v \in K_v^n$ for all $v \in M_K$ and $\mathbf{a}_v \in \mathcal{O}_v^n$ for almost all $v \in M_K^{\text{fin}}$. We call $(\mathbf{a}_v)_{v \in M_K^\infty}$ and $(\mathbf{a}_v)_{v \in M_K^{\text{fin}}}$ respectively the infinite part and finite part of $(\mathbf{a}_v)$. We endow $\mathbb{A}_K^n$ with the n-fold product topology of $\mathbb{A}_K$.

For an adèle $(\mathbf{a}_v) \in \mathbb{A}_K^n$ and $\lambda \in \mathbb{R}_{>0}$ we define scalar multiplication by $\lambda(\mathbf{a}_v) = (\lambda_v \mathbf{a}_v)$ with

$$\lambda_v = 1 \text{ for } v \in M_K^{\text{fin}};$$
$$\lambda_v = \lambda \text{ for } v \in M_K^\infty.$$

In the forthcoming sections we will state and prove results in the geometry of numbers in the adèle space. For this it is essential to generalize the notion of a convex body to the adèle space. In order to do this we first need a definition of a convex body in $\mathbb{C}^n$. We define a *convex body* in $\mathbb{C}^n$ by identifying $\mathbb{C}^n$ with $\mathbb{R}^{2n}$. A body in $\mathbb{C}^n$ is a non-empty connected subset of $\mathbb{C}^n$, which has the same closure as its interior. It is *convex* under the same condition as in $\mathbb{R}^n$. A body $\mathcal{C}$ in $\mathbb{C}^n$ is called $\mathbb{C}$-*symmetric* if it satisfies the following condition

$$\mathcal{C} = \alpha\mathcal{C} \text{ for all } \alpha \in \mathbb{C} \text{ with } |\alpha| = 1.$$

Definition 4.2. We define a *convex body in* $\mathbb{A}_K^n$ to be a Cartesian product of the following shape:

$$\mathcal{C} = \prod_{v \in M_K^\infty} \mathcal{C}_v \times \prod_{v \in M_K^{\text{fin}}} M_v,$$

where $\mathcal{C}_v$ is a convex body in K_v^n for all $v \in M_K^\infty$ and M_v is a free $\mathcal{O}_v$-module of rank n for all $v \in M_K^{\text{fin}}$, with $M_v = \mathcal{O}_v^n$ for almost all $v \in M_K^{\text{fin}}$. This convex body is called *symmetric* if $\mathcal{C}_v$ is symmetric for all real $v \in M_K^\infty$ and $\mathbb{C}$-symmetric for all complex $v \in M_K^\infty$. It is called bounded if $\mathcal{C}_v$ is bounded for all $v \in M_K^\infty$.

For every $v \in M_K$ there is a natural embedding of K in K_v. Define $\phi := K^n \hookrightarrow \mathbb{A}_K^n$ as the map that is the natural embedding on each coordinate. Let $\mathbf{k} \in K^n$ and let

$(\mathbf{a}_v) = \phi(\mathbf{k})$ then we have $\mathbf{a}_v = \mathbf{k}$ for each $v \in M_K$. To prove that $(\mathbf{a}_v) \in \mathbb{A}_K^n$ we have to show that $\|\mathbf{k}\|_v \leq 1$ for almost all $v \in M_K$. This follows directly from Lemma 2.25.

The set $\phi(K^n)$ may be viewed as a lattice in $\mathbb{A}_K^n$. We will take a closer look at this embeddding in the one-dimensional case. First we will look specifically at the embedding restricted to $\prod_{v \in M_K^\infty} K_v$.

Let K be a number field of degree d over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings, and let $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ be the complex embeddings ordered such that $\sigma_{r+s+i} = \overline{\sigma_{r+i}}$ for $i = 1, \ldots, s$. Define $x^{(i)} = \sigma_i(x)$ for $i = 1, \ldots, d$. Define

$$\begin{aligned} \phi^\infty : K &\hookrightarrow \mathbb{R}^r \times \mathbb{C}^s = \prod_{\sigma_i \in M_K^\infty} K_{\sigma_i} \\ x &\longmapsto (x^{(1)}, \cdots, x^{(r)}, x^{(r+1)}, \cdots, x^{(r+s)}). \end{aligned}$$

We may view ϕ^∞ as a map from K to $\mathbb{R}^d$

$$\begin{aligned} \phi^\infty \colon K &\longrightarrow \mathbb{R}^d \\ x &\longmapsto (x^{(1)}, \ldots, x^{(r)}, \mathrm{Re}(x^{(r+1)}), \mathrm{Im}(x^{(r+1)}), \ldots, \mathrm{Re}(x^{(r+s)}), \mathrm{Im}(x^{(r+s)})). \end{aligned}$$

Let $\mathcal{C}$ be a bounded symmetric convex body in $\mathbb{A}_K$. We have

$$\mathcal{C} = \prod_{v \in M_K^\infty} \mathcal{C}_v \times \prod_{v \in M_K^{\mathrm{fin}}} M_v,$$

with $\mathcal{C}_v$ and M_v as in Definition 4.2. Note that the set defined by $\{x \in K : x \in M_v \text{ for } v \in M_K^{\mathrm{fin}}\}$ is a fractional ideal of $\mathcal{O}_K$. The following lemma explains why $\phi(K)$ may be viewed as a lattice.

Lemma 4.3. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. The set $\mathcal{L} = \phi^\infty(\mathfrak{a})$ is a lattice of $\mathbb{R}^d$ of determinant* $\det \mathcal{L} = 2^{-s}\sqrt{|D_{K/\mathbb{Q}}(\mathfrak{a})|}$.

Proof. Choose a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_d\}$ of $\mathfrak{a}$. We define a $d \times d$ matrix A by

$$A = [\mathbf{a}_1, \ldots, \mathbf{a}_d] = (\alpha_l^{(k)})_{k,l=1}^d$$

and a $d \times d$ matrix B by

$$B = [\mathbf{b}_1, \ldots, \mathbf{b}_d] = [\phi^\infty(\alpha_1), \ldots, \phi^\infty(\alpha_d)].$$

Note that $\mathbf{b}_k = \mathbf{a}_k$ for $k = 1, \ldots, r$ and that $\mathbf{b}_{2k-r-1} = \frac{1}{2}(\mathbf{a}_k + \mathbf{a}_{k+s})$ and $\mathbf{b}_{2k-r} = -i(\mathbf{a}_k - \mathbf{b}_{2k-r-1})$ for $k = r+1, \ldots, r+s$. With elementary linear algebra we calculate $|\det B| = 2^s |\det A|$ and now we have

$$|D_{K/\mathbb{Q}}(\mathfrak{a})| = |\det(A)^2| = 2^{2s}(\det(\phi^\infty(\alpha_1), \ldots, \phi^\infty(\alpha_d))^2.$$

We conclude that $\{\phi^\infty(\alpha_1), \dots, \phi^\infty(\alpha_d)\}$ is an $\mathbb{R}$-basis of $\mathbb{R}^d$ as $D_{K/\mathbb{Q}}(\mathfrak{a}) \neq 0$ by Proposition 2.4. Hence, $\mathcal{L}$ is a lattice in $\mathbb{R}^d$. Now, the result follows from $\det \mathcal{L} = |\det(\phi^\infty(\alpha_1), \dots, \phi^\infty(\alpha_d))|$. □

Corollary 4.4. *A bounded symmetric convex body $\mathcal{C}$ in $\mathbb{A}_K^n$ contains only finitely many points of $\phi(K^n)$.*

Proof. We prove this in the case $n = 1$. For arbitrary n the argument must be applied to each of the coordinates. Let again $\mathcal{C}$ in $\mathbb{A}_K$ be given by

$$\mathcal{C} = \prod_{v \in M_K^\infty} \mathcal{C}_v \times \prod_{v \in M_K^{\text{fin}}} M_v.$$

Define

$$\mathfrak{a} := \{x \in K : x \in M_v \text{ for all } v \in M_K^{\text{fin}}\}.$$

Note that $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_K$. The set

$$\{\phi^\infty(x) : x \in \mathfrak{a}\}$$

is a lattice of $\prod_{v \in M_K^\infty} K_v$ by Lemma 4.3. We conclude that the intersection of $\phi(K)$ and $\mathcal{C}$ is finite, because $\mathcal{C}$ is bounded. □

Analogously to the classical case, we can define successive minima of convex bodies in $\mathbb{A}_K^n$. For $\mathcal{C}$ a convex body in $\mathbb{A}_K^n$ and $\lambda \in \mathbb{R}_{>0}$ let $\lambda\mathcal{C}$ be the convex body given by $\lambda\mathcal{C} := \{\lambda(\mathbf{a}_v) : (\mathbf{a}_v) \in \mathcal{C}\}$. We define the *$n$ successive minima* $\lambda_1(\mathcal{C}), \dots, \lambda_n(\mathcal{C})$ of $\mathcal{C}$ by

$$\lambda_i(\mathcal{C}) := \inf\{\lambda \in \mathbb{R}_{>0} : \dim(\lambda\mathcal{C} \cap \phi(K^n)) \geq i\}.$$

They satisfy $0 < \lambda_1 \leq \cdots \leq \lambda_n < \infty$. As in the classical case successive minima, defined as infima, are minima.

4.2 Strong Approximation Theorem

In this section we prove an effective version of the Strong Approximation Theorem. In the proof we use a non-effective version of the Strong Approximation Theorem, which is in fact a strong version of the Chinese Remainder Theorem.

Let $\mathbb{I}_K \subset \mathbb{A}_K$ be the set defined by

$$\mathbb{I}_K = \{(i_v) : i_v \in K_v^*,\ |i_v|_v = 1 \text{ for almost all } v \in M_K^{\text{fin}}\}.$$

If we endow $\mathbb{I}_K$ with componentwise multiplication, it becomes a group. We call this set the idèle group of K. Let $\|(i_v)\|$ be defined by

$$\|(i_v)\| = \prod_{v \in M_K} |i_v|_v.$$

Further, define

$$\begin{aligned} c(v) &= 0 \quad \text{for } v \in M_K^{\text{fin}} \\ &= 1 \quad \text{for real } v \in M_K^{\infty} \\ &= 2 \quad \text{for complex } v \in M_K^{\infty}. \end{aligned}$$

Theorem 4.5. (Strong Approximation Theorem) *Let $(i_v) \in \mathbb{I}_K$ and let $v_0 \in M_K$. Then for every adèle $(a_v) \in \mathbb{A}_K$ there exists an $x \in K$ such that*

$$|x - a_v|_v \leq |i_v|_v \quad \text{for all } v \in M_K \setminus \{v_0\}.$$

Proof. See Cassels and Fröhlich [6], Chapter 2, Section 15. □

Theorem 4.6. (Effective Strong Approximation Theorem) *Denote again by r the number of real places of K and by s the number of complex places of K. Choose an idèle $(i_v) \in \mathbb{I}_K$ such that*

$$\|(i_v)\| \geq \left(\frac{d}{2} \left(\frac{2}{\pi} \right)^s \sqrt{|D_K|} \right)^d. \tag{4.1}$$

Then for every adèle $(a_v) \in \mathbb{A}_K$ there exists $x \in K$, such that

$$|x - a_v|_v \leq |i_v|_v \quad \text{for all } v \in M_K.$$

Proof. Let $\mathfrak{a}$ be the fractional ideal of $\mathcal{O}_K$ given by

$$\mathfrak{a} = \{x \in K : |x|_v \leq |(i_v)|_v \text{ for all } v \in M_K^{\text{fin}}\}.$$

Let $\mathcal{L} = \phi^{\infty}(\mathfrak{a})$ be a lattice in $\mathbb{R}^d$ as in Lemma 4.3. Define $A_1, \ldots, A_{r+s} \in \mathbb{R}_{>0}$ by $A_j = |i_{\sigma_j}|_{\sigma_j}$ for $j = 1, \ldots, r+s$. Define

$$\mathcal{C} := \left\{ \begin{array}{cc} (y_1, \ldots, y_r, y_{r+1}, z_{r+1}, \ldots, y_{r+s}, z_{r+s}) & \in \mathbb{R}^d \text{ with} \\ |y_i| \leq A_i & \text{for } i = 1, \ldots, r \\ y_i^2 + z_i^2 \leq A_i & \text{for } i = r+1, \ldots, r+s \end{array} \right\}.$$

Note that $\mathcal{C}$ is a convex body in $\mathbb{R}^d$. By the Strong Approximation Theorem, Theorem 4.5, there exists $b \in K$ such that $|b - a_v|_v \leq |i_v|_v$ for all $v \in M_K^{\text{fin}}$. By definition of the covering radius $\mu = \mu(\mathcal{C}, \mathcal{L})$ there exists an $\mathbf{u} \in \mathcal{L}$ such that $\phi^\infty(b) - (a_v)_{v \in M_K^\infty} + \mathbf{u} \in \mu\mathcal{C}$. There exists a $\kappa \in \mathfrak{a}$ such that $\phi^\infty(\kappa) = \mathbf{u}$. Take $x = b - \kappa$, then we get $|x - a_v|_v \leq \mu^{c(v)} |i_v|_v$ for all $v \in M_K$.

Now, we are ready if we prove that $\mu \leq 1$. We will first give an upper bound for λ_d using Minkowski's convex body theorem and then apply Theorem 1.4 for the required upper bound for μ. In order to use Minkowski's Convex Body Theorem, we have to calculate $\det \mathcal{L}$ and $V(\mathcal{C})$.

We will start by calculating $\det \mathcal{L}$. We already know that

$$\det \mathcal{L} = 2^{-s} \sqrt{|D_{K/\mathbb{Q}}(\mathfrak{a})|} = 2^{-s} N(\mathfrak{a}) \sqrt{|D_K|} \tag{4.2}$$

by Lemma 4.3 and Proposition 2.5. So, we need to take a closer look at $N(\mathfrak{a})$. For $v \in M_K^{\text{fin}}$, let $\mathfrak{p}_v$ be the prime ideal given by $\{x \in \mathcal{O}_K : |x|_v < 1\}$. Using that

$$\mathfrak{a} = \{x \in K : \operatorname{ord}_{\mathfrak{p}_v}(x) \leq \operatorname{ord}_{\mathfrak{p}_v}(\mathfrak{a}) \text{ for all } v \in M_K^{\text{fin}}\}$$

we find

$$\mathfrak{a} = \prod_{v \in M_K^{\text{fin}}} \mathfrak{p}_v^{\operatorname{ord}_{\mathfrak{p}_v}(i_v)}.$$

Hence,

$$N(\mathfrak{a}) = \prod_{v \in M_K^{\text{fin}}} N(\mathfrak{p}_v)^{\operatorname{ord}_{\mathfrak{p}_v}(i_v)} = \prod_{v \in M_K^{\text{fin}}} |i_v|_v^{-1}.$$

Putting together this result with equation (4.2), we get

$$\det \mathcal{L} = 2^{-s} \sqrt{|D_K|} \prod_{v \in M_K^{\text{fin}}} |i_v|_v^{-1}.$$

Calculating the volume of the convex body $\mathcal{C}$ is actually quite easy:

$$V(\mathcal{C}) = 2^r \pi^s \prod_{v \in M_K^\infty} |i_v|.$$

Minkowski's Convex Body Theorem states that

$$\lambda_1 \cdots \lambda_d \leq 2^d \frac{\det \mathcal{L}}{V(\mathcal{C})}.$$

If we have a lower bound for $\lambda_1, \ldots, \lambda_{d-1}$, then we get an upper bound for λ_d. There exists an $\mathbf{u} \in \mathbb{R}^d$ with $\mathbf{u} \neq 0$ and $\mathbf{u} \in \lambda_1 \mathcal{C} \cap \mathcal{L}$ and there exists a $\kappa \in \mathfrak{a}$ such that $\phi^\infty(\kappa) = \mathbf{u}$. We have $|\kappa|_v \leq |i_v|_v$ for all $v \in M_K^{\text{fin}}$ and $|\kappa|_v \leq \lambda_1^{c(v)} |i_v|_v$ for all $v \in M_K^\infty$. Hence, we get

$$1 = \prod_{v \in M_K} |\kappa|_v \leq \lambda_1^d \|(i_v)\|.$$

We can use this to find the following upper bound

$$\lambda_d \leq \frac{\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|} \|(i_v)\|^{-1}}{\lambda_1^{d-1}} = \left(\frac{2}{\pi}\right)^s \sqrt{|D_K|} \|(i_v)\|^{-1/d}.$$

Using Theorem 1.4, we have

$$\mu \leq \frac{d}{2} \lambda_d \leq \frac{d}{2} \left(\frac{2}{\pi}\right)^s \sqrt{|D_K|} \|(i_v)\|^{-1/d}.$$

We conclude that $\mu \leq 1$ by inequality (4.1). This proves the theorem. □

4.3 Fundamental domain

Let again K be an algebraic number field.

Definition 4.7. A set $\mathcal{F} \subset \mathbb{A}_K$ is called a *fundamental domain* for $\mathbb{A}_K / \phi(K)$ if for every $(a_v) \in \mathbb{A}_K$ there exists precisely one $(a'_v) \in \mathcal{F}$, such that $(a_v) - (a'_v) \in \phi(K)$.

Let ϕ^∞ be the canonical embedding of K in $\prod_{v \in M_K^\infty} K_v$ as defined in Section 4.1. Let U be the set given by

$$U = \{\xi_1 \phi^\infty(\omega_1) + \cdots + \xi_n \phi^\infty(\omega_n) : \xi_i \in \mathbb{R}, -\tfrac{1}{2} \leq \xi_i < \tfrac{1}{2} \ (i = 1, \ldots, n)\},$$

where $\{\omega_1, \cdots, \omega_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. We define the set $\mathcal{F}$ by

$$\mathcal{F} \ = \ U \times \prod_{v \in M_K^{\text{fin}}} \mathcal{O}_v. \tag{4.3}$$

Theorem 4.8. *The set $\mathcal{F}$ is a fundamental domain for $\mathbb{A}_K / \phi(K)$.*

Proof. Let $(a_v) \in \mathbb{A}_K$ be an arbitrary adèle. We have to show that there exists precisely one $(a'_v) \in \mathcal{F}$ such that $(a_v) - (a'_v) \in \phi(K)$. This is equivalent with proving that there exists precisely one $x \in K$ with $(a_v) - \phi(x) \in \mathcal{F}$. We first show the existence and then the uniqueness.

There exists an $x' \in K$, such that $|x' - a_v|_v \leq 1$ for all $v \in M_K^{\text{fin}}$ by the Strong Approximation Theorem, Theorem 4.5. The set $\{\phi^\infty(\omega_1), \ldots, \phi^\infty(\omega_n)\}$ is an $\mathbb{R}$-basis by Lemma 4.3. Hence, we have

$$\phi^\infty(x') = \sum_{i=1}^{n} \alpha_i \phi^\infty(\omega_i),$$

where $\alpha_i \in \mathbb{R}$ for $i = 1, \ldots, n$. We can choose $z_1, \ldots, z_n \in \mathbb{Z}$ such that

$$-\tfrac{1}{2} \leq \alpha_i - z_i < \tfrac{1}{2}.$$

Now, $x = x' - (z_1\omega_1 + \cdots + z_n\omega_n)$ satisfies.

We still have to prove that there exists only one $x \in K$ with $(a_v) - \phi(x) \in \mathcal{F}$. Let $x, y \in K$ with $(a_v) - \phi(x) \in \mathcal{F}$ and $(a_v) - \phi(y) \in \mathcal{F}$. We have $|x - y|_v \leq 1$ for all $v \in M_K^{\text{fin}}$. Hence $x - y \in \mathcal{O}_K$ by Lemma 2.23. Expressing $\phi^\infty(x)$ and $\phi^\infty(y)$ on the basis $\{\phi^\infty(\omega_1), \ldots, \phi^\infty(\omega_n)\}$ of $\phi^\infty(K)$, we get

$$\begin{aligned} \phi^\infty(x) &= \sum_{i=1}^{n} x_i \phi^\infty(\omega_i), \\ \phi^\infty(y) &= \sum_{i=1}^{n} y_i \phi^\infty(\omega_i), \end{aligned}$$

with x_i, $y_i \in \mathbb{R}$ and $x_i - y_i$ in $\mathbb{Z}$ for $i = 1, \ldots, n$ As we have both $-\frac{1}{2} \leq x_i - (a_{v_i}) < \frac{1}{2}$ and $-\frac{1}{2} \leq y_i - (a_{v_i}) < \frac{1}{2}$ we find $-1 < x_i - y_i < 1$ for $i = 1, \ldots, n$. Hence, $x_i = y_i$ for $i = 1, \ldots, n$ and $x = y$. This proves the theorem. □

4.4 The Haar measure on the adèle space

For an introduction to measure theory we refer to Bartle [2]. The definitions of a σ-algebra, Borel set and measure can be found in this book. Let X be a topological space. The *Borel σ-algebra on X*, denoted $\mathcal{B}(X)$, is the σ-algebra generated by the open subsets of X. The sets in this σ-algebra are called *Borel sets*. This σ-algebra also contains all closed sets of X. From now on let X be Hausdorff. Every compact

set in a Hausdorff space is closed and hence a Borel set. A measure μ on X is called a *Borel measure* if all Borel sets are μ-measurable, and $\mu(S) < \infty$ for all compact subsets $S \subset X$. A Borel measure is called

1. *inner regular* if

$$\mu(E) = \sup\{\mu(S) : S \subset E,\ S \text{ compact}\} \text{ for all } E \in \mathcal{B}(X).$$

2. *outer regular* if

$$\mu(E) = \inf\{\mu(U) : U \supset E,\ U \text{ open}\} \text{ for all } E \in \mathcal{B}(X).$$

3. *regular* if it is both inner and outer regular.

On the Euclidean space $\mathbb{R}^n$ there is Borel measure, which agrees with the Lebesgue measure on Borel sets. This measure is unique up to a constant factor.

Let G be a locally compact abelian group. A *Haar measure* on G is a regular Borel measure μ on G such that the following two properties hold:

1. $\mu(E) < \infty$ if E is compact;
2. $\mu(E + x) = \mu(E)$ for all measurable subsets $E \subset G$ and all $x \in G$.

We have the following important theorem concerning the Haar measure.

Theorem 4.9. *On every locally compact abelian group G there exists a Haar measure, which is unique up to a multiplicative constant.*

Proof. See Loomis [14], Section 29, Chapter VI. □

Hence, by Theorem 4.9 and Lemma 4.1 there exists a Haar measure on the adèle space $\mathbb{A}_K^n$.

We will define a Haar measure on the adèle space $\mathbb{A}_K$ as the product of Haar measures on the spaces K_v with $v \in M_K$. Let $v \in M_K^{\text{fin}}$. Let p be the place on $\mathbb{Q}$ with $v|p$. From Theorem 4.9, we know there exists a Haar measure on K_v, since K_v is a locally compact group. Let β_v denote the Haar measure on K_v scaled such that $\beta_v(\mathcal{O}_v) = |D_K|_v^{1/2d}$. With this information it is possible to calculate the volume of free $\mathcal{O}_v$-modules. A free $\mathcal{O}_v$-module is of the form $x\mathcal{O}_v$ for some $x \in K_v$. The volume of $x\mathcal{O}_v$ is equal to $[\mathcal{O}_v : x\mathcal{O}_v]^{-1}|D_K|_v^{1/2d} = |N_{K_v/\mathbb{Q}_p}(x)|_v|D_K|_v^{1/2d}$.

As the adèle space is a locally compact group, we can define a Haar measure on it. We will do this in the following way:

1. If $v \in M_K^{\text{fin}}$, let β_v denote the Haar measure on K_v as explained above.

2. If $v \in M_K^\infty$ with $K_v = \mathbb{R}$, let β_v denote the ordinary Lebesgue measure on $\mathbb{R}$.
3. If $v \in M_K^\infty$ with $K_v = \mathbb{C}$, let β_v denote the ordinary Lebesgue measure on $\mathbb{C}$ multiplied by 2.

For every set of finite places P the product measure $\beta = \prod_v \beta_v$ is a Haar measure on $\mathbb{A}_K(P)$. The Haar measure on $\mathbb{A}_K$ is the measure β that agrees with all these measures on all subsets $\mathbb{A}_K(P)$. The n-fold product measure of β gives a Haar measure on $\mathbb{A}_K^n$. Denote the volume of a convex set $\mathcal{C}$ in $\mathbb{A}_K^n$ induced by this measure by $V(\mathcal{C})$.

The choice of the scaling $\beta_v(\mathcal{O}_v) = |D_K|_v^{1/2d}$ probably looks a bit arbitrary. This is not the case as shown in the following lemma.

Proposition 4.10. *Let K be a number field of degree $d = [K : \mathbb{Q}]$ over $\mathbb{Q}$ and let r and s be respectively the number of real and complex embeddings. Let $\mathcal{F}$ be the fundamental domain $\mathbb{A}_K/\phi(K)$ as defined in equation (4.3). Then we have $V(\mathcal{F}) = 1$.*

Proof. Let ϕ^∞ be the natural embedding of K in $\prod_{v \in M_K^\infty} K_v$ as defined in Section 4.1. Using Lemma 4.3 and the product formula, Theorem 2.28, we find that

$$\begin{aligned} V(\mathcal{F}) &= \det(\phi^\infty(\omega_1), \ldots, \phi^\infty(\omega_n)) \cdot 2^s \cdot \prod_{v \in M_K^{\text{fin}}} \beta_v(\mathcal{O}_v) = \\ &\sqrt{|D_K|} \prod_{v \in M_K^\infty} |D_K|_v^{-1/2d} = 1. \end{aligned}$$

This proves the proposition. □

4.5 Minkowski's Theorem for adèle spaces

In this section we state an adèlic version of the Minkowski's Theorem. This theorem will be of crucial importance for our proof of an adèlic version of Kronecker's Theorem. It was first proven in 1971 by R. McFeat [16] in a dissertation called "Geometry of numbers in adèle spaces". Unaware of this, E. Bombieri and J. Vaaler [3] published the same result in 1983.

Theorem 4.11. (Second Theorem of Minkowski for adèle spaces) *Let K be a number field of degree $d = [K : \mathbb{Q}]$ over $\mathbb{Q}$ and let r and s be respectively the number of real and complex embeddings. Let $\mathcal{C}$ be a bounded symmetric convex body in the adèle space $\mathbb{A}_K^n$. Then its successive minima $\lambda_1, \ldots, \lambda_n$ satisfy*

$$\frac{2^{dn}\pi^{sn}}{(n!)^r(2n!)^s|D_K|^{\frac{1}{2}n}} \leq (\lambda_1 \cdots \lambda_n)^d V(\mathcal{C}) \leq 2^{dn}.$$

Proof. See E. Bombieri and J. Vaaler [3], Theorem 3 and Theorem 6 for respectively the upper and the lower bound. □

We have the following relationship between the adèlic and classical version of Minkowski's Theorem, i.e., Theorem 1.2.

Corollary 4.12. *The adèlic version of Minkowski's Theorem implies Theorem 1.2.*

Proof. Let $\mathcal{C}$ be a symmetric convex body in $\mathbb{R}^n$. We only prove the corollary for the lattice $\mathbb{Z}^n$. To prove this result for other lattices we have to apply an invertible linear transformation. Define a convex body in $\mathbb{A}_{\mathbb{Q}}^n$ by:

$$\mathcal{C}' = \mathcal{C} \times \prod_{v \in M_{\mathbb{Q}}^{\text{fin}}} \mathcal{O}_v.$$

Note that the number of real embeddings $r = 1$, the number of complex embeddings $s = 0$, the degree $d = 1$ and the discriminant $D_{\mathbb{Q}} = 1$. After filling in these constants, Minkowski's Theorem for adèle spaces states that

$$\frac{2^n}{n!}\lambda_1(\mathcal{C}') \cdots \lambda_n(\mathcal{C}')V(\mathcal{C}') \leq 2^n.$$

As $D_{\mathbb{Q}} = 1$, we have $V(\mathcal{C}') = V(\mathcal{C})$ by definition. Hence, the corollary is proven if we show that $\lambda_i(\mathcal{C}') = \lambda_i(\mathcal{C}, \mathbb{Z}^n)$.

Let us recall the exact definitions of $\lambda_i(\mathcal{C}')$ and $\lambda_i(\mathcal{C}, \mathbb{Z}^n)$:

$$\begin{aligned} \lambda_i(\mathcal{C}') &= \inf\{\lambda \in \mathbb{R}_{>0} : \dim(\lambda\mathcal{C}' \cap \phi(\mathbb{Q}^n)) \geq i\}, \\ \lambda_i(\mathcal{C}, \mathbb{Z}) &= \inf\{\lambda \in \mathbb{R}_{>0} : \dim(\lambda\mathcal{C} \cap \mathbb{Z}^n) \geq i\}. \end{aligned}$$

Note that $\lambda_i(\mathcal{C}') = \lambda_i(\mathcal{C}, \mathbb{Z}^n)$ follows once we have proved that $\mathbf{x} \in \lambda C \cap \mathbb{Z}^n$ if and only if $\phi(\mathbf{x}) \in \lambda C \cap \phi(\mathbb{Q}^n)$. Let $\mathbf{x} \in \mathbb{Q}^n$ with $\phi(\mathbf{x}) \in \lambda\mathcal{C}'$. We have $\mathbf{x} \in \lambda\mathcal{C}$ and $|x_i|_p \leq 1$ for $i = 1, \ldots, n$ and all primes primes p. Hence, $\mathbf{x} \in \lambda\mathcal{C} \cap \mathbb{Z}^n$. Conversely, if $\mathbf{x} \in \lambda\mathcal{C} \cap \mathbb{Z}^n$ then $|x_i|_p \leq 1$ for all p, implying $\phi(\mathbf{x}) \in \lambda\mathcal{C}'$.

This proves the corollary. □

Chapter 5
Kronecker's Theorem over the adèles

5.1 Kronecker's theorem for adèle spaces

In this section we prove an adelic version of Kronecker's Theorem. We need some additional definitions and results first.

We already defined successive minima for convex bodies in the adèle space. There exists an adèlic analog of the covering radius too. The *covering radius* $\mu(\mathcal{C})$ of a convex body $\mathcal{C}$ in $\mathbb{A}_K^n$ is defined by

$$\mu(\mathcal{C}) = \inf\{\lambda \in \mathbb{R}_{>0} : \bigcup_{\mathbf{x}\in K^n} (\lambda\mathcal{C} + \phi(\mathbf{x})) = \mathbb{A}_K^n\}.$$

O'Leary and Vaaler proved a lower and upper bound for the covering radius μ of convex body in terms of its successive minima. To this purpose they introduced a constant $\nu(K)$ depending on the field K. For every number field K we can define a convex body $\mathcal{S}_K$ by

$$\mathcal{S}_K = \prod_{v\in M_K^\infty} \mathcal{C}_v \times \prod_{v\in M_K^{\text{fin}}} \mathcal{O}_v,$$

where $\mathcal{C}_v = \{x \in K_v : |x|_v \leq 1\}$ for all $v \in M_K^\infty$. Define $\nu(K) := \mu(\mathcal{S}_K)$. The following lemma gives an upper bound for $\nu(K)$.

Lemma 5.1. *The constant $\nu(K)$ is bounded by the following upper bound*

$$\nu(K) \leq \frac{d}{2}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}.$$

Proof. Define $(i_v) \in \mathbb{I}_K$ by $i_v = 1$ for all $v \in M_K^{\text{fin}}$ and $i_v = \frac{d}{2}(\frac{2}{\pi})^s\sqrt{|D_K|}$ for all $v \in M_K^\infty$. Then

$$\|(i_v)\| = \left(\frac{d}{2}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}\right)^d.$$

Now choose an arbitrary adèle $(a_v) \in \mathbb{A}_K$. By the effective Strong Approximation Theorem, Theorem 4.6, there exists an $x \in K$ such that $|x - a_v|_v \leq |i_v|_v$ for all $v \in M_K$. Hence, we have

$$(a_v) - \phi(x) \in \left(\frac{d}{2}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}\right)\mathcal{S}_K.$$

Hence, for $\lambda = \left(\frac{d}{2}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}\right)$ we have

$$\bigcup_{x\in K}(\lambda\mathcal{S}_K + \phi(x)) = \mathbb{A}_K$$

and

$$\nu(K) = \mu(\mathcal{S}_K) \le \frac{d}{2}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}.$$

This proves the lemma. □

Theorem 5.2. *Let $\mathcal{C}$ be a convex body in $\mathbb{A}_K^n$. Its successive minima $\lambda_1, \dots, \lambda_n$ and covering radius μ satisfy*

$$\tfrac{1}{2}\lambda_n \le \mu \le \nu(K)(\lambda_1 + \cdots + \lambda_n).$$

For the original proof by O'Leary and Vaaler, see [19], Theorem 5.

Proof. Let

$$\mathcal{C} = \prod_{v\in M_K^\infty} \mathcal{C}_v \times \prod_{v\in M_K^{\mathrm{fin}}} M_v$$

be a convex body in $\mathbb{A}_K^n$ as in Definition 4.2.

First we prove the lower bound by contradiction. Let t be the number of linearly independent vectors in $(\mu + \frac{1}{2}\lambda_n)\mathcal{C} \cap \phi(K)$. Suppose that $\mu + \frac{1}{2}\lambda_n < \lambda_n$, implying that $t < n$. Choose linearly independent $\mathbf{x}_1, \dots, \mathbf{x}_t \in K^n$ such that $\phi(\mathbf{x}_1), \dots, \phi(\mathbf{x}_t) \in (\mu + \frac{1}{2}\lambda_n)\mathcal{C}$. Choose $\mathbf{x} \in K^n$ such that $\phi(\mathbf{x}) \in \lambda_n\mathcal{C}$ and $\mathbf{x} \notin \mathrm{Span}\{\mathbf{x}_1, \dots, \mathbf{x}_t\}$. There exists $\mathbf{u} \in K^n$ such that $\frac{1}{2}\phi(\mathbf{x}) - \phi(\mathbf{u}) \in \mu\mathcal{C}$ by the definition of the covering radius. Recall that $\frac{1}{2}\phi(\mathbf{x}) = (\mathbf{x}_v)$ with $\mathbf{x}_v = \frac{1}{2}\mathbf{x}$ for $v \in M_K^\infty$, $\mathbf{x}_v = \mathbf{x}$ for $v \in M_K^{\mathrm{fin}}$. By symmetry and convexity of $\mathcal{C}_v$ we find that $\mathbf{u} = \mathbf{u} - \frac{1}{2}\mathbf{x} + \frac{1}{2}\mathbf{x}$ and $\mathbf{x} - \mathbf{u} = \frac{1}{2}\mathbf{x} - \mathbf{u} + \frac{1}{2}\mathbf{x}$ are both in $(\mu + \frac{1}{2}\lambda_n)\mathcal{C}_v$ for all $v \in M_K^\infty$. Further, $\mathbf{x} - \mathbf{u}, \mathbf{x} \in M_v$ for all $v \in M_K^{\mathrm{fin}}$. Hence, because M_v is a module, $\mathbf{u}, \mathbf{x} - \mathbf{u} \in M_v$ for all $v \in M_K^{\mathrm{fin}}$. We conclude that both $\phi(\mathbf{u}) \in (\mu + \frac{1}{2}\lambda_n)\mathcal{C}$ and $\phi(\mathbf{x} - \mathbf{u}) \in (\mu + \frac{1}{2}\lambda_n)\mathcal{C}$. Hence, $\mathbf{u}, \mathbf{x} - \mathbf{u} \in \mathrm{Span}\{\mathbf{x}_1, \dots, \mathbf{x}_t\}$, which contradicts with $\mathbf{x} \notin \mathrm{Span}\{\mathbf{x}_1, \dots, \mathbf{x}_t\}$. This proves the lower bound.

Now we prove the upper bound. Choose linearly independent $\mathbf{x}_1, \dots, \mathbf{x}_n \in K^n$ such that $\phi(\mathbf{x}_i) \in \lambda_i\mathcal{C}$. Let us take an arbitrary $(\mathbf{a}_v) \in \mathbb{A}_K^n$. For every $v \in M_K$ there exist $\alpha_{v,1}, \dots, \alpha_{v,n} \in \mathbb{R}$ such that $\mathbf{a}_v = \alpha_{v,1}\mathbf{x}_1 + \cdots + \alpha_{v,n}\mathbf{x}_n$. Note that $(\alpha_{v,i}) \in \mathbb{A}_K^n$ for $i = 1, \dots, n$. By definition of $\nu(K)$ there exist $\kappa_1, \dots, \kappa_n \in K$ such that $\|\alpha_{v,i} - \kappa_i\| \le$

$\nu(K)$ for all $v \in M_K^\infty$ and $\|\alpha_{v,i} - \kappa_i\|_v \leq 1$ for all $v \in M_K^{\mathrm{fin}}$. Recall that $\mathbf{x}_i \in \lambda_i \mathcal{C}_v$ for all $v \in M_K^{\mathrm{fin}}$. Hence, for all $v \in M_K$ we find

$$\mathbf{a}_v - \sum_{i=1}^{n} \kappa_i \mathbf{x}_i = \sum_{i=1}^{n} (\alpha_{v,i} - \kappa_i)\mathbf{x}_i \in \nu(K)(\lambda_1 + \cdots + \lambda_n)\mathcal{C}_v.$$

This proves the theorem. □

For $v \in M_K$ we define the maximum norm $\|\cdot\|_v$ with respect to v by

$$\|\mathbf{x}\|_v := \max\{|x_1|_v, \ldots, |x_n|_v\} \qquad \text{for } \mathbf{x} = (x_1, \ldots, x_n) \in K_v^n.$$

Let $A \in K_v^{m,n}$ be a matrix given by

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}.$$

Define the norm $\|\cdot\|_v$ on $K_v^{m,n}$ analogously to the norm on matrices in Section 1.4 by

$$\|A\|_v = \max_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} |\alpha_{ij}|_v \qquad \text{for } v \in M_K^{\mathrm{fin}},$$

$$\|A\|_v = \max_{1 \leq i \leq m} \sum_{j=1}^{n} |\alpha_{ij}|_v \qquad \text{for real } v \in M_K^\infty.$$

$$\|A\|_v = \max_{1 \leq i \leq m} \left(\sum_{j=1}^{n} |\alpha_{ij}|_v^{\frac{1}{2}} \right)^2 \qquad \text{for complex } v \in M_K^\infty.$$

Note that we have $\|A\mathbf{x}\|_v \leq \|A\|_v \|\mathbf{x}\|_v$ for all $v \in M_K$, $A \in K_v^{m,n}$, and $\mathbf{x} \in K_v^n$.

Let $\mathrm{GL}_n(\mathbb{A}_K)$ be the group of invertible matrices in $\mathbb{A}_K^{n,n}$. Each element $A \in \mathrm{GL}_n(\mathbb{A}_K)$ may be represented by a tuple (A_v) with $A_v \in \mathrm{GL}_n(K_v)$ for all $v \in M_K$ and $A_v \in \mathrm{GL}_n(\mathcal{O}_v)$ for almost all v in M_K^{fin} and then

$$\det A \in \mathbb{I}_K, \quad \|\det A\| = \prod_{v \in M_K} |\det A_v|_v.$$

Let $A \in \mathrm{GL}_n(\mathbb{A}_K^n)$ and define

$$\Pi := \{(\mathbf{a}_v) \in \mathbb{A}_K^n : \|A_v \mathbf{a}_v\|_v \leq 1 \text{ for all } v \in M_K\}.$$

This set may be viewed as the adèlic analog of a parallelepiped. The set given by

$$\Pi^* = \{(\mathbf{a}_v) \in \mathbb{A}_K^n : \|(A_v^{-1})^T \mathbf{a}_v\|_v \leq 1 \text{ for all } v \in M_K\}$$

may be viewed as the reciprocal of Π. Both Π and Π^* are convex bodies in $\mathbb{A}_K^n$. Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of Π and $\lambda_1^*, \ldots, \lambda_n^*$ the successive minima of Π^*. By Theorem 4.11 we have

$$(\lambda_1 \ldots \lambda_n)^d \leq 2^{dn} V(\Pi)^{-1} = |\det A|^{-1}, \tag{5.1}$$

and

$$(\lambda_1^* \ldots \lambda_n^*)^d \leq 2^{dn} V(\Pi^*)^{-1} = |\det A|. \tag{5.2}$$

In the following theorem we will prove an upper bound for $\lambda_i^* \lambda_{n+1-i}$.

Theorem 5.3. *The successive minima of* Π *and* Π^* *satisfy*

$$n^{-1} \leq \lambda_i^* \lambda_{n+1-i} \leq n^{n-1} \qquad \textit{for } i = 1, \ldots, n.$$

Proof. First we prove the lower bound. Choose linearly independent $\mathbf{x}_1, \ldots, \mathbf{x}_n \in K^n$ such that $\phi(\mathbf{x}_i) \in \lambda_i \Pi$ for $i = 1, \ldots, n$ and linearly independent $\mathbf{x}_1^*, \ldots, \mathbf{x}_n^* \in K^n$ such that $\phi(\mathbf{x}_i^*) \in \lambda_i^* \Pi^*$ for $i = 1, \ldots, n$. Note that

$$\|A_v \mathbf{x}_i\|_v \leq \lambda_i^{c(v)}, \ \|(A_v^{-1})^T \mathbf{y}_j\|_v \leq (\lambda_j^*)^{c(v)} \qquad \text{for all } v \in M_K.$$

We have for all $v \in M_K^{\text{fin}}$

$$\begin{aligned} |\mathbf{x}_i^T \mathbf{x}_j^*|_v &= |\mathbf{x}_i^T A_v^T (A_v^T)^{-1} \mathbf{x}_j^*|_v \\ &= |(A_v \mathbf{x}_i)^T (A_v^T)^{-1} \mathbf{x}_j^*|_v \\ &\leq \|A_v \mathbf{x}_i\|_v \|(A_v^T)^{-1} \mathbf{x}_j^*\|_v \\ &\leq 1. \end{aligned}$$

Hence, $\mathbf{x}_i^T \mathbf{x}_j^* \in \mathcal{O}_K$ and $N_{K/\mathbb{Q}}(\mathbf{x}_i^T \mathbf{x}_j^*) \in \mathbb{Z}$. By Theorem 2.27 we have

$$\prod_{v \in M_K^\infty} |\mathbf{x}_i^T \mathbf{x}_j^*|_v = |N_{K/\mathbb{Q}}(\mathbf{x}_i^T \mathbf{x}_j^*)| \in \mathbb{Z}$$

and so we get $\mathbf{x}_i^T \mathbf{x}_j^* = 0$ or $|\mathbf{x}_i^T \mathbf{x}_j^*|_v \geq 1$ for at least one $v \in M_K^\infty$.

In a similar way we derive for all $v \in M_K^\infty$ that

$$\begin{aligned} |\mathbf{x}_i^T \mathbf{x}_j^*|_v &= |\mathbf{x}_i^T A_v^T (A_v^T)^{-1} \mathbf{x}_j^*|_v \\ &= |(A_v \mathbf{x}_i)^T (A_v^T)^{-1} \mathbf{x}_j^*|_v \\ &\leq n^{c(v)} \|A_v \mathbf{x}_i\|_v \|(A_v^T)^{-1} \mathbf{x}_j^*\|_v \\ &\leq (n \lambda_i \lambda_j^*)^{c(v)}. \end{aligned}$$

The set $\{\mathbf{x}_1, \ldots, \mathbf{x}_i, \mathbf{x}_1^*, \ldots, \mathbf{x}_{n+1-i}^*\}$ contains $n+1$ vectors in K^n. We have $\mathbf{x}_k^T \mathbf{x}_l^* \neq 0$ for a k and l with $1 \leq k \leq i$ and $1 \leq l \leq n+1-i$, because there are maximal n K-linearly independent vectors in K^n. We conclude that

$$1 \leq |\mathbf{x}_k^T \mathbf{x}_l^*|_v \leq (n \lambda_k \lambda_l^*)^{c(v)} \leq (n \lambda_i \lambda_{n+1-i}^*)^{c(v)}$$

for at least one $v \in M_K^\infty$. This proves the lower bound

$$\lambda_i \lambda_{n+1-i}^* \geq \frac{1}{n}.$$

The upper bound is a direct consequence of the lower bound and inequalities (5.1) and (5.2).

$$\begin{aligned} (\lambda_i \lambda_{n+1-i}^*)^d &= \frac{(\lambda_1 \ldots \lambda_n)^d (\lambda_1^* \ldots \lambda_n^*)^d}{\prod_{\substack{k=1 \\ k \neq i}}^{n} (\lambda_k \lambda_{n+1-k}^*)^d} \\ &\leq n^{(n-1)d}. \end{aligned}$$

This proves the lemma. □

Corollary 5.4. *The first successive minimum of* Π *and the covering radius of* Π^* *satisfy*

$$\mu(\Pi) \lambda_1(\Pi^*) \leq \nu(K) n^n.$$

Proof. This follows directly from Theorem 5.2 and Theorem 5.3. □

Using this corollary we derive an adèlic version of Kronecker's Theorem in a way very similar to the proof of the effective version of the classical form of Kronecker's Theorem (Theorem 1.8). First we introduce some new notation to state the theorem more efficiently.

Let P be a finite set of places in M_K. We denote $\mathbb{A}_{K,P}^n = \prod_{v \in P} K_v^n$. A matrix $A \in \mathbb{A}_{K,P}^{m,n}$ may be represented as a tuple $(A_v)_{v \in P}$ with $A_v \in K_v^{m,n}$.

Theorem 5.5. *Let P be a finite set of places of a number field K and let $A \in \mathbb{A}_{K,P}^{m,n}$. Suppose*

$$\{\mathbf{z} \in K^m : \exists\, \mathbf{w} \in K^n \text{ such that } A_v^T \mathbf{z} = \mathbf{w} \text{ for all } v \in P\} = \{\mathbf{0}\}. \tag{5.3}$$

Then for every $\varepsilon > 0$, $(\mathbf{b}_v) \in \mathbb{A}_{K,P}^n$ there exist vectors $\mathbf{x} \in K^m$, $\mathbf{y} \in K^n$ such that

$$\begin{aligned} \|A_v\mathbf{x} - \mathbf{y} - \mathbf{b}_v\|_v \le \varepsilon \qquad & \text{for all } v \in P, \\ \|\mathbf{x}\|_v \le 1,\ \|\mathbf{y}\|_v \le 1 \qquad & \text{for all } v \in M_K \setminus P. \end{aligned}$$

Proof. Let $\varepsilon > 0$, $(\mathbf{b}_v) \in \mathbb{A}_K^n$. Define

$$\tau := \nu(K)(m+n)^{m+n}.$$

The set

$$V := \left\{ \mathbf{k} \in K^{m+n} : \begin{array}{cc} \|\mathbf{k}\|_v \le \tau^{c(v)}\frac{1}{\varepsilon} + \|A_v\|_v \tau^{c(v)}\frac{1}{\varepsilon} & \text{for all } v \in P, \\ \|\mathbf{k}\|_v \le 1 & \text{for all } v \in M_K \setminus P \end{array} \right\}$$

is finite by Lemma 4.4. Define for every $v \in P$ the set

$$V_v := \{\mathbf{k} \in V : (A_v^T \ \ I_n)\mathbf{k} \neq \mathbf{0}\}.$$

Note that $V \setminus \{\mathbf{0}\} = \cup_{v \in P} V_v$ by (5.3).

By the Strong Approximation Theorem there exist $\kappa \in K$ such that $|\kappa|_v \le \varepsilon$ for all $v \in P$ and $Q \in K$ such that

$$|Q|_v > \begin{cases} 1 & \text{for } v \in P \text{ with } V_v \text{ empty}, \\ \min\limits_{\mathbf{k} \in V_v} \dfrac{\tau^{c(v)}}{\|(A_v^T \ \ I_n)\,\mathbf{k}\|_v} & \text{for } v \in P \text{ with } V_v \text{ non-empty}. \end{cases}$$

Define $B \in \mathrm{GL}_{m+n}(\mathbb{A}_K)$ by

$$\begin{aligned} B_v &= \begin{pmatrix} \kappa^{-1} I_m & -\kappa^{-1} A_v \\ 0 & Q^{-1} I_n \end{pmatrix} \quad \text{for all } v \in P, \\ B_v &= I \quad \text{for all } v \in M_K \setminus P. \end{aligned}$$

We have

$$(B_v^{-1})^T = \begin{pmatrix} \kappa I_m & 0 \\ Q A_v^T & Q I_n \end{pmatrix} \quad \text{for all } v \in P.$$

Define

$$\Pi := \{(\mathbf{a}_v) \in \mathbb{A}_K^{m+n} : \|B_v \mathbf{a}_v\|_v \le 1 \text{ for all } v \in M_K\}.$$

Its reciprocal Π^* is given by

$$\Pi^* = \{(\mathbf{a}_v) \in \mathbb{A}_K^{m+n} : \|(B_v^{-1})^T \mathbf{a}_v\|_v \leq 1 \text{ for all } v \in M_K\}.$$

Suppose there exists a $\mathbf{k} \in K^{m+n}$ with $\mathbf{k} \in \tau\Pi$, then $\mathbf{k} \in V$. Hence, $\mathbf{k} = \mathbf{0}$ or

$$\|B_v^T \mathbf{k}\| \geq \|Q(A_v^T \quad I_n)\, \mathbf{k}\|_v \geq \tau^{c(v)}$$

for at least one $v \in P$. We conclude that

$$\lambda_1(\Pi^*) > \tau = \nu(K)(m+n)^{m+n}.$$

So, by Corollary 5.4 we get $\mu(\Pi) \leq 1$. This implies that for all $(\mathbf{b}'_v) \in \mathbb{A}_K^n$ there exist $\mathbf{x} \in K^m$, $\mathbf{y} \in K^n$ such that

$$\begin{aligned} \left\| B_v \begin{pmatrix} \mathbf{y} \\ \mathbf{x} \end{pmatrix} + \begin{pmatrix} \mathbf{b}'_v \\ \mathbf{0} \end{pmatrix} \right\|_v \leq 1 \qquad & \text{for all } v \in P, \\ \left\| I_v \begin{pmatrix} \mathbf{y} \\ \mathbf{x} \end{pmatrix} \right\|_v \leq 1 \qquad & \text{for all } v \in M_K \setminus P. \end{aligned}$$

Take $(\mathbf{b}'_v) = (\kappa^{-1}\mathbf{b}_v)$. We conclude that there exist $\mathbf{x} \in K^m$, $\mathbf{y} \in K^n$ such that

$$\begin{aligned} \|A_v\mathbf{x} - \mathbf{y} + \mathbf{b}_v\|_v \leq \varepsilon \qquad & \text{for all } v \in P, \\ \|\mathbf{x}\|_v \leq 1,\ \|\mathbf{y}\|_v \leq 1 \qquad & \text{for all } v \in M_K \setminus P. \end{aligned}$$

This proves the theorem. □

In this Kronecker's Theorem for adèle spaces we demanded that

$$\{\mathbf{z} \in K^m : \exists\, \mathbf{w} \in K^n \text{ such that } A_v^T \mathbf{z} = \mathbf{w} \text{ for all } v \in P\} = \{\mathbf{0}\}.$$

In the next lemma and theorem we prove that this condition is necessary for the adelic Kronecker's Theorem. We need the following auxiliary result.

Lemma 5.6. *Let P be a finite set of places of K. The condition*

$$\{\mathbf{z} \in K^m : \exists\, \mathbf{w} \in K^n \textit{ such that } A_v^T \mathbf{z} = \mathbf{w} \textit{ for all } v \in P\} = \{\mathbf{0}\} \tag{5.4}$$

is equivalent to

$$\{\mathbf{z} \in \mathcal{O}_K^m : \exists\, \mathbf{w} \in \mathcal{O}_K^n \textit{ such that } A_v^T \mathbf{z} = \mathbf{w} \textit{ for all } v \in P\} = \{\mathbf{0}\}. \tag{5.5}$$

Proof. Suppose there exist $\mathbf{z} \in K^m$, $\mathbf{w} \in K^n$ with $\mathbf{z} \neq 0$ and $A_v^T\mathbf{z} = \mathbf{w}$ for all $v \in P$. There exists $\kappa \in K^*$ such that $\kappa \leq \max\{\|\mathbf{z}\|_v, \|\mathbf{w}\|_v\}^{-1}$ for all $v \in M_K^{\text{fin}}$ by the Strong Approximation Theorem 4.5. Note that $\kappa\mathbf{z} \in \mathcal{O}_K^m$, $\kappa\mathbf{w} \in \mathcal{O}_K^n$ with $\mathbf{z} \neq 0$ and $A_v^T\kappa\mathbf{z} = \kappa\mathbf{w}$.

Further,

$$\{\mathbf{z} \in \mathcal{O}_K^m : \exists\, \mathbf{w} \in \mathcal{O}_K^n \text{ such that } A_v^T\mathbf{z} = \mathbf{w} \text{ for all } v \in P\} \subseteq$$
$$\{\mathbf{z} \in K^m : \exists\, \mathbf{w} \in K^n \text{ such that } A_v^T\mathbf{z} = \mathbf{w} \text{ for all } v \in P\} = \{\mathbf{0}\}.$$

Hence, (5.4) implies (5.5). The converse can be proved in a similar manner. □

Theorem 5.7. *Let K be a number field and let $d = [K : \mathbb{Q}]$. If for every $\varepsilon > 0$, $(\mathbf{b}_v) \in \mathbb{A}_{K,P}^n$ there exist vectors $\mathbf{x} \in K^m$, $\mathbf{y} \in K^n$ such that*

$$\begin{aligned} \|A_v\mathbf{x} - \mathbf{y} - \mathbf{b}_v\|_v \leq \varepsilon \qquad & \text{for all } v \in P, \\ \|\mathbf{x}\|_v \leq 1,\ \|\mathbf{y}\|_v \leq 1 \qquad & \text{for all } v \in M_K \setminus P, \end{aligned}$$

then condition (5.5) is satisfied.

Proof. This proof is by contradiction. Suppose there exist $\mathbf{z} \in \mathcal{O}_K^m$, $\mathbf{w} \in \mathcal{O}_K^n$ such that $\mathbf{z} \neq 0$ and $A_v^T\mathbf{z} = \mathbf{w}$ for all $v \in P$. Then

$$\mathbf{z}^T(A_v\mathbf{x} - \mathbf{y} - \mathbf{b}_v) = \mathbf{z}^TA_v\mathbf{x} - \mathbf{z}^T\mathbf{y} - \mathbf{z}^T\mathbf{b}_v = \mathbf{w}^T\mathbf{x} - \mathbf{z}^T\mathbf{y} - \mathbf{z}^T\mathbf{b}_v.$$

Choose $(\mathbf{b}_v) \in \mathbb{A}_{K,P}^n$ such that $0 < |\mathbf{z}^T\mathbf{b}_v|_v < (\frac{1}{2})^{d+1}$ for all $v \in P$ and choose $\varepsilon > 0$ such that $\varepsilon < m^{-c(v)}\|\mathbf{z}\|_v^{-1}|\mathbf{z}^T\mathbf{b}_v|_v$ for all $v \in P$. There exist $\mathbf{x} \in K^m$, $\mathbf{y} \in K^n$ such that

$$\begin{aligned} \|A_v\mathbf{x} - \mathbf{y} - \mathbf{b}_v\|_v \leq \varepsilon \qquad & \text{for all } v \in P, \\ \|\mathbf{x}\|_v \leq 1,\ \|\mathbf{y}\|_v \leq 1 \qquad & \text{for all } v \in M_K/\, P. \end{aligned}$$

Then

$$|\mathbf{x}^T\mathbf{w} - \mathbf{y}^T\mathbf{z} - \mathbf{z}^T\mathbf{b}_v|_v \leq \varepsilon m^{c(v)}\|\mathbf{z}\|_v < |\mathbf{z}^T\mathbf{b}_v|_v \qquad \text{for all } v \in P. \tag{5.6}$$

Hence,

$$\begin{aligned} |\mathbf{x}^T\mathbf{w} - \mathbf{y}^T\mathbf{z}|_v \leq |\mathbf{z}^T\mathbf{b}_v|_v + \varepsilon m^{c(v)}\|\mathbf{z}\|_v < (\tfrac{1}{2})^d \qquad & \text{for all } v \in P, \\ |\mathbf{x}^T\mathbf{w} - \mathbf{y}^T\mathbf{z}|_v \leq 2^{c(v)} \qquad & \text{for all } v \in M_K/\, P. \end{aligned}$$

Here we used that $\|\mathbf{x}\|_v \leq 1$, $\|\mathbf{y}\|_v \leq 1$ for $v \in M_K/\, P$ and that $\mathbf{z} \in \mathcal{O}_K^m$, $\mathbf{w} \in \mathcal{O}_K^n$. We conclude that

$$\prod_{v \in M_K} |\mathbf{x}^T\mathbf{w} - \mathbf{y}^T\mathbf{z}|_v < 1.$$

Since $\mathbf{x}^T\mathbf{w} - \mathbf{y}^T\mathbf{z} \in K$ we have $\mathbf{x}^T\mathbf{w} - \mathbf{y}^T\mathbf{z} = \mathbf{0}$ by the product formula. We conclude that

$$|\mathbf{x}^T\mathbf{w} - \mathbf{z}^T\mathbf{y} - \mathbf{z}^T\mathbf{b}_v|_v = |\mathbf{z}^T\mathbf{b}_v|_v \quad \text{for all } v \in P.$$

This contradicts with inequality (5.6), which proves the theorem. □

5.2 An effective adèlic Kronecker's Theorem

In this section we prove an effective version of the adèlic Kronecker's Theorem. We need the following proposition to calculate a lower bound.

Proposition 5.8. *Let K be a number field, let $v \in M_K$, and let $\alpha_1, \ldots, \alpha_n \in K_v$ be algebraic over K, H the absolute height. Define $L := K(\alpha_1, \ldots, \alpha_n)$ and $d := [L : \mathbb{Q}]$. Then we have*

$$|q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n|_v \geq H(1, \alpha_1, \ldots, \alpha_n)^{-d}(n+1)^{-d}H(\mathbf{q})^{-d}\|\mathbf{q}\|_v$$

for every $\mathbf{q} \in K^{n+1}$ for which $q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n \neq 0$.

The place v of K gives rise to a place of L as $L \subset K_v$, which we denote by v again. The standard representatives for these places are equal on K as $K_v = L_v$.

Proof. Using the product formula, Theorem 2.28, we find that

$$\begin{aligned} |q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n|_v &= \prod_{\substack{w \in M_L \\ w \neq v}} |q_0 + q_1\alpha_1 + \cdots + q_n\alpha_n|_w^{-1} \\ &\geq \prod_{\substack{w \in M_L \\ w \neq v}} (n+1)^{-1} \max\{1, |\alpha_1|_w, \ldots, |\alpha_n|_w\}^{-1}\|\mathbf{q}\|_w^{-1} \\ &\geq H(1, \alpha_1, \ldots, \alpha_n)^{-d}(n+1)^{-d}H(\mathbf{q})^{-d}\|\mathbf{q}\|_v. \end{aligned}$$

This proves the proposition. □

Let K be a number field. Let $A \in K_v^{m,n}$ be a matrix given by

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}$$

with elements α_{ij} algebraic over K. Define

$$d_j := [K(\alpha_{1j}, \ldots, \alpha_{1n}) : \mathbb{Q}] \ \ (j = 1, \ldots, n) \quad d := d(A) := \max(d_1, \ldots, d_n).$$

We define the height of A with respect to K by

$$H_K^*(A) = (n+1)^d \max_{j=1,\ldots,n} H(1, \alpha_{1j}, \ldots, \alpha_{mj})^d.$$

This notation is not standard.

Theorem 5.9. *Let K be a number field, P a finite set of places of K and put $d := [K : \mathbb{Q}]$, $t := \#P$. Further, let $A \in \mathbb{A}_{K,P}^{m,n}$. Suppose*

$$\{\mathbf{z} \in K^m : \exists\, \mathbf{w} \in K^n \text{ such that } A_v^T \mathbf{z} = \mathbf{w} \text{ for all } v \in P\} = \{\mathbf{0}\}. \tag{5.7}$$

For every $\varepsilon > 0$ and for every $v \in P$ define

$$Q_v(\varepsilon) := \tau^d H_K^*(A_v) \left(\prod_{w \in P} \|B_w^T\|_w \right)^{-d(A_v)} \|B_v\|_v \left(\frac{1}{\varepsilon} \right)^{t \cdot d(A_v) - 1}.$$

Then for every $\varepsilon > 0$, $(\mathbf{b}_v) \in \mathbb{A}_K^n$, there exist vectors $\mathbf{x} \in K^n$, $\mathbf{y} \in K^m$, such that

$$\begin{aligned} \|A_v \mathbf{x} - \mathbf{y} - \mathbf{b}_v\|_v \le \varepsilon, \ \|\mathbf{x}\|_v \le Q_v(\varepsilon) \quad & \text{for all } v \in P, \\ \|\mathbf{x}\|_v \le 1, \ \|\mathbf{y}\|_v \le 1 \quad & \text{for all } v \in M_K \setminus P. \end{aligned}$$

Proof. Let $\varepsilon > 0$. Denote $Q_v(\varepsilon)$ by Q_v. Define

$$|\varepsilon_v|_v = \max_{\kappa \in K_v : |\kappa|_v \le \varepsilon} |\kappa|_v \quad \text{for all } v \in P.$$

Let $B \in \mathrm{GL}(m+n, \mathbb{A}_K)$ be the linear transformation of $\mathbb{A}_K^{m+n}$ given by

$$\begin{aligned} B_v &= \begin{pmatrix} \varepsilon_v^{-1} I_m & -\varepsilon_v^{-1} A_v \\ 0 & Q_v^{-1} I_n \end{pmatrix} \quad \text{for all } v \in P, \\ B_v &= I \quad \text{for all } v \in M_K \setminus P. \end{aligned}$$

We define a parallelepiped Π given by

$$\Pi = \{(\mathbf{a}_v) \in \mathbb{A}_K^{m+n} : \|B_v \mathbf{a}_v\|_v \leq 1 \text{ for all } v \in M_K\}.$$

Its reciprocal Π^* is given by

$$\Pi^* = \{(\mathbf{a}_v) \in \mathbb{A}_K^{m+n} : \|(B_v^{-1})^T \mathbf{a}_v\|_v \leq 1 \text{ for all } v \in M_K\}.$$

Note that $(B_v^{-1})^T$ is given by

$$\begin{aligned} (B_v^{-1})^T &= \begin{pmatrix} \varepsilon_v I_m & 0 \\ Q_v A_v^T & Q_v I_n \end{pmatrix} \quad \text{for all } v \in P, \\ (B_v^{-1})^T &= I \quad \text{for all } v \in M_K \setminus P. \end{aligned}$$

Define again $\tau := \nu(K)(m+n)^{m+n}$. Let $\mathbf{k} \in K^{m+n} \setminus \{\mathbf{0}\}$. Suppose that $\phi(\mathbf{k}) \in \tau\Pi^*$, then we have $\|(B_v^T)^{-1}\mathbf{k}\|_v \leq \tau^{c(v)}$ for every $v \in M_K$. We can rewrite this as $\|\mathbf{k}\|_v \leq \|(B_v^T)\|_v \tau^{c(v)}$. Condition (5.7) gives that $(A_v^T \ I_n)\mathbf{k} \neq \mathbf{0}$ for at least one $v \in P$. By proposition 5.8 we get

$$\begin{aligned} \|(A_v^T \ I_n)\mathbf{k}\|_v &\geq H_K^*(A_v)^{-1} \left(\prod_{w \in M_K} \|\mathbf{k}\|_w \right)^{-d(A_v)} \|\mathbf{k}\|_v \\ &\geq H_K^*(A_v)^{-1} \tau^{-d} \left(\prod_{w \in P} \|B_w^T\|_w \right)^{-d(A_v)} \|B_v\|_v \tau^{c(v)} \varepsilon^{1-t \cdot d(A_v)}. \end{aligned}$$

Hence,

$$\|(B_v^T)^{-1}\mathbf{k}\|_v \geq \|Q_v(A_v^T \ I_n)\mathbf{k}\|_v \geq \tau^{c(v)}.$$

It follows that $\lambda_1(\Pi^*) \geq \tau$. We conclude in the same way as in the proof of the non-effective version of this theorem that $\mu(\Pi) \leq 1$. This proves the theorem. $\square$

5.3 A more general adèlic Kronecker's Theorem

In this section we prove a more general form of an adèlic Kronecker's Theorem as in Section 1.4. First we introduce some new notation. Let $A = (A_v) \in \mathbb{A}_{K,P}^{r,s}$, $U = (U_v) \in \mathbb{A}_{K,P}^{q,r}$ and $V \in K^{s,t}$. The product $\tilde{A} = UA$ is given by $\tilde{A}_v = U_v A_v$ and the product $\hat{A} = AV$ is given by $\hat{A} = A_v V$.

Let P be a finite set of places of a number field K containing M_K^∞. Define

$$\mathcal{O}_P = \{x \in K : |x|_v \leq 1 \text{ for all } v \in M_K \setminus P\}.$$

This is a ring called the *ring of P-integers* of K. We need the following theorem.

Theorem 5.10. *Let P be a finite set of places of a number field K containing M_K^∞ such that $\mathcal{O}_P$ is a principal ideal domain, let $A = (A_v) \in \mathbb{A}_{K,P}^{r,s}$, $m \in \mathbb{Z}_{\geq 0}$ such that $\operatorname{rank}(A_v) = m$ for all $v \in P$, and let $(\mathbf{b}_v) \in \mathbb{A}_{K,P}^r$. Then the following two assertions are equivalent.*

(i) For every $\varepsilon > 0$ there exists an $\mathbf{x} \in \mathcal{O}_P^s$ such that

$$\|A_v\mathbf{x} - \mathbf{b}_v\|_v \leq \varepsilon \qquad \text{for all } v \in P.$$

(ii)

$$\{(\mathbf{z}_v) \in \mathbb{A}_{K,P}^r : \exists\ \mathbf{w} \in \mathcal{O}_P^s \text{ such that } A_v^T\mathbf{z}_v = \mathbf{w} \text{ for all } v \in P\} \subseteq \{(\mathbf{z}_v) \in \mathbb{A}_{K,P}^r : \exists\ \omega \in \mathcal{O}_P \text{ such that } \mathbf{b}_v^T\mathbf{z}_v = \omega \text{ for all } v \in P\}.$$

In the proof of this theorem we need some lemmas, in which we refer repeatedly to *(i)* and *(ii)*. We follow the steps of the proof in Section 1.4 as much as possible.

Lemma 5.11. *Let $U = (U_v) \in \mathrm{GL}_r(\mathbb{A}_{K,P})$, $V = (V_v) \in \mathrm{GL}_s(\mathcal{O}_P)$. Put $\tilde{A} = (\tilde{A}_v) := UAV$ and define $(\tilde{\mathbf{b}}_v)$ by $\tilde{\mathbf{b}}_v := U_v\mathbf{b}_v$ for all $v \in P$. Then (i) is equivalent to the assertion that for every $\varepsilon > 0$ there exists $\mathbf{x} \in \mathcal{O}_P^s$ such that*

$$\|\tilde{A}_v\mathbf{x} - \tilde{\mathbf{b}}_v\|_v \leq \varepsilon \quad \text{for all } v \in P.$$

Proof. Suppose A and $(\mathbf{b}_v)$ satisfy assertion *(i)*. For every $\varepsilon > 0$ there exists $\mathbf{x} \in \mathcal{O}_P^s$ such that

$$\|A_v\mathbf{x} - \mathbf{b}_v\|_v \leq \varepsilon \qquad \text{for all } v \in P.$$

Define $\tilde{\mathbf{x}} := V^{-1}\mathbf{x}$. Using that $\|U_vA_vV\tilde{\mathbf{x}} - U_v\mathbf{b}_v\|_v = \|U_v(A_v\mathbf{x} - \mathbf{b}_v)\|_v$ we get

$$\begin{aligned} \|U_vA_v\tilde{\mathbf{x}} - U_v\mathbf{b}_v\|_v \leq \|U_v\|_v\varepsilon \qquad & \text{for all } v \in P, \\ \|\tilde{\mathbf{x}}\|_v = \|V^{-1}\mathbf{x}\|_v \leq \|V^{-1}\|_v\|\mathbf{x}\|_v \leq 1 \qquad & \text{for all } v \in M_K \setminus P. \end{aligned}$$

This proves the lemma. □

Lemma 5.12. *Let $U = (U_v) \in \mathrm{GL}_r(\mathbb{A}_{K,P})$, $V = (V_v) \in \mathrm{GL}_s(\mathcal{O}_P)$. Put $\tilde{A} = (\tilde{A}_v) := UAV$, and define $(\tilde{\mathbf{b}}_v)$ by $\tilde{\mathbf{b}}_v := U_v\mathbf{b}_v$ for all $v \in P$. Then (ii) is equivalent to the assertion that*

$$\{(\mathbf{z}_v) \in \mathbb{A}_{K,P}^r : \exists\ \mathbf{w} \in \mathcal{O}_P^s \text{ such that } \tilde{A}_v^T\mathbf{z}_v = \mathbf{w} \text{ for all } v \in P\} \subseteq \{(\mathbf{z}_v) \in \mathbb{A}_{K,P}^r : \exists\ \omega \in \mathcal{O}_P \text{ such that } \tilde{\mathbf{b}}_v^T\mathbf{z}_v = \omega \text{ for all } v \in P\}.$$

Proof. Suppose there exist $(\mathbf{z}_v) \in \mathbb{A}_K^r$, $\mathbf{w} \in \mathcal{O}_P^s$ such that $V^T A_v^T (U_v^T \mathbf{z}_v) = \mathbf{w}$ for all $v \in P$ then we have $A_v^T (U_v^T \mathbf{z}_v) = (V^T)^{-1}\mathbf{w} \in \mathcal{O}_P^s$ for all $v \in P$. By assertion*(ii)* there exists an $\omega \in \mathcal{O}_P$ such that $\mathbf{b}_v^T U_v^T \mathbf{z}_v = \omega$ for all $v \in P$. We conclude that

$$\{(\mathbf{z}_v) \in \mathbb{A}_{K,P}^r : \exists\ \mathbf{w} \in \mathcal{O}_P^s \text{ such that } \tilde{A}_v^T \mathbf{z}_v = \mathbf{w} \text{ for all } v \in P\} \subseteq$$
$$\{(\mathbf{z}_v) \in \mathbb{A}_{K,P}^r : \exists\ \omega \in \mathcal{O}_P \text{ such that } \tilde{\mathbf{b}}_v^T \mathbf{z}_v = \omega \text{ for all } v \in P\}.$$

This proves the lemma. □

Lemma 5.13. *There exist $U = (U_v) \in \mathrm{GL}_r(\mathbb{A}_{K,P})$, $V = (V_v) \in \mathrm{GL}_s(\mathcal{O}_P)$ such that*

$$U_v A_v V_v = \begin{pmatrix} I_m & -A'_v \\ 0 & 0 \end{pmatrix} \quad \textit{for all } v \in P, \tag{5.8}$$

where $A' = (A'_v) \in \mathbb{A}_{K,P}^{m,s-m}$.

Proof. This proof is by induction on k. Let $0 \le k \le m$. Our induction hypothesis is that there exist $U \in \mathrm{GL}_r(\mathbb{A}_{K,P})$, $V \in \mathrm{GL}_s(\mathcal{O}_K)$ such that

$$U_v A_v V_v = \begin{pmatrix} I_k & A'_v \\ 0 & A''_v \end{pmatrix} \quad \text{with } A'_v \in K_v^{k,s-k},\ A''_v \in K_v^{s-k,s-k} \text{ for all } v \in P.$$

This is trivial for $k = 0$. Assume that this induction hypothesis is true for some k with $0 \le k < m$. Note that $A''_v \neq 0$ for all $v \in P$. It is easy to find $\mathbf{v} = (v_1, \ldots, v_{s-k}) \in \mathcal{O}_K^{s-k}$, such that $v_1 = 1$ and $A''_v \mathbf{v} \neq \mathbf{0}$ for all $v \in P$. Let $\mathbf{e}_1, \ldots, \mathbf{e}_{s-k}$ be the unit vectors in K^{s-k}. Define $V'_k = [\mathbf{v}, \mathbf{e}_2 \ldots, \mathbf{e}_{s-k}]$. Note that $V'_k \in \mathcal{O}_K^{s-k}$. Define

$$V_k := \begin{pmatrix} I_k & 0 \\ 0 & V'_k \end{pmatrix}.$$

Note that $V_k \in \mathrm{GL}(s, K)$ and that $\|V_k\|_v \le 1$ for all $v \in M_K \setminus P$. Now, define $\hat{A} = (\hat{A}_v) = UAVV_k$. We have

$$\hat{A}_v = \begin{pmatrix} I_k & \hat{A}'_v \\ 0 & \hat{A}''_v \end{pmatrix} \quad \text{for all } v \in P,$$

where the first column of $\hat{A}''_v$, which is $\tilde{A}''_v \mathbf{v}_1$, is not equal to $\mathbf{0}$ for all $v \in P$. Using Gaussian elimination we can find an $U_k \in \mathrm{GL}_r(\mathbb{A}_{K,P})$ with $U_k \hat{A} = U_k UAVV_k$ in the desired shape for $k+1$. This proves the proposition. □

Lemma 5.14. *Assume (ii) holds. Then there exist* $U \in \mathrm{GL}_r(\mathbb{A}_{K,P}), V \in \mathrm{GL}_s(\mathcal{O}_P)$ *such that*

$$UAV = \begin{pmatrix} I_t & 0 & -A_1 \\ 0 & I_{m-t} & -A_2 \\ 0 & 0 & 0 \end{pmatrix}, \quad U\mathbf{b}_v = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2^{(v)} \\ \mathbf{0} \end{pmatrix} \text{ for all } v \in P,$$

where $0 \le t \le m \le r$, $A_1 \in K^{t,s-m}, A_2 = (A_2^{(v)}) \in \mathbb{A}_K^{m-t,s-m}$, $\mathbf{b}_1 \in K^t, (\mathbf{b}_2^{(v)}) \in \mathbb{A}_K^{m-t}$, *and*

$$\{\mathbf{z}_1 \in \mathcal{O}_P^t : A_1^T\mathbf{z}_1 \in \mathcal{O}_P^{s-m}\} \subseteq \{\mathbf{z}_1 \in \mathcal{O}_P^t : \mathbf{b}_1^T\mathbf{z}_1 \in \mathcal{O}_P\},$$
$$\{(\mathbf{z}_v) \in \mathcal{O}_P^{m-t} : \exists\ \mathbf{w} \in \mathcal{O}_P^{s-m} \text{ such that } A_2^{(v)T}\mathbf{z}_v = \mathbf{w} \text{ for all } v \in P\} = \{\mathbf{0}\}.$$

Proof. By Lemma 5.13 there exist $U_1 = U_1^{(v)} \in \mathrm{GL}_r(\mathbb{A}_K)$, $V_1 \in \mathrm{GL}_s(\mathcal{O}_P)$ such that

$$U_1AV_1 = \begin{pmatrix} I_m & -A' \\ 0 & 0 \end{pmatrix} \quad \text{with } A' \in \mathbb{A}_K^{m,s-m}.$$

By Lemmas 5.11 and 5.12, the validity of *(ii)* is unaffected if we replace A by U_1AV_1. Define $(\mathbf{b}'_v)$ by $U_v^{(1)}\mathbf{b}_v = (\mathbf{b}'_v, \mathbf{0})^T$ for all $v \in P$. Thus, assertion *(ii)* becomes

$$\begin{aligned} &\{(\mathbf{z}'_v) \in \mathcal{O}_P^m : \exists\ \mathbf{w} \in \mathcal{O}_P^{s-m} \text{ such that } A_v'^T\mathbf{z}'_v = \mathbf{w} \text{ for all } v \in P\} \subseteq \\ &\quad \{(\mathbf{z}'_v) \in \mathcal{O}_P^m : \exists\ \omega \in \mathcal{O}_P \text{ such that } \mathbf{b}_v'^T\mathbf{z}'_v = \omega \text{ for all } v \in P\} \end{aligned} \tag{5.9}$$

in the same way as in the proof of Theorem 1.12. The left-hand side is a sub-$\mathcal{O}_P$-module M of $\mathcal{O}_P^{s-m}$, hence free of rank $t \le m$. If $t = 0$ we are done. Suppose $t > 0$. Then by Theorem 1.11 there is a basis $\{\mathbf{d}_1, \dots, \mathbf{d}_m\}$ of $\mathcal{O}_P^m$ and there are $\delta_1, \dots, \delta_t \in \mathcal{O}_P$, such that $\{\delta_1\mathbf{d}_1, \dots, \delta_t\mathbf{d}_t\}$ is a $\mathcal{O}_P$-basis of M.

Now, let $D := [\mathbf{d}_1, \dots, \mathbf{d}_m]$ be the matrix with columns $\mathbf{d}_1, \dots, \mathbf{d}_m$. Then $D \in \mathrm{GL}_m(\mathcal{O}_P)$. Define $\hat{A} := D^TA'$, $\hat{\mathbf{b}} := D^T\mathbf{b}'$. Then

$$\begin{pmatrix} D^T & 0 \\ 0 & I_{r-t} \end{pmatrix} \begin{pmatrix} I_m & -A' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} (D^T)^{-1} & 0 \\ 0 & I_{s-m} \end{pmatrix} = \begin{pmatrix} I_m & -\hat{A} \\ 0 & 0 \end{pmatrix}. \tag{5.10}$$

The right-hand side is clearly of the shape UAV with $U \in \mathrm{GL}_r(\mathbb{A}_K), V \in \mathrm{GL}_s(\mathcal{O}_P)$. Writing $\hat{\mathbf{z}}_v := D^{-1}\mathbf{z}'_v$ for all $v \in P$ we see that (5.9) is equivalent to

$$\begin{aligned} &\{(\hat{\mathbf{z}}_v) \in \mathcal{O}_P^m : \exists\ \mathbf{w} \in \mathcal{O}_P^{s-m} \text{ such that } \hat{A}_v^T\hat{\mathbf{z}}_v = \mathbf{w} \text{ for all } v \in P\} \subseteq \\ &\quad \{(\hat{\mathbf{z}}_v) \in \mathcal{O}_P^m : \exists\ \omega \in \mathcal{O}_P \text{ such that } \hat{\mathbf{b}}_v^T\hat{\mathbf{z}}_v = \omega \text{ for all } v \in P\}. \end{aligned} \tag{5.11}$$

Let $A_1 = (A_1^{(v)}) \in \mathbb{A}_{K,P}^{t,n}$ and $A_2 = (A_2^{(v)})\mathbb{A}_{K,P}^{m-t,n}$ be defined by $A_1^{(v)}$ and $A_2^{(v)}$, which consist respectively of the first t rows and the last $m-t$ rows of $\hat{A}_v$ for all $v \in P$. Let $\mathbf{b}_1^{(v)} = (b_1^{(v)}, \dots, b_t^{(v)})$, $\mathbf{b}_2^{(v)} = (b_{t+1}^{(v)}, \dots, b_m^{(v)})$ be defined by $\mathbf{b}_1^{(v)}$ and $\mathbf{b}_2^{(v)}$, which consist of respectively the first t and the last $m-t$ coordinates of $\hat{\mathbf{b}}$. Notice that the left-hand side of (5.11) consists of all vectors of the shape $(\delta_1 z_1, \dots, \delta_r z_t, 0, \dots, 0)^T$ with $z_1, \dots, z_t \in \mathcal{O}_P$ for all $v \in P$. We have $A_v(\delta_1 z_1, \dots, \delta_r z_t, 0, \dots, 0) = \mathbf{w} \in \mathcal{O}_P^{s-m}$ and $\mathbf{b}_1^{(v)T}(\delta_1 z_1, \dots, \delta_r z_t, 0, \dots, 0) = \omega \in \mathcal{O}_P$ for all $v \in P$ and all $z_1, \dots, z_t \in \mathcal{O}_P$. Hence, $A_1 \in K^{t,s-m}$, $\mathbf{b}_1 = (\mathbf{b}_1^{(v)}) \in K^t$, and

$$\{\mathbf{z}_1 \in \mathcal{O}_P^t : A_1^T \mathbf{z}_1 \in \mathcal{O}_P^{s-m}\} \subseteq \{\mathbf{z}_1 \in \mathcal{O}_P^t : \mathbf{b}_1^T \mathbf{z}_1 \in \mathcal{O}_P\}.$$

Further, by applying (5.11) with vectors $(0, \dots, 0, z_{t+1}, \dots, z_m)^T$, we see that

$$\{(\mathbf{z}_v) \in \mathcal{O}_P^{m-t} : \exists\ \mathbf{w} \in \mathcal{O}_P^{s-m} \text{ such that } A_2^{(v)T} \mathbf{z}_v = \mathbf{w} \text{ for all } v \in P\} = \{\mathbf{0}\}.$$

This proves the lemma. □

Proof of Theorem 5.10. First we prove *(i)* ⇒ *(ii)*. This proof is by contradiction. Assume *(ii)* does not hold. Suppose there exist $(\mathbf{z}_v) \in \mathbb{A}_K^r$, $\mathbf{w} \in \mathcal{O}_P^s$ such that $A_v^T \mathbf{z}_v = \mathbf{w}$ for all $v \in P$ and there does not exist $\omega \in \mathcal{O}_P$ such that $\mathbf{b}_v^T \mathbf{z}_v = \omega$ for all $v \in P$.

Let $\varepsilon > 0$. Define

$$\mathcal{C} := \prod_{v \in M_K} \mathcal{C}_v,$$

where

$$\begin{aligned} \mathcal{C}_v &:= \{x \in K_v : |x|_v \le |\mathbf{b}_v^T \mathbf{z}_v|_v + \varepsilon r^{c(v)}\} \qquad \text{for all } v \in P, \\ \mathcal{C}_v &:= \{x \in K_v : |x|_v \le r^{c(v)} \|\mathbf{w}\|_v\} \qquad \text{for all } v \in M_K \setminus P. \end{aligned}$$

This convex set contains only finitely many points of $\phi(K)$ by Corollary 4.4. Hence, there are only finitely many $\kappa \in \mathcal{O}_P$ such that

$$\begin{aligned} |\kappa - \mathbf{b}_v^T \mathbf{z}_v|_v &\le \varepsilon r^{c(v)} \qquad \text{for all } v \in P, \\ |\kappa|_v &\le r^{c(v)} \|\mathbf{w}\|_v \qquad \text{for all } v \in M_K \setminus P. \end{aligned}$$

For each of these κ we have $\kappa - \mathbf{b}_v^T \mathbf{z}_v \neq 0$ for at least one $v \in P$, because there does not exist a $\omega \in \mathcal{O}_P$ such $\mathbf{b}_v^T \mathbf{z}_v = \omega$ for all $v \in P$. Hence, we can find an $\varepsilon > 0$ such that there does not exist κ satisfying these inequalities.

Hence, there does not exist $\mathbf{x} \in \mathcal{O}_P^s$, such that

$$\begin{aligned} |\mathbf{x}^T \mathbf{w} - \mathbf{b}_v^T \mathbf{z}_v|_v &\le \varepsilon r^{c(v)} \qquad \text{for all } v \in P, \\ |\mathbf{x}^T \mathbf{w}|_v &\le r^{c(v)} \|\mathbf{w}\|_v \qquad \text{for all } v \in M_K \setminus P. \end{aligned}$$

Using that $(A_v\mathbf{x}-\mathbf{b}_v)^T\mathbf{z}_v = \mathbf{x}^T\mathbf{w}-\mathbf{b}_v^T\mathbf{z}_v$, we conclude that there is no $\mathbf{x}\in\mathcal{O}_P^s$, such that

$$\begin{aligned}\|A_v\mathbf{x}-\mathbf{b}_v\|_v &\le \varepsilon \qquad \text{for all } v\in P,\\ \|\mathbf{x}\|_v &\le 1 \qquad \text{for all } v\in M_K\setminus P.\end{aligned}$$

Hence *(i)* does not hold.

Now we prove *(ii)* $\Rightarrow$ *(i)*. By Lemmas 5.11, 5.12, and 5.14 we may assume without loss of generality, that

$$A=(A_v)=\begin{pmatrix} I_t & 0 & -A_1\\ 0 & I_{m-t} & -A_2\\ 0 & 0 & 0\end{pmatrix},\quad \mathbf{b}_v=\begin{pmatrix}\mathbf{b}_1\\ \mathbf{b}_2^{(v)}\\ \mathbf{0}\end{pmatrix} \text{ for all } v\in P,$$

with $A_1, A_2, \mathbf{b}_1, (\mathbf{b}_2^{(v)})$ as in Lemma 5.14. Writing $\mathbf{x}^T=(\mathbf{q}^T,\mathbf{p}_1^T,\mathbf{p}_2^T)$, We can rewrite *(i)* as

$$\begin{aligned}\|A_1\mathbf{q}-\mathbf{p}_1-\mathbf{b}_1\|_v &\le \varepsilon \qquad \text{for all } v\in P,\\ \|A_2\mathbf{q}-\mathbf{p}_2-\mathbf{b}_2\|_v &\le \varepsilon \qquad \text{for all } v\in P,\end{aligned} \tag{5.12}$$

to be solved in $\mathbf{q}\in\mathcal{O}_P^{s-m}, \mathbf{p}_1\in\mathcal{O}_P^t, \mathbf{p}_2\in\mathcal{O}_P^{m-t}$. By Theorem 1.11 there exist $\mathbf{q}\in\mathcal{O}_P^{s-m}, \mathbf{p}_1'\in\mathcal{O}_P^t$ such that

$$A_1\mathbf{q}'-\mathbf{p}_1'=\mathbf{b}_1.$$

Recall that $A_1\in K^{t,s-m}$. By the Strong Approximation Theorem, i.e., Theorem 4.5 there exists non-zero $d\in\mathcal{O}_P$ such that $dA_1^T\in\mathcal{O}_P^{m,m}$. By Theorem 1.8, there exist $\mathbf{q}''\in\mathcal{O}_P^{s-m}$, $\mathbf{p}_2'\in\mathcal{O}_P^t$, such that

$$\|A_2\mathbf{q}''-\mathbf{p}_2'-\frac{1}{d}(\mathbf{b}_2-A_2\mathbf{q}')\|_v \le \frac{\varepsilon}{\max(1,|d|_v)} \quad \text{for all } v\in P.$$

Hence,

$$\begin{aligned}A_1(\mathbf{q}'+d\mathbf{q}'')-(\mathbf{p}_1'+dA_1\mathbf{q}'')-\mathbf{b}_1&=\mathbf{0},\\ \|A_2(\mathbf{q}'+d\mathbf{q}'')-d\mathbf{p}_2'-\mathbf{b}_2\|_v&<\varepsilon \quad \text{for all } v\in P,\end{aligned}$$

which implies that (5.12) is satisfied with $\mathbf{q}=\mathbf{q}'+d\mathbf{q}''$, $\mathbf{p}_1=\mathbf{p}_1'+dA_1\mathbf{q}''$, $\mathbf{p}_2=d\mathbf{p}_2'$. This proves the theorem. □

Bibliography

[1] Bachem, A., and Kannan, R. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *Siam. J. Comput. 8* (1979), 499–507.

[2] Bartle, R. G. *The elements of integration.* Wiley, 1966.

[3] Bombieri, E., and Vaaler, J. D. On Siegel's lemma. *Invent. math. 73* (1983), 11–32.

[4] Bourbaki, N. *Éléments de Mathématique Algèbre.* Hermann & C^{ie}, 1950.

[5] Cassels, J. W. S. *An introduction to Diophantine approximation.* Cambridge Univ. Press, 1957.

[6] Cassels, J. W. S., and Fröhlich, A. *Algebraic Number Theory.* Academic Press, 1967.

[7] Gruber, P. M., and Lekkerkerker, C. G. *Geometry of numbers.* North-Holland, 1969.

[8] Janusz, G. J. *Algebraic Number Fields.* Academic Press, 1973.

[9] Kannan, R., and Lovász, L. Covering minima and lattice-point-free convex bodies. *Ann. Math. 128*, 3 (1988), 577–602.

[10] Kronecker, L. Näherungsweise ganzzahlige Auflösung linearer Gleichungen. *Monatsber. Königlich. Preuss. Akad. Wiss. Berlin* (1884), 1179–1193, 1271–1299.

[11] Kuipers, L., and Niederreiter, H. *Uniform distributions of sequences.* Wiley, 1974.

[12] Lagarias, J. C., Lenstra, Jr., H. W., and Schnorr, C. P. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica 10*, 4 (1986), 333–348.

[13] Lang, S. *Algebraic Number Theory.* Springer-Verlag, 1970.

[14] Loomis, L. H. *An introduction to abstract harmonic analysis.* Van Nostrand, 1953.

[15] Mahler, K. A remark on Kronecker's theorem. *Enseignement math.* (1966), 183–189.

[16] McFeat, R. B. *Geometry of numbers in adele spaces.* Rozprawy Mat., 1971.

[17] Minkowski, H. *Geometry der Zahlen.* Leipzig-Berlin, 1896.

[18] Neukirch, J. *Algebraic number theory.* Springer, 1999.

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

[20] Schmidt, W. M. Norm form equations. *Ann. of Math. 96*, 3 (1972), 526–551.

[21] Smith, H. J. S. On systems of linear indeterminate equations and congruences. *Proceedings of the Royal Society of London 11* (1860), 86–89.

[22] Weyl, H. Über die Gleichverteilung von Zahlen modulo Eins. *Math. Ann. 77* (1916), 313–352.

List of symbols

We denote column vectors with boldface, $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{p}, \mathbf{q}, \mathbf{a}, \mathbf{b}$, prime ideals by $\mathfrak{p}$ and $\mathfrak{P}$, fractional ideals by $\mathfrak{a}$, fields by K and L and valuations by $|\cdot|_v$ and $|\cdot|_w$. Further, we denote adèles by (a_v) and idèles by (i_v).

$\mathcal{C}$	convex body	1
$\mathcal{C}^*$	polar of $\mathcal{C}$	1
$V(\mathcal{C})$	volume of $\mathcal{C}$	1
$\mathcal{L}$	lattice	1
$\mathcal{L}^*$	dual of $\mathcal{L}$	2
$\det \mathcal{L}$	determinant of $\mathcal{L}$	1
$\lambda_i(\mathcal{C}, \mathcal{L})$	i^{th} successive minima of $\mathcal{C}$ with respect to $\mathcal{L}$	2
$\mu(\mathcal{C}, \mathcal{L})$	covering radius of $\mathcal{C}$ with respect to $\mathcal{L}$	3
$\mathcal{F}$	fundamental domain	40
$\mathbf{e}_1, \ldots, \mathbf{e}_n$	the n unit vectors of $\mathbb{R}^n$	
$\mathbb{Z}$	ring of rational integers	
$\mathbb{Q}$	field of rational numbers	
$\mathbb{R}$	field of real numbers	
$\mathbb{C}$	field of complex numbers	
K	field	
R	ring	
R^n	n-dimensional column vectors over R	
$R^{m,n}$	$m \times n$ matrices over R	
$\mathrm{GL}_n(R)$	group of invertible $n \times n$ matrices over R	
$\mathbb{Q}_p$	field of p-adic rationals	
K_v	completion of K with respect to absolute value $\lvert\cdot\rvert_v$	17
$\overline{K}$	algebraic closure of K	
$\mathbb{A}_K$	adèle ring over K	34
$\mathbb{I}_K$	idèle group over K	37
ϕ	natural diagonal embedding of K^n in $\mathbb{A}_K^n$	35
$\mathrm{ord}_{\mathfrak{p}}$	valuation induced by prime ideal $\mathfrak{p}$	13

$\mathcal{O}_K$	ring of integers of K	12
$\mathcal{O}_v$	maximal compact subring	34
$\mathcal{O}_P$	ring of P-integers	55
$\mathcal{I}_K$	group of fractional ideals of $\mathcal{O}_K$	13
$\mathcal{P}_K$	group of principal fractional ideals of $\mathcal{O}_K$	13
D_K	discriminant of a number field K	14
$\mathrm{Tr}_{L/K}$	trace of L over K	13
$\mathrm{N}_{L/K}$	norm of L over K	13
$(x_k)_{k=1}^{\infty}$	sequence of reals	24
$(\mathbf{x}_k)_{k=1}^{\infty}$	sequence of real vectors	25
$\mathbf{0}$	zero vector	26
$\mathbf{1}$	$(1,\ldots,1)$	26
$\lvert\cdot\rvert_v$	absolute value	15
$\lvert\cdot\rvert_\infty$	standard absolute value	15
$\lvert\cdot\rvert_p$	p-adic absolute value	16
$\lvert\cdot\rvert_{\mathfrak{p}}$	absolute value induced by a prime ideal $\mathfrak{p}$	21
$\lvert\cdot\rvert_\sigma$	absolute value induced by an embedding σ	19
$M_{\mathbb{Q}}$	set of places of $\mathbb{Q}$	17
M_K	set of places of K	17
M_K^{fin}	set of non-archimedean places of K	17
M_K^{∞}	set of archimedean places of K	17
$H(\mathbf{x})$	height of $\mathbf{x} \in \overline{\mathbb{Q}}^n$	23
$\#$	cardinality of a set	
$\langle\ ,\ \rangle$	standard inner product on $\mathbb{R}^n$	1
$[\ :\ ]$	degree of a field extension	
$\lfloor x \rfloor$	floor function	24
$\lceil x \rfloor$	distance from x to the nearest integer	5
$\lceil \mathbf{x} \rfloor$	distance from $\mathbf{x}$ to nearest integer vector	28
$\lVert\mathbf{x}\rVert_\infty$	maximum norm of a real vector $\mathbf{x}$	4
$\lVert\mathbf{x}\rVert_1$	sum norm of $\mathbf{x}$	4
$\lVert\mathbf{x}\rVert_v$	maximum norm of $\mathbf{x}$ with respect to an absolute value $\lvert\cdot\rvert_v$	47
$\lVert A\rVert$	norm of matrix A	8
$\lVert A\rVert_v$	norm of matrix A with respect to $\lvert\cdot\rvert_v$	47

Index

absolute value, 15
    archimedean –, 16
    non-archimedean –, 16
    equivalent –s, 16
    extension of an –, 18
    non-trivial –, 15
    p-adic –, 16
    trivial –, 15
adèle ring, 34
adèles, 34
adèlic convex body, 35
adèlic covering radius, 45
adèlic successive minima, 37
archimedean absolute value, 16

completion, 18
complex place, 19
convex body, 1
    polar –, 1
    symmetric –, 1
    volume of a –, 1
    adèlic –, 35
covering radius, 3
    adèlic –, 45

diagonal matrix, 7
discriminant, 14
dual lattice, 2

equivalent absolute value, 16
extension of a place, 18
extension of an absolute value, 18

fractional ideal, 13
fundamental domain, 40

height, 23

idèle group, 37
ideal class group, 13
infinite prime, 15
inhomogeneous minimum, 3

lattice, 1
    dual –, 2
locally compact abelian group, 34

maximal compact subring, 34
maximum norm, 4

non-archimedean absolute value, 16
non-trivial absolute value, 15
norm, 4, 13
    maximum –, 4
    sum –, 4
number field, 12

p-adic absolute value, 16
P-integers
    ring of –, 55
place, 16
    complex –, 19
    extension of an –, 18
    real –, 19
polar convex body, 1
principal ideal domain, 7
product formula, 23

ramification index, 12
real place, 19
residue class degree, 12
ring of integers, 12

ring of P-integers, 55

Smith normal form, 7
successive minima, 3
    adèlic –, 37
sum norm, 4
symmetric convex body, 1

trace, 13
trivial absolute value, 15

uniform distribution, 24

valuation, 15
volume of a convex body, 1