VECTOR BUNDLES AND GEOMETRY OF NUMBERS

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van de Rector Magnificus Dr. D. D. Breimer,
hoogleraar in de faculteit der Wiskunde en
Natuurwetenschappen en die der Geneeskunde,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 18 november 2003
te klokke 14.15 uur

door

Richard Paul Groenewegen

geboren te Hoorn
in 1975

Samenstelling van de promotiecommissie:

promotor:	Prof. dr. H. W. Lenstra, Jr.
copromotor:	Dr. B. de Smit
referent:	Prof. dr. R. Schoof (*Università di Roma Tor Vergata*)
overige leden:	Dr. K. Belabas (*Université Paris-Sud*)
	Prof. dr. S. J. Edixhoven
	Prof. dr. F. J. Keune (*Katholieke Universiteit Nijmegen*)

PREFACE

This thesis consists of four articles which can be read independently. The first two articles deal with arithmetic analogues of well-known geometric theorems. In the correspondence between number fields and curves, the analogue of a geometric divisor is a metrized line bundle. An analogue of the function l from algebraic geometry that assigns to a divisor D the dimension $l(D)$ of the vector space of functions with poles prescribed by D is given by the size function h^0. Clifford's theorem says that for divisors D with $l(D) > 0$ and $l(K-D) > 0$, where K is the canonical divisor, we have $l(D) \leq \frac{1}{2}\deg D + 1$. In the first article we give an arithmetic analogue of Clifford's theorem. More precisely, let L be a line bundle over a number field of degree n over $\mathbb{Q}$ and let $L^\dagger$ be the (trace) dual. Assume that we have $\deg L \geq 0$ and $\deg L^\dagger \geq 0$. Then we have $h^0(L) \leq n \log \omega + n \log n + \frac{1}{2}\deg L$, where $\omega = \exp h^0(\mathbb{Z})$ denotes a constant smaller than 1.1. This article is published as

> An arithmetic analogue of Clifford's theorem, *Journal de Théorie des Nombres de Bordeaux* **13** (2001), pp. 143–156.

Apart from some minor changes the published article is the same as the first chapter in this thesis. For instance, the bold characters such as $\mathbf{Z}$ and $\mathbf{Q}$ have been replaced by the blackboard bold characters $\mathbb{Z}$ and $\mathbb{Q}$. Furthermore, information not present at the time of publication has been added to the references between square brackets.

In the second article *Torelli for number fields* we give an arithmetic analogue of Torelli's theorem, which says that a curve is uniquely determined by its canonically polarized Jacobian. We state and prove a precise theorem that says that a number field is uniquely determined by its size function h^0 as follows. Given two number fields K and L with sets of infinite primes $S_\infty K$ and $S_\infty L$, the size functions induce maps $h^0_K \colon \mathbb{R}^{S_\infty K} \to \mathbb{R}$ and $h^0_L \colon \mathbb{R}^{S_\infty L} \to \mathbb{R}$. When K and L are isomorphic, there is a bijection $S_\infty L \to S_\infty K$, respecting the degrees of the primes, such that h^0_K and h^0_L are equal with respect to this bijection. We prove that this occurs *only* when K and L are isomorphic. We also discuss in which ways the theorem might be generalized.

In the third article *Minkowski for vector bundles* we define metrized vector bundles. Given a vector bundle P we are interested in finding line bundles $L \subset P$ with small determinant. One way to find such line bundles is to use Minkowski's theorem which gives a point $x \in P$ with small length and hence a line bundle generated by x with bounded determinant. We raise the question if the bound can be improved if we do not restrict to cyclic line bundles.

The fourth article *Bounds for computing the tame kernel* is concerned with the calculation of the tame kernel of a number field. We give a bound, used for finding a set of generators for the tame kernel, that significantly improves the bounds that were currently known. When F is a number field with discrimant Δ and S is a set of finite primes of F, we write U_S for the S-unit group. We show that when S contains all primes with norm up to $4|\Delta|^{3/2}$, the image of $U_S \otimes U_S$ in K_2F contains the tame kernel. Moreover, we prove that the tame kernel is computable. The article is accepted for publication in the journal *Mathematics of Computations*.

Thomas Stieltjes Institute
for Mathematics

TABLE OF CONTENTS

AN ARITHMETIC ANALOGUE OF CLIFFORD'S THEOREM

Richard P. Groenewegen

Résumé — Nous considérons ici certains fibrés en droites métriques comme analogues des diviseurs sur les courbes. Van der Geer et Schoof ont défini une fonction h^0 sur les fibrés métriques dont les propriétés ressemblent à celles de la dimension de $H^0(X, \mathscr{L}(D))$, où D désigne un diviseur sur la courbe X. Ils obtiennent en particulier un analogue du théorème de Riemann-Roch. Nous proposons des analogues arithmétiques de trois théorèmes sur les courbes, notamment du théorème de Clifford.

Abstract — Number fields can be viewed as analogues of curves over fields. Here we use metrized line bundles as analogues of divisors on curves. Van der Geer and Schoof gave a definition of a function h^0 on metrized line bundles that resembles properties of the dimension $l(D)$ of $H^0(X, \mathscr{L}(D))$, where D is a divisor on a curve X. In particular, they get a direct analogue of the Riemann-Roch theorem. For three theorems of curves, notably Clifford's theorem, we will propose arithmetic analogues.

1. Introduction

A popular way to study number fields is to view them as analogues of curves over a field. The primes of the number field correspond with points on the curve. Divisors on curves find their analogue in Arakelov divisors for number fields or metrized line bundles.

Given a divisor D on a curve X, we have an associated line bundle $\mathscr{L}(D)$ and an integer $l(D)$, which is the dimension of the vector space $H^0(X, \mathscr{L}(D))$. One of the most well known theorems for curves is the Riemann-Roch theorem, which relates $l(D)$ to the degree $\deg D$ of a divisor. It states that there is a canonical divisor K such that for each divisor D we have

$$l(D) - \tfrac{1}{2}\deg D = l(D^\dagger) - \tfrac{1}{2}\deg(D^\dagger), \qquad \text{where } D^\dagger = K - D.$$

Following Van der Geer and Schoof [3], this article presents a function h^0 such that for a metrized line bundle L of a number field, we have

$$h^0(L) - \tfrac{1}{2}\deg L = h^0(L^\dagger) - \tfrac{1}{2}\deg L^\dagger.$$

In this article we will find analogues for three theorems for curves, stated here.

1. THEOREM.

(1) *Let D be a divisor on a curve. If $\deg D < 0$, then $l(D) = 0$.*
(2) *Let D be a divisor on a curve with $\deg D \geq 0$. Then $l(D) \leq 1 + \deg D$.*
(3) *(Clifford's theorem) Let D be a divisor on a curve such that $l(D) > 0$ and $l(D^\dagger) > 0$. Then $l(D) \leq \frac{1}{2}\deg D + 1$.*

PROOF. For (1) and (3), see Hartshorne [4, lemma IV.1.2 and IV.5.4]. For (2), see Fulton [2, proposition 8.2.3]. □

Arithmetic analogues to the three theorems above are also considered in the preprint of Van der Geer and Schoof [3]. As for the first one, they prove that $h^0(L)$ tends doubly exponentially fast to 0 in terms of the degree of L when $\deg L$ becomes negative. Our result is basically the same, although the bound that we will prove is more explicit. As for the second statement, Van der Geer and Schoof have a conjecture for number fields that are Galois over $\mathbb{Q}$ or over an quadratic imaginary number field. The conjecture has been proven by P. Francini for quadratic number fields [1].

2. Statement of Clifford's theorem for number fields

We give a working definition of a metrized line bundle now, in order to state Clifford's theorem. For a full definition, see section 6.

Let K be a number field with ring of integers R. We can write $R \otimes_{\mathbb{Z}} \mathbb{R}$ as a product

$$R \otimes_{\mathbb{Z}} \mathbb{R} = \prod_{v \in S^\infty} K_v,$$

where S^∞ is the set of infinite primes of K. Each K_v is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, so it should be clear what it means to take the complex conjugate of an element in K_v and hence of an element in $R \otimes_{\mathbb{Z}} \mathbb{R}$. A metrized line bundle is a projective R-module L of rank 1 together with an inner product $\langle \cdot\,, \cdot \rangle$ on $L \otimes_{\mathbb{Z}} \mathbb{R}$, such that for x, $y \in L \otimes_{\mathbb{Z}} \mathbb{R}$ and $a \in R \otimes_{\mathbb{Z}} \mathbb{R}$, we have

$$\langle ax, y \rangle = \langle x, a^* y \rangle,$$

where a^* is the complex conjugate of a. The dual of a metrized line bundle L is given by $L^\dagger = \mathrm{Hom}(L, \mathbb{Z})$. The elements of $L^\dagger$ can be identified with the elements of $L \otimes_{\mathbb{Z}} \mathbb{R}$ that have integer valued inner product with every element of L. The degree of a line bundle L is given by

$$\deg L = \log(\sqrt{|\Delta|}/\operatorname{vol} L),$$

where Δ is the discriminant of K and $\operatorname{vol} L$ is the covolume of the lattice L in $L \otimes_{\mathbb{Z}} \mathbb{R}$. Finally we define

$$k^0(L) = \sum_{x \in L} e^{-\pi\langle x, x\rangle} \qquad \text{and} \qquad h^0(L) = \log k^0(L).$$

These definitions give rise to the Riemann-Roch theorem from section 1.

The main goal is to give an analogue of Clifford's theorem, which we state here.

2. Theorem (Clifford's theorem). *Let K be a number field of degree n over $\mathbb{Q}$ and let L be a metrized line bundle with $\deg L \geq 0$ and $\deg L^\dagger \geq 0$. Then we have*

$$h^0(L) \leq n \log \omega + n \log n + \tfrac{1}{2} \deg L,$$

where $\omega = \sum_{n \in \mathbb{Z}} e^{-\pi n^2}$.

3. Riemann-Roch for lattices

A Euclidean space E is a finite dimensional vector space over $\mathbb{R}$, equipped with a positive definite symmetric $\mathbb{R}$-bilinear map

$$\langle \cdot\,, \cdot \rangle \colon E \times E \to \mathbb{R},$$

which we call the inner product or Euclidean structure. A norm $\| \cdot \|$ on E is constructed in the obvious way by setting $\|x\| = \sqrt{\langle x, x \rangle}$ for $x \in E$. The norm uniquely determines the inner product by

$$\langle x, y \rangle = \frac{\|x + y\|^2 - \|x\|^2 - \|y\|^2}{2}.$$

If we have $\langle x, y \rangle = 0$ for x, $y \in E$, then we say that x and y are perpendicular and we write $x \perp y$. Given a subspace V of E we write $V^\perp = \{\, x \in E : x \perp V \,\}$ for the orthogonal complement of V. Given a subset $S \subset E$ we write $\operatorname{span} S$ for the smallest linear subspace of E containing S.

A lattice in a Euclidean vector space is a discrete subgroup of E. A lattice has a $\mathbb{Z}$-basis and the rank is given by the cardinality of this basis. If the rank is equal to the dimension of the vector space E, it is said to have full rank. If L is of full rank and has basis $b_1, \ldots, b_n$, then the volume $\operatorname{vol} L$ of L is given by the volume of parallelepiped

$$\{\, \lambda_1 b_1 + \cdots + \lambda_n b_n : \lambda_i \in \mathbb{R}, 0 \leq \lambda_i < 1 \,\},$$

where the volume is measured by the Haar measure induced by the inner product. A lattice L has a dual lattice $L^\dagger$, defined by

$$L^\dagger = \{\, x \in \operatorname{span} L : \langle x, L \rangle \subset \mathbb{Z} \,\}.$$

The Riemann-Roch theorem for lattices is better known as the Poisson summation formula. If E is a Euclidean space and f is a C^∞-function $E \to \mathbb{C}$ such that for all m the function $x \mapsto |x|^m f(x)$ is bounded, we call such a function a *rapidly decreasing function*. We can take the Fourier transform of of a rapidly decreasing function f as follows. Let dx be the Haar measure on E induced by the inner product. Furthermore, define the function $[\,\cdot\,, \cdot\,] \colon E \times E \to \mathbb{T}$ to the circle $\mathbb{T}$ by

$$[x, y] = e^{-2\pi i \langle x, y \rangle}.$$

Then the Fourier transform $\hat{f} \colon E \to \mathbb{C}$ of f is defined by

$$\hat{f}(y) = \int_E f(x)[x, y]\, dx.$$

We can now state the Poisson summation formula.

3. Proposition. *Let L be a lattice of full rank in a Euclidean vector space E and let $L^\dagger$ be the dual lattice. Let f be a rapidly decreasing function on E. Then we have*

$$\sum_{x\in L} f(x) = \frac{1}{\operatorname{vol} L} \sum_{y\in L^\dagger} \hat{f}(y).$$

Proof. See Neukirch [5, VII.3.2]. □

Given a subset S of a Euclidean space, we define $k^0(S)$ as

$$k^0(S) = \sum_{x\in S} e^{-\pi\langle x,x\rangle}$$

if the sum converges. In particular, k^0 is well-defined on lattices and cosets of lattices. An application of the Poisson summation formula gives a multiplicative version of the Riemann-Roch theorem for lattices.

4. Theorem (Riemann-Roch). *For every lattice L, we have*

$$k^0(L)\sqrt{\operatorname{vol} L} = k^0(L^\dagger)\sqrt{\operatorname{vol} L^\dagger}.$$

Proof. The function $x \mapsto e^{-\pi\langle x,x\rangle}$ is self-dual with respect to taking Fourier transforms (see [5, VII.3.1]). Furthermore, we have $\operatorname{vol} L = (\operatorname{vol} L^\dagger)^{-1}$. The theorem now follows directly form the Poisson summation formula. □

4. Estimates for k^0

Let L be a lattice in a Euclidean space E. The *minimum* of L is the length of the shortest nonzero vector in L. A minimal vector is a vector with length equal to the minimum. We have the following lemma.

5. Lemma. *Let L be a lattice with minimum λ. Define α_t for $t \in \mathbb{R}_{\geq 0}$ as*

$$\alpha_t = \#\{\, x \in L : \langle x,x\rangle \leq \lambda^2 t \,\}.$$

Then we have

$$k^0(L) = \int_0^\infty \alpha_t \lambda^2 \pi e^{-\pi\lambda^2 t}\, dt.$$

Proof. We can write

$$k^0(L) = \sum_{x\in L} e^{-\pi\langle x,x\rangle} = \sum_{x\in L} \int_{\langle x,x\rangle}^\infty \pi e^{-\pi t}\, dt = \int_0^\infty \#\{\, x \in L : \langle x,x\rangle \leq t \,\}\pi e^{-\pi t}\, dt.$$

A substitution of $\lambda^2 t$ for t in the above expression yields the lemma. □

6. Lemma. *Let L be a lattice with minimum λ. Let α_t be defined as in lemma 5. Then we have*

$$\alpha_t \le (2\sqrt{t}+1)^n.$$

Proof. Let t be any positive real number and let A_t be the set

$$A_t = \{\, x \in L : \langle x, x\rangle \le \lambda^2 t \,\}.$$

The distance between any two points in A_t is at least λ. Hence, if x and y are two different points of A_t, the open balls $B_{\lambda/2}(x)$ and $B_{\lambda/2}(y)$ with radius $\lambda/2$ and center x and y are disjunct. The union of all balls $B_{\lambda/2}(x)$ for all $x \in A_t$ is a subset of a large ball with radius $\lambda\sqrt{t}+\lambda/2$. Hence, by taking the quotient of the volume of the large ball with radius $\lambda\sqrt{t}+\lambda/2$ and a small ball with radius $\lambda/2$ we get

$$\alpha_t = \#A_t \le \Big(\frac{\lambda\sqrt{t}+\lambda/2}{\lambda/2}\Big)^n = (2\sqrt{t}+1)^n. \qquad \square$$

7. Corollary. *Let L be a lattice with minimum λ. Then we have*

$$k^0(L) \le 1 + \int_1^\infty (2\sqrt{t}+1)^n \lambda^2 \pi e^{-\pi\lambda^2 t}\, dt.$$

8. Proposition. *Let L be a lattice of rank n and with minimum $\lambda \ge \sqrt{n}$. Then we have*

$$k^0(L) \le 1 + \frac{3^n\pi}{\pi - \log 3} e^{-\pi\lambda^2}.$$

Proof. We have $2\sqrt{t}+1 \le 3^t$ for $t \ge 1$. Hence by corollary 7, we get

$$\begin{aligned} k^0(L) - 1 &\le \pi\lambda^2 \int_1^\infty 3^{nt} e^{-\pi\lambda^2 t}\, dt = \pi\lambda^2 \int_1^\infty e^{(-\pi\lambda^2 + n\log 3)t}\, dt \\ &= \frac{\pi\lambda^2}{\pi\lambda^2 - n\log 3} e^{\pi\lambda^2 + n\log 3} = \frac{3^n\pi\lambda^2}{\pi\lambda^2 - n\log 3} e^{-\pi\lambda^2} \le \frac{3^n\pi}{\pi - \log 3} e^{\pi\lambda^2}. \end{aligned}$$

This proves the proposition. □

5. Clifford's theorem for lattices

We write $\mathbb{Z}$ for the unit bundle of $\mathbb{Q}$ and we write $\omega = k^0(\mathbb{Z})$. We have $\omega \approx 1.086$.

9. Lemma. *For $\lambda > 0$, we have $k^0(\lambda\mathbb{Z}) \leq \omega \max\{1, \lambda^{-1}\}$.*

Proof. It is clear that for $\lambda \geq 1$, we have $k^0(\lambda\mathbb{Z}) \leq k^0(\mathbb{Z}) = \omega$. Now assume $\lambda \leq 1$. The dual lattice of $\lambda\mathbb{Z}$ is equal to $\lambda^{-1}\mathbb{Z}$ and by Riemann-Roch for lattices, we get $k^0(\lambda\mathbb{Z}) \leq k^0(\lambda^{-1}\mathbb{Z}) \operatorname{vol}(\lambda^{-1}\mathbb{Z}) \leq \omega\lambda^{-1}$. □

10. Lemma. *Let L be a lattice of full rank in a Euclidean vector space E. The function $E/L \to \mathbb{R}$ that sends a coset Z of L to $k^0(Z)$ attains a unique maximum in L.*

Proof. Recall that for y, $z \in E$, we have defined $[y, z]$ as $[y, z] = e^{-2\pi i\langle y,z\rangle}$. Let f be a rapidly decreasing function $E \to \mathbb{C}$ and for $z \in E$ let g equal f, translated over z, i.e., $g(x) = f(x+z)$. Then we can express the Fourier transform of g in terms of $\hat{f}$ as

$$\begin{aligned}\hat{g}(y) = \int_E f(x+z)[x,y]\,dx = \int_E f(x)[x-z,y]\,dx \\ = \int_E f(x)[z,y]^{-1}[x,y]\,dx = [z,y]^{-1}\hat{f}(y).\end{aligned}$$

The Poisson summation formula gives us

$$\sum_{x\in z+L} f(x) = \sum_{x\in L} g(x) = \frac{1}{\operatorname{vol} L^\dagger} \sum_{y\in L^\dagger} [z,y]^{-1}\hat{f}(y).$$

We specialize for the case $f(x) = \hat{f}(x) = e^{-\pi\langle x,x\rangle}$. Then this sum is maximal if $[z, y]$ equals 1 for all y, hence if z is in L. □

11. Lemma. *Let L be a lattice of full rank in a Euclidean vector space E. Let π be an orthogonal projection on a subspace of E such that the image πL is discrete. Let $L' \subset L$ be the kernel of π. This gives an exact sequence*

$$0 \longrightarrow L' \longrightarrow L \xrightarrow{\pi} \pi L \longrightarrow 0.$$

Then we have

$$k^0(L) \leq k^0(L')k^0(\pi L).$$

Equality holds if and only if L is equal to the direct sum $L' \oplus \pi L$.

Proof. As for $x \in L'$ and $y \in \pi L$, we have $e^{-\pi\langle x,x\rangle}e^{-\pi\langle y,y\rangle} = e^{-\pi\langle y+x,y+x\rangle}$ we have $k^0(L' \oplus \pi L) = k^0(L')k^0(\pi L)$. For each $x \in \pi L$ choose an element $l(x) \in \pi^{-1}(x)$. Then we have

$$k^0(L' \oplus \pi L) = \sum_{x\in\pi L} k^0(x + L') \qquad \text{and} \qquad k^0(L) = \sum_{x\in\pi L} k^0(l(x) + L').$$

Let E' be the subspace of E spanned by L' and let x be an element of πL. For $y \in E'$ we have $\langle x+y, x+y\rangle = \langle x,x\rangle\langle y,y\rangle$ and hence

$$k^0(x+L') = e^{-\pi\langle x,x\rangle}k^0(L') \qquad \text{and} \qquad k^0(l(x)+L') = e^{-\pi\langle x,x\rangle}k^0(l(x)-x+L').$$

Hence, by lemma 10, we have $k^0(x+L') \geq k^0(l(x)+L')$, where we have equality only if $l(x) \in x+L'$. □

Given a lattice L, we want to have some way of bounding $k^0(L)$ in terms of its minimum. By lemma 9, this is trivial if the rank of L is 1. For the higher rank case we will use orthogonal projection and lemma 11 to reduce to the 1-dimensional case.

In order to give these bounds, we use Hermite constants, so here is a quick reminder what they are. The ith Hermite constant γ_i is defined as the smallest real number such that any lattice of rank i and with volume 1 has a vector with length at most $\gamma_i^{1/2}$. In general, a lattice L of rank i has a vector of length at most $\gamma_i^{1/2}(\operatorname{vol} L)^{1/2}$. It follows from the Minkowski bound that the inequality $\gamma_i \leq i$ holds.

12. Proposition. *Let L be a lattice of rank n with minimum λ. Then we have*

$$k^0(L) \leq \omega^n \prod_{i=1}^{n} \max\{1, \gamma_i/\lambda\}.$$

Proof. Let L be contained in a Euclidean vector space E. We inductively choose $b_1, \ldots, b_n \in E$ as follows. The element b_1 is equal to a minimal vector of the dual lattice $L^\dagger$. Then we project the lattice L orthogonally on $b_1\mathbb{R}$. The projection map is given by

$$x \longmapsto \frac{\langle x, b_1\rangle}{\langle b_1, b_1\rangle} b_1.$$

Let L_1 be the kernel of the projection map. That is, L_1 consists of all elements of L perpendicular to b_1. Then b_2 is chosen as a minimal vector of $L_1^\dagger$. In general, b_i is chosen such that it is a minimal vector of the dual $L_i^\dagger$ of the sublattice L_i of L given by all elements of L perpendicular to $\operatorname{span}\{b_1, \ldots, b_{i-1}\}$. The image of L_i under orthogonal projection on $b_i\mathbb{R}$ is

$$\frac{b_i}{\langle b_i, b_i\rangle}\mathbb{Z} \cong \frac{1}{\|b_i\|}\mathbb{Z}.$$

Hence, by lemma 11 we have

$$k^0(L) \leq \prod_{i=1}^{n} k^0(\|b_i\|^{-1}\mathbb{Z}).$$

We will now give bounds for $k^0(\|b_i\|^{-1}\mathbb{Z})$. If M is a lattice of rank i with minimum *at most* λ and if b is a minimal vector of the dual lattice $M^\dagger$, we have

$$\|b\| \leq \gamma_i^{1/2}(\operatorname{vol} M^\dagger)^{1/i} = \gamma_i^{1/2}(\operatorname{vol} M)^{-1/i} \leq \gamma_i/\lambda.$$

By lemma 9, we have

$$k^0(\|b_i\|^{-1}\mathbb{Z}) \leq \omega \max\{1, \|b_i\|\} \leq \max\{1, \gamma_i/\lambda\}.$$

This completes the proof. □

13. Proposition. *Let L be a lattice in E of rank n with minimum λ. Let W be the smallest subspace of E such that all points of L that are not in W have distance at least 1 to W. We write $l = \dim W$. Then we have*

$$k^0(L) \leq \omega^n \max\{1, n/\lambda\}^l n^{n-l}$$

Proof. Let l be the dimension of W and define L' as $L' = W \cap L$. Let π be orthogonal projection on $W^\perp$ and let the image of L be denoted πL. Then πL has minimum greater or equal to 1. Hence, by lemma 11, we have

$$k^0(L) \leq k^0(L')k^0(\pi L).$$

Applying proposition 12 twice yields

$$k^0(L) \leq \omega^n \prod_{i=1}^{l} \max\{1, \gamma_i/\lambda\} \prod_{i=1}^{n-l} \gamma_i.$$

We use $\gamma_i \leq n$ to get the wanted inequality. □

14. Lemma. *Let L be a lattice contained in a Euclidean vector space E and let W be the smallest subspace of E such that all points of L that are not in W have distance at least 1 to W. Similarly, let $W^\dagger$ be such a set for $L^\dagger$. Then W and $W^\dagger$ are perpendicular. In particular* $\dim W + \dim W^\dagger \leq \operatorname{rank} L$.

Proof. Suppose W and $W^\dagger$ are not perpendicular. Then there exists a $y \in L^\dagger \cap W^\dagger$ with $y \notin W^\dagger \cap W^\perp$. By minimality of $W^\dagger$ we can choose y with distance to $W^\dagger \cap W^\perp$ smaller than 1. Hence, there is a $y' \in W^\dagger \cap W^\perp$ with $\|y - y'\| < 1$. Similarly, there is a $z \in L \cap W$ with $z \notin W \cap (W^\dagger)^\perp$ and a $z' \in W \cap (W^\dagger)^\perp$ such that $\|z - z'\| < 1$. Hence we get

$$1 > \|z - z'\|\|y - y'\| \geq |\langle z - z', y - y'\rangle| = |\langle z, y\rangle|.$$

As $\langle z, y\rangle$ is an integer and z and y are not perpendicular, this is a contradiction. □

Combining proposition 13 and lemma 14, we get the following corollary. In section 7, Clifford's theorem for number fields follows directly from this corollary. Therefore, we see this corollary as an analogue of Clifford's theorem for lattices.

15. Corollary. *Let L be a lattice of rank n with minimum λ and let the dual $L^\dagger$ have minimum $\lambda^\dagger$. Then we have*

$$k^0(L) \leq \omega^n \max\{1, 1/\lambda\}^{n/2} n^n \qquad \text{or} \qquad k^0(L^\dagger) \leq \omega^n \max\{1, 1/\lambda^\dagger\}^{n/2} n^n.$$

6. Metrized line bundles

Now we turn to the number field case and prove arithmetic analogues of the geometric theorems mentioned in the introduction. As we shall see, almost all of the work is already done in the sections about lattices. We need a few facts about Euclidean spaces and finite étale algebras over $\mathbb{R}$ in order to define hermitian modules and metrized line bundles.

We state the following lemma without proof.

16. Lemma.

(1) *If E_1 and E_2 are Euclidean spaces, the tensor product $E_1 \otimes E_2$ has a unique Euclidean structure such that for x, $y \in E_1$ and x', $y' \in E_2$, we have*

$$\langle x \otimes x', y \otimes y' \rangle = \langle x, y \rangle \langle x', y' \rangle.$$

(2) *Every quotient space D of a Euclidean space E, given by $\phi\colon E \to D$, has an induced Euclidean structure given by $(\ker \phi)^\perp \cong D$ such that $\|z\| = \inf_{\phi(x)=z} \|x\|$ for $z \in D$.*

(3) *The Endomorphism $\mathrm{End}_{\mathbb{R}}(E)$ of a Euclidean space E has a natural involution $\phi \mapsto \phi^*$, where the adjoint ϕ^* of ϕ is the unique element of $\mathrm{End}_{\mathbb{R}}(E)$ such that the relation $\langle \phi a, b \rangle = \langle a, \phi^* b \rangle$ holds.*

The category of finite étale algebras over $\mathbb{R}$ consists of the finite $\mathbb{R}$-algebras A such that the map $\phi\colon A \to \mathrm{Hom}_{\mathbb{R}}(A, \mathbb{R})$ given by $\phi(x)(y) = \mathrm{Tr}(xy)$ is an isomorphism. Here Tr is the trace map from A over $\mathbb{R}$. If we let v range over the points of $S = \operatorname{spec} A$, we get a decomposition $A = \prod_v A_v$, where A_v is the residue class field. Every A_v is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. For every $v \in \operatorname{spec} A$, we have a projection map $\phi\colon A \to A_v$. We contend that the identity functor on the category of the finite étale algebras over $\mathbb{R}$ has exactly one nontrivial automorphism. Indeed, suppose we have a functorial automorphism $x \mapsto x^*$ on every finite étale algebra over $\mathbb{R}$. Then for all projections $\pi\colon A \to A_v$ and all elements $x \in A$ we have $\pi(x^*) = \phi(x)^*$. Hence, on each étale algebra our nontrivial automorphism is complex conjugation on the factors A_v that are isomorphic to $\mathbb{C}$ and is trivial on factors isomorphic to $\mathbb{R}$. When we talk about the involution of a finite étale algebra over $\mathbb{R}$ we mean this map.

Let M be a module over an étale algebra A over $\mathbb{R}$, with a Euclidean structure. Then M is called *hermitian* if the natural map $A \to \mathrm{End}_{\mathbb{R}}(M)$ preserves involutions. This is equivalent to the condition that for all $a \in A$ and m_1, $m_2 \in M$ we have

$$\langle a m_1, m_2 \rangle = \langle m_1, a^* m_2 \rangle.$$

If we are given two Hermitian modules M and N over A, then $M \otimes_{\mathbb{R}} N$ is a Euclidean space and the quotient space $M \otimes_A N$ has a natural Euclidean structure. Furthermore, we can view A as a module over itself and give it the unique Euclidean structure such that the inner product on A and the induced inner product on $A \otimes_A A$ is compatible with the map $A \otimes_A A \xrightarrow{\sim} A$. This is the canonical inner product for A. A trace of the definitions results in the following lemma.

17. Lemma.

(1) *Let M and N be hermitian modules, free of rank 1 over a field A, algebraic over $\mathbb{R}$. For $m \in M$, $n \in N$ and $m \otimes n \in M \otimes_A N$, we have*

$$\|m \otimes n\| = [A : \mathbb{R}]^{-1/2} \|m\| \cdot \|n\|.$$

(2) *Let A be a finite étale algebra over $\mathbb{R}$ and let M and N be hermitian modules over A, free of rank 1. Then, for $v \in \operatorname{spec} A$, we have an isomorphism*

$$(M \otimes_A N)_v \cong M_v \otimes_{A_v} N_v$$

as hermitian modules.

(3) *Let A be a finite étale algebra, viewed as a hermitian module over itself with the canonical inner product. Let v be an element of* $\operatorname{spec} A$ *and let $\|\cdot\|_v$ be the restriction of $\|\cdot\|$ to A_v. Then we have $\|1\|_v = [A_v : \mathbb{R}]^{1/2}$.*

We are now ready to give the definition of a metrized line bundle. Let K be a number field and let R be its ring of integers. A line bundle on R is a projective R-module L of rank 1. Now $R \otimes_{\mathbb{Z}} \mathbb{R}$ is a finite étale algebra over $\mathbb{R}$ and $L \otimes_{\mathbb{Z}} \mathbb{R}$ is a module of rank 1 over $R \otimes_{\mathbb{Z}} \mathbb{R}$. We call L a *metrized line bundle* over R if $L \otimes_{\mathbb{Z}} \mathbb{R}$ is given a Euclidean structure such that it becomes an hermitian module over $R \otimes_{\mathbb{Z}} \mathbb{R}$.

Two metrized line bundles are isomorphic if there is an R-module isomorphism that preserves the inner product. Given two metrized line bundles L_1, L_2 over R, their product $L_1 L_2$ is given by the module $L_1 \otimes_R L_2$. The inner product on $(L_1 \otimes_R L_2) \otimes_{\mathbb{Z}} \mathbb{R}$ is given by the canonical isomorphism

$$(L_1 \otimes_R L_2) \otimes_{\mathbb{Z}} \mathbb{R} \cong (L_1 \otimes_{\mathbb{Z}} \mathbb{R}) \otimes_{R \otimes \mathbb{R}} (L_2 \otimes_{\mathbb{Z}} \mathbb{R}).$$

The set of isomorphism classes of metrized line bundles over R is denoted $\operatorname{Pic} K$ and with this multiplication it is a group. The unit element is equal to R with the canonical Euclidean structure on $R \otimes_{\mathbb{Z}} \mathbb{R}$. We call R with this structure the *unit bundle*.

Let L be a metrized line bundle over R and let S^∞ be the set of infinite primes of K. Then we have a decomposition $L \otimes_{\mathbb{Z}} \mathbb{R} = \prod_{v \in S^\infty} L_v$, where $L_v = L \otimes K_v$ is a 1-dimensional K_v-vector space. The factors L_v are perpendicular and we write $\|\cdot\|_v$ for the restriction of the norm to L_v. For instance, if R is the unit bundle and $\|\cdot\|_v$ is the restricted norm on $R_v = K_v$, we have

$$\|1\|_v = \sqrt{[K_v : \mathbb{R}]}.$$

We define the *norm* of a metrized line bundle L as

$$N(L) = \frac{\operatorname{vol} R}{\operatorname{vol} L} = \frac{\sqrt{|\Delta|}}{\operatorname{vol} L},$$

where Δ is the discriminant of K. The *degree* is defined as $\deg L = \log N(L)$.

18. Proposition.
(1) *The norm function is a group homomorphism* $\operatorname{Pic} K \to \mathbb{R}_{>0}$.
(2) *If L is a metrized line bundle and $t \in L$ is any nonzero element, then*

$$N(L) = \#(L/Rt) \Big/ \prod_{v \in S^\infty} \frac{\|t\|^{[K_v:\mathbb{R}]}}{[K_v : \mathbb{R}]}.$$

Proof. Define M_t by

$$M_t = \prod_{v \in S^\infty} \frac{\|t\|_v^{[K_v:\mathbb{R}]}}{[K_v : \mathbb{R}]}.$$

As we have $\|1\|_v = \sqrt{[K_v : \mathbb{R}]}$, we can also write

$$M_t = \prod_{v \in S^\infty} \Big(\frac{\|t\|_v}{\|1\|_v}\Big)^{[K_v:\mathbb{R}]}.$$

Consider the map $R \otimes_{\mathbb{Z}} \mathbb{R} \to L \otimes_{\mathbb{Z}} \mathbb{R}$ given by multiplication with t. It blows up the measure by a factor M_t. Hence, we have

$$M_t \operatorname{vol} R = \operatorname{vol} R_t = (\operatorname{vol} L)/[L : Rt].$$

This proves (2). To prove (1) one uses (2) together with some explicit calculations. □

Let L be a metrized line bundle over R. Then it can be viewed as a lattice in $L \otimes_{\mathbb{Z}} \mathbb{R}$. Hence, we have a definition for $k^0(L)$, given as

$$k^0(L) = \sum_{x \in L} e^{-\pi \langle x, x \rangle}.$$

Furthermore, we define $h^0(L)$ as

$$h^0(L) = \log k^0(L).$$

Both k^0 and h^0 induce functions from $\operatorname{Pic} K$ to $\mathbb{R}$. In order to state the Riemann-Roch theorem, we need the notion of the dual of a metrized line bundle L. Consider the map

$$\begin{aligned} L \otimes_{\mathbb{Z}} \mathbb{R} &\longrightarrow \operatorname{Hom}_{\mathbb{R}}(L \otimes_{\mathbb{Z}} \mathbb{R}, \mathbb{R}) \\ x &\longmapsto \langle x, \cdot \rangle. \end{aligned}$$

This map is an isomorphism, giving

$$\operatorname{Hom}_{\mathbb{R}}(L \otimes_{\mathbb{Z}} \mathbb{R}, \mathbb{R}) = \operatorname{Hom}_{\mathbb{Z}}(L, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$$

a canonical Euclidean structure. We let $L^\dagger$ be $\operatorname{Hom}(L, \mathbb{Z})$ with this structure.

19. Proposition (Riemann-Roch). *Let L be a metrized line bundle. Then we have*

$$h^0(L) - \tfrac{1}{2} \deg L = h^0(L^\dagger) - \tfrac{1}{2} \deg L^\dagger.$$

Proof. This follows directly from the Riemann-Roch theorem for lattices. This formula also appears in [3, Proposition 1] in a different form. □

7. Analogues of theorems for curves

We have set up everything to prove in quick succession the analogues of the geometric theorems mentioned in section 1. The only lemma we need to tie the results for lattices to metrized line bundles is the following lemma, that relates the minimum of a lattice to the norm of the line bundle.

20. Lemma. *Let n be the degree of a number field K, and let L be a metrized line bundle. Then for all elements $x \in L$, we have*

$$\|x\|^2 \geq nN(L)^{-2/n}.$$

Proof. The geometric-arithmetic mean inequality and proposition 18 give for nonzero $x \in L$ the estimate

$$\begin{aligned}\|x\|^2 = \sum_{v\in S^\infty} \|x\|_v^2 = \sum_{v\in S^\infty} [K_v:\mathbb{R}]\frac{\|x\|_v^2}{[K_v:\mathbb{R}]} &\geq n\Big(\prod_{v\in S^\infty}\Big(\frac{\|x\|_v^2}{[K_v:\mathbb{R}]}\Big)^{[K_v:\mathbb{R}]}\Big)^{1/n}\\ &= n\Big(\prod_{v\in S^\infty}\frac{\|x\|^{[K_v:\mathbb{R}]}}{[K_v:\mathbb{R}]}\Big)^{2/n} \geq n\Big(\frac{\#(L/Rx)}{N(L)}\Big)^{2/n} \geq nN(L)^{-2/n}. \quad \square\end{aligned}$$

First, we will prove the analogue of the geometric fact that $l(D) = 0$ if the degree of a divisor D is negative. The proposition states that $h^0(L)$ tends doubly exponentially fast to zero in terms of the degree of L when the degree becomes negative. This was already noted by Van der Geer and Schoof [3, Corollary 1 to Proposition 2].

21. Proposition. *Let K be a number field of degree n over $\mathbb{Q}$ and let L be a metrized line bundle of degree at most* 0*. Then we have*

$$h^0(L) < \frac{3^n\pi}{\pi - \log 3}e^{-\pi n e^{-\frac{2}{n}\deg L}}.$$

Proof. Immediate from proposition 8 and lemma 20 and the fact that $h^0(L) \leq k^0(L) - 1$. $\square$

Second, we prove the analogue of the geometric theorem that $l(D) \leq 1 + \deg D$ if D is effective.

22. Proposition. *Let K be a number field of number field of degree n over $\mathbb{Q}$ and let L be a metrized line bundle with* $\deg L \geq 0$*. Then we have*

$$h^0(L) \leq n\log\omega + \tfrac{1}{2}n\log n + \deg L.$$

PROOF. Let λ be the minimum of the lattice L. The assumption $\deg L \geq 0$ translates into $N(L) \geq 1$. Using proposition 12, the fact that $\gamma_i \leq n$ and lemma 20, we get

$$k^0(L) \leq \omega^n \max\{1, \left(\frac{n}{\lambda}\right)^n\} \leq \omega^n \max\{1, \frac{n^n}{n^{n/2}} N(L)\} = \omega^n n^{n/2} N(L).$$

Finally, take the logarithm to prove the proposition. □

The third analogue is Clifford's theorem for number fields, of which a sneak preview was given in section 2, theorem 2.

23. THEOREM (Clifford's theorem). *Let K be a number field of degree n over $\mathbb{Q}$ and let L be a metrized line bundle with $\deg L \geq 0$ and $\deg L^\dagger \geq 0$. Then we have*

$$h^0(L) \leq n \log \omega + n \log n + \tfrac{1}{2} \deg L.$$

PROOF. By corollary 15, we have $k^0(M) \leq \omega^n n^n \max\{1, 1/\mu\}^{n/2}$, where M is either L or $L^\dagger$ and μ is the minimum of M. Using $1/\mu \leq N(M)^{1/n}$, we get

$$k^0(M) \leq \omega^n n^n N(M)^{1/2}.$$

and hence

$$h^0(M) \leq n \log \omega + n \log n + \tfrac{1}{2} \deg M.$$

Using Riemann-Roch, we also have

$$h^0(M^\dagger) \leq n \log \omega + n \log n + \tfrac{1}{2} \deg M^\dagger.$$

As we have $L = M$ or $L = M^\dagger$, this proves the theorem. □

References

[1] P. FRANCINI, The function h^0 for quadratic number fields, these proceedings. [The size function h^0 for quadratic number fields, *Journal de Théorie des Nombres de Bordeaux* **13** (2001), pp. 125–135.]

[2] W. FULTON, *Algebraic Curves*, Addison Wesley, 1989.

[3] G. VAN DER GEER and R. SCHOOF, Effectivity of Arakelov Divisors and the Theta Divisor of a Number Field, preprint 1999, version 3. URL: *http://xxx.lanl.gov/abs/math/9802121.*
[Effectivity of Arakelov Divisors and the Theta Divisor of a Number Field, *Selecta Mathematica, New Series* **6** (2000), pp. 377–398.]

[4] R. HARTSHORNE, *Algebraic Geometry*, Springer-Verlag, 1977.

[5] J. NEUKIRCH, *Algebraische Zahlentheorie*, Springer-Verlag, 1992.

TORELLI FOR NUMBER FIELDS

Richard P. Groenewegen

Abstract — When we view number fields as analogues of curves, the analogue of a line bundle on a curve is an Arakelov divisor or metrized line bundle over the ring of integers. A metrized line bundle is a projective module of rank 1 over the ring of integers and it has an inner product on its tensor product with the real numbers. Given a metrized line bundle L, we use the inner product to produce a weighted sum $h^0(L)$ over the points in L. The function h^0 was proposed by Van der Geer and Schoof and they remarked that, when given the metrized line bundles of certain degree together with this function h^0, one should be able to reconstruct the number field. This is the analogue of Torelli's theorem for curves. We make this remark precise and prove a weaker form where we are given all metrized line bundles instead of just the ones of a particular degree. We discuss in what ways the theorem might be generalized and what problems occur in trying to prove the generalizations.

1. Introduction

It is well accepted to view number fields as analogues of curves. In the correspondence between curves and number fields, the analogue of the divisor on a curve is an Arakelov divisor. Van der Geer and Schoof introduced in [2] the notion of the size of an Arakelov divisor. This is also related to earlier work of Iwasawa [4] and Tate [7]. Given an Arakelov divisor D, the size $h^0(D)$ can be interpreted as an analogue of the dimension of the vector space of sections of the line bundle associated to a geometric divisor on an algebraic curve. Using the size function h^0, arithmetical analogues of standard geometrical theorems like the Riemann-Roch theorem can be stated and proved, as is done in [2]. In [3], the definition of the size function is repeated using the language of metrized line bundles instead of Arakelov divisors and an arithmetic analogue of Clifford's theorem is given.

This article deals with an analogue of Torelli's theorem. The interest for Torelli's theorem was raised by the following remark in [2]:

> *"Let $d = \frac{1}{2}\log|\Delta|$. We view the restriction of the function h^0 to $\mathrm{Pic}^{(d)}(F)$ as the analogue of the theta divisor Θ. The function h^0 is a real analytic function on the space $\mathrm{Pic}^{(d)}(F)$. It should be possible to reconstruct the arithmetic of the number field F from $\mathrm{Pic}^{(d)}$ together with this function."*

This remark refers to Torelli's theorem that says that a curve is uniquely determined by its canonically polarized Jacobian (see [6]). Part of the problem we face is making the remark above precise and another part of the problem is proving our precise statement. The two problems combined, however, have the virtue that we can customize the precise statement to what we can prove. Consequently, there are some conditions in our suggested analogue of Torelli's theorem that we would like to relax. For instance, contrary to what the remark above suggests, we will not restrict the

function h^0 to $\mathrm{Pic}^{(d)}$, but use the function h^0 on the entire Picard group. In the last section of this article we discuss briefly what kind of problems arise when we use weaker conditions.

Let K be a number field with ring of integers O_K. Write $S_{\mathrm{fin}}K$ for the set of finite primes of K and $S_\infty K$ for the set of infinite primes. The group of divisors $\mathrm{Div}\, K$ is defined as the group

$$\mathbb{R}^{S_\infty K} \times \bigoplus_{\mathfrak{p}\in S_{\mathrm{fin}}K} \mathbb{Z}.$$

A divisor D has a corresponding fractional ideal I defined by $I = \prod_{\mathfrak{p}\in S_{\mathrm{fin}}K} \mathfrak{p}^{-D_\mathfrak{p}}$. Furthermore, every element $x \in I$ has an absolute value $\|x\|$ given by

$$\|x\|^2 = \sum_{\mathfrak{p}\in S_\infty K} n(\mathfrak{p})|x|_\mathfrak{p}^2 e^{-2D_\mathfrak{p}/n(\mathfrak{p})},$$

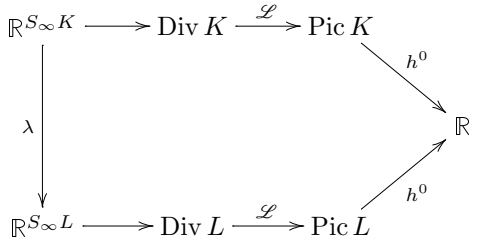
where $|\cdot|_\mathfrak{p}\colon K_\mathfrak{p} \to \mathbb{R}$ is the usual absolute value and $n(\mathfrak{p})$ is equal to the degree $[K_\mathfrak{p} : \mathbb{R}]$. We will define metrized line bundles in section 2, but for now it is sufficient to know that an isomorphism class of metrized line bundles can be represented by giving a fractional ideal and an absolute value for every element in the ideal. The set of isomorphism classes of metrized line bundles on K is called $\mathrm{Pic}\, K$ and we get a map

$$\mathscr{L}\colon \mathrm{Div}\, K \longrightarrow \mathrm{Pic}\, K.$$

We have a natural map $h^0\colon \mathrm{Pic}\, K \to \mathbb{R}$ defined as follows. Given an element Λ of $\mathrm{Pic}\, K$, represented by an ideal of K, which we will also call Λ, and an absolute value $\|\cdot\|$, we have

$$h^0(\Lambda) = \log \sum_{x\in\Lambda} e^{-\pi\|x\|^2}.$$

Let L be another number field. We will prove a theorem that says that there is an isomorphism $K \to L$ if and only if there exists a map $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ satisfying certain conditions such that the diagram



is commutative. We will also check that the map λ is induced by the isomorphism $K \to L$. The condition we impose on λ is that it is a 'strongly monomial' map. This terminology is invented specifically for this article and it is not used anywhere else in the literature. We call a map $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ *monomial* if it is a

non-singular $\mathbb{R}$-linear map which can be represented by a matrix with exactly one nonzero entry in each row and in each column. We can state this more precisely as follows. The map λ is monomial if there exists an element $x \in (\mathbb{R}^*)^{S_\infty K}$ and a bijection $\tau\colon S_\infty L \to S_\infty K$ such that λ is equal to the composition of coordinate-wise multiplication by x, followed by the map $\tau^*\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ induced by τ. If we denote multiplication by x by $m_x\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty K}$, we can write

$$\lambda = \tau^* \circ m_x.$$

We call the map λ *strongly monomial* if the underlying bijection τ respects the degree of the primes. More precisely, λ is strongly monomial if there are $x \in (\mathbb{R}^*)^{S_\infty K}$ and a bijection $\tau\colon S_\infty L \to S_\infty K$ such that λ is equal to $\tau^* \circ m_x$ and we have

$$[L_\mathfrak{p} : \mathbb{R}] = [K_{\tau(\mathfrak{p})} : \mathbb{R}] \qquad \text{for all } \mathfrak{p} \in S_\infty L.$$

We write h^0_K for the composition of the maps

$$\mathbb{R}^{S_\infty K} \longrightarrow \operatorname{Div} K \xrightarrow{\mathscr{L}} \operatorname{Pic} K \xrightarrow{h^0} \mathbb{R}.$$

Using this notation, the statement that the diagram above commutes can be written more succinctly as $h^0_K = h^0_L \circ \lambda$.

We denote the set of field isomorphisms from K to L by $\operatorname{Isom}(K, L)$. When K and L are not isomorphic, this set is empty. Suppose $\phi\colon K \to L$ is an isomorphism. Then this map induces a bijection $\phi^*\colon S_\infty L \to S_\infty K$ and this induces a strongly monomial map $\phi^{**}\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ such that we have $h^0_K = h^0_L \circ \phi^{**}$. The next theorem says that all strongly monomial maps λ with $h^0_K = h^0_L \circ \lambda$ are of the form ϕ^{**}. By a CM-field we mean a totally imaginary quadratic extension of a totally real field.

1. Theorem. *Let K and L be number fields. Then the map*

$$\operatorname{Isom}(K, L) \longrightarrow \{\, \textit{strongly monomial } \lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L} : h^0_K = h^0_L \circ \lambda \,\}$$

given by $\phi \mapsto \phi^{**}$ is surjective. The map is injective unless K and L are isomorphic CM-fields. When K and L are isomorphic CM-fields the map is 2 to 1 and ϕ and ϕ' in $\operatorname{Isom}(K, L)$ have the same image if and only if they are the same or each other's complex conjugate.

The bulk of this article is concerned with the proof of this theorem. The first and easiest step in the proof shows that if a monomial map $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ satisfies $h^0_K = h^0_L \circ \lambda$, it is equal to τ^* for some bijection $\tau\colon S_\infty L \to S_\infty K$. It is useful however to allow (strongly) monomial maps. To see why, we note that the map $\mathscr{L}\colon \operatorname{Div} K \to \operatorname{Pic} K$, we presented is not a canonical map. For $x \in (\mathbb{R}^*)^{S_\infty K}$ we write $m_x\colon \operatorname{Div} K \to \operatorname{Div} K$ for the map that multiplies an Arakelov divisor coordinate-wise with x and leaves the coordinates at the finite primes untouched. In lemma 4, we will prove that every 'reasonable' map $\mathscr{L}'\colon \operatorname{Div} K \to \operatorname{Pic} K$ is of the form $\mathscr{L}' = \mathscr{L} \circ m_x$ for some $x \in (\mathbb{R}^*)^{S_\infty K}$. Say we do not agree with the scaling used in the definition of $\mathscr{L}$ and we use another map $\mathscr{L}'\colon \operatorname{Div} K \to \operatorname{Pic} K$ of the form $\mathscr{L} \circ m_x$ instead of $\mathscr{L}$. Likewise, we may have preferred to use a map $\mathscr{L}''\colon \operatorname{Div} L \to \operatorname{Pic} L$ of the form $\mathscr{L}' = \mathscr{L} \circ m_y$ for an element $y \in (\mathbb{R}^*)^{S_\infty L}$. Now the following follows trivially from theorem 1.

2. Corollary. *Let K, L, $\mathscr{L}'$, $\mathscr{L}''$, x and y be given as above. Then the map*

$$\mathrm{Isom}(K,L) \longrightarrow \{\textit{strongly monomial } \lambda : \begin{array}{ccccc} \mathbb{R}^{S_\infty K} & \to & \mathrm{Div}\, K & \xrightarrow{\mathscr{L}'} & \mathrm{Pic}\, K \\ \downarrow{\scriptstyle \lambda} & & & & \searrow^{h^0} \\ \mathbb{R}^{S_\infty L} & \to & \mathrm{Div}\, L & \xrightarrow{\mathscr{L}''} & \mathrm{Pic}\, L \end{array} \mathbb{R} \quad \textit{commutes}\}$$

given by $\phi \mapsto m_y^{-1} \circ \phi^{**} \circ m_x$ is surjective. The map is injective unless K and L are isomorphic CM-fields and the map is 2-to-1 if they are CM-fields, in the same way as in theorem 1.

If there are values c and $r \in \mathbb{R}^*$ for which we have $y_\mathfrak{p} = x_\mathfrak{p} = r$ for all real primes $\mathfrak{p}$ and $y_\mathfrak{q} = x_\mathfrak{q} = c$ for all complex primes $\mathfrak{q}$, then $m_y^{-1} \circ \phi^{**} \circ m_x$ is equal to ϕ^{**} and in that case corollary 2 has the same form as theorem 1.

The proof of theorem 1 is divided over three sections. In section 4 we prove that every monomial $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ with $h^0_K = h^0_L \circ \lambda$ is of the form $\lambda = \tau^*$ with $\tau\colon S_\infty L \to S_\infty K$ a bijection. This follows in just a few steps from the Riemann-Roch theorem for number fields. In section 5, we write h^0_K in terms of something which we call the multi-length of K. The multi-length is a function $\mathbb{R}^{S_\infty K} \to \mathbb{Z}$ given by

$$y \longmapsto \#\{\, a \in O_K : y_\mathfrak{p} = |a|^2_\mathfrak{p} \text{ for all } \mathfrak{p} \in S_\infty K \,\}.$$

We use standard analysis to prove that the multi-length of K and the multi-length of L are 'the same' if we have $h^0_K = h^0_L \circ \tau^*$. In section 6, we embed K and L in a number field $M \subset \mathbb{C}$ which is Galois over $\mathbb{Q}$. We write $G = \mathrm{Gal}(M/\mathbb{Q})$ and let S be the G-set of embeddings of K in M and T the G-set of embeddings of L in M. Proving that K and L are isomorphic is the same as proving that S and T are isomorphic G-sets. We take a prime $\mathfrak{q} \in S_{\mathrm{fin}} M$ above a prime in $\mathbb{Q}$ that splits completely. Using the bijection $\tau\colon S_\infty L \to S_\infty K$, identify $S_\infty K = S_\infty$ and $S_\infty L$ and assume the multi-length functions of K and L are the same. Consider the set

$$\{\, (|a|^2_\mathfrak{p})_{\mathfrak{p} \in S_\infty} : a \in O_K \,\} = \{\, (|a|^2_\mathfrak{p})_{\mathfrak{p} \in S_\infty} : a \in O_L \,\}.$$

This set is actually contained in $(O_M \cap \mathbb{R})^{S_\infty}$. Now, on each coordinate we can apply the map $v\colon O_M \smallsetminus \{0\} \to \mathbb{Z}^G_{\geq 0}$ given by $x \mapsto (\mathrm{ord}_\mathfrak{q}\, \sigma x)_{\sigma \in G}$ and in this way we get a subset of $\mathbb{Z}^{G \times S_\infty}_{\geq 0}$ on which we have a natural G-action. Assuming we are not in the CM-case, it turns out that the elements in the subset with 'minimal sum' form a G-set which is isomorphic to S and by symmetry also to T. Hence, the G-sets S and T are isomorphic.

In section 7, we address possible improvements of theorem 1 and the kinds of problems that arise when we try to prove them.

2. Metrized line bundles and Arakelov divisors

The setting is the same as in the introduction. We have a number field K with ring of integers $O = O_K$. We write $S_{\text{fin}}K$ for the set of finite primes of K and $S_\infty K$ for the set of infinite primes. When there is no confusion possible about the number field we are working in, we omit the K from the notation and simply write S_{fin} and S_∞. We define the group of divisors as

$$\operatorname{Div} K = \mathbb{R}^{S_\infty} \times \bigoplus_{\mathfrak{p} \in S_{\text{fin}}} \mathbb{Z}.$$

For $x \in \mathbb{R}^{S_\infty}$ we write $m_x \colon \operatorname{Div} K \longrightarrow \operatorname{Div} K$ for the map that multiplies a divisor coordinate-wise with x at infinity and leaves the finite coordinates untouched.

Divisors are closely related to metrized line bundles, which we will define next. It would have been possible to use Arakelov divisors exclusively in this article and not mention metrized line bundles at all, but the language of metrized line bundles makes it easier to justify the definitions and the theorems. For instance, there are canonical definitions of h^0 and degree on metrized line bundles, whereas on $\operatorname{Div} K$ it depends on the scaling of the coordinates at the infinite primes. The proofs of the properties stated here can be found in [3].

Let Λ be a projective module of rank 1 over O. Then $\Lambda_\mathbb{R} = \Lambda \otimes_\mathbb{Z} \mathbb{R}$ is a finite étale algebra over $\mathbb{R}$ and we can write

$$\Lambda_\mathbb{R} = \prod_{\mathfrak{p} \in S_\infty} \Lambda_\mathfrak{p} \qquad \text{with} \quad \Lambda_\mathfrak{p} = \Lambda \otimes_O K_\mathfrak{p}.$$

Each factor $\Lambda_\mathfrak{p}$ is a 1-dimensional vector space over $K_\mathfrak{p}$. Clearly, $\Lambda_\mathbb{R}$ is a module over

$$O_\mathbb{R} = O \otimes_\mathbb{Z} \mathbb{R} = \prod_{\mathfrak{p} \in S_\infty} K_\mathfrak{p}.$$

On each factor $K_\mathfrak{p}$, we have complex conjugation and this yields a convolution $*$ on $O_\mathbb{R}$, given by complex conjugation on each coordinate. A positive definite symmetric $\mathbb{R}$-bilinear map

$$\langle \cdot\,, \cdot \rangle \colon \Lambda_\mathbb{R} \times \Lambda_\mathbb{R} \longrightarrow \mathbb{R}$$

is called a hermitian structure if for all $a, b \in \Lambda_\mathbb{R}$ and for all $m \in O_\mathbb{R}$, we have $\langle a, mb \rangle = \langle m^* a, b \rangle$. A projective O-module Λ of rank 1 with a hermitian structure on $\Lambda_\mathbb{R}$ is called a *metrized line bundle*.

We call elements a and b perpendicular and write $a \perp b$ if we have $\langle a, b \rangle = 0$. Two sets A and B are perpendicular if for all $a \in A$ and $b \in B$, the elements a and b are perpendicular. If Λ is a metrized line bundle and $\mathfrak{p}$ is an infinite prime, we view $\Lambda_\mathfrak{p}$ as a subspace of $\Lambda_\mathbb{R}$. It follows from the definition that for any two infinite primes $\mathfrak{p}, \mathfrak{q} \in S_\infty$ with $\mathfrak{p} \neq \mathfrak{q}$, the factors $\Lambda_\mathfrak{p}$ and $\Lambda_\mathfrak{q}$ are perpendicular. Also, when

$\mathfrak{p}$ is a complex prime and $i \in K_\mathfrak{p}$ is an element with $i^2 = -1$, we have $ia \perp a$ for all $a \in \Lambda_\mathfrak{p}$ and we also have $\langle a, a\rangle = \langle ia, ia\rangle$.

A metrized line bundle Λ has a norm map

$$\|\cdot\|\colon \Lambda_\mathbb{R} \longrightarrow \mathbb{R}_{\geq 0},$$

given by $\|x\| = \langle x, x\rangle^{1/2}$ for $x \in \Lambda_\mathbb{R}$. The inner product is uniquely determined by the norm map. For each infinite prime $\mathfrak{p}$, we have a local norm map

$$\|\cdot\|_\mathfrak{p}\colon \Lambda_\mathfrak{p} \longrightarrow \mathbb{R}_{\geq 0}$$

that is the restriction of the norm map to $\Lambda_\mathfrak{p} \subset \Lambda_\mathbb{R}$. Given a projective O-module Λ of rank 1 and a nonzero element $\lambda \in \Lambda$, specifying a hermitian structure on $\Lambda_\mathbb{R}$ is equivalent to specifying a positive value $\|\lambda\|_\mathfrak{p}$ for every $\mathfrak{p} \in S_\infty$. The norm map is then given by

$$\|x\|^2 = \sum_{\mathfrak{p}\in S_\infty} \|x_\mathfrak{p}\|_\mathfrak{p}^2, \qquad \text{for} \quad x \in \Lambda_\mathbb{R}.$$

We are using here that $\Lambda_\mathfrak{p}$ is 1-dimensional over $K_\mathfrak{p}$, that $i\lambda$ and λ are perpendicular and have the same length and that for $\alpha \in \mathbb{R}$, we have $\|\alpha\lambda\|_\mathfrak{p} = |\alpha|\|\lambda\|_\mathfrak{p}$.

Metrized line bundles can be multiplied in a natural way. Let Λ and M be two metrized line bundles. The product $\Lambda\mathrm{M}$ is the module $\Lambda \otimes_O \mathrm{M}$ with a hermitian structure defined as follows. The $\mathbb{R}$-module $\Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R}$ has a natural inner product which is uniquely determined by

$$\langle \lambda \otimes \mu, \lambda' \otimes \mu'\rangle = \langle \lambda, \lambda'\rangle\langle \mu, \mu'\rangle \qquad \text{for all} \quad \lambda, \lambda' \in \Lambda,\ \mu, \mu' \in \mathrm{M}.$$

Now $(\Lambda\mathrm{M})_\mathbb{R}$ is a quotient of $\Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R}$. This means that we have a natural surjective homomorphism

$$\phi\colon \Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R} \twoheadrightarrow \Lambda_\mathbb{R} \otimes_{O_\mathbb{R}} \mathrm{M}_\mathbb{R} \cong (\Lambda\mathrm{M})_\mathbb{R}.$$

Hence, $(\Lambda\mathrm{M})_\mathbb{R}$ is isomorphic to the orthogonal complement $(\ker\phi)^\perp$ of the kernel of this map. As a subspace of $\Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R}$, the space $(\ker\phi)^\perp$ is endowed with a natural hermitian structure and $(\Lambda\mathrm{M})_\mathbb{R}$ is given the induced hermitian structure.

3. Lemma. *Let Λ and M be two metrized line bundles over O with norm maps $\|\cdot\|_\Lambda$ and $\|\cdot\|_\mathrm{M}$. Write $\|\cdot\|$ for the norm map of $\Lambda\mathrm{M}$. Then for all $\mathfrak{p} \in S_\infty$ and all $\lambda \in \Lambda$ and $\mu \in \mathrm{M}$ we have*

$$\|\lambda \otimes \mu\|_\mathfrak{p}^2 = \frac{1}{[K_\mathfrak{p} : \mathbb{R}]}\|\lambda\|_{\Lambda,\mathfrak{p}}^2\|\mu\|_{\mathrm{M},\mathfrak{p}}^2.$$

Proof. The map $\phi\colon \Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R} \to (\Lambda\mathrm{M})_\mathbb{R}$ factors as

$$\Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R} = \prod_{\mathfrak{p},\mathfrak{q}\in S_\infty} \Lambda_\mathfrak{p} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{q} \longrightarrow \prod_{\mathfrak{p}\in S_\infty} \Lambda_\mathfrak{p} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{p} \longrightarrow \prod_{\mathfrak{p}\in S_\infty} \Lambda_\mathfrak{p} \otimes_{K_\mathfrak{p}} \mathrm{M}_\mathfrak{p} = (\Lambda\mathrm{M})_\mathbb{R}.$$

Let $\lambda \in \Lambda$ and $\mu \in \mathrm{M}$ be two nonzero elements. For a real prime $\mathfrak{p}$, the map $\phi_\mathfrak{p}\colon \Lambda_\mathfrak{p} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{p} \to \Lambda_\mathfrak{p} \otimes_{K_\mathfrak{p}} \mathrm{M}_\mathfrak{p}$ is the identity map and therefore $\lambda \otimes \mu$ is an element in $(\ker \phi_\mathfrak{p})^\perp$, mapping to $\lambda \otimes \mu \in \Lambda_\mathfrak{p} \otimes_{K_\mathfrak{p}} \mathrm{M}_\mathfrak{p}$. Hence, $\lambda \otimes \mu \in \Lambda_\mathfrak{p} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{p} \subset \Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R}$ is also in $(\ker \phi)^\perp$ and we clearly have $\|\lambda \otimes \mu\|_\mathfrak{p}^2 = \|\lambda\|_{\Lambda,\mathfrak{p}}^2 \|\mu\|_{\mathrm{M},\mathfrak{p}}^2$. A note of caution is in order here. The element $\lambda \otimes \mu \in \Lambda_\mathfrak{p} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{p} \subset \Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R}$ is zero on all the factors $\Lambda_\mathfrak{q} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{r}$ with either $\mathfrak{q} \neq \mathfrak{p}$ or $\mathfrak{r} \neq \mathfrak{p}$. This element is *not* equal to the element $\lambda \otimes \mu \in \Lambda_\mathbb{R} \otimes_\mathbb{R} \mathrm{M}_\mathbb{R}$, which is equal to $\lambda \otimes \mu$ on all the factors $\Lambda_\mathfrak{q} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{r}$. The local norm at $\mathfrak{p}$ is the same in both cases, however.

Although the proof for the case where we have a real prime $\mathfrak{p}$ may seem a bit intimidating, the point is that nothing is actually happening because $\phi_\mathfrak{p}$ is the identity map. The map $\phi_\mathfrak{p}\colon \Lambda_\mathfrak{p} \otimes_\mathbb{R} \mathrm{M}_\mathfrak{p} \to \Lambda_\mathfrak{p} \otimes_{K_\mathfrak{p}} \mathrm{M}_\mathfrak{p}$ is only interesting when $\mathfrak{p}$ is a complex prime. So, suppose $\mathfrak{p}$ is complex. Then the kernel of $\phi_\mathfrak{p}$ is the $\mathbb{R}$-vector space generated by $\lambda \otimes \mu + \lambda i \otimes \mu i$ and $\lambda i \otimes \mu - \lambda \otimes \mu i$. Because we have $\lambda i \perp \lambda$ and $\mu i \perp \mu$, the element

$$\frac{-\lambda i \otimes \mu i + \lambda \otimes \mu}{2}$$

is in $(\ker \phi_\mathfrak{p})^\perp$ and it clearly maps to $\lambda \otimes \mu \in \Lambda_\mathfrak{p} \otimes_{K_\mathfrak{p}} \mathrm{M}_\mathfrak{p}$. The square of the local norm of $(-\lambda i \otimes \mu i + \lambda \otimes \mu)/2$ is equal to

$$\frac{\|\lambda i\|_{\Lambda,\mathfrak{p}}^2 \|\mu i\|_{\mathrm{M},\mathfrak{p}}^2 + \|\lambda\|_{\Lambda,\mathfrak{p}}^2 \|\mu\|_{\mathrm{M},\mathfrak{p}}^2}{4} = \frac{1}{2}\|\lambda\|_{\Lambda,\mathfrak{p}}^2 \|\mu\|_{\mathrm{M},\mathfrak{p}}^2.$$

This proves our lemma in the same way as for the real case. □

Two metrized line bundles are isomorphic if they are isomorphic as O-modules and the isomorphism preserves the hermitian structure. The multiplication defined above induces a group structure on the set of isomorphism classes of metrized line bundles. This group is called the Picard group and is denoted $\operatorname{Pic} K$. The unit element of this group is the ring of integers O and the hermitian structure is given locally by $\|1\|_\mathfrak{p}^2 = [K_\mathfrak{p} : \mathbb{R}]$.

A careful inspection of the definitions we gave so far, shows that we have an exact sequence

$$0 \longrightarrow O^* \longrightarrow \mathbb{R}_{>0}^{S_\infty} \longrightarrow \operatorname{Pic} K \longrightarrow \operatorname{Cl} K \longrightarrow 0,$$

where $\operatorname{Cl} K$ is the class group of K. The map $\mathbb{R}_{>0}^{S_\infty} \to \operatorname{Pic} K$ sends an element $x \in \mathbb{R}_{>0}^{S_\infty}$ to the metrized line bundle O with hermitian structure given by $\|1\|_\mathfrak{p}^2 = [K_\mathfrak{p} : \mathbb{R}] x_\mathfrak{p}^2$ for $\mathfrak{p} \in S_\infty$. The map $O^* \to \mathbb{R}_{>0}^{S_\infty}$ sends an element η to $(|\eta|_\mathfrak{p})_{\mathfrak{p} \in S_\infty}$. As every projective O-module of rank 1 is isomorphic to an ideal of O, this yields the map $\operatorname{Pic} K \to \operatorname{Cl} K$. We give $\mathbb{R}_{>0}^{S_\infty}$ the usual Euclidean topology and give $\operatorname{Cl} K$ the discrete topology. This induces a natural *topology* on $\operatorname{Pic} K$.

Now, let D be an Arakelov divisor. Then the fractional ideal corresponding to D is defined by

$$I = \prod_{\mathfrak{p} \in S_\mathrm{fin}} \mathfrak{p}^{-D_\mathfrak{p}}.$$

As are all nonzero fractional ideals, I is a projective O-module of rank 1. We are going to use the coordinates at the infinite primes to define a hermitian structure on $I_{\mathbb{R}}$. We use the exponential map to go from additive coordinates to multiplicative coordinates. By lemma 3, we need a factor 2 in the complex case in order to get a homomorphism. For $\lambda \in I$ nonzero and $\mathfrak{p} \in S_\infty$, we define

$$\|\lambda\|_{\mathfrak{p}}^2 = \begin{cases} |\lambda|_{\mathfrak{p}}^2 \exp(-2D_{\mathfrak{p}}) & \text{if } \mathfrak{p} \text{ is real;} \\ 2|\lambda|_{\mathfrak{p}}^2 \exp(-D_{\mathfrak{p}}) & \text{if } \mathfrak{p} \text{ is complex.} \end{cases}$$

Here, $|\cdot|_{\mathfrak{p}} \colon K_{\mathfrak{p}} \to \mathbb{R}$ is the usual absolute value with $|x|_{\mathfrak{p}} = |x|$ for all $x \in \mathbb{Q}$. The map that assigns to a divisor D the line bundle I together with this hermitian structure is called

$$\mathscr{L} \colon \operatorname{Div} K \longrightarrow \operatorname{Pic} K.$$

It should be stressed however, that $\mathscr{L}$ is not the only possible map from $\operatorname{Div} K$ to $\operatorname{Pic} K$. The scaling we used above is the same that appeared in [2] and is convenient to use in this article. However, in many ways it would be better to use $\|\lambda\|_{\mathfrak{p}}^2 = 2|\lambda|_{\mathfrak{p}}^2 \exp(-2D_{\mathfrak{p}})$ for complex primes $\mathfrak{p}$. But up to scaling of the coordinates, this and any other feasible map $\operatorname{Div} K \to \operatorname{Pic} K$ is equal to $\mathscr{L}$. In fact, if we supply a topology on $\operatorname{Div} K$ by giving $\mathbb{Z}$ the discrete topology and $\mathbb{R}$ the Euclidean topology, we have the following lemma.

4. Lemma. *Let K be a number field and let*

$$\mathscr{L}' \colon \operatorname{Div} K \longrightarrow \operatorname{Pic} K$$

be a continuous homomorphism such that for all $D \in \operatorname{Div} K$ the underlying module of $\mathscr{L}'(D)$ is equal to $I = \prod_{\mathfrak{p} \in S_{\text{fin}}} \mathfrak{p}^{-D_{\mathfrak{p}}}$ and the local norm map $\|\cdot\|_{\mathfrak{p}}$ of $\mathscr{L}'(D)$ at a prime $\mathfrak{p} \in S_\infty$ only depends on $D_{\mathfrak{p}}$. Then there is an element $x \in (\mathbb{R}^*)^{S_\infty}$ with

$$\mathscr{L}' = \mathscr{L} \circ m_x.$$

Proof. This follows from lemma 3 and the fact that $x \mapsto e^x$ is the only continuous homomorphism $\mathbb{R} \to \mathbb{R}_{>0}$ that maps 1 to e. □

For a metrized line bundle Λ, we define the norm as

$$N(\Lambda) = \frac{\sqrt{|\Delta|}}{\det \Lambda},$$

where Δ is the discriminant of K. The degree is defined as $\deg \Lambda = \log N(\Lambda)$.

5. Lemma.
(1) *The degree function is a group homomorphism* $\operatorname{Pic} K \to \mathbb{R}$.
(2) *If* Λ *is metrized line bundle and* $t \in \Lambda$ *is any nonzero element, then we have*

$$\deg \Lambda = \log \#(\Lambda/Ot) - \sum_{\mathfrak{p}\in S_\infty} \log \frac{\|t\|_{\mathfrak{p}}^{[K_{\mathfrak{p}}:\mathbb{R}]}}{[K_{\mathfrak{p}} : \mathbb{R}]}.$$

(3) *The map* $(\deg \circ \mathscr{L})\colon \operatorname{Div} K \to \mathbb{R}$ *sends a divisor* D *to*

$$\deg \mathscr{L}(D) = \sum_{\mathfrak{p}\in S_{\mathrm{fin}}} D_{\mathfrak{p}} \log N(\mathfrak{p}) + \sum_{\mathfrak{p}\in S_\infty} D_{\mathfrak{p}}.$$

Proof. The first two statements are proved in [3, proposition 6.3]. It is possible to derive the third statement from (2) but we choose to prove it directly. It suffices to prove

$$N(\mathscr{L}(D)) = N(I)^{-1} \prod_{\mathfrak{p}\in S_\infty} \exp(D_{\mathfrak{p}}),$$

where $I = \prod_{\mathfrak{p}\in S_{\mathrm{fin}}} \mathfrak{p}^{-D_{\mathfrak{p}}}$ is the underlying ideal of $\mathscr{L}(D)$. When $D_{\mathfrak{p}}$ is 0 for all $\mathfrak{p} \in S_\infty$, this formula is obviously correct. When $D_{\mathfrak{p}}$ is nonzero at some real prime $\mathfrak{p}$, the metrics are scaled with a factor $\exp(-D_{\mathfrak{p}})$ at that prime and hence the determinant is scaled with a factor $\exp(D_{\mathfrak{p}})$. When $D_{\mathfrak{p}}$ is nonzero at some complex prime $\mathfrak{p}$, the metrics are scaled at that prime with a factor $\exp(-D_{\mathfrak{p}}/2)$, and therefore the determinant is scaled with a factor $\exp(D_{\mathfrak{p}})$ also. □

3. The functions k^0 and h^0

Following Van der Geer and Schoof [2], we define a function $k^0\colon \operatorname{Pic} K \longrightarrow \mathbb{R}_{>0}$ by

$$k^0(\Lambda) = \sum_{x\in\Lambda} e^{-\pi\langle x,x\rangle}.$$

Furthermore, we define $h^0\colon \operatorname{Pic} K \to \mathbb{R}$ by $h^0(\Lambda) = \log k^0(\Lambda)$. Let $\operatorname{Pic}^{(0)} K$ be the kernel of the degree map $\deg\colon \operatorname{Pic} K \to \mathbb{R}$. We first prove that $\operatorname{Pic}^{(0)} K$ is a compact group and then we give a variant of the Riemann-Roch theorem, linking the function h^0 to the degree map.

6. Lemma. *Let* K *be a number field. Then* $\operatorname{Pic}^{(0)} K$ *is a compact group.*

Proof. Let $l\colon \mathbb{R}_{>0}^{S_\infty} \to \mathbb{R}^{S_\infty}$ be the map given by

$$x \longmapsto ([K_{\mathfrak{p}} : \mathbb{R}] \log x_{\mathfrak{p}})_{\mathfrak{p}\in S_\infty}.$$

The map l is an isomorphism of topological groups. We let $O^* \to \mathbb{R}^{S_\infty}$ be the composition of the maps $O^* \to \mathbb{R}^{S_\infty}_{>0}$ and l and we get an exact sequence

$$0 \longrightarrow O^* \longrightarrow \mathbb{R}^{S_\infty} \longrightarrow \operatorname{Pic} K \longrightarrow \operatorname{Cl} K \longrightarrow 0.$$

When we apply the map $\mathbb{R}^{S_\infty}_{>0} \to \operatorname{Pic} K$ to an element $x \in \mathbb{R}^{S_\infty}_{>0}$, we see from lemma 5 that we get an element of degree 0 if and only if $\prod_{\mathfrak{p}\in S_\infty} x_{\mathfrak{p}}^{[K_\mathfrak{p}:\mathbb{R}]} = 1$ holds. Using the map l, this corresponds to the elements of $\mathbb{R}^{S_\infty}$ with the sum of the coordinates equal to 0. Let H be the hyperplane $\{\, x \in \mathbb{R}^{S_\infty} : \sum_{\mathfrak{p}\in S_\infty} x_\mathfrak{p} = 0 \,\}$. Then we have an exact sequence

$$0 \longrightarrow H/\operatorname{im} O^* \longrightarrow \operatorname{Pic}^{(0)} K \longrightarrow \operatorname{Cl} K \longrightarrow 0.$$

By the Dirichlet unit theorem (see [5, section V.1]), the group $\operatorname{im} O^* \subset H$ forms a lattice of full rank. It follows that the topological group $H/\operatorname{im} O^*$ is compact. Hence, $\operatorname{Pic}^{(0)} K$ has a compact subgroup of finite index and is therefore itself compact. □

7. Lemma. *Let K be a number field. We have*

$$\lim_{d\to-\infty} \sup_{\substack{\Lambda\in\operatorname{Pic} K\\ \deg\Lambda=d}} h^0(\Lambda) = 0.$$

Proof. This follows from some elementary estimates of the functions h^0 and this lemma is also a weak form of [3, proposition 7.2]. □

8. Theorem (*Riemann-Roch*). *Let Λ be a metrized line bundle with non-negative degree. Then we have*

$$\lim_{\substack{n\in\mathbb{Z}\\ n\to\infty}} \frac{h^0(\Lambda^n)}{n} = \deg\Lambda \quad \textit{and} \quad \lim_{\substack{n\in\mathbb{Z}\\ n\to-\infty}} \frac{h^0(\Lambda^n)}{n} = 0.$$

Proof. If the degree of Λ is zero then for each $n \in \mathbb{Z}$, we have $\Lambda^n \in \operatorname{Pic}^{(0)} K$. Because $\operatorname{Pic}^{(0)} K$ is a compact group by lemma 6, and $h^0\colon \operatorname{Pic} K \to \mathbb{R}$ is continuous, the set $\{\, h^0(\Lambda^n) : n \in \mathbb{Z} \,\}$ is bounded. Consequently, the two limits above are both equal to 0 and of course also both equal to $\deg\Lambda$.

Now assume $\deg\Lambda > 0$. The second limit follows directly from lemma 7. Write $\Lambda^\dagger = \operatorname{Hom}(L, \mathbb{Z})$. Consider the map

$$\Lambda_\mathbb{R} \longrightarrow \operatorname{Hom}_\mathbb{R}(\Lambda_\mathbb{R}, \mathbb{R}) = \Lambda^\dagger_\mathbb{R},$$

given by $x \longmapsto \langle x, \cdot\,\rangle$. This map is an isomorphism, giving $\Lambda^\dagger_\mathbb{R}$ a canonical hermitian structure. The Riemann-Roch theorem (see [3, proposition 19]) says that we have

$$h^0(\Lambda) - \frac{1}{2}\deg\Lambda = h^0(\Lambda^\dagger) - \frac{1}{2}\deg\Lambda^\dagger,$$

We have $\det \Lambda^\dagger = (\det \Lambda)^{-1}$ and therefore we have $\deg \Lambda^\dagger = -\deg \Lambda + \log|\Delta|$. When we do the same for Λ^n instead of Λ, we get

$$\deg(\Lambda^n)^\dagger = -\deg \Lambda^n + \log|\Delta| = -n \deg \Lambda + \log|\Delta|.$$

We substitute this in the Riemann-Roch formula and we obtain

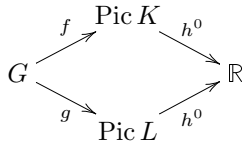
$$h^0(\Lambda^n) = n \deg \Lambda - \frac{1}{2}\log|\Delta| + h^0((\Lambda^n)^\dagger).$$

As the degree of $(\Lambda^n)^\dagger$ goes to minus infinity when n goes to infinity, the value of $h^0((\Lambda^n)^\dagger)$ tends to 0 by lemma 7. Dividing by n and taking the limit for n to infinity yields the theorem. □

4. The monomial map is induced by a bijection

In this section we handle the first step in the proof of theorem 1. We prove that if $\lambda = \tau^* \circ m_x$ is a monomial map $\mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ with $h^0_K = h^0_L \circ \lambda$, the element x is equal to 1 and λ is actually equal to τ^*. This turns out to follow quite easily from the Riemann-Roch theorem. We use a lemma.

9. Lemma. *Let K and L be number fields and let G be a group. Suppose that $f\colon G \to \operatorname{Pic} K$ and $g\colon G \to \operatorname{Pic} L$ are homomorphisms such that the diagram*



commutes. Then we have $\deg \circ f = \deg \circ g$.

Proof. Let x be an element of G. By theorem 8, we have

$$\max\Big\{ \lim_{\substack{n\in\mathbb{Z}\\ n\to\infty}} \frac{h^0(f(x^n))}{n}, \lim_{\substack{n\in\mathbb{Z}\\ n\to\infty}} \frac{h^0(f(x^{-n}))}{n} \Big\} = |\deg f(x)|.$$

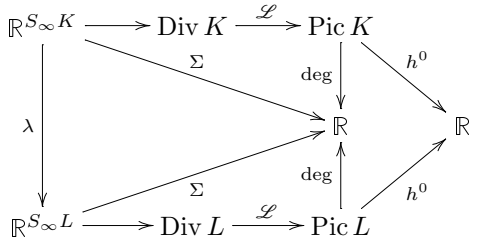
The commutativity of the diagram now ensures that we have $|\deg f(x)| = |\deg g(x)|$. Furthermore, we have

$$\deg f(x) > 0 \iff \lim_{\substack{n\in\mathbb{Z}\\ n\to\infty}} \frac{h^0(f(x^n))}{n} > 0 \iff \lim_{\substack{n\in\mathbb{Z}\\ n\to\infty}} \frac{h^0(g(x^n))}{n} > 0 \iff \deg g(x) > 0.$$

It follows that $\deg g(x)$ is equal to $\deg f(x)$. □

10. Proposition. *Let K and L be number fields and let $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ be a monomial map with $h^0_K = h^0_L \circ \lambda$. Then there is a bijection $\tau\colon S_\infty L \to S_\infty K$ such that λ is equal to τ^*.*

Proof. Write $\Sigma\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}$ for the map $y \mapsto \sum_{\mathfrak{p}\in S_\infty K} y_\mathfrak{p}$ and also write $\Sigma\colon \mathbb{R}^{S_\infty L} \to \mathbb{R}$ for the corresponding map for L. Using lemma 5 part (2) and lemma 9, we see that the diagram



commutes. In other words, we have $\Sigma(y) = \Sigma(\lambda(y))$ for all $y \in S_\infty K$. Because λ is monomial, by definition there is a bijection $\tau\colon S_\infty L \to S_\infty K$ and an element $x \in (\mathbb{R}^*)^{S_\infty K}$ with $\lambda = \tau^* \circ m_x$. Let $\mathfrak{p}$ be any element of $S_\infty K$ and let y be the element of $\mathbb{R}^{S_\infty K}$ with $y_\mathfrak{p} = 1$ and $y_\mathfrak{q} = 0$ for all $\mathfrak{q} \in S_\infty K \smallsetminus \{\mathfrak{p}\}$. Then we have $1 = \Sigma(y) = \Sigma(\lambda(y)) = x_\mathfrak{p} \cdot 1$ and we conclude that $x_\mathfrak{p}$ is equal to 1. As $\mathfrak{p}$ was chosen arbitrarily, we conclude that λ is equal to τ^*. □

5. Finding the multi-length function

Let K be a number field and write $S_\infty = S_\infty K$ and $O = O_K$. We define the map $c_K\colon \mathbb{R}^{S_\infty} \to \mathbb{Z}$ by sending $y \in \mathbb{R}^{S_\infty}$ to

$$c_K(y) = \#\{\, a \in O : y_\mathfrak{p} = |a|^2_\mathfrak{p} \text{ for all } \mathfrak{p} \in S_\infty \,\}.$$

We call c_K the multi-length of K. Furthermore, let $n = n_K\colon S_\infty \to \{1, 2\}$ be the function sending a prime $\mathfrak{p} \in S_\infty$ to the degree $n(\mathfrak{p}) = [K_\mathfrak{p} : \mathbb{R}]$. It is easy to express h^0 and k^0 in terms of the multi-length function and the degree function n, but we choose to work with a transformation of k^0. The short-term goal is to get rid of as much ugly notation as possible. We define k^0_K as the composition of the maps

$$\mathbb{R}^{S_\infty K} \longrightarrow \operatorname{Div} K \xrightarrow{\mathscr{L}} \operatorname{Pic} K \xrightarrow{k^0} \mathbb{R}_{\geq 0}.$$

Furthermore, we write $-\log\colon \mathbb{R}^{S_\infty}_{>0} \to \mathbb{R}^{S_\infty}$ for the map

$$t \longmapsto (-\log t_\mathfrak{p})_{\mathfrak{p}\in S_\infty}.$$

Let $d = d_K \colon \mathbb{R}_{>0}^{S_\infty} \to \mathbb{R}_{>0}^{S_\infty}$ be the map given on the $\mathfrak{p}$-th coordinate by

$$d(t)_\mathfrak{p} = \frac{t_\mathfrak{p}^{n(\mathfrak{p})/2}}{\pi n(\mathfrak{p})}.$$

For y and t in $\mathbb{R}^{S_\infty}$, we define the dot-product of y and t by $y \cdot t = \sum_{\mathfrak{p} \in S_\infty} y_\mathfrak{p} t_\mathfrak{p}$. Then the map $(k_K^0 \circ - \log \circ d) \colon \mathbb{R}_{>0}^{S_\infty} \to \mathbb{R}_{>0}$ can be written as

$$t \longmapsto \sum_{y \in \mathbb{R}^{S_\infty}} c_K(y) e^{-y \cdot t}.$$

Let L be another number field and assume there is a strongly monomial map λ with $h_K^0 = h_L^0 \circ \lambda$. By proposition 10, the map λ is induced by a bijection $\tau \colon S_\infty L \to S_\infty K$. Using this bijection, we can identify $S_\infty L$ with $S_\infty K = S_\infty$ and view k_L^0 and d_L as a functions on $\mathbb{R}_{>0}^{S_\infty}$ and the multi-length function c_L as a function on $\mathbb{R}^{S_\infty}$. Because the underlying permutation of λ respects the degree of the primes, the maps d_K and d_L are the same and therefore we have

$$0 = (k_K^0 \circ - \log \circ d)(t) - (k_L^0 \circ - \log \circ d)(t) = \sum_{y \in \mathbb{R}^{S_\infty}} (c_K(y) - c_L(y)) e^{-y \cdot t}$$

for all t in $\mathbb{R}_{>0}^{S_\infty}$. In this section we prove that this implies that c_K is equal to c_L.

11. Lemma. *Let S be a finite set with $\#S > 0$ and let $Y \subset \mathbb{R}_{>0}^S$ be a non-empty such that Y is closed and discrete in $\mathbb{R}^S$. Then there is an element $t \in \mathbb{R}_{>0}^S$ and an element $z \in Y$ with $y \cdot t > z \cdot t$ for all $y \in Y \smallsetminus \{z\}$.*

Proof. For every $t \in \mathbb{R}_{>0}^S$, let Y_t be the set

$$Y_t = \{\, z \in Y : z \cdot t \leq y \cdot t \text{ for all } y \in Y \,\}.$$

Because Y is closed and discrete in $\mathbb{R}^S$, every set set Y_t is finite. It is also non-empty and we need to prove there exists an element t for which Y_t contains exactly one element z. Let t be an element for which the cardinality of Y_t is minimal. In other words, we have

$$\#Y_t = \min_{t' \in \mathbb{R}_{>0}^S} \#Y_{t'}.$$

We assume that $\#Y_t$ is at least 2 and derive a contradiction. In this case, there is an element $\mathfrak{p} \in S$ and two elements z and $y \in Y_t$ with $z_\mathfrak{p} < y_\mathfrak{p}$. Without loss of generality we can and will assume that for all $y' \in Y_t$ we have $z_\mathfrak{p} \leq y'_\mathfrak{p}$. For $\varepsilon > 0$, we write t_ε for the element $\mathbb{R}_{>0}^S$ given by

$$(t_\varepsilon)_\mathfrak{q} = \begin{cases} t_\mathfrak{p} + \varepsilon & \text{if } \mathfrak{p} = \mathfrak{q}; \\ t_\mathfrak{q} & \text{otherwise.} \end{cases}$$

For every $\varepsilon > 0$ and all $y' \in Y_t$ we have $z \cdot t_\varepsilon \leq y' \cdot t_\varepsilon$ and we have $z \cdot t_\varepsilon < y \cdot t_\varepsilon$. The number of points $y' \in Y \smallsetminus Y_t$ with $y' \cdot t_\varepsilon \leq z \cdot t_\varepsilon$ is finite and for small enough values of ε this number is 0. Hence, for such an ε, we have

$$Y_{t_\varepsilon} \subset Y_t \smallsetminus \{y\}.$$

But this is a contradiction, because we assumed that $\#Y_t$ was minimal. □

12. Proposition. *Let K and L be two number fields with multi-length functions c_K and c_L and let $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ be a strongly monomial map with $h^0_K = h^0_L \circ \lambda$. Then c_K and $c_L \circ \lambda$ are equal.*

Proof. As λ is induced by a bijection $S_\infty L \to S_\infty K$, we identify $S_\infty L$ and $S_\infty K = S_\infty$. As we have seen before, the map κ given by

$$t \longmapsto \sum_{y \in \mathbb{R}^{S_\infty}} (c_K(y) - c_L(y)) e^{-y \cdot t}$$

is the zero map. Write $Y = \{\, y \in \mathbb{R}^{S_\infty} : c_K(y) - c_L(y) \neq 0 \,\}$. We want to prove that Y is empty. Assume it is not empty and let $z \in Y$ and $t \in \mathbb{R}^{S_\infty}_{>0}$ be elements such that $y \cdot t > z \cdot t$ for all $y \in Y \smallsetminus \{z\}$, as provided by lemma 11. For $u \in \mathbb{R}_{>0}$, write $g_y(u) = (c_K(y) - c_L(y)) e^{u(z \cdot t - y \cdot t)}$ and consider the function $\mathbb{R}_{>0} \to \mathbb{R}$, given by

$$u \longmapsto e^{uz \cdot t} \kappa(ut) = c_K(z) - c_L(z) + \sum_{y \in Y \smallsetminus \{z\}} g_y(u).$$

For any $u \in \mathbb{R}_{>0}$, the sum

$$\sum_{y \in Y \smallsetminus \{z\}} |g_y(u)|$$

is convergent. The terms $|g_y(u)|$ tend to 0 when u goes to infinity and the derivative of $u \mapsto |g_y(u)|$ is negative for all u and every $y \in Y \smallsetminus \{z\}$. It follows that the sum tends to zero when u goes to infinity and we conclude that we have

$$\lim_{u \to \infty} e^{uz \cdot t} \kappa(ut) = c_K(z) - c_L(z) \neq 0.$$

On the other hand, we also concluded that κ was the zero function and hence the limit should be 0. This contradiction leads to the conclusion that Y is empty and c_K and c_L are equal. □

6. Finding the field from the multi-length

Let K and L be two number fields and let $M \subset \mathbb{C}$ be a totally complex number field which is Galois over $\mathbb{Q}$ such that there are embeddings $K \to M$ and $L \to M$. Let $G = \mathrm{Gal}(M/\mathbb{Q})$ be the Galois group of M over $\mathbb{Q}$ and write $S = \mathrm{Hom}_{\mathbb{Q}}(K, M)$ for the set of embeddings of K in M and let $T = \mathrm{Hom}_{\mathbb{Q}}(L, M)$ be the set of embeddings of L in M. The set S has a natural left action from G and becomes a transitive G-set. Write $M^+ = M \cap \mathbb{R}$ and write $\rho \in \mathrm{Gal}(M/M^+)$ for the complex conjugation map. We identify $S_\infty K$ with $\langle\rho\rangle\backslash S$, the orbits of S under the action of ρ, and we identify $S_\infty L$ with $\langle\rho\rangle\backslash T$. This notation is fixed for the remainder of this section and all lemmas and propositions in this section assume that the fields and sets above are given, without explicitly mentioning that. After lemma 15, a prime $\mathfrak{q}$ of M and a corresponding map v are chosen. Apart from that, all statements are self-contained and do not contain hidden assumptions. In particular, a statement such as lemma 14, which deals only with $K \subset M$ and S, is also true when we replace K by L and S by T.

There are many G-sets appearing in this section and we feel that defining the G-action when they appear distracts too much from the flow of the argument. Moreover, for easy reference it is better to have all the sets with their G-action collected in one place. Therefore, we give a table of the G-sets we use here after we spend a few words on notation. For instance, we have a choice of writing elements f in $\mathbb{Z}_{\geq 0}^G$ as maps $f\colon G \to \mathbb{Z}_{\geq 0}$ or in the coordinate notation $f = (f_g)_{g \in G}$. We use both notations, depending on which one is most convenient at the moment. Also, we will often write elements in $\mathrm{Map}(S, \mathbb{Z}_{\geq 0}^G)$ as maps $S \times G \to \mathbb{Z}_{\geq 0}$. For the next table, let the notation be as above and let σ be an element of G.

set		*element f in set*	σf
S	$\ni$	f	$\sigma \circ f$
M	$\ni$	f	$\sigma(f)$
$\mathbb{Z}_{\geq 0}^G$	$\ni$	$f\colon G \to \mathbb{Z}_{\geq 0}$	$g \mapsto f(g\sigma)$
$\mathbb{Z}_{\geq 0}^S$	$\ni$	$f\colon S \to \mathbb{Z}_{\geq 0}$	$s \mapsto f(\sigma^{-1}s)$
$\mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^G)$	$\ni$	$f\colon S \times G \to \mathbb{Z}_{\geq 0}$	$(s, g) \mapsto f(s, \sigma^{-1}g)$
$\mathbb{Z}_{\geq 0}^{G \times S_\infty K}$	$\ni$	$f\colon G \times S_\infty K \to \mathbb{Z}_{\geq 0}$	$(g, \mathfrak{p}) \mapsto f(\sigma^{-1}g, \mathfrak{p})$

13. Lemma. *The set of G-maps $\mathrm{Map}_G(S, M)$ from S to M is a field and it is naturally isomorphic to K. The isomorphism $K \to \mathrm{Map}_G(S, M)$ sends an element $x \in K$ to the map $s \mapsto s(x)$. There is a bijective correspondence*

$$\mathrm{Hom}_{\mathbb{Q}}(K, L) \longrightarrow \mathrm{Map}_G(T, S),$$

mapping $\phi \in \mathrm{Hom}_{\mathbb{Q}}(K, L)$ to the element $\phi^* \in \mathrm{Map}_G(T, S)$ given by $\phi^*(t) = t \circ \phi$.

PROOF. It is clear that sending $x \in K$ to the map $s \mapsto s(x)$ gives a well-defined, injective homomorphism $K \to \mathrm{Map}_G(S, M)$. We shall prove that the map is surjective. Let x be an element of $\mathrm{Map}_G(S, M)$ and choose $s \in S$. Let $H = G_s$ be the point stabilizer of s in G. Then we have $H = \mathrm{Gal}(M/s(K))$. Because x is a G-map, the element $x(s)$ is stable under the action of H. In other words, we have $x(s) \in M^H$ and by standard Galois theory we have $M^H = s(K)$. Let $y \in K$ be an element with $s(y) = x(s)$. Then for all $g \in G$ we have

$$(gs)(y) = g(s(y)) = g(x(s)) = x(gs).$$

Hence, y is an element that maps to x.

Next, let another number field L and a corresponding non-empty G-set T be given. Write $i\colon K \to \mathrm{Map}_G(S, M)$ for the isomorphism between K and $\mathrm{Map}_G(S, M)$ and let $j\colon L \to \mathrm{Map}_G(T, M)$ be the corresponding map for L. For an element $f\colon T \to S$ in $\mathrm{Map}_G(T, S)$ we write $f^*\colon \mathrm{Map}_G(S, M) \to \mathrm{Map}_G(T, M)$ for the map $x \mapsto x \circ f$. By abuse of notation we will also write $f^*\colon K \to L$ for the map $j^{-1} \circ f^* \circ i$. This yields a map $\mathrm{Map}_G(T, S) \to \mathrm{Hom}_{\mathbb{Q}}(K, L)$ given by $f \mapsto f^*$ and we will prove that it is the inverse of the map stated in the lemma. For $s \in S$ we write $\mathrm{ev}_s\colon \mathrm{Map}_G(S, M) \to s(K)$ for the map that sends $x \in \mathrm{Map}_G(S, M)$ to $x(s)$. The inverse of the map i is equal to $s^{-1} \circ \mathrm{ev}_s$ for every $s \in S$. Likewise, the inverse of j is equal to $t^{-1} \circ \mathrm{ev}_t$ for every $t \in T$. Let ϕ be an element of $\mathrm{Hom}_{\mathbb{Q}}(K, L)$. Then for $x \in K$, we have

$$\begin{aligned}\phi^{**}(x) = (j^{-1} \circ \phi^{**} \circ i^{-1})(x) &= (j^{-1} \circ \phi^{**})(s \mapsto s(x)) \\ &= j^{-1}(t \mapsto \phi^*(t)(x)) = j^{-1}(t \mapsto t(\phi(x))) = \phi(x).\end{aligned}$$

Hence, ϕ is equal to ϕ^{**}. Now, let f be an element of $\mathrm{Map}_G(T, S)$, let t be an element of T and let x be an element of K. Then we have

$$\begin{aligned}f^{**}(t)(x) = (t \circ f^*)(x) &= t\big((j^{-1} \circ f^* \circ i)(x)\big) \\ &= t\big((t^{-1} \circ \mathrm{ev}_t \circ f^*)(s \mapsto s(x))\big) = \mathrm{ev}_t\big(t' \mapsto f(t')(x)\big) = f(t)(x),\end{aligned}$$

which shows that f is equal to f^{**}. This is what we needed to prove. □

The lemma shows that all information we want to know about K is already encoded in the G-set S. The next lemma shows what it means in terms of S and G that K is a CM-field. Recall that our definition of a CM-field is a totally complex number field of degree 2 over a totally real field.

14. LEMMA. *The following three statements are equivalent.*

(1) *The field K is a CM-field.*
(2) *For all $s \in S$ and all $g \in G$ we have $\rho s \neq s$ and $g\rho s = \rho g s$.*
(3) *There is an element $s \in S$ with $\rho s \neq s$ such that for all $g \in G$ we have $g\rho s = \rho g s$.*

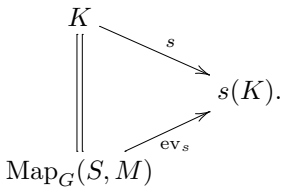
PROOF. Assume K is a CM-field and let $K^+ \subset K$ be a totally real field with $[K : K^+] = 2$. Let α be an element in K of degree 2 over K^+ with $\alpha^2 = a \in K^+$.

Let $s \in S$ and $g \in G$ be arbitrary elements. Then we have $\rho s \neq s$ and $\rho g s \neq gs$, for otherwise s or gs would be a real embedding. It also follows that $g\rho s$ is not equal to gs. On the other hand, because every embedding of K^+ into M has a real image, we do have $g\rho s|_{K^+} = gs|_{K^+} = \rho gs|_{K^+}$. Hence, we also have $(g\rho s(\alpha))^2 = g\rho s(a) = gs(a) = gs(\alpha)^2$. Because $g\rho s(\alpha)$ cannot be equal to $gs(\alpha)$, this shows that we have $g\rho s(\alpha) = -gs(\alpha)$. In the same way we prove that $\rho gs(\alpha)$ is equal to $-gs(\alpha)$. We conclude that ρgs and $g\rho s$ are the same on α and on K^+, which shows they are equal. This proves (1) $\Rightarrow$ (2).

Now suppose $s \in S$ is an element with $\rho s \neq s$ and such that for all $g \in G$ we have $g\rho s = \rho gs$. Let $s' \in S$ be any element and write $s' = g's$ for some $g' \in G$. Then we have $\rho gs' = \rho gg's = gg'\rho s = g\rho g's = g\rho s'$. We also have $\rho s' = \rho g's = g'\rho s \neq g's = s'$. This proves (2) $\Leftrightarrow$ (3).

Now assume (2) holds. Let s be an element of S and write $H = G_s = \mathrm{Gal}(M/s(K))$. Let H' be the group generated by ρ and the elements of H. By assumption, for $h \in H$ the commutator $[\rho, h] = \rho h \rho^{-1} h^{-1}$ is in H and therefore H' is equal to $H \cup \rho H$. Hence, the index of H in H' is 2. Write $K^+ = s^{-1}M^{H'}$. Then K is of degree 2 over K^+. Because $\rho s' \neq s'$ for all $s' \in S$ it is clear that K is totally imaginary. It suffices to prove that K^+ is totally real. Let s' be any element of S and write $s' = g's$. Then we have $\rho s'|_{K^+} = \rho gs|_{K^+} = g\rho s|_{K^+} = gs|_{K^+} = s'|_{K^+}$, and hence ρ is the identity on $s'(K^+)$. □

In light of lemma 13, we will simply identify K with $\mathrm{Map}_G(S, M)$ and L with $\mathrm{Map}_G(T, M)$. We write $\mathrm{ev}_s \colon \mathrm{Map}_G(S, M) \to s(K)$ for the map evaluating an element $x \colon S \to M$ in s and we obtain a commutative diagram



The map $s \colon K \to s(K)$ sends an element $x \in K$ to $s(x)$. Identifying x with a G-map $S \to M$, we see it is sent to $\mathrm{ev}_s(x) = x(s)$. We choose to write $x(s)$ instead of $s(x)$, which allows us to think of S as just a set of elements with a G-action, instead of a set of embeddings.

15. Lemma. *Let $\mathfrak{q}$ be a finite prime of M above a prime of $\mathbb{Q}$ that splits completely. Let*

$$v \colon O_M \smallsetminus \{0\} \longrightarrow \mathbb{Z}^G_{\geq 0}$$

be the map given by $x \mapsto (\mathrm{ord}_{\mathfrak{q}}\, gx)_{g \in G}$. Then v is surjective.

Proof. Let σ be an element of G and let π be an element with $\mathrm{ord}_{\sigma^{-1}\mathfrak{q}}\, \pi = 1$. Such an element exists because every element in $\sigma^{-1}\mathfrak{q}$ with valuation at $\sigma^{-1}\mathfrak{q}$ at least 2 is in $(\sigma^{-1}\mathfrak{q})^2$ and not every element of $\sigma^{-1}\mathfrak{q}$ is in $(\sigma^{-1}\mathfrak{q})^2$. For $g \in G \smallsetminus \{\sigma^{-1}\}$,

let y_g be an element with $\operatorname{ord}_{g\mathfrak{p}} y_g = 0$ and write $y_{\sigma^{-1}} = \pi$. Because $\mathfrak{q}$ lies above a splitting prime, the set $\{\, g\mathfrak{p} : g \in G \,\}$ consists of $\#G$ different primes. Hence, the ideals $(g\mathfrak{p})^2$ for $g \in G$ are pairwise coprime. By the Chinese remainder theorem there exists an element $x \in O_M$ with $x \equiv y_g \bmod (g\mathfrak{p})^2$. In other words, we have $\operatorname{ord}_{g\mathfrak{p}}(x - y_g) \geq 2$ and it follows that x is an element of $O_M \smallsetminus \{0\}$ that maps to the element in $\mathbb{Z}_{\geq 0}^G$ that is 1 at the σ-coordinate and 0 everywhere else. It follows that v is surjective. □

We fix a prime $\mathfrak{q}$ of M as in lemma 15 and let $v\colon O_M \smallsetminus \{0\} \to \mathbb{Z}_{\geq 0}^G$ be the corresponding map. For an element $s \in S$ we denote the ρ-orbit by $\langle\rho\rangle s \in S_\infty K$. Given an element $x \in K = \operatorname{Map}_G(S, M)$ and a prime $\langle\rho\rangle s \in S_\infty K$, the square of the length of x at that prime is equal to $x(s) \cdot x(\rho s) \in M^+ \subset \mathbb{R}$. We write

$$\mu\colon O_K \smallsetminus \{0\} \longrightarrow (O_{M^+} \smallsetminus \{0\})^{S_\infty K}$$

for the map sending $x \in O_K \smallsetminus \{0\}$ to $(x(s) \cdot x(\rho s))_{\langle\rho\rangle s \in S_\infty K}$. The corresponding map for L is also called μ. We are interested in the image of the map $O_K \smallsetminus \{0\} \to \mathbb{Z}_{\geq 0}^{G \times S_\infty K}$, given by the composition of the maps

$$O_K \smallsetminus \{0\} \xrightarrow{\mu} (O_{M^+} \smallsetminus \{0\})^{S_\infty K} \xrightarrow{v^{S_\infty K}} \mathbb{Z}_{\geq 0}^{G \times S_\infty K}.$$

The idea is that if K is not a CM-field, the set S is encoded in $\mathbb{Z}_{\geq 0}^{G \times S_\infty K}$. Because the image of μ is basically the image of the multi-length function, it will follow that if K and L have 'the same' multi-length functions then the G-sets S and T are also 'the same'.

16. Lemma. *Let $\tau\colon S_\infty L \to S_\infty K$ be a bijection and assume that the multi-length of K and the multi-length of L are the same with respect to this bijection. Then the image of the map $(\tau^* \circ v^{S_\infty K} \circ \mu)\colon O_K \to \mathbb{Z}_{\geq 0}^{G \times S_\infty L}$ is the same as the image of the map $(v^{S_\infty L} \circ \mu)\colon O_L \to \mathbb{Z}_{\geq 0}^{G \times S_\infty L}$.*

Proof. Let c_K be the multi-length of K. Then the image of the map μ in $(O_{M^+} \smallsetminus \{0\})^{S_\infty K} \subset \mathbb{R}^{S_\infty K}$ consists exactly of the elements $y \in \mathbb{R}^{S_\infty K}$ with $c_K(y) \neq 0$. Hence, we have $(\tau^* \circ \mu)(O_K) = \mu(O_L)$ and therefore also $(\tau^* \circ v^{S_\infty K} \circ \mu)(O_K) = (v^{S_\infty L} \circ \mu)(O_L)$. □

We factorize the map $v^{S_\infty K} \circ \mu$ over the set $\operatorname{Map}_G(S, \mathbb{Z}_{\geq 0}^G)$. Write

$$v\colon O_K \smallsetminus \{0\} \longrightarrow \operatorname{Map}_G(S, \mathbb{Z}_{\geq 0}^G)$$

for the map sending a nonzero $x \in O_K = \operatorname{Map}_G(S, O_M)$ to $v \circ x$. Furthermore, let

$$m\colon \operatorname{Map}_G(S, \mathbb{Z}_{\geq 0}^G) \longrightarrow \mathbb{Z}_{\geq 0}^{G \times S_\infty K}$$

be the map sending $f\colon S \times G \to \mathbb{Z}_{\geq 0}$ to the map $(g, \langle\rho\rangle s) \mapsto f(s, g) + f(\rho s, g)$. We will prove that the map $v^{S_\infty K} \circ \mu$ is equal to $m \circ v$, but first we give a lemma that gives a simpler representation of $\operatorname{Map}_G(S, \mathbb{Z}_{\geq 0}^G)$.

17. Lemma. *The map*

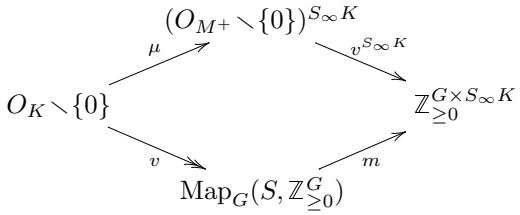
$$\mathbb{Z}_{\geq 0}^{S} \xrightarrow{\sim} \mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^{G})$$

that sends $f \in \mathbb{Z}^S$ to the map $(s, g) \mapsto f(gs)$ is an isomorphism of G-sets. The inverse is given by sending an element $f\colon S \to \mathbb{Z}_{\geq 0}^{G}$ to its composition with the projection map $\mathbb{Z}_{\geq 0}^{G} \to \mathbb{Z}_{\geq 0}$ on the coordinate $1 \in G$.

Proof. Obvious. □

The G-set $\mathbb{Z}_{\geq 0}^{S}$ is also a monoid with a natural basis $S \subset \mathbb{Z}_{\geq 0}^{S}$. Here, the inclusion is given by identifying $s \in S$ with a map $\chi_s\colon S \to \mathbb{Z}_{\geq 0}$ with $\chi_s(s) = 1$ and $\chi_s(s') = 0$ for every $s' \neq s$. It is easily checked that this inclusion respects the G-action.

18. Lemma. *The diagram*



commutes. The map $v\colon O_K \smallsetminus \{0\} \to \mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^{G})$ is surjective and m is a G-map.

Proof. We only prove surjectivity because the rest is obvious. We write $\tilde{v}\colon O_K \smallsetminus \{0\} \to \mathbb{Z}_{\geq 0}^{S}$ for the map $v\colon O_K \smallsetminus \{0\} \to \mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^{G})$ composed with the map $\mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^{G}) \to \mathbb{Z}_{\geq 0}^{S}$ from lemma 17. We prove that $\tilde{v}$ is surjective. As $\tilde{v}$ is a monoid-homomorphism it suffices to prove that $\tilde{v}$ hits every element of the basis S. Let s be an element of S and let $\chi_s\colon S \to \mathbb{Z}_{\geq 0}$ be the corresponding map. Let $\pi \in M$ be an element with $v(\pi)_1 = 1$ and $v(\pi)_g = 0$ for $g \neq 1$. Write $H = G_s = \{\, g \in G : gs = s \,\}$ for the stabilizer of the point s. Let a be the element

$$a = \prod_{h \in H} h\pi.$$

Because a is stable under the action of H, it is in $s(K)$ and it follows that there is a unique $x \in O_K$ with $x(s) = a$. We have

$$\tilde{v}(x)(s) = \big((v \circ x)(s)\big)_1 = \big(v(\prod_{h \in H} h\pi)\big)_1 = \sum_{h \in H} \big(hv(\pi)\big)_1 = \sum_{h \in H} (v(\pi))_{h^{-1}} = 1.$$

Likewise, we have $\tilde{v}(x)(gs) = 0$ for $g \notin H$. Hence, we have $\tilde{v}(x) = \chi_s$. □

19. Proposition. *Let $S' \subset \mathbb{Z}_{\geq 0}^{G \times S_\infty K}$ be the set of elements in the image $m(\mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^{G}))$ with the sum of the coordinates equal to $2 \cdot \#G \cdot \#S_\infty K / \#S$.*

Then the pre-image $m^{-1}(S')$ is the same as the image of S in $\mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^G)$. The map $S \to \mathbb{Z}_{\geq 0}^{G \times S_\infty K}$ is injective if K is not a CM-field. If K is a CM-field, the map is 2 to 1 and for every $s \in S$ the elements s and ρs have the same image.

PROOF. Let s be an element in S and let $(s, g) \mapsto \chi_s(gs)$ be the corresponding map in $\mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^G)$. Let s' be an element of S and write $s' = g's$ for $g' \in G$. We have

$$\sum_{g \in G} \chi_s(gs') = \#\{\, g \in G : gs' = s \,\} = \#G_s g'^{-1} = \#G_s = \#G/\#Gs = \#G/\#S.$$

Let $\tilde{\chi}_s \colon G \times S_\infty K \to \mathbb{Z}_{\geq 0}$ be the image of $(s, g) \mapsto \chi_s(gs)$ under m. Then for any fixed prime $\langle \rho \rangle s' \in S_\infty K$ we have

$$\sum_{g \in G} \tilde{\chi}_s(g, \langle \rho \rangle s') = \sum_{g \in G} \chi_s(gs') + \sum_{g \in G} \chi_s(g\rho s') = 2\#G/\#S.$$

Hence, the sum of the coordinates of $\tilde{\chi}_s$ is indeed equal to

$$\sum_{\substack{g \in G \\ \mathfrak{p} \in S_\infty K}} \tilde{\chi}_s(g, \mathfrak{p}) = \frac{2 \cdot \#G \cdot S_\infty K}{\#S}.$$

Every other nonzero element in the image of m in $\mathbb{Z}_{\geq 0}^{G \times S_\infty K}$ can be written as a sum of elements coming from S and will consequently have a larger coordinate sum. This proves that $m^{-1}(S')$ is exactly the image of S in $\mathrm{Map}_G(S, \mathbb{Z}_{\geq 0}^G)$.

Denote the image of an element $s \in S$ under the map $S \to \mathbb{Z}_{\geq 0}^{G \times S_\infty K}$ by $\tilde{\chi}_s$. Let $s \neq s'$ be two elements in S and suppose that $\tilde{\chi}_s$ is equal to $\tilde{\chi}_{s'}$. We have

$$1 + \chi_s(\rho s) = \chi_s(s) + \chi_s(\rho s) = \tilde{\chi}_s(1, \langle \rho \rangle s) = \tilde{\chi}_{s'}(1, \langle \rho \rangle s) = \chi_{s'}(s) + \chi_{s'}(\rho s) = \chi_{s'}(\rho s).$$

This shows that we have $\chi_s(\rho s) = 0$ and $\chi_{s'}(\rho s) = 1$. In other words, $\langle \rho \rangle s$ is a complex prime and s' is equal to ρs. Now, let $g \in G$ be arbitrary and write $t = gs$. Then we have $\tilde{\chi}_s(g^{-1}, \langle \rho \rangle t) = 1$ and hence

$$1 = \tilde{\chi}_{s'}(g^{-1}, \langle \rho \rangle t) = \chi_{s'}(g^{-1}t) + \chi_{s'}(g^{-1}\rho t) = \chi_{g\rho s}(gs) + \chi_{g\rho s}(\rho g s).$$

Because $g\rho s = gs'$ is not equal to gs, we conclude that $\chi_{g\rho s}(\rho g s)$ is equal to 1 and that $g\rho s$ is equal to $\rho g s$. As g was arbitrary, it follows from lemma 14 that K is a CM-field. □

20. LEMMA. *Let the notation be as in proposition 19. Let $\chi \colon G \times S_\infty K \to \mathbb{Z}_{\geq 0}$ be an element in S' and let $s \in S$ be an element that maps to χ. Let $\mathfrak{p}$ be a prime in $S_\infty K$. Then we have $\chi(1, \mathfrak{p}) \neq 0$ if and only if $\mathfrak{p}$ is equal to $\langle \rho \rangle s$.*

PROOF. Let χ_s be the element of $\mathbb{Z}_{\geq 0}^S$ corresponding to s. Write $\mathfrak{p} = \langle\rho\rangle s'$ for some $s' \in S$. Then we have

$$\chi(1,\mathfrak{p}) = \chi_s(s') + \chi_s(\rho s') = \chi_s(s') + \chi_{\rho s}(s'),$$

which is nonzero only when s' is equal to s or to ρs. □

The set S' from proposition 19 contains a lot of information. For instance, by comparing the cardinality with the cardinality of S we immediately see whether K is CM-field. And in the case that K is not a CM-field, the set S' is isomorphic as a G-set to S. Hence, in this case we can construct $\mathrm{Map}_G(S', M)$ which is isomorphic to K. Before we formulate this in a theorem we first turn to the CM-field case.

21. LEMMA. *Let $\tau\colon S_\infty L \to S_\infty K$ be a bijection and assume that the multi-length of K and the multi-length of L are the same with respect to this bijection. Then the following statements are true.*

(1) *The field K is a CM-field if and only if L is a CM-field.*
(2) *Assume K and L are CM-fields and let K^+ and L^+ be the real subfields of K and L. Then there is a unique isomorphism $\phi\colon K^+ \to L^+$ such that the diagram*

$$\begin{array}{ccc} S_\infty L & \xrightarrow{\tau} & S_\infty K \\ \downarrow & & \downarrow \\ S_\infty L^+ & \xrightarrow{\phi^*} & S_\infty K^+ \end{array}$$

commutes.

PROOF. Let S' be the set from proposition 19 and let $T' \subset \mathbb{Z}_{\geq 0}^{G\times S_\infty L}$ be the corresponding set for L. By lemma 16, the set S' is G-isomorphic to T'. From proposition 19 we see that we have

$$K \text{ is a CM-field} \iff 2\#S' = \#S \iff 2\#T' = \#T \iff L \text{ is a CM-field.}$$

Now assume that K and L are CM-fields. In this case $S_\infty K$ and $S_\infty L$ are G-sets and the maps $S \to S_\infty K = \langle\rho\rangle\backslash S$ and $T \to S_\infty L = \langle\rho\rangle\backslash T$ are G-maps. From proposition 19 we see that the map $S \to S'$ factorizes over $S_\infty K$ and this gives a G-isomorphism $S_\infty K \to S'$ and a G-isomorphism $S_\infty L \to T'$. The map τ induces a G-map $\tau^*\colon \mathbb{Z}_{\geq 0}^{G\times S_\infty K} \to \mathbb{Z}_{\geq 0}^{G\times S_\infty L}$ as in lemma 16 and by restriction a G-map $\tau^*\colon S' \to T'$. We claim that the diagram

$$\begin{array}{ccc} S_\infty K & \xrightarrow{\tau^{-1}} & S_\infty L \\ \downarrow & & \downarrow \\ S' & \xrightarrow{\tau^*} & T' \end{array}$$

commutes. Let $\langle\rho\rangle s$ be a prime in $S_\infty K$ and write $\langle\rho\rangle t = \tau^{-1}(\langle\rho\rangle s)$. Let $\tilde{\chi}_s$ be the image of s in S' and let $\tilde{\chi}_t$ be the image of t in T'. Then we have $\tau^*\tilde{\chi}_s(1, \langle\rho\rangle t) = \tilde{\chi}_s(1, \langle\rho\rangle s) = 1 = \tilde{\chi}_t(1, \langle\rho\rangle t)$. But $\tilde{\chi}_t$ is the unique element of T' that is 1 when evaluated in $(1, \langle\rho\rangle t)$ by lemma 20 and proposition 19. Hence $\tau^*\tilde{\chi}_s$ and $\tilde{\chi}_t$ are the same and the diagram commutes. It follows that τ^{-1} and also τ is a G-map.

Write $S^+ = \mathrm{Hom}_{\mathbb{Q}}(K^+, M)$ and $T^+ = \mathrm{Hom}_{\mathbb{Q}}(L^+, M)$. There are natural identifications $S^+ = S_\infty K^+ = S_\infty K$ and $T^+ = S_\infty L^+ = S_\infty L$ and hence τ induces a G-isomorphism $T^+ \to S^+$. By lemma 13, we get an induced isomorphism $\phi\colon K^+ \to L^+$ and it is now clear that the diagram in this lemma commutes. □

22. Lemma. *Assume K and L are of of degree 2 over a number field Q. Let $N_Q^K\colon K \to Q$ and $N_Q^L\colon L \to Q$ be the norm maps. Suppose $N_Q^K(K)$ is equal to $N_Q^L(L)$. Then K and L are isomorphic over Q.*

Proof. Let $\mathfrak{p}$ be a finite prime of Q which does not ramify in K or L. Suppose $\mathfrak{p}$ splits in K and is inert in L. Let $\mathfrak{P}$ and $\mathfrak{Q}$ be the two primes of K lying above $\mathfrak{p}$. By a similar argument as used in lemma 15, there is an element $\pi \in K$ with $\mathrm{ord}_{\mathfrak{P}}\,\pi = 1$ and $\mathrm{ord}_{\mathfrak{Q}}\,\pi = 0$. Hence, we have $\mathrm{ord}_{\mathfrak{p}}\,N_Q^K(\pi) = 1$. However, for every element $x \in L$ we have $\mathrm{ord}_{\mathfrak{p}O_L}\,x \in \mathbb{Z}$ and thus $\mathrm{ord}_{\mathfrak{p}}\,N_Q^L(x) \in 2\mathbb{Z}$. This is in contradiction with the assumption $N_Q^K(K) = N_Q^L(L)$. We conclude that, aside from a finite set of ramifying primes, the set of primes of Q that split in K is the same as the set of primes of Q that split in L. From [5, theorem VIII.4.9], we know that the splitting behavior of the primes in a Galois extension determines the extension. In our case, it follows that K and L are isomorphic over Q. □

We are now ready to prove the main theorem, which we will restate here.

23. Theorem. *Let K and L be number fields. Then the map*

$$\mathrm{Isom}(K, L) \longrightarrow \{\textit{strongly monomial } \lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L} : h_K^0 = h_L^0 \circ \lambda\,\}$$

given by $\phi \mapsto \phi^{**}$ is surjective. The map is injective unless K and L are isomorphic CM-fields. When K and L are isomorphic CM-fields the map is 2 to 1 and ϕ and ϕ' in $\mathrm{Isom}(K, L)$ have the same image if and only if they are the same or each other's complex conjugate.

Proof. If there are no strongly monomial maps λ with $h_K^0 = h_L^0 \circ \lambda$, the fields K and L are not isomorphic and then there is nothing to prove. Suppose $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ is a strongly monomial map with $h_K^0 = h_L^0 \circ \lambda$. By proposition 10, we can write $\lambda = \tau^*$ for a bijection $\tau\colon S_\infty L \to S_\infty K$, respecting the degree of the primes. Let c_K be the multi-length of K and let c_L be the multi-length of L. By proposition 12, we have $c_K = c_L \circ \tau^*$. Using lemma 16, we see that $\tau^* \circ v^{S_\infty K} \circ \mu$ and $v^{S_\infty L} \circ \mu$ have the same image in $\mathbb{Z}_{\geq 0}^{G \times S_\infty L}$. Let S' be the set from proposition 19 and let $T' \subset \mathbb{Z}_{\geq 0}^{G \times S_\infty L}$ be the corresponding set for L. The map $\tau^*\colon \mathbb{Z}_{\geq 0}^{G \times S_\infty K} \to \mathbb{Z}_{\geq 0}^{G \times S_\infty L}$ induces an isomorphism $\tau^*\colon S' \to T'$ of G-sets. Now, suppose that K and L

are not CM-fields. Then by proposition 19, the set S maps bijectively to S' and T maps bijectively to T'. Hence, we get an induced isomorphism $\tau^*: S \to T$. By lemma 20, the diagram

$$\begin{array}{ccc} T & \xrightarrow{(\tau^*)^{-1}} & S \\ \downarrow & & \downarrow \\ S_\infty L & \xrightarrow{\tau} & S_\infty K \end{array}$$

commutes. We now apply lemma 13 and conclude that $(\tau^*)^{-1}: T \to S$ induces an isomorphism $\phi: K \to L$ with $\phi^*: T \to S$ equal to $(\tau^*)^{-1}$ and therefore $\phi^*: S_\infty L \to S_\infty K$ equal to τ. This shows that $\phi \mapsto \phi^{**}$ is surjective when K and L are not CM-fields.

From lemma 21, we know that K and L are either both CM-fields or they both are not. We assume now that they are both CM-fields. Let K^+ and L^+ be the real subfields of K and L and let $\phi: K^+ \to L^+$ be the unique isomorphism from lemma 21, inducing $\tau: S_\infty L \to S_\infty K$. Let s be an element of S. Let $Y \subset \mathbb{R}^{S_\infty K}$ be the set of elements y with $c_K(y) \neq 0$. Furthermore, let N be the set $\{ y_{\langle\rho\rangle s} : y \in Y \}$. Then N is a subset of $s(K^+)$ and in fact it is equal to the image of the norm map $N^{s(K)}_{s(K^+)}$. Hence, the norm maps $N^K_{K^+}$ and $N^L_{L^+}$ have the same image with respect to the isomorphism ϕ. By lemma 22, we see that ϕ can be extended to an isomorphism $\phi: K \to L$ and of course ϕ^* is still equal to τ. This shows that $\phi \mapsto \phi^{**}$ is surjective in the CM-case.

Now assume that K and L are (not necessarily CM) isomorphic fields. Suppose ϕ_1 and ϕ_2 are two different elements in $\mathrm{Isom}(K, L)$ with $\phi_1^* = \phi_2^*$. For all $t \in T$, we have $t \circ \phi_1 = \rho \circ t \circ \phi_2$. This is easy to see, because $t \circ \phi_1$ and $t \circ \phi_2$ are not the same on K and the prime $\langle\rho\rangle t\phi_1$ is equal to the prime $\langle\rho\rangle t\phi_2$ by assumption. Let s be an element of S and let g be an element of G. Furthermore, let $t \in T$ be an element with $t\phi_1 = gs$. It follows that we have $g^{-1}t\phi_1 = s$. When we replace ϕ_1 by ϕ_2, we have to multiply with ρ and this yields $\rho gs = t\phi_2 = g(g^{-1}t\phi_2) = g(\rho s) = g\rho s$. We conclude that K is a CM-field and that ϕ_1 and ϕ_2 are each other's complex conjugate. □

7. Relaxing the conditions of the main theorem

So far, we have spent all our efforts on the proof that the map

$$\mathrm{Isom}(K, L) \longrightarrow \{\text{strongly monomial } \lambda: \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L} : h^0_K = h^0_L \circ \lambda \}$$

is surjective for any two number fields K and L. In all honesty, we should admit that it would desirable to have a theorem that is stronger in a number of ways. First of all, it would be interesting to relax the condition 'strongly monomial' to just 'monomial' or even 'non-singular'. In proposition 25, we prove that K and L are number fields

of the same degree over $\mathbb{Q}$ if there exists a monomial map λ with $h^0_K = h^0_L \circ \lambda$. In example 27, we show what obstacles arise when we try to prove that a monomial map λ with $h^0_K = h^0_L \circ \lambda$ is automatically strongly monomial. Secondly, it would also be interesting to relax the condition $h^0_K = h^0_L \circ \lambda$ to equality on just the part of fixed degree, for instance degree 0. More precisely, if $H \subset S_\infty K$ is the hyperplane of all points with coordinate-wise sum equal to 0, we could relax the condition $h^0_K = h^0_L \circ \lambda$ to $h^0_K|_H = (h^0_L \circ \lambda)|_H$. In example 29, we discuss obstacles that arise when we try to reconstruct the arithmetic of the number field using that $h^0_K|_H$ is periodic on the image of the unit-lattice in H.

24. Lemma. *Let K be a number field with multi-length $c = c_K \colon \mathbb{R}^{S_\infty} \to \mathbb{Z}$. Then the following statements are true.*

(1) *If $y \in \mathbb{R}^{S_\infty}$ is a point with $c(y) \neq 0$ then we have $y_\mathfrak{p} > 0$ for all $\mathfrak{p} \in S_\infty$ and*

$$\prod_{\mathfrak{p} \in S_\infty} y_\mathfrak{p}^{n(\mathfrak{p})} \geq 1.$$

(2) *Call an element $y \in \mathbb{R}^{S_\infty}$ a unit if we have $c(y) \neq 0$ and $\prod_\mathfrak{p} y_\mathfrak{p}^{n(\mathfrak{p})} = 1$. For all $M > 0$ and all $\delta > 1$ and all $\mathfrak{p} \in S_\infty$, there is a unit y such that for all $\mathfrak{q}, \mathfrak{r} \in S_\infty \smallsetminus \{\mathfrak{p}\}$ the quotient $y_\mathfrak{q}/y_\mathfrak{r}$ is in the interval $[\delta^{-1}, \delta]$ and for all $\mathfrak{q} \in S_\infty \smallsetminus \{\mathfrak{p}\}$ we have $y_\mathfrak{q}/y_\mathfrak{p} \geq M$.*

Proof. Every element $y \in \mathbb{R}^{S_\infty}_{>0}$ with $c(y) \neq 0$ comes from an element in the ring of integers. The expression $\prod_\mathfrak{p} y_\mathfrak{p}^{n(\mathfrak{p})}$ is equal to the norm of this element and this is at least 1. This proves statement (1). Statement (2) is trivially true when the cardinality of S_∞ is 1. Hence, assume S_∞ has at least 2 elements. Let $\mathfrak{p}$ be an element of S_∞ and write $S'_\infty = S_\infty \smallsetminus \{\mathfrak{p}\}$. For notational convenience later in the proof, we assume that M is at least 1. Write O for the ring of integers of K. We have an inclusion map $\psi \colon O^* \to \mathbb{R}^{S'_\infty}$, sending an element $\eta \in O^*$ to $(\log |\eta|_\mathfrak{q})_{\mathfrak{q} \in S'_\infty}$. This way, $\psi(O^*)$ becomes a lattice in $\mathbb{R}^{S'_\infty}$. Let $\mathfrak{q}$ be an element of S'_∞. We write $\varepsilon = \log \delta$ and for $t \in \mathbb{R}$, we define

$$F_t = \{\, z \in \mathbb{R}^{S'_\infty} : |z_\mathfrak{q}| \leq t \text{ and for all } \mathfrak{r}, \mathfrak{s} \in S'_\infty : z_\mathfrak{r} - z_\mathfrak{s} \in [-\varepsilon, \varepsilon] \,\}.$$

The set F_t is symmetric around the origin, convex and closed. For positive t, the volume of F_t is linear in t. By the Minkowski lattice theorem, the number of points of $\psi(O^*)$ in F_t becomes arbitrarily large when we let t go to infinity. Let z be a point in $\psi(O^*) \cap \bigcup_{t \in \mathbb{R}_{>0}} F_t$ with $z_\mathfrak{q} \geq \log M + \varepsilon$. Let $y \in \mathbb{R}^{S_\infty}$ be the element corresponding to $\psi^{-1}(z)$. Then for all $\mathfrak{r}, \mathfrak{s} \in S'_\infty$, we have

$$\frac{y_\mathfrak{r}}{y_\mathfrak{s}} = e^{\log y_\mathfrak{r} - \log y_\mathfrak{s}} \in [e^{-\varepsilon}, e^{\varepsilon}] = [\delta^{-1}, \delta].$$

Hence, for all $\mathfrak{r} \in S'_\infty$, we have $y_\mathfrak{r} \geq \delta^{-1} y_\mathfrak{q} \geq \delta^{-1} e^{\varepsilon} M = M$. It follows that $y_\mathfrak{p}$ is smaller than 1 and we have $y_\mathfrak{r}/y_\mathfrak{p} \geq y_\mathfrak{r} \geq M$. This proves (4). □

In section 5, we used the transformation $k_K^0 \circ - \log \circ d$ of the function k^0. The idea was that if K and L have the same h^0 with respect to a strongly monomial map, they also have the same transformation of k^0. Because the map d uses information about degrees, we cannot use this map if we only consider equality with respect to monomial maps. We write $m_{1/\pi}\colon \mathbb{R}_{>0}^{S_\infty} \to \mathbb{R}_{>0}^{S_\infty}$ for the map multiplying each coordinate with $1/\pi$ and we use the transformation $k_K^0 \circ - \log \circ m_{1/\pi}$.

25. Proposition. *Let K be a number field of degree n over $\mathbb{Q}$ and let $\mathfrak{p} \in S_\infty$ be a prime. Let $\mathbb{R}_{>0} \to \mathbb{R}_{>0}^{S_\infty}$ be the inclusion map, sending an element $t \in \mathbb{R}_{>0}$ to the element of $\mathbb{R}_{>0}^{S_\infty}$ that is t at the $\mathfrak{p}$-coordinate and 1 at all other coordinates. Let $\kappa\colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be the composition of the maps*

$$\mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}^{S_\infty} \xrightarrow{m_{1/\pi}} \mathbb{R}_{>0}^{S_\infty} \xrightarrow{-\log} \mathbb{R}^{S_\infty} \xrightarrow{k_K^0} \mathbb{R}_{>0}.$$

Then for all $\varepsilon > 0$, we have

$$\limsup_{t\to\infty} \exp(t^{2/n+\varepsilon})\kappa(t) = \infty \qquad \text{and} \qquad \lim_{t\to\infty} \exp(t^{2/n-\varepsilon})\kappa(t) = 0.$$

Proof. Let c be the multi-length of K. Define $d = 2/n(\mathfrak{p})$ and for $y \in \mathbb{R}^{S_\infty}$ and $t \in \mathbb{R}$ write $y * t$ for

$$y * t = y_{\mathfrak{p}} t^d + \sum_{\mathfrak{q} \in S_\infty \smallsetminus \{\mathfrak{p}\}} y_{\mathfrak{q}}.$$

For all $t \in \mathbb{R}_{>0}$, we have

$$\exp(t^{2/n+\varepsilon})\kappa(t) \geq \sum_{y \in \mathbb{R}^{S_\infty}} c(y) \exp(t^{2/n+\varepsilon} - 2y * t).$$

Let $M > 0$ be an arbitrarily large number and write $\delta = 1/(2n)$. Now apply lemma 24(2) to find a unit y such that for all $\mathfrak{q}, \mathfrak{r} \in S_\infty \smallsetminus \{\mathfrak{p}\}$ we have $y_{\mathfrak{q}}/y_{\mathfrak{r}} \in [\delta^{-1}, \delta]$ and $y_{\mathfrak{q}}/y_{\mathfrak{p}} \geq M$. Let $\mathfrak{q}$ be any prime in $S_\infty \smallsetminus \{\mathfrak{p}\}$ and let $t \in \mathbb{R}_{>0}$ be such that we have $t^d = y_{\mathfrak{q}}/y_{\mathfrak{p}}$. For any $\mathfrak{r} \in S_\infty \smallsetminus \{\mathfrak{p}\}$, we write $z_{\mathfrak{r}} = y_{\mathfrak{r}}$ and we write $z_{\mathfrak{p}} = t^d y_{\mathfrak{p}}$. For each two elements in the set $Z = \{\, z_{\mathfrak{r}} : \mathfrak{r} \in S_\infty \}$, the quotient is in $[\delta^{-1}, \delta]$. Moreover, we have

$$\prod_{\mathfrak{r} \in S_\infty} z_{\mathfrak{r}}^{n(\mathfrak{r})} = t^{dn(\mathfrak{p})} \prod_{\mathfrak{r} \in S_\infty} y_{\mathfrak{r}}^{n(\mathfrak{r})} = t^2.$$

Hence, each element in the set Z is at most $\delta t^{2/n}$. We conclude that we have

$$t^{2/n+\varepsilon} - 2y * t = t^{2/n+\varepsilon} - \sum_{\mathfrak{r} \in S_\infty} 2z_{\mathfrak{r}} \geq t^{2/n+\varepsilon} - 2\delta t^{2/n} \# S_\infty \geq t^{2/n+\varepsilon} - t^{2/n}.$$

Hence, for arbitrarily large $M > 0$ there is an element t with $t \geq M$ such that $\exp(t^{2/n+\varepsilon})\kappa(t) \geq \exp(t^{2/n+\varepsilon} - t^{2/n})$. This proves the first limit of this proposition.

For the second limit, note that for all $t \in \mathbb{R}_{>0}$ we also have

$$\exp(t^{2/n-\varepsilon})\kappa(t) \leq \sum_{y \in \mathbb{R}^{S_\infty}} c(y) \exp(t^{2/n-\varepsilon} - y * t).$$

If $y \in \mathbb{R}^{S_\infty}_{>0}$ is a point with $y_\mathfrak{p} \geq 1$, the function $t \mapsto t^{2/n-\varepsilon} - y * t$ has a negative derivative for $t \geq 1$ and we conclude

$$\lim_{t \to \infty} \sum_{\substack{y \in \mathbb{R}^{S_\infty} \\ y_\mathfrak{p} \geq 1}} c(y) \exp(t^{2/n-\varepsilon} - y * t) = 0.$$

We call the set $X = \{\, x \in \mathbb{R}^{S_\infty}_{>0} : x_\mathfrak{p} < 1 \,\}$ the 'critical strip.' For y ranging over the points in the critical strips, the sum $\sum_y c(y) \exp(-\frac{1}{2} y * 0)$ converges and we call the sum s. For fixed $t \in \mathbb{R}_{>0}$ and $y \in \mathbb{R}^{S_\infty}_{>0}$, the geometric-arithmetic mean inequality gives us

$$y_\mathfrak{p} t^d + \frac{1}{2} \sum_{\mathfrak{q} \in S_\infty \smallsetminus \{\mathfrak{p}\}} y_\mathfrak{q} \geq \frac{n}{4} \sqrt[n]{(y_\mathfrak{p} t^d)^{n(\mathfrak{p})} \prod_{\mathfrak{q} \in S_\infty \smallsetminus \{\mathfrak{p}\}} y_\mathfrak{q}^{n(\mathfrak{q})}} \geq \frac{n}{4} t^{2/n}.$$

For fixed $t \in \mathbb{R}_{>0}$, we get

$$\sum_{y \in X} c(y) \exp(t^{2/n-\varepsilon} - y * t) \leq \sum_{y \in X} c(y) \exp(t^{2/n-\varepsilon} - \frac{1}{2} y * 0 - \frac{n}{4} t^{2/n}) = \exp(t^{2/n-\varepsilon} - \frac{n}{4} t^{2/n}) s.$$

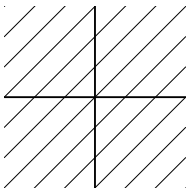
When t goes to infinity, this goes to 0. □

26. Corollary. *Let K and L be number fields and let $\lambda \colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ be a monomial map with $h^0_K = h^0_L \circ \lambda$. Then we have $[K : \mathbb{Q}] = [L : \mathbb{Q}]$.*

The technique we used in proposition 25 and also in proposition 12 was to take the function $k^0_K \colon \mathbb{R}^{S_\infty} \to \mathbb{R}_{>0}$ and deduce information about K from the behavior of $k^0_K(x)$ when x goes to infinity in some way. In the next example we show that this technique cannot easily be employed to deduce which coordinates belong to real primes and which ones belong to complex primes.

27. Example. Let K be any number field of degree 3 over $\mathbb{Q}$ with one complex prime and one real prime. For instance, $K = \mathbb{Q}(\sqrt[3]{2})$ will do nicely. We assume the function k^0_K is given as a function $\mathbb{R}^2 \to \mathbb{R}_{>0}$ and we are not told which coordinate corresponds to the real prime. Let R be the regulator of K. The function k^0_K is periodic modulo $(R, -R)$. In particular, the function k^0_K is the same on the lines

obtained from the diagonal in $\mathbb{R}^2$ shifted by multiples of $(R, -R)$, as depicted in the next graph.



A path in $\mathbb{R}^2$ that goes to infinity either stays between two of these lines eventually, or it keeps crossing these lines. Let $\bar{k}^0_K$ be the map given by $x \mapsto k^0_K(x_2, x_1)$. For every point on one of the lines above, we have $k^0_K(x) = \bar{k}^0_K(x)$. Hence, for every path that keeps crossing these lines we keep running into points x for which we have $k^0_K(x) = \bar{k}^0_K(x)$. Hence, in this case we get no information from the limit behavior about which coordinate belongs to the real prime. We do not know how to exploit the limit behavior to deduce information from going to infinity by staying on a path between two lines.

It is reasonable to try to use the fact that h^0_K is periodic modulo the image of the unit lattice in $\mathbb{R}^{S_\infty}$ to our advantage. In particular, let K and L be two number fields with the same number of primes and let $\lambda\colon \mathbb{R}^{S_\infty K} \to \mathbb{R}^{S_\infty L}$ be a monomial map with $h^0_K = h^0_L \circ \lambda$. By corollary 26, the fields K and L have the same degree. If both fields are totally complex, the map λ is strongly monomial and we can apply theorem 23 to see that K and L are isomorphic. Hence, we can assume that both fields have a real prime. Write $S_\infty = S_\infty K$ and let $H \subset \mathbb{R}^{S_\infty}$ be the hyperplane consisting of the points of which the coordinates sum to zero. Furthermore, *assume* that h^0_K is not constant on lines through the origin. It follows that $h^0_K|_H$ has a periodicity lattice of finite index in the image of $U = O^*_K$. For simplicity, assume that K is embedded in $\mathbb{R}$. We take the projection of the periodicity lattice of $h^0_K|_H$ on the real coordinate corresponding to the embedding $K \subset \mathbb{R}$ and we take the exponential of the resulting elements. We call the set of elements we get this way E. Let $\|U\|$ be the set of squares of absolute values of U. We clearly have $\|U\| \subset E$. For every set $V \subset \mathbb{C}$ such that $\mathbb{Q}(V)$ is a number field, we write $V^k = \{\, v^k : v \in V \,\}$ for $k \in \mathbb{Z}_{>0}$. We write $\mathbb{Q}\{V\}$ for the field $\bigcap_{k \in \mathbb{Z}_{>0}} \mathbb{Q}(V^k)$. For $k \in \mathbb{Z}_{>0}$ sufficiently close to 0 in $\hat{\mathbb{Z}}$, we have $\mathbb{Q}\{V\} = \mathbb{Q}(V^k)$. We claim that we have $\mathbb{Q}\{\|U\|\} = K$. Indeed, write r_1 for the number of real primes and r_2 for the number of complex primes. Then $\|U\|^k$ has rank $r_1 + r_2 - 1$. The degree of a subfield of K is at most $\frac{1}{2}(r_1 + 2r_2)$ and hence, when $\mathbb{Q}\{U\}$ is a subfield of K, the unit-rank is at most $\frac{1}{2}r_1 + r_2 - 1$, which is a contradiction. Hence, we have $\mathbb{Q}\{\|U\|\} = K$. Because there is a $k \in \mathbb{Z}_{>0}$ with $E^k \subset \|U\|$ and we have $\|U\| \subset E$, we also have $\mathbb{Q}\{E\} = K$. We conclude that, given a real coordinate, we can construct E and we can construct a field isomorphic to K. If we know this real coordinate corresponds to a real coordinate of L, we could conclude that K and L are isomorphic.

Of course, the whole point is that we do not know which coordinates belong to

real primes. However, it might pay to just pick any coordinate and treat it as if it were a real coordinate. We construct the set E corresponding to this randomly chosen coordinate and construct the field $\mathbb{Q}\{E\}$. Hopefully, this field is either isomorphic to the field K we started with, or there is something wrong with it. For instance, it might have the wrong degree or signature.

28. Example. Let $K \subset \mathbb{C}$ be a number field of degree 3 with one complex prime and write U for the group of units of K. Let $\|U\|$ be the set of squares of absolute values of K with respect to the embedding $K \subset \mathbb{C}$. Then we have $K \cong \mathbb{Q}\{\|U\|\}$, even when $K \subset \mathbb{C}$ is not a real embedding. Hence, when k_K^0 is not constant on lines through the origin and we let E be the exponential of projection of the periodicity lattice of k_K^0 on any of the two coordinates, we have $K \cong \mathbb{Q}\{E\}$.

In the next example we give an example of a field L with an embedding $L \subset \mathbb{C}$ and unit group U such that $\mathbb{Q}\{\|U\|\}$ is a field of the same signature as L, but not isomorphic. This shows that our strategy of using the periodicity lattice of k_L^0 and taking the projection on just any coordinate does not work.

29. Example. Write $x = 1 + \sqrt{3} \in \mathbb{R}_{>0}$ and write $K = \mathbb{Q}(\sqrt[4]{x}) \subset \mathbb{R}$ and $L = \mathbb{Q}(\sqrt[4]{-4x}) \subset \mathbb{C}$. Both fields have two real primes and three complex primes. Write U for the group of units of L and write $\|U\|$ for the set of squares of the absolute values of the elements in U using the suggested embedding $L \subset \mathbb{C}$. Then we have $\mathbb{Q}\{\|U\|\} = K$. To see this let $M = K(i)$ be the normal closure of $K/\mathbb{Q}(x)$ in $\mathbb{C}$ with Galois group $G = \mathrm{Gal}(M/\mathbb{Q}(x))$ and write σ for the generator of $D_K = \mathrm{Gal}(M/K)$. It is easy to see that L is contained in M and we denote $\mathrm{Gal}(M/L)$ by D_L. The field $\mathbb{Q}(x)$ has two real primes and we identify the primes of M above the first prime with G/D_K and the other primes of M with G/D_L. We claim there is a $\mathbb{Q}[G]$-module isomorphism

$$f\colon O_M^* \otimes_{\mathbb{Z}} \mathbb{Q} \oplus \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}[G/D_K] \oplus \mathbb{Q}[G/D_L].$$

When we tensor both sides with $\mathbb{R}$, we get an $\mathbb{R}[G]$-module homomorphism by the Dirichlet unit theorem and by [1, lemma after proposition 12], this proves the existence of the isomorphism of $\mathbb{Q}[G]$-modules. Taking D_L-invariants gives $f(U \otimes \mathbb{Q} \oplus \mathbb{Q}) = \mathbb{Q}[G/D_K]^{D_L} \oplus \mathbb{Q}[G/D_L]^{D_L}$. There is a natural embedding $\mathbb{Q}[G/D_K] \subset \mathbb{Q}[G]$ and $\mathbb{Q}[G/D_L] \subset \mathbb{Q}[G]$ and when we apply $1 + \sigma$, we get

$$f(\|U\| \otimes \mathbb{Q} \oplus \mathbb{Q}) = (1+\sigma)\mathbb{Q}[G/D_K]^{D_L} \oplus (1+\sigma)\mathbb{Q}[G/D_L]^{D_L}.$$

Let H be the subgroup of G given by

$$H = \{\, h \in G : h \text{ is the identity on } \|U\| \otimes \mathbb{Q} \,\}.$$

We clearly have $\sigma \in H$ and we claim that H is equal to $\langle \sigma \rangle$. We prove this claim by showing there are no elements outside $\langle \sigma \rangle$ that are the identity on $f(\|U\| \otimes \mathbb{Q} \oplus \mathbb{Q})$. The group G is isomorphic to D_4. It is generated by σ and an element ρ of order 4 for

which we have $\rho\sqrt[4]{x} = -i\sqrt[4]{x}$ and $\rho(i) = i$. It follows that D_L is equal to $\langle\sigma\rho\rangle$. For $i \in \{0,1,2,3\}$, we write $\infty_i = \{\rho^i, \sigma\rho^{-i}\} \in G$ and we have $G/D_K = \{\infty_0, \infty_1, \infty_2, \infty_3\}$. An easy calculation shows that we have $\sigma\rho(\infty_i) = \infty_{3-i}$ for $i \in \{0,1,2,3\}$ and hence elements of $\mathbb{Q}[G/D_K]^{D_L}$ are of the form $x\infty_0 + y\infty_1 + y\infty_2 + x\infty_3$ with $x, y \in \mathbb{Q}$. We apply $1 + \sigma$ and get

$$(1+\sigma)(x\infty_0 + y\infty_1 + y\infty_2 + x\infty_3) = 2x\infty_0 + (x+y)\infty_1 + 2y\infty_2 + (x+y)\infty_3.$$

When we take $x = 1$ and $y = 0$, we see that the only elements of G that act trivially on the element above are 1 and σ. As every element in H acts trivially on the element above, we conclude that H is equal to $\langle\sigma\rangle$. It follows that $\|U\|$ is contained in K and not in a strict subfield of K and $\mathbb{Q}(x)$ and the same is true for $\|U\|^k$ for every $k \in \mathbb{Z}_{>0}$. For every $k \in \mathbb{Z}_{>0}$, we have $\mathbb{Q}(x) \subset \mathbb{Q}(\|U\|^k)$, because $2 + \sqrt{3} = 1 + x$ is in $\|U\|$. This proves that $\mathbb{Q}\{\|U\|\}$ is equal to K. On the other hand, the fields K and L are not isomorphic because they have a different splitting behavior at the prime 11 of $\mathbb{Q}$. The two fields do have the same discriminant, however!

References

[1] M. F. Atiyah and C. T. C. Wall, Cohomology of Groups. Chapter IV in: J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington D.C. (1967), pp. 94–115.

[2] G. van der Geer and R. Schoof, Effectivity of Arakelov Divisors and the Theta Divisor of a Number Field, *Selecta Mathematica, New Series* **6** (2000), pp. 377–398.

[3] R. P. Groenewegen, An arithmetic analogue of Clifford's theorem, *Journal de Théorie des Nombres de Bordeaux* **13** (2001), pp. 143–156.

[4] K. Iwasawa, Letter to Dieudonné, April 8, 1952. In: N. Kurokawa and T. Sunuda, *Zeta Functions in Geometry*, Advanced Studies in Pure Mathematics, **21** (1992), pp. 445–450.

[5] S. Lang, *Algebraic Number Theory*, second edition, Graduate Texts in Mathematics, 110. Springer (1994).

[6] J. S. Milne, Jacobian Varieties. In: G. Cornell and J. H. Silverman, *Arithmetic Geometry*, Springer (1991), Chapter VII, pp. 167–212.

[7] J. Tate, Fourier Analysis and Hecke's Zeta-functions, Thesis Princeton 1950. Printed in: J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington D.C. (1967), pp. 305–347.

MINKOWSKI FOR VECTOR BUNDLES

Richard P. Groenewegen

Abstract — In this article we define vector bundles over the ring of integers of a number field. Given a vector bundle P we are interested in finding a line bundle $L \subset P$ such that L has a small determinant. One way to find such line bundles is to find a short nonzero element in P using the Minkowski lattice theorem and then let L be the line bundle generated by this element. In this way, we see that for every P there is a line bundle L in P with $\det L \leq r^{n/2}|\Delta|^{1/2}(\det P)^{1/r}$, where n is the degree of the number field, Δ is the discriminant and r is the rank of P. The line bundles generated by one element are called cyclic. In this article we raise the question if we would get a better result if we did not restrict to cyclic line bundles. In particular, can the exponent $1/2$ of $|\Delta|$ be lowered in favor of a larger constant than $r^{n/2}$? We show that, given any r and any positive constant C, there is a number field of degree 2 and a vector bundle P over this field of rank r such that for all line bundles $L \subset P$, we have $\det L > C|\Delta|^{1/2-1/(2r)}(\det P)^{1/r}$. Hence, the exponent cannot be lowered below $\frac{1}{2}(1-1/r)$. We have not been able to close the gap between $\frac{1}{2}(1-1/r)$ and $1/2$.

1. Introduction

Finding short nonzero elements in lattices is both of practical and theoretical use. Given the determinant and rank of a lattice, the Minkowski theorem provides an upper bound on the length of the shortest nonzero element. In this article, by a lattice, or a lattice over $\mathbb{Z}$, we mean a free $\mathbb{Z}$-module P of finite rank r, together with an inner product on the r-dimensional $\mathbb{R}$-vector space $P_{\mathbb{R}} = P \otimes_{\mathbb{Z}} \mathbb{R}$. Later in this section, we will define (metrized) vector bundles over a ring of integers of a number field. For $\mathbb{Z}$ however, the definition of lattice and vector bundle over $\mathbb{Z}$ coincide. Given a nonzero element x in a vector bundle P over $\mathbb{Z}$, we get a vector bundle $x\mathbb{Z}$, where the inner product on $(x\mathbb{Z})_{\mathbb{R}}$ is given by taking the restriction of the inner product on $P_{\mathbb{R}}$ with respect to the inclusion $(x\mathbb{Z})_{\mathbb{R}} \subset P_{\mathbb{R}}$. Because $x\mathbb{Z}$ has rank 1, this is called a line bundle and for obvious reasons it is a sub-bundle of P. Finding a short nonzero element in P is equivalent to finding a sub-bundle of rank 1 of P with small determinant.

Let K be a number field of degree n with ring of integers O. A *(metrized) vector bundle* over O is a projective O-module P of finite rank r over O together with a hermitian inner product on $P_{\mathbb{R}}$. We will give an elaborate introduction to vector bundles in the next sections. For now it suffices to define hermitian inner products. The $\mathbb{R}$-vector space $P_{\mathbb{R}}$ is naturally an $O_{\mathbb{R}}$-module. Writing S_∞ for the set of infinite primes of K, we have a decomposition

$$O_{\mathbb{R}} = \prod_{v \in S_\infty} K_v,$$

where each of the completions K_v is either isomorphic to $\mathbb{R}$ or $\mathbb{C}$. Given an element $a \in O_{\mathbb{R}}$, we write a_v for its coordinate in K_v. On K_v we have the notion of complex conjugation—which is trivial if K_v is isomorphic to $\mathbb{R}$—and the complex conjugation a^* of a is given by taking the complex conjugation on every coordinate. A *hermitian inner product* on $P_{\mathbb{R}}$ is an $\mathbb{R}$-bilinear symmetric positive definite map

$$\langle \cdot\,, \cdot \rangle \colon P_{\mathbb{R}} \times P_{\mathbb{R}} \longrightarrow \mathbb{R},$$

such that for all x_1, $x_2 \in P_{\mathbb{R}}$ and $a \in O_{\mathbb{R}}$, we have $\langle ax_1, x_2\rangle = \langle x_1, a^* x_2\rangle$. Given an inner product, there is an induced *norm map* $\|\cdot\| \colon P_{\mathbb{R}} \to \mathbb{R}_{\geq 0}$, given by $\|x\| = \langle x, x\rangle^{1/2}$ for $x \in P_{\mathbb{R}}$. A vector bundle P is naturally a lattice over $\mathbb{Z}$ and by the determinant $\det P$ we mean the determinant of P as a lattice. Vector bundles of rank 1 over O are called *line bundles*.

Instead of finding short elements in a vector bundle, we are interested in finding sub-bundles of rank 1 with small determinant. More precisely, we want to find an upper bound for the determinant of the smallest line bundle in terms of the rank and determinant of the vector bundle and the degree, the discriminant and the class number of K. We get a 'trivial' upper bound when we view the vector bundle as a lattice over $\mathbb{Z}$, use Minkowski to find a short nonzero element and consider what line bundle this element generates.

1. Theorem. *Let K be a number field of degree n over $\mathbb{Q}$, with ring of integers O and discriminant Δ. Let P be a vector bundle of rank r over O. Then there exists a sub-bundle L of P of rank 1 with*

$$\det L \leq r^{n/2} |\Delta|^{1/2} (\det P)^{1/r}.$$

Although the proof is quite short and elementary, we postpone the proof until theorem 23. The appearance of the discriminant in the formula above is disturbing. When the rank of P is equal to 1, it says there is a sub-bundle L with $\det L \leq |\Delta|^{1/2} \det P$. However, in this case we can trivially take L equal to P and the upper bound in the rank 1 case is a factor $|\Delta|^{1/2}$ too large.

Given a set $\mathscr{F}$ of vector bundles with the same rank r, we write $\delta(\mathscr{F})$ for the infimum of all $\delta \in \mathbb{R}$ such that there is a constant $c \in \mathbb{R}$ such that for all vector bundles P in $\mathscr{F}$ there is a sub-bundle $L \subset P$ of rank 1 with

$$\det L \leq c |\Delta|^{\delta} (\det P)^{1/r}.$$

Given the rank r and degree n, we write $\mathscr{P}_{n,r}$ for a set of representatives for the set of isomorphism classes of all vector bundles of rank r over a ring of integers of a number field of degree n. We also write $\delta(n,r) = \delta(\mathscr{P}_{n,r})$. By theorem 1, we have $\delta(n,r) \leq 1/2$ for all $n, r \in \mathbb{Z}_{\geq 1}$. Trivially, we have $\delta(n,1) = 0$ for all $n \in \mathbb{Z}_{\geq 1}$. In this article, we prove the following theorem.

2. THEOREM. *For all $r \in \mathbb{Z}_{>0}$ we have $\delta(2,r) \geq \frac{1}{2}(1-1/r)$.*

The theorem says that, given any $r \in \mathbb{Z}_{>0}$, an element $\delta \leq \frac{1}{2}(1-1/r)$ and any positive constant C, there is a number field of degree 2 and a vector bundle P over this number field such that for all line bundles $L \subset P$, we have

$$\det L > C|\Delta|^{\delta}(\det P)^{1/r}.$$

This theorem is restated and proved in theorem 33. This still leaves a gap $\frac{1}{2}(1-1/r) \leq \delta(2,r) \leq \frac{1}{2}$ and we did not succeed in closing the gap, or even narrowing it. In section 6, we give an example of an explicit family $\mathscr{F}$ of vector bundles of rank r over rings of integers of imaginary quadratic fields. Even for this specific family $\mathscr{F}$, we do not know more than $\frac{1}{2}(1-1/r) \leq \delta(\mathscr{F}) \leq \frac{1}{2}$.

2. Hermitian modules

The category of finite étale algebras over $\mathbb{R}$ consists of finite $\mathbb{R}$-algebras A such that the map

$$A \longrightarrow \mathrm{Hom}_{\mathbb{R}}(A, \mathbb{R})$$

sending $x \in A$ to the $\mathbb{R}$-linear map $y \mapsto \mathrm{Tr}(xy)$ is an isomorphism of $\mathbb{R}$-vector spaces. Here Tr is the trace map from A over $\mathbb{R}$. If we let v range over the points of $S = \operatorname{spec} A$, we have a decomposition $A = \prod_v A_v$, where A_v is the residue class field. Every A_v is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. In the next section, we will specifically look at the situation with A equal to $O_{\mathbb{R}}$, where O is the ring of integers of a number field K. In that case, S is identified with the set S_∞ of infinite primes and A_v is equal to the completion K_v. That is why we will call S the set of primes of A. The identity functor on the category of the finite étale algebras over $\mathbb{R}$ has exactly one nontrivial automorphism $x \mapsto x^*$. Given a finite étale $\mathbb{R}$-algebra A and an element $x \in A$, the element x^* is given by complex conjugation on all factors A_v. When we talk about the involution of a finite étale algebra over $\mathbb{R}$ we mean this map.

Let M be a free module of finite rank r over an étale $\mathbb{R}$-algebra A. An inner product or *Euclidean structure* on M is an $\mathbb{R}$-bilinear symmetric positive definite map $\langle \cdot, \cdot \rangle \colon M \times M \to \mathbb{R}$. When M is endowed with a Euclidean structure, the endomorphism group $\mathrm{End}_{\mathbb{R}}(M)$ has a natural involution $\phi \mapsto \phi^*$, where the adjoint ϕ^* of ϕ is the unique element of $\mathrm{End}_{\mathbb{R}}(M)$ such that the relation $\langle \phi a, b \rangle = \langle a, \phi^* b \rangle$ holds. The Euclidean structure on M is called *hermitian* if the natural map $A \to \mathrm{End}_{\mathbb{R}}(M)$ preserves involutions. This is equivalent to the condition that for all $a \in A$ and $m_1, m_2 \in M$ we have $\langle a m_1, m_2 \rangle = \langle m_1, a^* m_2 \rangle$. A module with a hermitian structure is called a *hermitian module*. The module M has a decomposition $M = \prod_v M_v$, where v ranges over the elements of S and M_v is defined as $M_v = M \otimes_A A_v$. Given an element $m \in M$ and an element $v \in S$, we denote the image of m in M_v by m_v. Using the decomposition $M = \prod_v M_v$ we see that there is an injective A-module homomorphism $M_v \to M$ and we identify M_v with its image in M. In particular,

for an element $m \in M_v$, we have $m_w = 0$ for all $w \notin S \smallsetminus \{v\}$. Consequently, the image of the element 1 of A in A_v is denoted 1_v and we have $m_v = 1_v m$. Each of the factors M_v is an r-dimensional vector space over A_v. For $v \in S$, we write $\langle \cdot, \cdot \rangle_v \colon M_v \times M_v \to \mathbb{R}$ for the restriction of the inner product to $M_v \times M_v$ and for $m_1, m_2 \in M$ we also write $\langle m_1, m_2 \rangle_v$ for $\langle (m_1)_v, (m_2)_v \rangle_v = \langle (m_1)_v, (m_2)_v \rangle$.

The following lemma says that the factors $M_v \subset M$ are perpendicular if M is endowed with a hermitian structure. Given two elements m_1, $m_2 \in M$, we write $m_1 \perp m_2$ when m_1 and m_2 are perpendicular, meaning that we have $\langle m_1, m_2 \rangle = 0$. For two sets $X, Y \subset M$ we write $X \perp Y$ when we have $x \perp y$ for all $x \in X$ and $y \in Y$.

3. Lemma. *Let M be a free module of finite rank r over an étale $\mathbb{R}$-algebra A and let S be the set of primes of A. Furthermore, suppose M is endowed with a hermitian structure. Then for all $v, w \in S$ with $v \neq w$, we have $M_v \perp M_w$. Suppose v is an element of S for which A_v is isomorphic to $\mathbb{C}$ and let $i \in A_v$ be an element with $i^2 = -1$. Then for all $m \in M_v$, we have $m \perp im$ and $\langle m, m \rangle = \langle im, im \rangle$.*

Proof. Let v and w be two different elements from S. For $m_1 \in M_v \subset M$ and $m_2 \in M_w \subset M$, we have

$$\langle m_1, m_2 \rangle = \langle 1_v m_1, 1_w m_2 \rangle = \langle m_1, 1_v^* 1_w m_2 \rangle = \langle m_1, 0 m_2 \rangle = 0.$$

This proves $M_v \perp M_w$. Now suppose $v \in S$ is an element for which A_v is isomorphic to $\mathbb{C}$ and suppose m is an element of M_v. We have

$$\langle im, m \rangle = \langle m, -im \rangle = \langle -im, m \rangle = -\langle im, m \rangle$$

and hence $\langle im, m \rangle$ is zero. Finally, we have $\langle im, im \rangle = \langle m, -i^2 m \rangle = \langle m, m \rangle$. □

We now present a way of specifying a hermitian structure on a module M by choosing a basis of M over A. A basis is a sequence $(m_i)_{1 \leq i \leq r}$ of elements in M with $r = \operatorname{rank}_A M$ such that we have $M = Am_1 + \cdots + Am_r$. We usually write $\mathfrak{m} = (m_i)$ for a basis, where it is understood that i runs from 1 to the rank of M. Finally, we use the notation $m \in \mathfrak{m}$ as shorthand for $m \in \{m_1, \ldots, m_r\}$.

Suppose A is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. Choosing a basis of A^r over A is equivalent to giving an element of $\mathrm{GL}_r(A)$, the group of non-singular $r \times r$-matrices with coefficients in A. We write $O_r(A) \subset \mathrm{GL}_r(A)$ for the subgroup of orthonormal matrices with respect to the inner product $\langle x, y \rangle = [A : \mathbb{R}]^{-1} \sum_{i=1}^r \operatorname{Tr}(x_i y_i^*)$ on A^r. There is a correspondence between the set of hermitian structures on A^r and $\mathrm{GL}_r(A)/O_r(A)$. Given an element $m \in \mathrm{GL}_r(A)$, the corresponding basis of A^r over A consists of the columns $m_1, \ldots, m_r$ of the matrix m. Let $d \in \{1, 2\}$ be the degree $[A : \mathbb{R}]$. Given this basis, we define a hermitian structure on A^r by setting $\langle m_i, m_i \rangle = d$ for all $i \in \{1, \ldots, r\}$ and by requiring that the basis-elements are pairwise perpendicular. In the complex case, it follows from lemma 3 above that the Euclidean structure is uniquely determined. For the real case, this is trivial. Now let M be a finite free module over A. Given a basis of M over A, we have an isomorphism of M with A^r and hence there is an induced correspondence between $\mathrm{GL}_r(A)/O_r(A)$ and M. We record our observations in the lemma below.

4. Lemma. *Let A be isomorphic to $\mathbb{R}$ or $\mathbb{C}$ and let d be the degree of A over $\mathbb{R}$. Let M be a vector space of finite dimension over A. Given a basis $\mathfrak{m}$ of M over A, we have an induced hermitian structure on M, uniquely determined by*

$$\langle m, m\rangle = d \qquad \text{for all } m \in \mathfrak{m}$$

and the requirement $m \perp m'$ for $m, m' \in \mathfrak{m}$ with $m \neq m'$. Given a basis, there is an induced correspondence between $\mathrm{GL}_r(A)/O_r(A)$ and the set of hermitian structures on M.

When A is any finite étale $\mathbb{R}$-algebra and M is a finite free A-module of rank r, specifying a hermitian structure on M is equivalent to specifying a hermitian structure on each factor M_v over A_v. This gives a corollary to lemma 4 above.

5. Proposition. *Let A be a finite étale $\mathbb{R}$-algebra and M a finite free A-module. Let S be the set of primes of A and for $v \in S$, let d_v be equal to the degree $[A_v : \mathbb{R}]$. Given a basis $\mathfrak{m}$ of M over A, we have an induced hermitian structure on M, uniquely determined by*

$$\langle m, m\rangle_v = d_v \qquad \text{for all } v \in S \text{ and } m \in \mathfrak{m}$$

and the requirement $m_v \perp m'_v$ for $v \in S$ and $m, m' \in \mathfrak{m}$ with $m \neq m'$. Given a basis, there is an induced correspondence between $\bigoplus_{v\in S} \mathrm{GL}_r(A_v)/O_r(A_v)$ and the set of hermitian structures on M.

Proof. Let r be the rank of M over A. Given a basis $\mathfrak{m} = (m_i)$ of M over A and an element $v \in S$, the sequence $(\,(m_i)_v\,)_{1\leq i\leq r}$ forms a basis of M_v over A_v. Conversely, given a basis $(m_{i,v})_{1\leq i\leq r}$ of M_v over A_v for every $v \in S$, we get an induced basis (m_i) of M over A by setting $m_i = \sum_{v\in S} m_{i,v}$ for all i. The proposition thus reduces to the local case, which was already done in lemma 4. □

When M is a hermitian module, a basis $\mathfrak{m}$ for M is called *orthonormal* if it induces the hermitian structure as in proposition 5.

Let M be a finite free module over a finite étale $\mathbb{R}$-algebra A. Let $\overline{M}$ be the module with the same underlying group as M, but such that the action of an element $a \in A$ on an element $m \in \overline{M}$ is given by a^*m. Then a hermitian inner product on M becomes a map $M \times \overline{M} \to \mathbb{R}$ which factorizes over the tensor product $M \otimes_A \overline{M}$. In fact, the set of hermitian inner products on M is in this way identified with a subset of $\mathrm{Hom}_{\mathbb{R}}(M \otimes_A \overline{M}, \mathbb{R})$.

6. Proposition. *Let M be a module over a finite étale $\mathbb{R}$-algebra A. There is an isomorphism*

$$\mathrm{Hom}_A(M \otimes_A \overline{M}, A) \longrightarrow \mathrm{Hom}_{\mathbb{R}}(M \otimes_A \overline{M}, \mathbb{R}),$$

given by $\phi \mapsto \mathrm{Tr} \circ \phi$.

PROOF. We use two ingredients. First of all, we use that $A \to \mathrm{Hom}_{\mathbb{R}}(A, \mathbb{R})$ given by $x \mapsto \mathrm{Tr}(x\,\cdot\,)$ is an isomorphism. It follows that $\mathrm{Hom}_A(M \otimes_A \overline{M}, A)$ is isomorphic to $\mathrm{Hom}_A(M \otimes_A \overline{M}, \mathrm{Hom}_{\mathbb{R}}(A, \mathbb{R}))$. The second ingredient we use is lemma 7 below, which implies that this module is isomorphic to $\mathrm{Hom}_{\mathbb{R}}((M \otimes_A \overline{M}) \otimes_A A, \mathbb{R}) = \mathrm{Hom}_{\mathbb{R}}(M \otimes_A \overline{M}, \mathbb{R})$. □

7. LEMMA. *Let R be a commutative ring with 1 and let A be an R-module. Let B and C be A-modules and let D be an R-module. Then we have an isomorphism*

$$\mathrm{Hom}_A(B, \mathrm{Hom}_R(C, D)) \longrightarrow \mathrm{Hom}_R(B \otimes_A C, D),$$

given by $\phi \longmapsto [b \otimes c \mapsto \phi(b)(c)]$.

PROOF. It is easily checked that, given $\phi \in \mathrm{Hom}_A(B, \mathrm{Hom}_R(C, D))$, the map $b \otimes c \mapsto \phi(b)(c)$ is well-defined and R-linear. The inverse is given by sending $\psi \in \mathrm{Hom}_R(B \otimes_A C, D)$ to the map $b \mapsto [c \mapsto \psi(b \otimes c)]$ in $\mathrm{Hom}_A(B, \mathrm{Hom}_R(C, D))$. □

8. PROPOSITION. *Let M be a finite free module over a finite étale $\mathbb{R}$-algebra A with set of primes S. Let $\Psi \subset \mathrm{Hom}_{\mathbb{R}}(M \otimes_A \overline{M}, \mathbb{R})$ be the set of hermitian inner products on M and let $\Phi \subset \mathrm{Hom}_A(M \otimes_A \overline{M}, A)$ the corresponding set under the isomorphism from proposition 6. The set Φ consists of the elements ϕ such that for all $m_1, m_2 \in M$ we have $\phi(m_1 \otimes m_2) = \phi(m_2 \otimes m_1)^*$ and for all nonzero $m \in M$ we have $\phi(m \otimes m) \neq 0$ and $\phi(m \otimes m)_v \in \mathbb{R}_{\geq 0}$ for all $v \in S$.*

PROOF. Let ψ be an element of $\mathrm{Hom}_{\mathbb{R}}(M \otimes_A \overline{M}, \mathbb{R})$ and assume ψ is symmetric. Let $\phi \in \mathrm{Hom}_A(M \otimes_A \overline{M}, A)$ be an element with $\mathrm{Tr} \circ \phi = \psi$. For every element $a \in A$, we have $\mathrm{Tr}(a) = \mathrm{Tr}(a^*)$. Hence, the image of the map $M \times M \to A$ given by

$$(a, b) \longmapsto \phi(a \otimes b) - \phi(b \otimes a)^*$$

is contained in the kernel of Tr. Actually, because the map is A-bilinear, the image is contained in a subset of the kernel of Tr which is stable under the action of A. We conclude that this image is zero and we have $\phi(a \otimes b) = \phi(b \otimes a)^*$. Now assume that ψ is not only symmetric but also positive definite. Using the equality $\phi(a \otimes a) = \phi(a \otimes a)^*$, we see that we have $\phi(a \otimes a) \in \prod_{v \in S} \mathbb{R}$. Suppose there is an element $v \in S$ for which $\phi(a \otimes a)_v$ is negative. Then we have

$$\psi(1_v a \otimes 1_v a) = \mathrm{Tr}\, 1_v 1_v \phi(a \otimes a) = \mathrm{Tr}_{A_v/\mathbb{R}}\, \phi(a \otimes a)_v = [A_v : \mathbb{R}] \phi(a \otimes a)_v < 0.$$

This is a contradiction. Hence, we have $\phi(a \otimes a)_v \geq 0$ for all $v \in S$. □

9. PROPOSITION. *Let A be a finite étale $\mathbb{R}$-algebra and M a finite free A-module. Given a basis $\mathfrak{m}$ of M over A, there is an A-sesquilinear map $(\,\cdot\,,\,\cdot\,)\colon M \times M \to A$, given by*

$$(\sum_{m \in \mathfrak{m}} a_m m, \sum_{m \in \mathfrak{m}} a'_m m) = \sum_{m \in \mathfrak{m}} a_m a'^*_m$$

for $a, a' \in A^{\mathfrak{m}}$. The map $\operatorname{Tr} \circ(\,\cdot\,,\,\cdot\,)$ is the inner product from proposition 5.

PROOF. Let S be the set of primes of A and let v be an element of S. Let m be an element of $\mathfrak{m}$. We have

$$\operatorname{Tr}(m_v, m_v) = \operatorname{Tr}(1_v m, 1_v m) = \operatorname{Tr} 1_v = \operatorname{Tr}_{A_v/\mathbb{R}} 1 = d_v,$$

where d_v is the degree of A_v over $\mathbb{R}$. Let m' be another element of $\mathfrak{m}$. Then we have

$$\operatorname{Tr}(m_v, m'_v) = \operatorname{Tr}(1_v m, 1_v m') = \operatorname{Tr} 0 = 0.$$

Hence, $\operatorname{Tr} \circ(\,\cdot\,,\,\cdot\,)$ satisfies the same requirements as the inner product from proposition 5. □

Let M and N be two hermitian modules over a finite étale $\mathbb{R}$-algebra A. Then $M \otimes_A N$ is a finite free A-module and it has a natural hermitian structure. Let $(\,\cdot\,,\,\cdot\,)_M \colon M \times M \to A$ be the map corresponding to the inner product $\langle\,\cdot\,,\,\cdot\,\rangle_M \colon M \times M \to \mathbb{R}$ of M, as provided by proposition 6. In other words, we have $\langle m_1, m_2\rangle_M = \operatorname{Tr}(m_1, m_2)_M$ for $m_1, m_2 \in M$. Likewise, let $(\,\cdot\,,\,\cdot\,)_N \colon N \times N \to A$ be the map corresponding to the inner product $\langle\,\cdot\,,\,\cdot\,\rangle_N$ of N. We define an A-sesquilinear map

$$(\,\cdot\,,\,\cdot\,) \colon (M \otimes_A N) \times (M \otimes_A N) \longrightarrow A$$

by $(m_1 \otimes n_1, m_2 \otimes n_2) = (m_1, m_2)_M (n_1, n_2)_N$. The canonical inner product on $M \otimes_A N$ is given by taking the composition with the trace map. This shows how to multiply hermitian modules. Given bases $\mathfrak{m} = (m_i)_{1 \le i \le r}$ and $\mathfrak{n} = (n_j)_{1 \le j \le s}$ of M and N respectively, we write $\mathfrak{mn}$ for the basis of $M \otimes_A N$ given by $(e_k)_{1 \le k \le rs}$ with $e_{(i-1)s+j} = m_i \otimes n_j$. The following two propositions give alternative ways of deriving the hermitian structure on the tensor product.

10. PROPOSITION. *Let M and N be hermitian modules over a finite étale $\mathbb{R}$-algebra A with orthonormal bases $\mathfrak{m}$ and $\mathfrak{n}$ respectively (as defined below proposition 5). Then the set $\mathfrak{mn}$ is an orthonormal basis of $M \otimes_A N$.*

PROOF. Let S be the set of primes of A. It suffices to check that $\langle x, x\rangle_v$ is equal to $d_v = [A_v : \mathbb{R}]$ for $x \in \mathfrak{mn}$ and that $\langle x, y\rangle_v$ equals 0 for $x, y \in \mathfrak{mn}$ with $x \neq y$. Both checks are routine and follow easily from proposition 9. □

When M and N are hermitian modules with inner products $\langle\,\cdot\,,\,\cdot\,\rangle_M$ and $\langle\,\cdot\,,\,\cdot\,\rangle_N$, the $\mathbb{R}$-vector space $M \otimes_{\mathbb{R}} N$ has an inner product uniquely determined by

$$\langle m_1 \otimes n_1, m_2 \otimes n_2\rangle = \langle m_1, m_2\rangle_M \langle n_1, n_2\rangle_N$$

for $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Let $\phi \colon M \otimes_{\mathbb{R}} N \to M \otimes_A N$ be the natural projection map. The orthogonal complement $(\ker \phi)^{\perp}$ of the kernel has a natural inner product inherited from the inner product on $M \otimes_{\mathbb{R}} N$.

11. Proposition. *Let M and N be hermitian modules over a finite étale $\mathbb{R}$-algebra A and let $\phi\colon M \otimes_{\mathbb{R}} N \to M \otimes_A N$ be the projection map. The isomorphism $(\ker\phi)^\perp \to M \otimes_A N$ preserves the inner product.*

Proof. The proof is easily reduced to the local case where A is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. The case $A \cong \mathbb{R}$ is completely trivial, so we will assume that A is isomorphic to $\mathbb{C}$. Let $i \in A$ be an element with $i^2 = -1$. Let r be the rank of M over A and let s be the rank of N over A. Furthermore, let $\mathfrak{m}$ and $\mathfrak{n}$ be orthonormal bases for M and N. The kernel of the map $\phi\colon M \otimes_{\mathbb{R}} N \to M \otimes_A N$ has $\mathbb{R}$-dimension $2rs$ and an $\mathbb{R}$-basis is given by the elements of the set

$$\bigcup_{\substack{m\in\mathfrak{m}\\ n\in\mathfrak{n}}} \{im \otimes in + m \otimes n, im \otimes n - m \otimes in\}.$$

Let $\mathfrak{mn}$ be the basis for $M \otimes_A N$, defined before proposition 10, and let $m \otimes n$ be an element from $\mathfrak{mn}$. Clearly, $x = \frac{1}{2}(-im \otimes in + m \otimes n)$ is an element of $(\ker\phi)^\perp$, mapping to $m \otimes n$. Write $\langle \cdot, \cdot \rangle_{M\otimes_{\mathbb{R}} N}$ for the inner product on $M \otimes_{\mathbb{R}} N$, and write $\langle \cdot, \cdot \rangle$ for the inner product on $M \otimes_A N$. We have

$$\langle x, x\rangle_{M\otimes_{\mathbb{R}} N} = \tfrac{1}{4}(2\langle m, m\rangle\langle n, n\rangle) = 2 = \langle m \otimes n, m \otimes n\rangle.$$

It follows from a similar calculation that the elements in the inverse image of $\mathfrak{mn}$ in $(\ker\phi)^\perp$ are pairwise perpendicular. □

We have now seen several ways to multiply hermitian modules. The A-module A with hermitian structure induced by the basis (1) is a neutral element for multiplication. By this we mean that for a hermitian A-module M, the induced hermitian structure on $M \otimes_A A$ is the same as the one induced by the natural isomorphism $M \to M \otimes_A A$. When we talk about the hermitian module A without specifying the hermitian structure explicitly, we will always mean this structure.

Given two hermitian modules M and N, the canonical hermitian structure on $M \oplus N$ is given by $\langle (m, n), (m', n')\rangle = \langle m, m'\rangle + \langle n, n'\rangle$ for $m, m' \in M$ and $n, n' \in N$. For $k \in \mathbb{Z}_{>0}$, we write M^k for the direct sum of k copies of M. When $\mathfrak{m} = (m_i)_{1\le i\le r}$ is a basis of M over A, inducing the inner product, the isomorphism $A^r \to M$, sending $(a_i)_{1\le i\le r}$ to $\sum_{i=1}^r a_i m_i$ preserves the hermitian structure.

We have shown what the canonical hermitian structure is on the tensor product and the direct sum of two hermitian modules. Finally, we also define a canonical structure on exterior powers of hermitian modules. Given a commutative ring R with 1, a module E over R and a positive integer k, the k-th exterior power of E over R is the R-module

$$\bigwedge^k E = E^{\otimes k}/J_k,$$

where J_k is the submodule of $E^{\otimes k}$ generated by tensors of the form $x_1 \otimes \cdots \otimes x_k$ with $x_i = x_j$ for some $i \neq j$. The image of an element $x_1 \otimes \cdots \otimes x_k$ of $E^{\otimes k}$ in $\bigwedge^k E$ is denoted $x_1 \wedge \cdots \wedge x_k$. When F is another R-module and $f\colon E \to F$ is an R-linear

map, we have an induced map $\bigwedge^k f\colon \bigwedge^k E \to \bigwedge^k F$ such that for $x_1, \ldots, x_k \in E$, we have

$$(\bigwedge^k f)(x_1 \wedge \cdots \wedge x_k) = f(x_1) \wedge \cdots \wedge f(x_k).$$

When E is a free R-module of rank r, we have $\bigwedge^k E = 0$ for $k > r$ and for $1 \leq k \leq r$, we have

$$\operatorname{rank}_R \bigwedge^k E = \binom{r}{k}.$$

For a proof of this statement, see [4, proposition XIX.1.1]. In particular, the module $\bigwedge^r E$ has rank 1 and if (e_i) is a basis of E over R then $(e_1 \wedge \cdots \wedge e_r)$ is a basis of $\bigwedge^r E$ over R.

Let M be a hermitian module over A and let $(\,\cdot\,,\,\cdot\,)\colon M \times M \to A$ be the A-sesquilinear map corresponding to the inner product. Let k be a positive integer. We define an A-sesquilinear map $(\,\cdot\,,\,\cdot\,)\colon \bigwedge^k M \times \bigwedge^k M \to A$ by

$$(m_1 \wedge \cdots \wedge m_k, m'_1 \wedge \cdots \wedge m'_k) = \det\left((m_i, m'_j)\right)_{i,j=1}^k,$$

for $m_i, m'_j \in M$. Taking the composition with the trace map yields the inner product on $\bigwedge^k M$.

12. Proposition. *Let M be a hermitian module of rank r with orthonormal basis (m_i). Then $\bigwedge^r M$ has orthonormal basis $(m_1 \wedge \cdots \wedge m_r)$.*

Proof. Let A be the étale $\mathbb{R}$-algebra over which M is a hermitian module and let S be the set of primes of A. Let v be an element of S. There is a canonical isomorphism $\bigwedge^r M_v \cong (\bigwedge^r M)_v$, where the first exterior power is taken over A_v. Explicitly, for $x_1, \ldots, x_r \in M$ and $a_1, \ldots, a_r \in A_v$, the element $x_1 \otimes a_1 \wedge \cdots \wedge x_r \otimes a_r \in \bigwedge^r M_v$ is sent to $(x_1 \wedge \cdots \wedge x_r) \otimes a_1 a_2 \ldots a_r$. The element $(m_1 \wedge \cdots \wedge m_r)_v \in (\bigwedge^r M)_v$ corresponds to the element

$$1_v m_1 \wedge m_2 \wedge \cdots \wedge m_r = 1_v m_1 \wedge 1_v m_2 \wedge \cdots \wedge 1_v m_r = (m_1)_v \wedge \cdots \wedge (m_r)_v$$

in M. The matrix I_v with (i,j)-th coordinate equal to $((m_i)_v, (m_j)_v)$ is equal to the identity matrix over A_v and we have

$$\langle m_1 \wedge \cdots \wedge m_r, m_1 \wedge \cdots \wedge m_r \rangle_v = \operatorname{Tr} \det I_v = \operatorname{Tr} 1_v = [A_v : \mathbb{R}].$$

Hence, $(m_1 \wedge \cdots \wedge m_r)$ is indeed an orthonormal basis. □

Remark. One might wonder if there is an analogue of proposition 11 for exterior powers. To be more precise, if M is a hermitian module of rank r, the exterior power $\bigwedge^r M$ is a quotient of $M^{\otimes r}$ and as such is isomorphic as an A-module to the orthogonal complement of the kernel of the quotient map $\phi\colon M^{\otimes r} \to \bigwedge^r M$. However, if (m_i) is a basis for M, the element of $(\ker \phi)^\perp$ that is sent to the element $m_1 \wedge \cdots \wedge m_r$ is

$$x = \frac{1}{r!} \sum_{\sigma \in S_r} \operatorname{sign}(\sigma) m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(r)}.$$

For v in the set of primes of A, we have $\langle x, x \rangle_v = [A_v : \mathbb{R}]/r!$ and this differs by a factor $r!$ from $\langle \phi(x), \phi(x) \rangle_v$.

3. Vector bundles

Let K be a number field with ring of integers O. A metrized vector bundle over O is a projective O-module P of finite rank together with an inner product on $P_{\mathbb{R}}$ such that $P_{\mathbb{R}}$ becomes a hermitian module over $O_{\mathbb{R}}$. In this article we drop the annotation 'metrized' and just talk about vector bundles. We write $\langle \cdot, \cdot \rangle$ for the inner product on $P_{\mathbb{R}}$ and we have a norm function $\| \cdot \| \colon P_{\mathbb{R}} \to \mathbb{R}_{\geq 0}$, given by $\|x\| = \langle x, x \rangle^{1/2}$ for $x \in P_{\mathbb{R}}$. Given two vector bundles P and Q, the product $P \otimes Q$ is given by the O-module $P \otimes_O Q$ with the canonical structure on $(P \otimes_O Q)_{\mathbb{R}} = P_{\mathbb{R}} \otimes_{O_{\mathbb{R}}} Q_{\mathbb{R}}$. Likewise, the direct sum $P \oplus Q$ is naturally a vector bundle. A vector bundle of rank 1 is called a line bundle. When P is of rank r, the projective module $\bigwedge^r P$ is in a natural way a line bundle, because we have $(\bigwedge^r P)_{\mathbb{R}} = \bigwedge^r P_{\mathbb{R}}$.

The set of isomorphism classes of metrized line bundles with multiplication forms a group which is called the Picard group $\operatorname{Pic} K$. The isomorphism class of the line bundle O, where the orthonormal basis of $O_{\mathbb{R}}$ over $O_{\mathbb{R}}$ is (1), is the neutral element for the multiplication in the Picard group.

Given a vector bundle P, the inner product induces a measure on $P_{\mathbb{R}}$—the Haar measure that gives a box spanned by an orthonormal $\mathbb{R}$-basis measure 1—and hence it is clear what we mean by the determinant $\det P$ of $P \subset P_{\mathbb{R}}$ as a lattice. The norm of a *line* bundle L is defined by

$$N(L) = \frac{\det O}{\det L} = \frac{|\Delta|^{1/2}}{\det L},$$

where Δ is the discriminant of K. For a vector bundle P of rank r, we define the norm by the formula

$$N(P) = N(\textstyle\bigwedge^r P).$$

The degree of a vector bundle is defined by $\deg P = \log N(P)$.

For $r \in \mathbb{Z}_{>0}$, the module O^r has rank r over O and an orthonormal basis is given by the r elements that have one coordinate equal to 1 and all other coordinates equal to 0. The induced orthonormal basis of $(\bigwedge^r O^r)_{\mathbb{R}}$ over $O_{\mathbb{R}}$ is also a basis of $\bigwedge^r O^r$ over O and hence $\bigwedge^r O^r$ is isomorphic to O as a line bundle. We conclude that for $P = O^r$, we have $\det P = |\Delta|^{(r-1)/2} \det \bigwedge^r P$. We will prove that this formula holds for all vector bundles of degree r. First, we give a few definitions and lemmas concerning exterior powers and determinants.

Let R be a commutative ring with 1 and let V be a finite free module of rank r over R. Let ϕ be an element of $\operatorname{End}_R(V)$. Then $\bigwedge^r \phi$ is a linear map $\bigwedge^r V \to \bigwedge^r V$ and hence it is given by multiplication with an element a of R. We define $\det_R \phi = a$. Equivalent definitions of the determinant can be found in [1, III §8]. When we have two linear maps ϕ and ψ, we have $\det_R(\phi \circ \psi) = (\det_R \phi)(\det_R \psi)$. When R is equal to $\mathbb{R}$, we write $\det \phi$ instead of $\det_{\mathbb{R}} \phi$.

13. Lemma. *Let P be a lattice in $\mathbb{R}^k$ for $k \in \mathbb{Z}_{>0}$ with a Haar measure on $\mathbb{R}^k$ and let $\phi \in \operatorname{End}_{\mathbb{R}}(\mathbb{R}^k)$ be a linear map. Then we have*

$$\frac{\det \phi P}{\det P} = |\det \phi|.$$

PROOF. Let $(e_i)_{1\leq i\leq k}$ be the basis of $\mathbb{R}^k$ such that the i-th coordinate of e_i is 1 and all other coordinates are 0. By the box spanned by the basis (e_i), we mean the set $\{\, a_1e_1+\cdots+a_ke_k : a_1,\dots,a_k\in[0,1]\,\}$. Because the statement of the lemma does not depend on the choice of the Haar measure, we will assume without loss of generality that a box spanned by the basis (e_i) has volume 1. Let $\phi\in\mathrm{End}_{\mathbb{R}}(\mathbb{R}^k)$ be an elementary linear map. That is, the matrix corresponding to ϕ is obtained from the identity matrix by either swapping two columns or adding a column to another column. When a column is added to another column we have $e_1\wedge\cdots\wedge e_k=\phi e_1\wedge\cdots\wedge\phi e_k$ and hence $\det\phi=1$. When two rows are swapped we have $\det\phi=-1$. Clearly, the volume of the box given by (ϕe_i) is the same as the volume of the box given by (e_i). Hence, we have $\det\phi\mathbb{Z}^k/\det\mathbb{Z}^k=|\det\phi|$. It is easy to see that this formula also holds when the matrix corresponding to ϕ is a diagonal matrix. Because every matrix can be made into diagonal form by multiplying with elementary matrices, we use the multiplicity of the determinant to see that we have $\det\phi\mathbb{Z}^k/\det\mathbb{Z}^k=|\det\phi|$ for *all* maps $\phi\in\mathrm{End}_{\mathbb{R}}(\mathbb{R}^k)$. Now let $\psi\in\mathrm{End}_{\mathbb{R}}(\mathbb{R}^k)$ be a map with $\psi\mathbb{Z}^k=P$. Then we have

$$\frac{\det\phi P}{\det P}=\frac{\det(\phi\psi\mathbb{Z}^k)}{\det\mathbb{Z}^k}\frac{\det\mathbb{Z}^k}{\det\psi\mathbb{Z}^k}=|\det(\phi\circ\psi)|\frac{1}{|\det\psi|}=|\det\phi|.$$

This concludes the proof. □

The following lemma is not used in this section, but this is the most obvious place to state it.

14. LEMMA. *Let P be a lattice in $\mathbb{R}^k$ for $k\in\mathbb{Z}_{>0}$ with an inner product on $\mathbb{R}^k$. Let (p_i) be an $\mathbb{R}$-basis for P. Then we have*

$$\det P=|\det(\langle p_i,p_j\rangle)_{i,j}|^{1/2}$$

PROOF. Let (e_i) be an orthonormal basis and let $A=(a_{ij})_{i,j}$ be the matrix corresponding to the linear map sending e_i to p_i. Then we have

$$(\langle p_i,p_j\rangle)_{i,j}=\big(\sum_{k,l}a_{ik}a_{jl}\langle e_k,e_l\rangle\big)_{i,j}=\big(\sum_k a_{ik}a_{jk}\big)_{i,j}=AA^T,$$

where A^T is the transposed of A. Hence, by lemma 13, we have $|\det(\langle p_i,p_j\rangle)_{i,j}|=|\det A|^2=((\det P)/(\det\sum_i e_i\mathbb{Z}))^2=(\det P)^2$. □

15. LEMMA. *Let R be a commutative ring with 1 and let A be an R-algebra which is finite free as an R-module. Let V be a finite free module over A. For $\phi\in\mathrm{End}_A(V)\subset\mathrm{End}_R(V)$, we have $\det_R\phi=N_{A/R}(\det_A\phi)$, where $N_{A/R}$ denotes the norm of A over R.*

PROOF. This is proved in [2, theorem A.1]. □

16. Proposition. *Let P be a vector bundle over O such that P is free of rank r as a module over O. Then we have* $\det P = |\Delta|^{(r-1)/2} \det \bigwedge^r P$.

Proof. We write $A = O_{\mathbb{R}}$ and we denote the hermitian A-module $(O^r)_{\mathbb{R}}$ by V. Let (v_i) be an orthonormal basis for V and let (p_i) be an orthonormal basis for $P_{\mathbb{R}}$. We let $\phi\colon V \to P_{\mathbb{R}}$ be the A-linear map which sends v_i to p_i for $1 \leq i \leq r$. The map ϕ preserves the inner product. Because P is free of rank r over O, we have an O-module isomorphism $P \to O^r$ and this induces an A-module isomorphism $i\colon P_{\mathbb{R}} \to V$. We identify P with its pre-image $\phi^{-1}(P)$ in V and we identify ϕ with the endomorphism $i \circ \phi \in \mathrm{End}_A(V)$. We have $\phi P = O^r$ and we have already calculated

$$\frac{\det \phi P}{\det \bigwedge^r \phi P} = \frac{\det O^r}{\det \bigwedge^r O^r} = \frac{\det O^r}{\det O} = |\Delta|^{(r-1)/2}.$$

From lemma 13, we know that $(\det \phi P)/(\det P)$ is equal to $|\det \phi|$. We claim that we also have

$$\frac{\det \bigwedge^r \phi P}{\det \bigwedge^r P} = |\det \phi|$$

and once we have proven that, we can conclude

$$\frac{\det P}{\det \bigwedge^r P} = \frac{\det P}{\det \bigwedge^r P} \frac{\det \phi P}{\det P} \frac{\det \bigwedge^r P}{\det \bigwedge^r \phi P} = \frac{\det \phi P}{\det \bigwedge^r \phi P} = |\Delta|^{(r-1)/2}.$$

Write $a = \det_A \phi \in A$. Then we have

$$\textstyle\bigwedge^r \phi P = (\bigwedge^r \phi) \bigwedge^r P = a \bigwedge^r P.$$

Multiplication by a is an $\mathbb{R}$-linear map and by definition the determinant is equal to $N(a)$. Hence, by lemma 13, we have

$$\frac{\det a \bigwedge^r P}{\det \bigwedge^r P} = |N(a)|.$$

Furthermore, by lemma 15, this is equal to $|\det \phi|$. This proves our claim. □

Next, we will show that when P and Q are projective O-modules of finite rank r with $P \subset Q$ of finite index, the index $[Q : P]$ is the same as $[\bigwedge^r Q : \bigwedge^r P]$. Actually, we will prove something stronger: Q/P and $\bigwedge^r Q / \bigwedge^r P$ are the same in the Grothendieck group. Let A be a Noetherian integrally closed domain and let $\mathscr{C}_A$ be the category of A-modules of finite length. Given a module M of length m there is a composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_m = M$ such that each quotient M_i/M_{i-1} is isomorphic to a non-zero prime ideal $\mathfrak{p}_i$ of A. We put $\chi_A(M) = \prod_i \mathfrak{p}_i$. The Grothendieck group is $\mathscr{C}_A$, where modules with the same χ_A are identified. For exact sequences

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

we have $\chi_A(M) = \chi_A(M')\chi(M'')$. For more information, we refer to [7, §I.6]. The following lemma comes directly from this reference.

17. Lemma. *Let A be a principal ideal domain and $u\colon A^n \to A^n$ a linear map with $\det(u) \neq 0$. Then $\det(u)A = \chi_A(\operatorname{coker} u)$.*

Proof. This is [7, lemma I.6.3]. □

18. Proposition. *Let P and Q be projective modules of rank r over O with $P \subset Q$. Then we have $\chi_O(Q/P) = \chi_O(\bigwedge^r Q/\bigwedge^r P)$. In particular, we have $[Q : P] = [\bigwedge^r Q : \bigwedge^r P]$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of O. The localizations $Q_\mathfrak{p}$ and $P_\mathfrak{p}$ are free $O_\mathfrak{p}$-modules. We write $A = O_\mathfrak{p}$ and we fix isomorphisms $P_\mathfrak{p} = A^r$ and $Q_\mathfrak{p} = A^r$. The inclusion map $P_\mathfrak{p} \to Q_\mathfrak{p}$ becomes an A-linear map $u\colon A^r \to A^r$. Hence, by lemma 17, we have $\chi_A(Q/P) = \chi_A(\operatorname{coker} u) = \det(u)A$. We also have

$$\chi_A(\textstyle\bigwedge^r Q_\mathfrak{p}/\bigwedge^r P_\mathfrak{p}) = \chi_A(A/(\bigwedge^r u)A) = \chi_A(A/\det(u)A) = \det(u)A.$$

It now follows that we have

$$\begin{aligned}\chi_O(Q/P)_\mathfrak{p} = \chi_A(Q_\mathfrak{p}/P_\mathfrak{p}) = \chi_A(\textstyle\bigwedge^r Q_\mathfrak{p}/\bigwedge^r P_\mathfrak{p}) \\ = \chi_A((\textstyle\bigwedge^r Q)_\mathfrak{p}/(\bigwedge^r P)_\mathfrak{p}) = \chi_O(\bigwedge^r Q/\bigwedge^r P)_\mathfrak{p}.\end{aligned}$$

Because $\mathfrak{p}$ was arbitrary, we can now conclude $\chi_O(Q/P) = \chi_O(\bigwedge^r Q/\bigwedge^r P)$. □

19. Proposition. *Let P be a vector bundle of rank r over O. Then we have $\det P = |\Delta|^{(r-1)/2} \det \bigwedge^r P$.*

Proof. Let Q be a free O-module of rank r with $P \subset Q$ and give $Q_\mathbb{R}$ the inner product induced by the map $P_\mathbb{R} \to Q_\mathbb{R}$. Let k be the index $[Q : P] = [\bigwedge^r Q : \bigwedge^r P]$. Then by proposition 16, we have

$$\det P = k^{-1} \det Q = |\Delta|^{(r-1)/2} k^{-1} \det \textstyle\bigwedge^r Q = |\Delta|^{(r-1)/2} \det \bigwedge^r P.$$

This proves the proposition. □

20. Proposition. *Let P and Q be two vector bundles over O with $\operatorname{rank} P = r$ and $\operatorname{rank} Q = s$. Then the vector bundle $P \otimes Q$ had rank rs and we have*

$$\textstyle\bigwedge^{rs}(P \otimes Q) = (\bigwedge^r P)^{\otimes s} \otimes (\bigwedge^s Q)^{\otimes r}.$$

Proof. First, let P and Q be two finite free modules of rank r and s over a commutative ring A with 1. Then there is a canonical isomorphism $\bigwedge^{rs}(P \otimes Q) \to (\bigwedge^r P)^{\otimes s} \otimes (\bigwedge^s Q)^{\otimes r}$ given as follows. Choose a basis (p_i) for P and a basis (q_i) for Q. Then

$$p_1 \otimes q_1 \wedge \cdots \wedge p_1 \otimes q_s \wedge p_2 \otimes q_1 \wedge \cdots \wedge p_r \otimes q_s$$

is a basis for $\bigwedge^{rs}(P \otimes Q)$. The canonical homomorphism sends this basis element to the basis element

$$\underbrace{(p_1 \wedge \cdots \wedge p_r) \otimes \cdots \otimes (p_1 \wedge \cdots \wedge p_r)}_{s \text{ times}} \otimes \underbrace{(q_1 \wedge \cdots \wedge q_s) \otimes \cdots \otimes (q_1 \wedge \cdots \wedge q_s)}_{r \text{ times}}$$

of $(\bigwedge^r P)^{\otimes s} \otimes (\bigwedge^s Q)^{\otimes r}$. Given another basis (p_i') of P there is a matrix $g \in \mathrm{GL}_r(A)$ with $(p_i') = g \cdot (p_i)$. When we replace the basis (p_i) by (p_i'), the basis for $\bigwedge^{rs}(P \otimes Q)$ is multiplied with a factor $(\det_A g)^s$. To see this, we first note that this is easy to check for elementary matrices g—the ones corresponding to swapping two basis vectors or adding one to another. Hence, we can assume that g is a diagonal matrix. Furthermore, a diagonal matrix can be decomposed as a product of diagonal matrices where at most one entry on the diagonal is not equal to 1. But for these matrices the statement is also trivial. Likewise, when we replace (p_i) by (p_i'), the basis for $(\bigwedge^r P)^{\otimes s} \otimes (\bigwedge^s Q)^{\otimes r}$ also changes with a factor $(\det_A g)^s$. By symmetry, a similar statement holds when we replace the basis (q_i). We conclude that the canonical homomorphism does not depend on the choice of the basis.

Now, let P and Q be vector bundles over O as in the statement of this proposition. Then $P_K = P \otimes_O K$ and $Q_K = Q \otimes_O K$ are free K modules of rank r and s and we have shown there is a canonical K-module isomorphism

$$\phi_K \colon \bigwedge^{rs}(P_K \otimes Q_K) \longrightarrow (\bigwedge^r P_K)^{\otimes s} \otimes (\bigwedge^s Q_K)^{\otimes r}.$$

Given a finite prime $\mathfrak{p}$ of O, the modules $P_\mathfrak{p}$ and $Q_\mathfrak{p}$ are free over $O_\mathfrak{p}$. Localization commutes with taking exterior powers and tensor products. A basis of $P_\mathfrak{p}$ over $O_\mathfrak{p}$ is also a basis of P_K over O_K. Hence, we get an isomorphism $\phi_\mathfrak{p} \colon \bigwedge^{rs}(P_\mathfrak{p} \otimes Q_\mathfrak{p}) \to (\bigwedge^r P_\mathfrak{p})^{\otimes s} \otimes (\bigwedge^s Q_\mathfrak{p})^{\otimes r}$ that extends to ϕ_K. Taking the intersection over all finite primes, shows that the restriction ϕ of ϕ_K to $\bigwedge^{rs}(P \otimes Q)$ is an isomorphism with $(\bigwedge^r P)^{\otimes s} \otimes (\bigwedge^s Q)^{\otimes r}$.

When we tensor with $\mathbb{R}$, we get an isomorphism $\phi_\mathbb{R} \colon \bigwedge^{rs}(P_\mathbb{R} \otimes Q_\mathbb{R}) \longrightarrow (\bigwedge^r P_\mathbb{R})^{\otimes s} \otimes (\bigwedge^s Q_\mathbb{R})^{\otimes r}$ of hermitian modules by propositions 10 and 12. The restriction of $\phi_\mathbb{R}$ to $\bigwedge^{rs}(P \otimes Q)$ is still ϕ. This can be seen by embedding P_K in $P_\mathbb{R} = P_K \otimes_\mathbb{Z} \mathbb{R}$ and Q_K in $Q_\mathbb{R}$, which shows that ϕ_K is a restriction of $\phi_\mathbb{R}$ and hence ϕ is a restriction of $\phi_\mathbb{R}$. □

21. Corollary. *Let P and Q be vector bundles over O with* $\operatorname{rank} P = r$ *and* $\operatorname{rank} Q = s$. *Then the vector bundle $P \otimes Q$ has rank rs and we have*

$$N(P \otimes Q)^{1/(rs)} = N(P)^{1/r} N(Q)^{1/s}.$$

4. Finding small line bundles

We now give a proof of theorem 1, which was stated in the introduction. We use the Minkowski lattice theorem and the following lemma, which relates the norm of a line bundle to the length of the shortest nonzero element in the line bundle. In this section, K is a number field of degree n over $\mathbb{Q}$ with ring of integers O and discriminant Δ.

22. Lemma. *Let L be a line bundle over O. Then for all nonzero elements $x \in L$, we have*

$$\|x\|^2 \geq nN(L)^{-2/n}.$$

Proof. This is [3, lemma 20]. □

23. Theorem. *Let P be a vector bundle of rank $r > 0$ over O. Then there exists a sub-bundle L of P of rank 1 with*

$$\det L \leq r^{n/2}|\Delta|^{1/2}(\det P)^{1/r}.$$

Proof. Let $B \subset P_{\mathbb{R}}$ be a box with side $2\det(P)^{1/(nr)}$ with respect to the inner product on $P_{\mathbb{R}}$, centered around the origin. The volume of B equals $2^{\dim_{\mathbb{R}} P_{\mathbb{R}}} \det P$ and it follows from the Minkowski lattice theorem that there is a nonzero element $x \in P \cap B$. Let L be the line bundle generated by x. Because x is in B, we have $\|x\| \leq \sqrt{rn}\det(P)^{2/(nr)}$. On the other hand, we have lemma 22, which says $nN(L)^{-2/n} \leq \|x\|^2$. When we tie the inequalities together, we get

$$nN(L)^{-2/n} \leq rn\det(P)^{2/(nr)}.$$

Considering that $N(L)$ is equal to $|\Delta|^{1/2}/\det L$, the theorem follows immediately from this inequality. □

Using the notation $\delta(n, r)$ from the introduction, we have the following corollary.

24. Corollary. *We have $\delta(n, r) \leq 1/2$ for all $n, r \in \mathbb{Z}_{>0}$.*

5. Vector bundles with not so small sub-bundles

Let K be an imaginary quadratic field with ring of integers O and discriminant Δ, class number h and number of roots of unity $w = \#\mu_K$. Let r be a positive integer. We are going to construct so many vector bundles of rank r in O^r that they cannot all have small sub-bundles of rank 1. A precise statement is given in proposition 31. After that proposition, we will vary the field K and prove theorem 2. Until we state otherwise the field K is fixed and the propositions and lemmas implicitly refer to it.

Let $\mathfrak{p}$ be a prime of O of degree 1. We are going to vary $\mathfrak{p}$ later. Given an element $\alpha \in \mathbb{P}^{r-1}(O/\mathfrak{p})$ of the $(r-1)$-dimensional projective space over $O/\mathfrak{p}$, we can write $\alpha = (\overline{a}_1 : \overline{a}_2 : \cdots : \overline{a}_r)$ for some elements $a_i \in O$ with reductions $\overline{a}_i \in O/\mathfrak{p}$. We define

$$P_\alpha = \{\, (x_1, \ldots, x_r) \in O^r : a_i x_j \equiv a_j x_i \bmod \mathfrak{p} \,\}$$

Clearly, P_α does not depend on the choice of the elements $a_i \in O$. The hermitian structure on $P_{\mathbb{R}}$ is given by the inclusion $P_{\mathbb{R}} \subset (O^r)_{\mathbb{R}}$ and hence we have a well-defined vector bundle. We write $p = N\mathfrak{p}$ and we write $\mathbb{P} = \mathbb{P}^{r-1}(O/\mathfrak{p})$. We have the following lemma.

25. Lemma. *For $\alpha \in \mathbb{P}$, we have $[P_\alpha : \mathfrak{p}^r] = p$. For all vector bundles P with $\mathfrak{p}^r \subset P \subset O^r$ and $[P : \mathfrak{p}^r] = p$, there is a unique $\alpha \in \mathbb{P}$ with $P = P_\alpha$. Finally, the cardinality of $\mathbb{P}$ is $p^{r-1} + p^{r-2} + \cdots + 1$.*

Proof. Let $\alpha \in \mathbb{P}$ be given. Let $i \in \{1, \ldots, r\}$ be one of the indices for which α at i is nonzero. The map $P_\alpha \to O/\mathfrak{p}$ given by the projection on the i-th coordinate, followed by reduction modulo $\mathfrak{p}$ is a surjective map and the kernel is equal to $\mathfrak{p}^r$. Hence, we have $P_\alpha/\mathfrak{p}^r \cong O/\mathfrak{p}$ and therefore the index $[P_\alpha : \mathfrak{p}^r]$ is equal to $\#(O/\mathfrak{p}) = N\mathfrak{p} = p$.

Now, let P be a vector bundle with $\mathfrak{p}^r \subset P \subset O^r$ and $[P : \mathfrak{p}^r] = p$. Let a be an element in $P \smallsetminus \mathfrak{p}^r$. Let $\alpha = (\overline{a}_1 : \cdots : \overline{a}_r)$ be the element in $\mathbb{P}$ corresponding to a. We claim that P_α is contained in P. Let x be an element in P_α. Let i be an index with $\overline{a}_i \neq 0$ and let $y \in O$ be an element with $\overline{y} = \overline{x}_i/\overline{a}_i \in O/\mathfrak{p}$. Let $1 \leq j \leq r$ be an arbitrary index. Then we have

$$ya_j \equiv \frac{x_i a_j}{a_i} \equiv \frac{x_j a_i}{a_i} \equiv x_j \bmod \mathfrak{p}.$$

In other words, we have $ya \equiv x \bmod \mathfrak{p}^r$ and hence x is in P. We have shown that we have $P_\alpha \subset P$ and because the index $[P : \mathfrak{p}^r]$ is equal to $[P_\alpha : \mathfrak{p}^r]$ we conclude that P_α is equal to P. Because every element in $P = P_\alpha$ outside $\mathfrak{p}^r$ induces the same element in $\mathbb{P}$, uniqueness of α follows. The statement about the cardinality of $\mathbb{P}$ is easy combinatorics. □

We now know what vector bundles P with $\mathfrak{p}^r \subset P \subset O^r$ and $[P : \mathfrak{p}^r] = p$ look like and how many there are. We are now going to examine line bundles in O^r and count how many 'small' ones there are. Given a line bundle $L \subset O^r$ and an index $1 \leq i \leq r$, we write $\pi_i \colon L_\mathbb{R} \to O_\mathbb{R}$ for the projection on the i-th coordinate.

26. Proposition. *Let $L \subset O^r$ be a line bundle. Then we have*

$$\det L = \sum_{i=1}^{r} \det \pi_i L.$$

Proof. Let $\pi = \pi_i$ be one of the projection maps. Then π is either the zero map on $L_\mathbb{R}$, or it is injective. Indeed, suppose $a, a' \in L_\mathbb{R}$ are two different elements with $\pi(a) = \pi(a')$. Then $a - a'$ is a nonzero element of $L_\mathbb{R}$ and we have $(a - a')O_\mathbb{R} \subset L_\mathbb{R}$. In fact, because the $O_\mathbb{R}$-rank of $L_\mathbb{R}$ is 1, we have $(a - a')O_\mathbb{R} = L_\mathbb{R}$. Thus, we have $\pi L_\mathbb{R} = \pi((a - a')O_\mathbb{R}) = 0$, which is what we had to show.

Now suppose that the proposition is true for a specific line bundle L and let L' be a line bundle with $L \subset L'$ of finite index. Let Π be the set of projections π_i for $i \in \{1, \ldots, r\}$ with π_i not the zero map. Then we have for all $\pi \in \Pi$ an equality $[L' : L] = [\pi L' : \pi L]$. Hence, using our assumption on L, we can conclude

$$\det L' = [L' : L]^{-1} \det L = \sum_{\pi \in \Pi} [\pi L' : \pi L]^{-1} \det \pi L = \sum_{i=1}^{r} \pi_i L'.$$

Let $L' \subset O^r$ be any line bundle and let $a \in L'$ be a nonzero element. Then $L = aO$ is of finite index in L'. In light of the remarks above it suffices to prove the proposition for L and the corresponding statement for L' follows. Let (e_1, e_2) be a $\mathbb{Z}$-basis for O. By lemma 14, we have

$$\det L = \left| \det \begin{pmatrix} \langle ae_1, ae_1 \rangle & \langle ae_1, ae_2 \rangle \\ \langle ae_2, ae_1 \rangle & \langle ae_2, ae_2 \rangle \end{pmatrix} \right|^{1/2}.$$

Each of the entries of the matrix can be expanded as

$$\langle ae_i, ae_j \rangle = \sum_{k=1}^{r} \langle a_k e_i, a_k e_j \rangle = \langle e_i, e_j \rangle \sum_{k=1}^{r} |a_k|^2.$$

It follows that the determinant of L is equal to

$$\det L = (\det O) \sum_{i=1}^{r} |a_i|^2.$$

A similar calculation shows that for $\pi_i L = a_i O$, we have

$$\det \pi_i L = (\det O)|a_i|^2.$$

The formula $\det L = \sum_i \det \pi_i L$ now follows immediately. □

27. Lemma. *Given ideals $I_1, \ldots, I_r \subset O$, there are at most $w^{r-1} = (\#\mu_K)^{r-1}$ line bundles $L \subset O^r$ with $I_i = \pi_i L$ for $1 \leq i \leq r$.*

Proof. Suppose L is a line bundle satisfying the conditions. Without loss of generality we will assume that I_1 is nonzero. For every k for which I_k is nonzero, we have an O-isomorphism

$$I_1 \xrightarrow{\pi_1^{-1}} L \xrightarrow{\pi_k} I_k.$$

Any other isomorphism $I_1 \to I_k$ is given by the map $\pi_k \circ \pi_1^{-1}$ followed by multiplication with a unit $\eta \in \mu_K$. Let L' be another line bundle satisfying the same conditions from the lemma with L replaced by L'. Let $\eta_k \in \mu_K$ be the unit such that the isomorphism $I_1 \to I_k$ induced by L followed by multiplication by η_k is the isomorphism $I_1 \to I_k$ induced by L'. When we let $J \subset \{2, \ldots, r\}$ be the set of indices k with I_k nonzero, we claim that, given L, the line bundle L' is uniquely determined by $(\eta_k)_{k \in J}$. Indeed, when we define $\eta_k = 0$ for $k \notin J$, the isomorphism $I_1 \to L'$ is given by the isomorphism $I_1 \to L$ followed by multiplication by $(\eta_k)_{1 \leq k \leq r}$ coordinate-wise. Hence, the number of line bundles fitting the requirements of the lemma is bounded by $\#(\mu_K)^J \leq w^{r-1}$. □

For $t \in \mathbb{R}$, we write $\mathscr{L}_t$ for the set of line bundles $L \subset O^r$ with $\det L \leq t$. We want to estimate the number of elements of $\mathscr{L}_t$. We use an estimate on the number of ideals of O with bounded norm.

28. Theorem. *The number of ideals in O in one specific ideal class and with norm at most t is equal to*

$$\frac{2\pi}{w|\Delta|^{1/2}}t + O(t^{1-1/n}),$$

Proof. This is a weak form of the formula given in [5, theorem VI.3.3]. □

It is important to note that the norm in the previous theorem refers to the ideal norm and not to the norm of the ideal viewed as a line bundle in O. In particular, the determinant of an ideal with ideal norm t is equal to $t \det O = t|\Delta|^{1/2}$.

29. Proposition. *For large enough $t \in \mathbb{R}$, we have $\#\mathscr{L}_t \leq (2\pi)^r h|\Delta|^{-r}t^r$.*

Proof. For every $L \in \mathscr{L}_t$ the projections $\pi_i L$ have determinant at most t by proposition 26. Moreover, all the projections that are nonzero are in the same class of the class group. Let $\mathfrak{c}$ be an element of the class group. Using theorem 28, we have

$$\#\{\, I \subset O : \det I \leq t \text{ and } [I] = \mathfrak{c} \,\} = \frac{2\pi}{w|\Delta|}t + O(t^{1-1/n}).$$

Hence, when we also use lemma 27 and sum over the h elements in the class group, we get

$$\#\mathscr{L}_t \leq h\Big(\frac{2\pi}{w|\Delta|}t + O(t^{1-1/n})\Big)^r w^{r-1}.$$

For t large, the term

$$hw^{r-1}\Big(\frac{2\pi}{w|\Delta|}t\Big)^r = \frac{1}{w}\frac{h(2\pi)^r}{|\Delta|^r}t^r$$

dominates and because w is at least 2 we have

$$\#\mathscr{L}_t \leq \frac{h(2\pi)^r}{|\Delta|^r}t^r$$

for t large enough. □

30. Lemma. *For all line bundles $L \subset O^r$ with $L \not\subset \mathfrak{p}^r$, there is a unique $\alpha \in \mathbb{P}$ with $L \subset P_\alpha$. For $t < p|\Delta|^{1/2}$, we have $L \not\subset \mathfrak{p}^r$ for all $L \in \mathscr{L}_t$.*

Proof. Let L be a line bundle with $L \not\subset \mathfrak{p}^r$. Let π be a projection map with $\pi L \not\subset \mathfrak{p}$. Then the map $L \to O/\mathfrak{p}$ induced by $\mathfrak{p}$ is surjective. Moreover, the kernel is contained in $\mathfrak{p}^r$. Hence, we have $[L+\mathfrak{p}^r : \mathfrak{p}^r] = p$ and hence there is an $\alpha \in \mathbb{P}$ with $L + \mathfrak{p}^r = P_\alpha$ by lemma 25. This is the unique α for which we have $L \subset \mathbb{P}_\alpha$.

Let t be smaller than $p|\Delta|^{1/2}$ and let L be in $\mathscr{L}_t$. Let π be a projection with πL nonzero. By proposition 26, we have $\det \pi L \leq t$. Therefore πL cannot be contained in $\mathfrak{p}$. It follows that L is not contained in $\mathfrak{p}^r$. □

31. Proposition. *There exists a vector bundle P of rank r such that for all line bundles $L \subset P$, we have*

$$\det L > (\det P)^{1/r} \frac{|\Delta|^{1/2}}{h^{1/r}}.$$

Proof. We keep the field K fixed, but we are going to vary the prime ideal $\mathfrak{p}$. Given a $\mathfrak{p}$ of degree 1, we write $p = N\mathfrak{p}$ and

$$t = p^{(r-1)/r} \frac{|\Delta|}{h^{1/r} 2\pi}.$$

We take the norm of the prime $\mathfrak{p}$ so large that t is smaller than $p|\Delta|^{1/2}$ and such that t is large enough such that proposition 29 applies. By lemma 30, every line bundle $L \in \mathscr{L}_t$ is contained in exactly one vector bundle P_α. By proposition 29, the number of line bundles in $\mathscr{L}_t$ is at most p^{r-1}, which by lemma 25 is smaller than $\#\mathbb{P}$. Hence, there is an $\alpha \in \mathbb{P}$ such that the line bundle L in P_α with the smallest determinant is not contained in $\mathscr{L}_t$. Hence, for the determinant of L we have

$$\det L > t > p^{(r-1)/r} \frac{|\Delta|}{h^{1/r}} = (\det P_\alpha)^{1/r} \frac{|\Delta|^{1/2}}{h^{1/r}}.$$

We take $P = P_\alpha$ and the proposition follows. □

We are now going to vary the number field K. First we state a result that the class number is bounded in terms of the discriminant.

32. Lemma. *For all $\varepsilon > 0$, there is a positive constant $c \in \mathbb{R}$ such that for all imaginary quadratic fields K with discriminant Δ and class number h, we have $h \leq c|\Delta|^{1/2+\varepsilon}$.*

Proof. This is a weak form of the 'trivial' inequality of the Brauer-Siegel theorem [5, chapter XVI]. It also follows from the explicit bound

$$h \leq d(1 + \log d), \qquad \text{with} \quad d = \frac{2}{\pi}|\Delta|^{1/2},$$

which is given in [6, theorem 6.5]. □

We can now prove theorem 2 from the introduction.

33. Theorem. *For all $r \in \mathbb{Z}_{>0}$ we have $\delta(2, r) \geq \frac{1}{2}(1 - 1/r)$.*

Proof. Let $r \in \mathbb{Z}_{>0}$ be given and write $y = \frac{1}{2}(1 - 1/r)$. Let δ be any value smaller than y and let C be any positive number. Write $\varepsilon = \frac{1}{2}r(y - \delta)$ and let c be the constant from lemma 32 with $h \leq c|\Delta|^{1/2+\varepsilon}$ for all imaginary quadratic fields. For imaginary quadratic field with $|\Delta|$ large enough, we have

$$\frac{|\Delta|^{1/2}}{h^{1/r}} \geq \frac{|\Delta|^{1/2}}{(c|\Delta|^{1/2+\varepsilon})^{1/r}} = \frac{1}{c^{1/r}} |\Delta|^{\delta + (y-\delta)/2} \geq C|\Delta|^{\delta}.$$

Hence, there is an imaginary quadratic number field with discriminant Δ such that by proposition 31, there exists a vector bundle P of rank r such that for all line bundles $L \subset P$, we have $\det L > C|\Delta|^{\delta}(\det P)^{1/r}$. As C was arbitrary, this shows that δ is smaller than $\delta(2, r)$. □

6. An example family

When given a vector bundle with a particularly small nonzero vector relative to the determinant, the strategy of finding a small sub-bundle of rank 1 by looking what is generated by the smallest nonzero vector obviously works. Hence, when we want to construct a vector bundle without small sub-bundles, it is a good idea to make sure that the successive minima are roughly equal. We give a family of vector bundles that satisfies this requirement.

Let $d \equiv 1 \bmod 4$ be a positive square-free integer and write $K = \mathbb{Q}(\sqrt{-d}\,)$ with ring of integers $O = \mathbb{Z}[\sqrt{-d}\,]$. We identify the completion of K at the infinite prime with $\mathbb{C}$ and we give $\mathbb{C} \oplus \mathbb{C}$ orthonormal basis $\big((2^{-1/2}, 0), (0, 2^{-1/2})\big)$ over $\mathbb{C}$ in the sense of lemma 4. Hence, we have $\|(1,0)\|^2 = \|(0,1)\|^2 = 1$. We write i for a primitive 4-th root of unity in $\mathbb{C}$, we define $\varepsilon = 1/\sqrt{d}$ and let F be the vector bundle

$$F = (1,0)O + (i,\varepsilon)O \subset \mathbb{C} \oplus \mathbb{C}.$$

A $\mathbb{Z}$-basis for F is given by the elements $e_1 = (1,0)$, $e_2 = (i\sqrt{d}, 0)$, $e_3 = (i,\varepsilon)$, $e_4 = (\sqrt{d}, i\varepsilon\sqrt{d}\,)$. For $a_1, \ldots, a_4 \in \mathbb{Z}$, we have

$$\|a_1e_1 + \cdots + a_4e_4\|^2 = (a_1 + a_4\sqrt{d}\,)^2 + (a_3 + a_2\sqrt{d}\,)^2 + a_3^2d^{-1} + a_4^2.$$

Either e_1 or $e_2 - \lfloor\sqrt{d}\rfloor e_3$ is a smallest nonzero vector. When d goes to infinity, the length of the shortest nonzero vector converges to 1. Another $\mathbb{Z}$-basis of F is given by the elements e_1 and $e_2 - \lfloor\sqrt{d}\rfloor e_3$ together with the elements e_3 and $e_4 - \lfloor\sqrt{d}\rfloor e_1$. When d goes to infinity, the lengths of all these vectors tend to 1. Moreover, this new basis is roughly orthogonal. Hence, one would expect the determinant of F to be about $1^4 = 1$. This is precisely the case.

34. Lemma. *For every d, the determinant of F is equal to* 1.

Proof. By lemma 14, the determinant of F is equal to $|\det(\langle e_i, e_j\rangle)_{i,j}|^{1/2}$ which by calculation is equal to

$$\left|\det\begin{pmatrix} 1 & 0 & 0 & \sqrt{d} \\ 0 & d & \sqrt{d} & 0 \\ 0 & \sqrt{d} & 1 + 1/d & 0 \\ \sqrt{d} & 0 & 0 & d+1 \end{pmatrix}\right|^{1/2} = 1.$$

This proves the lemma. □

Let $\mathscr{F}$ be the set of all F for all positive square-free $d \equiv 1 \bmod 4$. Theorem 23 only states that for each $F \in \mathscr{F}$ there is a sub-bundle L of rank 1 with $\det L \leq 2|\Delta|^{1/2}$. In fact by taking $L = e_1 O$, we have a line bundle $L \subset F$ with $\det L = \frac{1}{2}|\Delta|^{1/2}$. Using the notation from the introduction, this is nothing more than $\delta(\mathscr{F}) \leq \frac{1}{2}$. For every line bundle $L \subset F$ there is a line bundle M of degree 0 such that $L \otimes M \subset F \otimes M$ is cyclic, i.e., generated over O by one element. For every line bundle M of degree 0, we write $\lambda_M(F)$ for the shortest nonzero vector in the twist $F \otimes M$ of F. Of course, the determinant of $F \otimes M$ is still 1. If $\delta(\mathscr{F})$ is smaller than $\frac{1}{2}$, this would mean in particular that $\min_M \lambda_M(F)$ tends to 0 when d goes to infinity. However, we have not succeeded in proving anything more than what can already be derived from theorem 23 and theorem 33, namely: $\frac{1}{4} \leq \delta(\mathscr{F}) \leq \frac{1}{2}$.

References

[1] N. Bourbaki, *Elements of Mathematics: Algebra I*, Chapters 1–3, Springer (1991). Translated from the French original (Éléments de Mathématique, Algèbre 1–3, 1970).

[2] J. W. S. Cassels, Global Fields. Chapter II in: J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington D.C. (1967), pp. 42–84.

[3] R. P. Groenewegen, An arithmetic analogue of Clifford's theorem, *Journal de Théorie des Nombres de Bordeaux* **13** (2001), pp. 143–156.

[4] S. Lang, *Algebra*, third edition, Addison-Wesley (1993).

[5] S. Lang, *Algebraic Number Theory*, second edition, Graduate Texts in Mathematics, 110, Springer (1994).

[6] H. W. Lenstra, Jr., Algorithms in algebraic number theory, *Bulletin of the American Mathematical Society (New Series)* **26**, (1992), no. 2, pp. 211-244.

[7] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, 67, Springer (1979). Translated from the French original (Corps locaux).

BOUNDS FOR COMPUTING THE TAME KERNEL

Richard P. Groenewegen

Abstract — The tame kernel of the K_2 of a number field F is the kernel of some explicit map $K_2F \to \bigoplus k_v^*$, where the product runs over all finite primes v of F and k_v is the residue class field at v. When S is a set of primes of F, containing the infinite ones, we can consider the S-unit group U_S of F. Then $U_S \otimes U_S$ has a natural image in K_2F. The tame kernel is contained in this image if S contains all finite primes of F up to some bound. This is a theorem due to Bass and Tate. An explicit bound for imaginary quadratic fields was given by Browkin. In this article we give a bound, valid for any number field, that is smaller than Browkin's bound in the imaginary quadratic case and has better asymptotics. A simplified version of this bound says that we only have to include in S all primes with norm up to $4|\Delta|^{3/2}$, where Δ is the discriminant of F. Using this bound, one can find explicit generators for the tame kernel, and a 'long enough' search would also yield all relations. Unfortunately, we have no explicit formula to describe what 'long enough' means. However, using theorems from Keune we can show that the tame kernel is computable.

1. Introduction and statement of the main theorem

The explicit determination of the tame kernel of a number field is similar to the determination of class groups. As a consequence of a suitable Minkowski bound, the computations are restricted to a finite set of primes with small norms. Using these primes one searches for relations until finally one can prove, or at least conjecture, that the found generators and relations yield the whole group. It is useful to have a small upper bound on the norm of the primes used.

In order to make the above discussion more explicit, we give some definitions. Let F be a number field, with ring of integers $\mathcal{O}$ and discriminant Δ. We define the group K_2F as

$$K_2F = (F^* \otimes F^*)/\langle\, a \otimes b : a, b \in F^*, a + b = 1\rangle.$$

All tensor products in this article are taken over $\mathbb{Z}$. The class belonging to $a \otimes b$ is written as $\{a, b\}$ and the group operation is written multiplicatively. There is a more general definition of the K_2 of a ring, as a group of non-obvious matrix relations, but we do not need it here. It can be found in [12].

For $v\colon F \to \mathbb{Z} \cup \{\infty\}$ a non-archimedean valuation corresponding to the prime ideal $\mathfrak{p}_v$ of $\mathcal{O}$ with residue class field $k_v = \mathcal{O}/\mathfrak{p}_v$, we define a map $t_v\colon K_2F \to k_v^*$ by

$$\{a, b\} \longmapsto (-1)^{v(a)v(b)} \frac{a^{v(b)}}{b^{v(a)}} \bmod \mathfrak{p}_v.$$

2000 *Mathematics Subject Classification.* Primary 11R70; Secondary 11Y40, 19C20.

Key words and phrases. K-theory, tame kernel, calculations, S-units.

We will often refer to valuations as primes. The *tame kernel* is defined as the kernel of the map

$$(t_v)_{v<\infty}\colon K_2F \longrightarrow \bigoplus_{v<\infty} k_v^*.$$

Using the more general definition of the K_2, one can show that the tame kernel is equal to $K_2\mathcal{O}$ (see [13, §5, corollary to theorem 5]). It is a finite group (see [6]) and when we talk about determining it explicitly, we mean giving a finite number of generators and relations for the group.

The determination of the tame kernel is made manageable with the use of a filtration of K_2F. For any set S of primes of F that contains the set S_∞ of infinite primes, we define U_S as the group of S-units of F, i.e., $U_S = \{\, x \in F^* : v(x) = 0 \text{ for all } v \notin S \,\}$. For every positive integer m, we write

$$U_m = U_{S_m}, \qquad \text{where} \quad S_m = S_\infty \cup \{\text{all finite primes } v \text{ with } Nv \le m\}.$$

Here, the norm Nv denotes the order $\#k_v$ of the residue class field. Now we can define

$$K^{(m)} = (U_m \otimes U_m)/\langle a \otimes b : a, b \in U_m, a + b = 1 \text{ or } a + b = 0\rangle.$$

In K_2F, we have $\{-a, a\} = 1$ for all $a \in F^*$. For $a \neq 1$ we see this from the computation $\{-a, a\} = \{-a, a\}\{1 - a^{-1}, a^{-1}\}^{-1} = \{-a + 1, a\} = 1$. That is why there is a natural map $K^{(m)} \to K_2F$. We write K^m for the image of $K^{(m)}$ in K_2F. The maps $K^{m-1} \to K^m$ are injective, whereas the maps $K^{(m-1)} \to K^{(m)}$ may not be. For every m we have an 'approximation' $K_2^{(m)}\mathcal{O}$ of the tame kernel, defined by

$$K_2^{(m)}\mathcal{O} = \ker\bigl[K^{(m)} \longrightarrow \bigoplus_{Nv\le m} k_v^*\bigr],$$

where the direct sum is taken over all finite primes with norm up to m. The groups $K_2^{(m)}\mathcal{O}$ have two important virtues. As we will see, $K_2^{(m)}\mathcal{O}$ is computable as a function of m and F, meaning that there is an algorithm that, given m and F in some explicit way, computes the group in a finite number of steps. Furthermore, when m is large enough, the group $K_2^{(m)}\mathcal{O}$ is equal to the tame kernel.

We can now state a simplified version of the main theorem of this article.

1. Theorem. *For every number field F, there are constants c_F, c'_F such that*
   (1) *for all $m > c_F$, the map $K^{(m)}/\operatorname{im} K^{(m-1)} \to \bigoplus_{Nv=m} k_v^*$ induced by the maps t_v is an isomorphism. The direct sum is taken over all finite primes with norm equal to m.*
   (2) *for all $m > c'_F$, the map $K^{(m)} \to K^m$ is an isomorphism.*

For $m > c_F$, the image of $K_2^{(m)}\mathcal{O}$ in K_2F is equal to the tame kernel. For $m > \max\{c_F, c'_F\}$, the natural map $K_2^{(m)}\mathcal{O} \to K_2\mathcal{O}$ is an isomorphism. We can take $c_F = 4|\Delta|^{3/2}$. The group $K_2^{(m)}\mathcal{O}$ is computable as a function of m and F.

This theorem is a consequence of theorem 15, in which we give a different c_F, which is smaller by proposition 21. Anyone who wants to use our theorem for calculations should use the results in section 8.

Part 1 of the theorem, without an explicit c_F, is a reformulation of theorem II.3.1 in an article of Bass and Tate [1]. Careful inspection of their arguments led to explicit bounds, and for imaginary quadratic number fields the best bound so far was given by Browkin [2]. He proves that we can take $c_F = 2^6\pi^{-10/3}|\Delta|^{5/3}$ when F is imaginary quadratic and $|\Delta|$ is at least 15. Clearly, the bound in our theorem above is asymptotically better. In section 8, we work out what the bound in theorem 15 amounts to in the imaginary quadratic case. It turns out our bound outperforms Browkin's bound for small discriminants also. Our results are compared to those of Browkin in section 8.

One can find explicit generators for the tame kernel by finding generators for $K_2^{(m)}\mathcal{O}$, where we have $m > c_F$. Unfortunately, we have no explicit formula for c'_F. However, using theorems from Keune [8] that allow us to determine the order of the p-primary part of the tame kernel, we can compute the tame kernel and hence also c'_F.

2. Theorem. *The smallest feasible value of c'_F and the tame kernel $K_2\mathcal{O}$ are computable as a function of the number field F.*

This theorem is a combination of theorem 19 and theorem 20 from section 8. Basically, we take an $m > c_F$ that is large enough such that the kernel of the map $K^{(m)} \to \bigoplus_{Nv \le m} k_v^*$ is finite. Then the tame kernel is a quotient of this kernel, which gives a bound on the order of the tame kernel and allows us to use Keune's theorems.

The first calculations of tame kernels were done by Tate, who computed the tame kernels for the six imaginary quadratic fields with $|\Delta| \le 15$ in the appendix of [1]. Recent, but currently unpublished, calculations using the bound in this article are done by K. Belabas and H. Gangl. They have independently been using Keune's theorems to prove correctness of their results. Some of their results are stated in the appendix of [2].

While proving the main theorem, we need to find 'small' generators of S-unit groups. In section 5, we prove the following theorem.

3. Theorem. *Let s be the number of complex primes of F and let T be a finite set of primes of F containing S_∞ and all finite primes with norm at most $(2/\pi)^s|\Delta|^{1/2}$. Write $m_T = \max(\{1\} \cup \{\, Nv : v \in T - S_\infty \,\})$. Then U_T is generated by the set of all $a \in \mathcal{O} \cap U_T$ with $|a_v|_v \le (2/\pi)^{2s}|\Delta|m_T$ for all $v \in S_\infty$.*

Remark. By saying the tame kernel $K_2\mathcal{O}$ is computable as a function of F, we mean that the function that sends a number field F to the tame kernel $K_2\mathcal{O}$ is computable. More generally, we say $f(x)$ is computable as a function of x, when we actually mean that f is computable. Furthermore, our statements about computability depend on how the input of the function is represented. We feel it is not necessary to be very precise about this, because any non-contrived representation usually works

well. For instance, a natural number can be represented as a finite bit-string, giving the binary representation. A number field is represented by a generating element and this element itself is represented by a fundamental polynomial with coefficients in $\mathbb{Z}$. For the representation of other objects, we refer to [4], particularly chapter 4. In [4] one can also find algorithms to compute the maximal order and the class group of a number field.

2. Notation and outline of the article

This section is mainly concerned with setting the notation and explaining the strategy we use to prove the main theorem. At the end of this section, we give an outline of the remainder of the article.

The setting is the same as in the introduction: we have a number field F with ring of integers $\mathcal{O}$ and discriminant Δ. Let $n = r + 2s$ be the degree of F, where r is the number of real primes and s is the number of complex primes. In the introduction we constructed groups $K^{(m)}$ which gave a filtration of K_2F. Here, we will make the filtration even finer. Let v_1, v_2, v_3, ... be an ordering of all the finite primes with non-decreasing norms. Let v be a finite prime. Then there is an index j with $v_j = v$. We define the sets $S = S_\infty \cup \{v_1, v_2, \ldots, v_{j-1}\}$ and $S' = S \cup \{v\}$ and we write

$$\begin{aligned} U = U_S, &\quad K = (U \otimes U)/\langle a \otimes b : a, b \in U : a + b = 1 \text{ or } a + b = 0\rangle, \\ U' = U_{S'}, &\quad K' = (U' \otimes U')/\langle a \otimes b : a, b \in U' : a + b = 1 \text{ or } a + b = 0\rangle. \end{aligned}$$

Hence, S, S', U, U', K, K' depend on v and on the numbering of the primes, although this is not visible in the notation. We will prove that under certain conditions on the norm of v, the map $K'/\operatorname{im} K \to k_v^*$ is an isomorphism and deduce the main theorem from that.

It is crucial for the remainder of this article that the sequence

$$0 \longrightarrow U \longrightarrow U' \xrightarrow{v} \mathbb{Z} \longrightarrow 0$$

is exact. It is, however, not true in general that the valuation map is surjective when the norm of v is very small.

4. Lemma. *Define*

$$d = \frac{2^n \Gamma(n/2+1)}{(\pi n)^{n/2}} |\Delta|^{1/2}$$

and let $\rho = \rho_n$ be the packing density of an n-dimensional sphere. Then the valuation map $U' \xrightarrow{v} \mathbb{Z}$ is surjective as long as $Nv > \rho d$. We have $\rho d \geq 1$.

Before we give the proof, we want to give some definitions and explain the constant ρ. First we explain packing densities. Let K_0 be a measurable, bounded subset of $\mathbb{R}^n$ with nonempty interior. A packing of K_0 in $\mathbb{R}^n$ is a collection $\mathcal{K}$ of translates of K_0

such that the interiors do not meet pairwise. Let C_r (for $r \in \mathbb{R}_{>0}$) be the hypercube in $\mathbb{R}^n$ consisting of points with each of the coordinates in absolute value at most r. Then we define the density of $\mathcal{K}$ as

$$\rho_+(\mathcal{K}) = \limsup_{r\to\infty} \big(\mathrm{vol}(C_r)^{-1} \sum_{\substack{K_0' \in \mathcal{K} \\ K_0' \cap C_r \neq \emptyset}} \mathrm{vol}(K_0')\big),$$

where 'vol' is the volume given by the Lebesgue measure on $\mathbb{R}^n$. Intuitively, $\rho_+(\mathcal{K})$ is the proportion of the entire space covered by the union of the elements in $\mathcal{K}$. The *packing density* of K_0 is defined as

$$\rho(K_0) = \sup_{\mathcal{K}} \rho_+(\mathcal{K}),$$

where the supremum is taken over all packings $\mathcal{K}$ of K_0. In the case K_0 is an n-dimensional sphere, we have

$$\rho = \rho_n = \rho(K_0) \leq \frac{n+2}{2}\Big(\frac{1}{\sqrt{2}}\Big)^n, \qquad \text{and } \rho_n = \pi/\sqrt{12} \quad \text{if } n = 2.$$

Asymptotically stronger is the Kabatiansky-Levenshtein bound, which says

$$\rho_n \leq 2^{-0.599n+o(n)} \qquad \text{for} \quad n \to \infty.$$

For references and more information about packings, we refer to Rogers [14] and Conway and Sloane [5].

5. Lemma (*Minkowski*). *Let L be a lattice of $\mathbb{R}^n$ of full rank, with determinant* $\det(L)$. *Let K_0 be a closed, convex, symmetric subset of $\mathbb{R}^n$ such that* $\mathrm{vol}\, K_0 \geq 2^n \rho(K_0) \det(L)$. *Then there is a nonzero point in $L \cap K_0$.*

Proof. This is a trivial adaptation from [10, V.3.theorem 3]. □

The $\mathbb{R}$-vector space we will be working in, is $F_\mathbb{R} = F \otimes \mathbb{R}$. The additive group of $F_\mathbb{R}$ is naturally equivalent to its own character group by sending $x \in F_\mathbb{R}$ to the character $y \mapsto e^{-2\pi i \,\mathrm{Tr}(xy)}$, where Tr denotes the trace from $F_\mathbb{R}$ to $\mathbb{R}$. Using this equivalence we let the measure on $F_\mathbb{R}$ be the self-dual one. This means we take the measure dx such that we have

$$f(x) = \hat{\hat{f}}(-x)$$

for continuous complex valued functions $f \in L_1 F_\mathbb{R}$ for which the Fourier transform $\hat{f}(y) = \int f(x) e^{2\pi i \,\mathrm{Tr}(xy)} dx$ is also continuous and in $L_1 F_\mathbb{R}$ (see [15]). Consequently, the determinant of $\mathcal{O}$ is equal to $|\Delta|^{1/2}$.

In order to apply Minkowski, we need a supply of closed, convex, symmetric sets. We will mainly use balls, cubes and diamonds. We define these shapes in terms of three corresponding metrics. Write $F_\mathbb{R}$ as the product

$$F_\mathbb{R} = \prod_{v \in S_\infty} F_v.$$

An element $x \in F_{\mathbb{R}}$ has coordinates $x_v \in F_v$. Each factor in the product has an absolute value $|\cdot|_v$ by embedding F_v into $\mathbb{C}$. For $t \in \mathbb{R}_{>0}$, we define

$$\begin{array}{lll} \text{balls:} & B_t = \{\, x \in F_{\mathbb{R}} : \|x\|_2 \ \leq t^{1/n} \,\}, & \text{with } \|x\|_2 \ = (\frac{1}{n}\sum_{w\in S_\infty} n_w |x_w|_w^2)^{1/2}, \\ \text{cubes:} & C_t = \{\, x \in F_{\mathbb{R}} : \|x\|_\infty \leq t^{1/n} \,\}, & \text{with } \|x\|_\infty = \max_{w\in S_\infty} |x_w|_w, \\ \text{diamonds:} & D_t = \{\, x \in F_{\mathbb{R}} : \|x\|_1 \ \leq t^{1/n} \,\}, & \text{with } \|x\|_1 \ = \frac{1}{n}\sum_{w\in S_\infty} n_w |x_w|_w, \end{array}$$

where n_w is equal to the degree $[K_w : \mathbb{R}]$.

The basic properties that we use of these sets are listed in the lemma below.

6. Lemma. *Let d be defined as in lemma 4 and define $\tilde{d} = (2/\pi)^s |\Delta|^{1/2}$. When x is an element of F, we write $N(x)$ for the absolute value of the norm of x to $\mathbb{Q}$. For $t \in \mathbb{R}_{>0}$, the norm $N(x)$ of an element x in either B_t, C_t or D_t is at most t. The volumes of B_{dt} and $C_{\tilde{d}t}$ are given by*

$$\operatorname{vol} B_{dt} = \operatorname{vol} C_{\tilde{d}t} = 2^n |\Delta|^{1/2} t.$$

For t, $t' \in \mathbb{R}_{>0}$, we have

$$B_t B_{t'} \subset D_{tt'}, \qquad B_t C_{t'} \subset B_{tt'}.$$

Remarks and proof. The volume of an n-dimensional sphere with radius 1 in $\mathbb{R}^n$ is

$$\frac{\pi^{n/2}}{\Gamma(n/2+1)}.$$

We have $\Gamma(1/2) = \sqrt{\pi}$ and Γ satisfies the functional relation $\Gamma(x) = (x-1)\Gamma(x-1)$. The measure on $F_{\mathbb{R}}$ induced by $\|\cdot\|_2$ and the canonical measure on $F_{\mathbb{R}}$ we use to calculate volumes differ a factor $n^{n/2}$. From this, the formula for the volume of B_{dt} follows.

The statement that norms of elements in B_t, C_t and D_t are bounded by t is an easy application of the inequality of the means. By $B_t B_{t'}$ we mean the set $\{\, xy : x \in B_t, y \in B_{t'} \}$ and $B_t B_{t'} \subset D_{tt'}$ follows from the Cauchy-Schwarz inequality. □

We are now ready to prove lemma 4.

Proof of lemma 4. Let d and ρ be defined as in the lemma. We have

$$\operatorname{vol} B_{d\rho} = 2^n \rho |\Delta|^{1/2} = 2^n \rho \det(\mathcal{O}).$$

Hence, by Minkowski there is a nonzero point in $\mathcal{O} \cap B_{d\rho}$. The norm of this element is at least 1 because it is in $\mathcal{O}$, and is at most $d\rho$ because it is in $B_{d\rho}$. Hence, $d\rho$ is at least 1.

Now let $\mathfrak{p} = \mathfrak{p}_v$ be the prime ideal corresponding to v and set $t = d\rho N v$. We have $\operatorname{vol} B_t = 2^n \rho |\Delta|^{1/2} N v = 2^n \rho \det(\mathfrak{p})$ and therefore there exists a nonzero point π in $\mathfrak{p} \cap B_t$, for which we clearly have $v(\pi) \geq 1$. Because π is an integral element, $v(\pi)$ can

only be greater than 1 if $N\pi$ is at least $(Nv)^2$. But we have $N\pi \leq t = d\rho Nv < (Nv)^2$. Hence, we have $v(\pi) = 1$ and $\pi \in U'$, which proves the surjectivity of the valuation map. □

We adopt the notation for d and ρ from the lemma and we will make the following assumption:

Assumption 1: $Nv > \rho d$.

With this assumption, the set

$$\Pi = \{\, \pi \in U' : v(\pi) = 1 \,\}$$

is not empty. Let π be any element from Π and consider the map

$$U \longrightarrow K'/\operatorname{im} K, \quad \text{given by} \quad u \longmapsto \{u, \pi\}.$$

By abuse of notation, $\{u, \pi\}$ denotes both an element in K' and in the quotient.

7. Lemma. *The map $U \to K'/\operatorname{im} K$ does not depend on the choice of $\pi \in \Pi$. The map is surjective and the kernel contains $U \cap (1 + \Pi)$.*

Proof. For any $\pi' \in \Pi$ we can write $\pi' = u'\pi$ for some $u' \in U$ and we have

$$\{u, \pi'\}/\{u, \pi\} = \{u, u'\} \in \operatorname{im} K.$$

Hence, the map does not depend on π. To see that the map is surjective, first notice that $K'/\operatorname{im} K$ is certainly generated by elements of the form $\{u, \pi\}$, $\{\pi, u\}$, $\{\pi, \pi\}$, for $u \in U$. It follows from the definitions that $\{\,\cdot\,,\,\cdot\,\}$ is anti-symmetric: for all a, $b \in U'$, we have

$$\{a, b\}\{b, a\} = \{a, b\}\{-b, b\}\{b, a\}\{-a, a\} = \{-ab, ab\} = 1.$$

So, we can omit the generators $\{\pi, u\}$ in favor of $\{u, \pi\}$. We rewrite

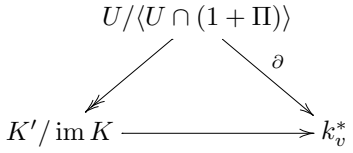
$$\{\pi, \pi\} = \{\pi, \pi\}/\{-\pi, \pi\} = \{-1, \pi\},$$

so this element is also covered by elements of the form $\{u, \pi\}$. Finally, if $\pi' \in \Pi$ is an element with $1 + \pi' \in U$, we have $-\pi' \in \Pi$ and $\{1 + \pi', \pi\} = \{1 + \pi', -\pi'\} = 1$. Hence, $U \cap (1 + \Pi)$ is in the kernel. □

The reduction map $\partial\colon U \to k_v^*$ also has $U \cap (1 + \Pi)$ in the kernel. Abusing notation, we write ∂ for the induced map

$$\partial\colon U/\langle U \cap (1 + \Pi)\rangle \longrightarrow k_v^*,$$

where by $\langle U \cap (1+\Pi)\rangle$ we mean the subgroup of U generated by the elements in the set $U \cap (1+\Pi)$. By the previous lemma we have a well-defined and commutative triangle



and we see that if ∂ is an isomorphism, all maps are isomorphisms. This allows us to divert all attention to the map ∂ and forget about K-theory, tame kernels, symbols and even the newly defined K' and K.

We shall prove that ∂ is an isomorphism if Nv exceeds a constant depending on F. How large we want Nv to be gradually becomes clear. At several points in the argument we need a lower bound on Nv, and we keep track of these bounds by means of boxed assumptions, an example being assumption 1 above.

In section 3, we define a set-theoretical map $\gamma\colon k_v^* \to U/\langle U \cap (1+\Pi)\rangle$ for which $\partial \circ \gamma$ is the identity. In sections 4 and 6 we show that $\gamma \circ \partial$ is the identity on a set of generators for $U/\langle U \cap (1+\Pi)\rangle$. In the course of doing that we find a set of small generators for the group $U_0 = \{\, x \in U : v'(x) = 0 \text{ for all } v' \text{ with } Nv' > d\}$ in section 5. In section 7 we prove that γ is a homomorphism. The definition of γ together with the proofs that $\gamma \circ \partial$ is the identity on a set of generators and that γ is a homomorphism all rely on assumptions on the norm of v. Combining these assumptions, we have proved that $K'/\operatorname{im} K \to k_v^*$ is a isomorphism. In section 8, we formulate this as a theorem and deduce the main theorem from it. We also discuss the results for quadratic fields and give asymptotic results.

3. A candidate inverse map

In this section, we give a candidate inverse map γ for ∂. In order to define the map, we will make a stronger assumption on the norm of v.

In section 6, we will use balls that are somewhat stretched in one direction and squeezed in another direction. We want the following lemma to be applicable in that situation too, so we need some notation for these stretched and squeezed balls. Let X be the set

$$X = \{\, \xi \in \prod_{w \in S_\infty} \mathbb{R}_{>0} : \prod_{w \in S_\infty} \xi_w^{n_w} = 1 \,\}, \qquad n_w = [K_w : \mathbb{R}].$$

The set X is a group under pointwise multiplication. By ξA for $A \subset F_{\mathbb{R}}$ and $\xi \in X$ we mean the set

$$\xi A = \{\, (\xi_w a_w)_{w \in S_\infty} : a \in A \,\}.$$

Multiplication with ξ preserves volumes of measurable sets and norms of elements. Hence, the norm of an element of ξB_t or ξC_t is still at most t.

Apart from these squeezed balls we also use cross products of balls. The following lemma relates the packing density of products of balls to the packing densities of balls. For a proof, see [7].

8. Lemma (*Hlawka*). *If $K_0 \subset \mathbb{R}^m$ and $K_0' \subset \mathbb{R}^n$ are bounded symmetric, convex subsets then the packing density of $K_0 \times K_0'$ in $\mathbb{R}^{m+n}$ is at most* $\min\{\rho(K_0), \rho(K_0')\}$.

9. Lemma. *If $t \in \mathbb{R}_{>0}$ satisfies $t^2 \geq \rho d^2 Nv$ and $t < Nv$ then for each $u \in k_v^*$ and $\xi \in X$, there are x, $y \in \xi B_t \cap U \cap \mathcal{O}$ with $\partial(x/y) = u$.*

Proof. Let u be an element of k_v^* and let L be the kernel of the map $\mathcal{O} \times \mathcal{O} \to k_v$, given by

$$(x, y) \longmapsto \bar{x} - u\bar{y}.$$

The determinant of L is equal to $|\Delta| Nv$. Let t satisfy the premises of the lemma. The volume of $\xi B_t \times \xi B_t$ is equal to $2^{2n} d^{-2} t^2 |\Delta|$ and by assumption this is at least $2^{2n} \rho Nv |\Delta| = 2^{2n} \rho \det(L)$. As $\xi B_t \times \xi B_t$ has packing density at most ρ by lemma 8, we conclude that there is a nonzero element (x, y) in $(\xi B_t \times \xi B_t) \cap L$. The elements x and y have norm smaller than Nv and therefore they are either 0 or in U. As at least one of them is nonzero, the relation $\bar{x} = u\bar{y}$ tells us that the other element is also nonzero. Hence, they are both in U and we have $\partial(x/y) = u$. □

Whenever we have $Nv > \rho d^2$, we see that $t = \rho^{1/2} d (Nv)^{1/2}$ satisfies the premises of lemma 9 and hence the map ∂ is surjective. We need Nv a little bigger in order to ensure that choosing a 'random section' gives a well-defined map.

10. Proposition. *Suppose t, $t' \in \mathbb{R}_{>0}$ satisfy the inequality $2^n tt' < (Nv)^2$ and let ξ and ξ' be elements of X. Assume*

$$x, y \in \xi B_t \cap U \cap \mathcal{O}, \quad x', y' \in \xi' B_{t'} \cap U \cap \mathcal{O}$$

are elements with $\partial(x/y) = \partial(x'/y')$. Then x/y and x'/y' have the same image in $U/\langle U \cap (1 + \Pi) \rangle$.

Proof. It is certainly sufficient to prove that xy' and $x'y$ have the same image in $U/\langle U \cap (1 + \Pi) \rangle$. By lemma 6, we know that xy' and $x'y$ are in $\xi\xi' D_{tt'}$ and we have

$$xy' - x'y \in \xi\xi' D_{2^n tt'}.$$

Write $\pi = xy' - x'y$. It is clear that the valuation of π is at least 1. As we have $N(\pi) \leq 2^n tt' < (Nv)^2$, we see that π is either 0 or in Π. When π is 0, the elements x/y and x'/y' are equal in U and therefore also in $U/\langle U \cap (1 + \Pi) \rangle$. When π is in Π, we just write

$$\frac{xy'}{x'y} = 1 + \frac{\pi}{x'y} \in 1 + \Pi$$

and we are done. □

The existence of a t that satisfies both the requirements in lemma 9 and the inequality $2^n t^2 < (Nv)^2$ from proposition 10 is assured by assumption 2:

Assumption 2: $Nv > 2^n \rho d^2$.

We use this assumption in the definition of γ.

DEFINITION OF γ. We define a map

$$\gamma\colon k_v^* \longrightarrow U/\langle U \cap (1+\Pi)\rangle$$

as follows. Let u in k_v^* be given. Write $t = \rho^{1/2} d (Nv)^{1/2}$. We can find $x, y \in B_t \cap U \cap \mathcal{O}$ with $\partial(x/y) = u$ by lemma 9. We define

$$\gamma(u) = \overline{x/y} \in U/\langle U \cap (1+\Pi)\rangle.$$

By proposition 10 and assumption 2, the map γ is well defined.

It is clear that $\partial \circ \gamma$ is the identity on k_v^*. In order to prove that $\gamma \circ \partial$ is the identity on $U/\langle U \cap (1+\Pi)\rangle$ we shall use more assumptions.

4. $\gamma \circ \partial$ on a set of generators (part 1)

Recall that S is the set of primes of F such that $U = U_S$. Let v' be a finite prime in S with

$$Nv' > \tilde{d}, \qquad \text{with} \quad \tilde{d} = \left(\frac{2}{\pi}\right)^s |\Delta|^{1/2}.$$

Let $\mathfrak{p}' = \mathfrak{p}_{v'}$ be the corresponding prime ideal. The determinant $\det(\mathfrak{p}'^{-1})$ is equal to $|\Delta|^{1/2}(Nv')^{-1}$. Using Minkowski, we see that there exists a nonzero element

$$\pi' \in \mathfrak{p}'^{-1} \cap C_{\tilde{d}/Nv'}.$$

Now $\pi'\mathfrak{p}'$ is an integral ideal and we have

$$N(\pi'\mathfrak{p}') \leq (\tilde{d}/Nv')Nv' = \tilde{d} < Nv'.$$

Therefore, the prime ideal factorization of (π') is $\mathfrak{p}'^{-1}$ times prime ideals of norm smaller than Nv'. In particular, we have $v'(\pi') = -1$ and $\pi' \in U$. Let $\overline{\pi'}$ be the image of π' in $U/\langle U \cap (1+\Pi)\rangle$. We prove that $\gamma \circ \partial$ is the identity on $\overline{\pi'}$. Define $t = \rho^{1/2} d (Nv)^{1/2}$ and let $x, y \in B_t \cap U \cap \mathcal{O}$ be elements with $\partial(\pi') = \partial(x/y)$. By lemma 6, we have

$$\pi' y \in B_{t\tilde{d}/Nv'} \subset B_t$$

and therefore also

$$\pi' y - x \in B_{2^n t}.$$

This means that the norm of $\pi' y - x$ is bounded by $2^n t = 2^n \rho^{1/2} d (Nv)^{1/2}$. We want this to be smaller than Nv, so we need another assumption:

Assumption 3: $Nv > 2^{2n} \rho d^2$.

Now we can conclude

$$N(\mathfrak{p}'(\pi' y - x)) < Nv' Nv \leq (Nv)^2.$$

If $\pi' y - x$ is nonzero, this tells us that $\pi' y - x$ is in Π. Then we have $\pi'/(x/y) = \pi' y/x \in 1 + \Pi$, which proves $(\gamma \circ \partial)(\overline{\pi'}) = \overline{x/y} = \overline{\pi'}$.

Let U_0 be the group

$$U_0 = \{\, x \in U : v'(x) = 0 \text{ for all } v' \text{ with } Nv' > \tilde{d} \,\}.$$

Then U is generated by the set

$$\{\text{all } \pi' \text{ for all finite } v' \in S \text{ with } Nv' > \tilde{d}\,\} \cup U_0.$$

In the next section we find a set of generators for U_0 and in section 6 we show that $\gamma \circ \partial$ is the identity on the image of this set in $U/\langle U \cap (1 + \Pi) \rangle$.

5. Finding good generators for U_0

Finding 'good' generators for U_0 is almost completely worked out in section 6 of an article by Lenstra [11]. However, we do have to refer to one of the *proofs* in this article. While we are at it, we give a refinement of theorem 6.2 in [11].

Let T be *any* finite set of primes from F, containing S_∞ and all finite primes with norm at most $\tilde{d}$. Write $m_T = \max(\{1\} \cup \{\, Nv : v \in T - S_\infty \,\})$. According to the proof of theorem 6.2 in [11], the group U_T (which is written there as K_S) is generated by the set

$$\bigcup_{\substack{\mathfrak{b} \subset \mathcal{O} \\ N\mathfrak{b} \leq \tilde{d}}} \Big\{\, a \in \mathfrak{b}^{-1} \cap U_T : \prod_{w \in S_\infty} \max\{1, |a_w|_w^{n_w}\} \leq \frac{\tilde{d} m_T}{N\mathfrak{b}} \,\Big\}. \qquad (*)$$

Although we will not use it, it does not take too much effort to state and prove the next theorem, which is a nice improvement of theorem 6.2 in [11]. Apart from formulation this is identical to theorem 3.

11. THEOREM. *The group U_T is generated by the set $C_{\tilde{d}^2 m_T} \cap \mathcal{O} \cap U_T$.*

PROOF. Let a and $\mathfrak{b}$ be as in $(*)$. Write

$$t = \tilde{d} N\mathfrak{b} \prod_{w \in S_\infty} \max\{1, |a_w|_w^{n_w}\}.$$

Then by Minkowski, there is a nonzero $b' \in \mathfrak{b}$ with

$$|b'_w|_w \le t^{1/n} / \max\{1, |a_w|_w\} \quad (w \in S_\infty).$$

Because b' is in the integral ideal $\mathfrak{b}$ and the norm of $\mathfrak{b}$ is at most $\tilde{d}$, we have $b' \in \mathcal{O} \cap U_T$. From $a \in \mathfrak{b}^{-1} \cap U_T$ it follows that $b'a$ is in $b'(\mathfrak{b}^{-1} \cap U_T) \subset \mathcal{O} \cap U_T$. Because t is at most $\tilde{d}^2 m_T$, we have b', $b'a \in C_{\tilde{d}^2 m_T}$. We use these elements as generators instead of a. This finishes the proof of the theorem. □

If we let T be the set $\{\text{finite } v' : Nv' \le \tilde{d}\} \cup S_\infty$, we have $U_0 = U_T$. The generators we use for U_0 are the ones given in $(*)$.

6. $\gamma \circ \partial$ on a set of generators (part 2)

By Minkowski, the set $C_{\tilde{d}}$ contains a nonzero element of $\mathcal{O}$ and this implies that $\tilde{d}$ is at least 1. Hence, in our case we can bound m_T by $\tilde{d}$. Let $\mathfrak{b} \subset \mathcal{O}$ be an ideal with $N\mathfrak{b} \le \tilde{d}$ and let $a \in \mathfrak{b}^{-1}$ be an element with $\prod_w \max\{1, |a_w|_w^{n_w}\} \le \tilde{d}^2 / N\mathfrak{b}$. We prove that $\gamma \circ \partial$ is the identity on the image $\overline{a}$ of a in $U/\langle U \cap (1+\Pi)\rangle$ and we can conclude that $\gamma \circ \partial$ is the identity on the image of a set of generators of U_0 in $U/\langle U \cap (1+\Pi)\rangle$.

Now is the time we are going to use the ξ's mentioned in lemma 9 and proposition 10. Let $\xi \in X$ be the element such that for $w' \in S_\infty$ we have

$$\xi_{w'} = \frac{\left(\prod_{w \in S_\infty} \max\{1, |a_w|_w^{n_w}\}\right)^{1/n}}{\max\{1, |a_{w'}|_{w'}\}}.$$

We have chosen ξ in such a way that a is an element of $\xi^{-1} C_{\tilde{d}^2 / N\mathfrak{b}}$. Define $t = \rho^{1/2} d (Nv)^{1/2}$ and let $x, y \in \xi B_t \cap U \cap \mathcal{O}$ be elements with $\partial(x/y) = \partial(a)$ as in lemma 9. As usual, we want to prove that ay/x is in $\{1\} \cup (1 + \Pi)$. It would be sufficient if $N(\mathfrak{b}(ay - x))$ is smaller than $(Nv)^2$. Indeed, in this case $\pi = ay - x$ is either 0 or in Π and in the latter case we can write $ay/x = 1 + \pi/x \in 1 + \Pi$.

Clearly, we have

$$ay \in B_{t\tilde{d}^2 / N\mathfrak{b}} \quad \text{and} \quad x \in \xi B_t \subset B_{t\tilde{d}^2 / N\mathfrak{b}} \quad \text{and hence} \quad ay - x \in B_{2^n t\tilde{d}^2 / N\mathfrak{b}}.$$

Therefore, we have $N(\mathfrak{b}(ay - x)) \le 2^n t\tilde{d}^2 = 2^n \rho^{1/2} d\tilde{d}^2 (Nv)^{1/2}$. For this to be smaller than $(Nv)^2$, we need assumption 4:

Assumption 4: $Nv > 2^{2n/3} \rho^{1/3} (d\tilde{d}^2)^{2/3}$.

7. When is γ a homomorphism?

Now that we know that $\gamma \circ \partial$ is the identity on a set of generators—at least, under assumptions 3 and 4—and $\partial \circ \gamma$ is the identity everywhere, it suffices to prove that γ is a homomorphism. The following lemma is inspired by [1, II.3.2.c].

12. Lemma (*denominator-trick*). *If $t \in \mathbb{R}$ satisfies $t^3 \geq \rho d^3 (Nv)^2$ and $t < Nv$, then for each u, $u' \in k_v^*$, there are x, y, $z \in B_t \cap U \cap \mathcal{O}$ with $\partial(x/z) = u$ and $\partial(y/z) = u'$.*

Proof. This is almost completely identical to lemma 9. Let u and u' be elements from k_v^* and let L be the kernel of the map $\mathcal{O} \times \mathcal{O} \times \mathcal{O} \to k_v \times k_v$, given by

$$(x, y, z) \longmapsto (\bar{x} - u\bar{z}, \bar{y} - u'\bar{z}).$$

The determinant of L is equal to $|\Delta|^{3/2}(Nv)^2$. The packing density of the cross product of three spheres, each of dimension n, is at most ρ. Therefore, there is a nonzero element in (x, y, z) in $(B_t \times B_t \times B_t) \cap L$. The details can easily be adapted from the proof of lemma 9. □

The existence of a t as in lemma 12 is assured by assumption 5:

Assumption 5: $Nv > \rho d^3$.

For the next proposition, we also use

Assumption 6: $Nv > 2^{6n/5} \rho d^{12/5}$.

13. Proposition. *Under assumptions 2, 5 and 6, the map γ is an homomorphism.*

Proof. Let u, u', $u'' \in k_v^*$ be given with $uu' = u''$. Write $t = \rho^{1/3} d (Nv)^{2/3}$ and $t' = \rho^{1/2} d (Nv)^{1/2}$ and choose $x, y, z \in B_t \cap U \cap \mathcal{O}$ according to lemma 12 and $x', z' \in B_{t'} \cap U \cap \mathcal{O}$ according to lemma 9 with

$$u = \partial(x/z), \quad u' = \partial(x'/z'), \quad u'' = \partial(y/z).$$

Assumption 6 is chosen precisely to make sure that we have

$$2^n t t' < (Nv)^2.$$

Hence by proposition 10, we have $\gamma(u) = \overline{x/z}$ and $\gamma(u'') = \overline{y/z}$ in $U/\langle U \cap (1 + \Pi) \rangle$. We want xx' and yz' to have the same image in $U/\langle U \cap (1+\Pi) \rangle$. As usual, this follows from the fact that $xx' - yz'$ is in $D_{2^n tt'}$ and hence, the norm is smaller than $(Nv)^2$. □

REMARK. For specific calculations, the bounds can probably be improved, by not considering all $u' \in k_v^*$ in proposition 13, but only generators for k_v^*. For many v's, the group k_v^* is generated by the images of elements in small balls. To use this, it is probably necessary to use a different ordering on the primes—not necessarily with non-decreasing norms—where the v's with 'large' generators appear later in the ordering.

8. Discussion

For the main theorem of this article, we only have to reap what we have sowed. Under assumptions 1 to 6, the map γ is the inverse map of ∂ and as we explained in section 2, it follows that $K'/\operatorname{im} K \to k_v^*$ is an isomorphism. We define

$$c_F = \max\bigl\{2^{2n}\rho d^2, 2^{2n/3}\rho^{1/3}(d\tilde{d}^2)^{2/3}, \rho d^3\bigr\} \qquad (**)$$

and for easy reference, we recall the definitions

$$d = \frac{2^n\Gamma(n/2+1)}{(\pi n)^{n/2}}|\Delta|^{1/2} \quad \text{and} \quad \tilde{d} = \Big(\frac{2}{\pi}\Big)^s|\Delta|^{1/2}.$$

Furthermore, ρ is the packing density of an n-dimensional sphere.

14. THEOREM. *The map $K'/\operatorname{im} K \to k_v^*$ is an isomorphism if we have $Nv > c_F$.*

PROOF. It suffices to show that assumptions 1 to 6 follow from $Nv > c_F$. Assumptions 1 and 2 clearly follow from $Nv > 2^{2n}\rho d^2$. We see that

$$2^{2n}\rho d^2, \quad 2^{6n/5}\rho d^{12/5} \quad \text{and} \quad \rho d^3$$

are equal when we have $d = 2^{2n}$. Hence $2^{6n/5}\rho d^{12/5}$ is smaller than either $2^{2n}\rho d^2$ or ρd^3. Therefore, assumption 6 follows. □

15. THEOREM. *For every number field F, there are constants c_F, c'_F such that*

(1) *for all $m > c_F$, the map $K^{(m)}/\operatorname{im} K^{(m-1)} \to \bigoplus_{Nv=m} k_v^*$ induced by the maps t_v is an isomorphism. The direct sum is taken over all finite primes with norm equal to m.*

(2) *for all $m > c'_F$, the map $K^{(m)} \to K^m$ is an isomorphism.*

For $m > c_F$, the image of $K_2^{(m)}\mathcal{O}$ in K_2F is equal to the tame kernel. For $m > \max\{c_F, c'_F\}$, the natural map $K_2^{(m)}\mathcal{O} \to K_2\mathcal{O}$ is an isomorphism. We can take c_F as defined by $(**)$. The group $K_2^{(m)}\mathcal{O}$ is computable as a function of m and F.

PROOF. Let m be larger than c_F and suppose we are in the nontrivial case where there exists a prime with norm equal to m. Impose an ordering on the finite primes of F and suppose $w_1, w_2, \ldots, w_k$ are all primes with norm m, appearing in

this order. Let v one of the these primes and define K' and K as in section 2. In the case $v = w_k$, we have $K' = K^{(m)}$ and by theorem 14, we know that the map $K^{(m)}/\operatorname{im} K \to k_v^*$ is an isomorphism. If $v = w_j$ for an arbitrary index j we assume $K^{(m)}/\operatorname{im} K' \to \bigoplus_{i=j+1}^{k} k_{w_i}^*$ is an isomorphism and we use this to show that $K^{(m)}/\operatorname{im} K \to \bigoplus_{i=j}^{k} k_{w_i}^*$ is an isomorphism. Consider the diagram below:

$$\begin{array}{ccccccccc} & & K'/\operatorname{im} K & \longrightarrow & K^{(m)}/\operatorname{im} K & \longrightarrow & K^{(m)}/\operatorname{im} K' & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow & & \downarrow \cong & & \\ 0 & \longrightarrow & k_{w_j} & \longrightarrow & \bigoplus_{i=j}^{k} k_{w_i}^* & \longrightarrow & \bigoplus_{i=j+1}^{k} k_{w_i}^* & \longrightarrow & 0\,. \end{array}$$

The diagram has exact rows and all maps are compatible. With the snake lemma 'without the snake' we see that the middle vertical arrow is in fact an isomorphism. Using induction, we have now proved (1).

As for (2), let $\ker_m$ be the kernel of the map $K^{(m)} \to K^m$. Suppose $m > c_F$ and consider the commutative and exact diagram

$$\begin{array}{ccccccccc} & & \ker_{m-1} & & \ker_m & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & K^{(m-1)} & \longrightarrow & K^{(m)} & \longrightarrow & \bigoplus k_v^* & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & K^{m-1} & \longrightarrow & K^m & \longrightarrow & \bigoplus k_v^* & \longrightarrow & 0\,. \end{array}$$

By applying the snake lemma to the diagram, we see that the map $\ker_{m-1} \to \ker_m$ is surjective. In fact, for every $M \geq m$, the map $\ker_m \to \ker_M$ is surjective. Because K_2F is equal to the direct limit $\lim K^{(m)}$, for each element $x \in \ker_m$ there is an $M \geq m$ such that x maps to 1 in $\ker_M$. Because of the surjectivity of the maps $\ker_m \to \ker_M$ and the fact that $\ker_m$ is finitely generated, this means there is an M such that $\ker_M = 0$.

In order to prove that the groups $K_2^{(m)}\mathcal{O}$ are computable, we show that we can compute $K^{(m)}$. We can determine $K^{(m)}$, because there are only finitely many solutions to the equation $a + b = 1$ with a, $b \in U_m$ and we can find them all [3]. Furthermore, factoring out by all elements $a \otimes -a$ for all $a \in U_m$ is the same as factoring out by all elements $a \otimes -a$ and $(a \otimes b)(b \otimes a)$ for a and b in a set of generators of U_m.

It is clear that for $m > c_F$, the image of $K_2^{(m)}\mathcal{O}$ in K_2F is equal to the tame kernel and that for $m > c'_F$, the map $K_2^{(m)}\mathcal{O} \to K_2\mathcal{O}$ is an isomorphism. □

It follows from theorem 15 that the tame kernel is computable if we know its order. We use theorems from Keune to find the order of the p-primary part of the tame kernel.

16. Lemma (*Keune*). *The function $(p, F) \mapsto \#(K_2\mathcal{O})_2$ that maps a prime number p and a number field F to the order of the p-primary part of the tame kernel of F is computable if we either restrict to odd primes or to number fields containing i.*

Proof. By [8, theorem 6.6], we can compute the p-primary part $W(F)_p$ of the wild kernel $W(F)$ when p is an odd prime or F contains i, using the isomorphism

$$\Big(\mu_q \otimes \mathrm{Cl}\big(\mathcal{O}_{F(\zeta_q)}[\tfrac{1}{p}]\big)/q\Big)_\Gamma \xrightarrow{\sim} W(F)_p,$$

where we have $\Gamma = \mathrm{Gal}(F(\zeta_q)/F)$ and q is a high enough power of p such that $\mu(F_\mathfrak{p})_p \subset \mu_q$ for all $\mathfrak{p} \mid p$ and q kills the p-primary part of $K_2\mathcal{O}_F$. Still for an odd prime p, we have a sequence

$$0 \to W(F)_p \to (K_2\mathcal{O}_F)_p \to \bigoplus_{\mathfrak{p}|p} \mu(F_\mathfrak{p})_p \to \mu(F)_p \to 0$$

from [8, (1.10)], which we use to calculate the order of the p-primary part of $K_2\mathcal{O}_F$. All maps are explicitly given in [8]. □

17. Lemma. *The tame kernel $K_2\mathcal{O}$ is computable as a function of number fields F containing i.*

Proof. By theorem 15, there exists a value of $m > c_F$ such that $K_2^{(m)}\mathcal{O}$ is isomorphic to the tame kernel and in particular we can *find* a value of $m > c_F$ such that $K_2^{(m)}\mathcal{O}$ is finite. The tame kernel is a quotient of this group and that implies we have an upper bound on the primes occurring in the order. By lemma 16, we can calculate the order of the tame kernel and by theorem 15, we can compute the tame kernel. □

18. Lemma. *The order $\#(K_2\mathcal{O})_2$ of the 2-primary part of the tame kernel is computable as a function of the number field F.*

Proof. We define $E = F(i)$ and write $\mathcal{O}_F$ and $\mathcal{O}_E$ for the ring of integers of F and E respectively. By lemma 17 we can compute $K_2\mathcal{O}_E$. Let S be the set of infinite primes of F and let T be the set of infinite primes of E. Then we can apply [8, proposition 6.2], which says that the transfer map $K_2E \to K_2F$ induces an isomorphism $(K_2^+\mathcal{O}_{E,T})_\Gamma \to K_2^+\mathcal{O}_{F,S}$, where Γ is the Galois group $\mathrm{Gal}(E/F)$. In our case, $K_2^+\mathcal{O}_{E,T}$ is equal to $K_2\mathcal{O}_E$ and $K_2^+\mathcal{O}_{F,S}$ is equal to the kernel of the surjective map $K_2\mathcal{O}_F \to \bigoplus_{\mathfrak{p} \text{ real infinite}} \mu_2$ induced by Hilbert symbols. We can now compute $(K_2^+\mathcal{O}_{F,S})_2 \cong ((K_2\mathcal{O}_E)_\Gamma)_2 = ((K_2\mathcal{O}_E)_2)_\Gamma$ and hence we can compute the order of $(K_2\mathcal{O}_F)_2$. □

19. Theorem. *The tame kernel is computable as a function of the number field.*

Proof. As in the proof of lemma 17, we can find an upper bound on the primes occurring in the order of the tame kernel. By lemma 16 and lemma 18, we

can calculate the order of the tame kernel. It follows from theorem 15 that we can now calculate the tame kernel. □

20. Theorem. *The smallest feasible value of c'_F is computable as a function of the number field F.*

Proof. If for some $m > c_F$, the map $K^{(m)} \to K^m$ is an isomorphism, then the map $K^{(m+1)} \to K^{m+1}$ is also an isomorphism. If, given any m, we can check whether the map $K^{(m)} \to K^m$ is injective, or equivalently, whether the map $K^{(m)} \to K_2F$ is injective, it follows that we can find a smallest feasible value of c'_F. We use that we can write $K^{(m)}$ and $K_2\mathcal{O}$ with a finite number of generators and relations. First, find explicit generators for the kernel A of the map $K^{(m)} \to \bigoplus_{v<\infty} k_v^*$. The images of these generators in K_2F are actually in $K_2\mathcal{O}$. By a finite search, we can find a representation for these elements in $K_2\mathcal{O}$ and we can calculate the kernel of A to $K_2\mathcal{O}$ and check if this kernel is 0 in $K^{(m)}$. □

21. Proposition. *For every number field F, we have $c_F \leq 4|\Delta|^{3/2}$.*

Proof. For $n = 1$, we have $c_F = 4$. A numerical approximation shows that the proposition holds for $n = 2$. Hence, we assume $n \geq 3$.

Writing $c = 2^n\Gamma(n/2+1)/(\pi n)^{n/2}$, we have $d = c|\Delta|^{1/2}$. Using $d \geq 1$ and $\tilde{d} \leq |\Delta|^{1/2}$ and $\rho \leq 1$, we get

$$c_F \leq \max\{2^{2n}d^3, 2^{2n/3}d^{5/3}\tilde{d}^{4/3}\} \leq |\Delta|^{3/2}\max\{2^{2n}c^3, 2^{2n/3}c^{5/3}\}.$$

It is enough to prove the inequality $2^{2n}c^3 \leq 4$, because that proves that c is smaller than 1 and therefore we have $2^{2n/3}c^{5/3} \leq (2^{2n}c^3)^{1/3} \leq 4$. Stirling's formula says that for every $y > 0$ we have $\Gamma(y+1) = \sqrt{2\pi y}(y/e)^y e^{R(y)}$, where $R(y) \leq 1/(12y)$ holds (see [9, XIV §64.B]). Hence, using $n \geq 3$, we have

$$c^2 \leq n\pi^{1-n}2^n e^{-n+1/9}.$$

It follows that $\log(2^{4n}c^6)$ is at most $n(7\log 2 - 3\log\pi - 3) + 3\log\pi + 1/3 + 3\log n$. A numerical approximation shows that for $n = 3$ this is smaller than $\log(4^2)$ and that the derivative is smaller than 0 for $n \geq 3$. □

If we specialize to the quadratic case, we have $n = 2$, $s \leq 1$, $\rho = \pi/\sqrt{12}$. We get the following corollary.

22. Corollary. *Let F be a quadratic field with discriminant Δ. Then the c_F from theorem 14 is equal to*

$$c_F = \begin{cases} 2^5 3^{-1/2}\pi^{-1}|\Delta| < 5.8809|\Delta| & \text{if } |\Delta| \leq 631; \\ 2^2 3^{-1/2}\pi^{-2}|\Delta|^{3/2} < 0.2340|\Delta|^{3/2} & \text{if } |\Delta| > 631. \end{cases}$$

Proof. In the quadratic case $2^{2n/3}\rho^{1/3}(d\tilde{d}^2)^{2/3}$ is smaller than $2^{2n}\rho d^2$, no matter if s is 1 or 0. We have $2^{2n}\rho d^2 = \rho d^3$ for $|\Delta| = 64\pi^2 \doteq 631.6$. □

The best bounds we have found in the literature are given by Browkin [2]. He proves for imaginary quadratic number fields F that the map $K^{(m)}/\operatorname{im} K^{(m-1)} \to \bigoplus_{Nv=m} k_v^*$ is an isomorphism when we have $Nv > 2^6\pi^{-10/3}|\Delta|^{5/3} \doteq 1.41|\Delta|^{5/3}$ and $|\Delta| \geq 15$. It is clear that our results are better asymptotically. But also for small discriminants, our bound competes well, as the small table below shows.

Discriminant	-15	-19	-20	-23	...	-148	-151	...	-871
Browkin's bound	128.5	190.6	207.6	262.1	...	5836.0	6034.5	...	111955.1
c_F	88.2	111.7	117.6	135.2	...	870.3	888.0	...	6014.8

The following theorem gives the asymptotic results.

23. Theorem. *There are constants c_n and a_n such that for every number field F of degree n with discriminant Δ, we have $c_F < c_n|\Delta|^{3/2}$ whenever we have $|\Delta| \geq a_n$. We can take $c_n < (2^{-0.599}2^{3/2}e^{-3/2}\pi^{-3/2})^{n+o(n)} < 0.0749^{n+o(n)}$ and $a_n < (2^{-1}2^{0.599\cdot 4/3}\pi^{7/3}e^{7/3})^{n+o(n)} < 129.65^{n+o(n)}$ for $n \to \infty$.*

Proof. First of all, the magic '0.599' comes from the Kabatiansky and Levenshtein bound on packing densities of the sphere. They proved that the packing density of an n-dimensional sphere is at most $2^{-0.599n+o(n)}$. This is described in [5, Ch. 9]. An application of Stirling's formula on the bounds in theorem 14 yields the formulas above. □

References

[1] H. Bass and J. Tate, The Milnor ring of a global field, *Lecture Notes in Mathematics*, Vol. 342, pp. 349–446, Springer, Berlin (1973).

[2] J. Browkin, Computing the tame kernel of quadratic imaginary fields. With an appendix by Karim Belabas and Herbert Gangl, *Mathematics of Computation* **69** (2000), no. 232, pp. 1667–1683.

[3] Y. Bugeaud and G. Kálmán, Bounds for the solutions of unit equations, *Acta Arithmetica* **74** (1996), no. 1, 67–80.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, second corrected printing, Graduate Texts in Mathematics, 138, Springer (1995).

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren der mathematischen Wissenschaften, Vol. 290, Springer (1991).

[6] H. Garland, A finiteness theorem for K_2 of a number field, *Annals of Mathematics (2)*, **94**, (1971), pp. 534–548.

[7] E. Hlawka, Ausfüllung und Überdeckung durch Zylinder, *Anzeiger der Österreichischen Akademie der Wissenschaften.* Mathematisch-Naturwissenschaftliche Klasse, **85** (1948), nr. 11, pp. 116–119.

[8] F. Keune, On the Structure of the K_2 of the Ring of Integers in a Number Field, *K-Theory* **2**, (1989), pp. 625–645.

[9] K. Knopp, *Theorie und Anwendung der unendlichen Reihen*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Band 2, fünfte Auflage, Springer (1964).

[10] S. Lang, *Algebraic Number Theory*, second edition, Graduate Texts in Mathematics, 110, Springer (1994).

[11] H. W. Lenstra, Jr., Algorithms in algebraic number theory, *Bulletin of the American Mathematical Society (New Series)* **26**, (1992), no. 2, pp. 211-244.

[12] J. Milnor, *Introduction to algebraic K-theory*, Annals of Mathematics Studies, No. **72**, Princeton University Press, Princeton, (1971).

[13] D. Quillen, Higher algebraic K-theory I. In: *Algebraic K-Theory I.* Lecture Notes in Mathematics, **341**, 85–147, Springer (1973).

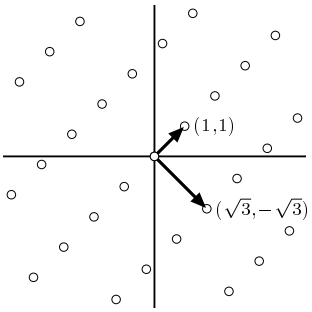
[14] C. A. Rogers, *Packing and covering*. Cambridge Tracts in Mathematics and Mathematical Physics, no. 54, Cambridge University Press, New York (1964).

[15] J. Tate, Fourier Analysis in Number Fields and Hecke's Zeta-functions, Thesis Princeton (1950). In: J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington D.C. (1967).

SAMENVATTING

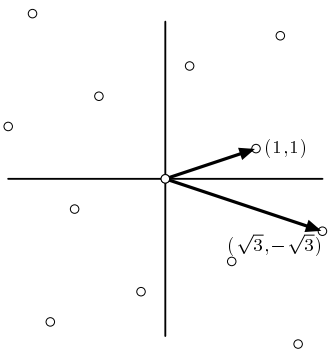
Vectorbundels en meetkunde der getallen

In dit proefschrift nemen *roosters* een belangrijke plaats in. Een voorbeeld van een rooster in het platte vlak krijgen we door twee vectoren te kiezen die niet in elkaars verlengde liggen en alle punten te nemen die te schrijven zijn als som van veelvouden van deze vectoren. Bijvoorbeeld, als we de vectoren $(1,1)$ en $(\sqrt{3},-\sqrt{3})$ kiezen, krijgen we het rooster in figuur 1. De twee vectoren heten de basisvectoren en samen vormen ze een *basis* voor het rooster. Het platte vlak kunnen we voorzien van een *inproduct* en daarmee meten we hoeken en lengtes. Als we gebruik maken van het standaard inproduct, staan de twee basisvectoren loodrecht op elkaar en heeft de vector $(1,1)$ lengte $\sqrt{2}$. We kunnen het inproduct echter ook een beetje aanpassen. Wanneer we bijvoorbeeld de assen loodrecht op elkaar houden, maar de lengtes in de horizontale richting met een factor 3 vergroten, krijgen we het plaatje in figuur 2. De twee basisvectoren zijn nu niet meer loodrecht en de vector $(1,1)$ heeft ten opzichte van dit inproduct lengte $\sqrt{1^2+3^2}=\sqrt{10}$. In het algemeen is een rooster een verzameling punten in een reële vectorruimte, voortgebracht door een $\mathbb{R}$-lineair onafhankelijke basis, met een inproduct op de vectorruimte dat zorgt voor hoek- en lengtebegrip.



figuur 1: rooster voortgebracht door $(1,1)$ en $(\sqrt{3},-\sqrt{3})$.

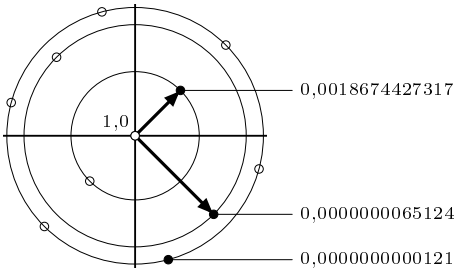
Voordat we de inhoud van dit proefschrift kunnen beschrijven, moeten we ook vertellen wat *getallenlichamen* zijn. Het eenvoudigste getallenlichaam is het lichaam $\mathbb{Q}$ der rationale getallen, bestaande uit alle getallen die geschreven kunnen worden als een quotiënt van twee gehele getallen. Andere getallenlichamen krijgen we door aan $\mathbb{Q}$ een eindig aantal wortels van polynomen toe te voegen. Als voorbeeld nemen we het lichaam $\mathbb{Q}(\sqrt{3})$ dat bestaat uit alle getallen die geschreven kunnen worden in de vorm $a+b\sqrt{3}$ met a en b in $\mathbb{Q}$. Dus $\frac{1}{2}+\frac{3}{7}\sqrt{3}$ zit in $\mathbb{Q}(\sqrt{3})$, maar $\sqrt{2}$ niet. De *ring van gehelen* van $\mathbb{Q}(\sqrt{3})$ is dan $\mathbb{Z}[\sqrt{3}]$, bestaande uit getallen van de vorm $a+b\sqrt{3}$ met a en b geheel. De ring van gehelen $\mathbb{Z}[\sqrt{3}]$ heeft een basis over $\mathbb{Z}$ gegeven door 1 en $\sqrt{3}$. Als we 1 in het platte vlak tekenen met coördinaten $(1,1)$ en $\sqrt{3}$ met coördinaten $(\sqrt{3},-\sqrt{3})$ en we nemen het standaard inproduct, krijgen we precies het rooster uit figuur 1. Elk getallenlichaam heeft een ring van gehelen en elke ring van gehelen kan op een vergelijkbare manier worden voorgesteld als een rooster. We hoeven natuurlijk niet het standaard inproduct te gebruiken. We staan in dit proefschrift *hermitese* inproducten toe, wat in ons voorbeeld erop neerkomt dat alles is toegestaan zolang de assen loodrecht op elkaar



figuur 2: zelfde rooster als in figuur 1, maar met lengtes in horizontale richting 3 keer zo groot.

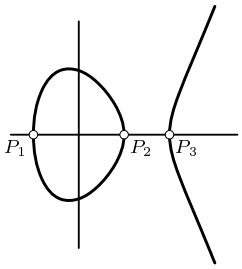
staan. Wanneer we een ring van gehelen geven, tezamen met een interpretatie als rooster met een hermites inproduct, geven we eigenlijk een *gemetriseerde lijnbundel*. Er zijn ook andere gemetriseerde lijnbundels, maar voorlopig voldoet het om hieraan te denken. De figuren 1 en 2 zijn twee grafische weergaven van twee verschillende gemetriseerde lijnbundels.

Gegeven een gemetriseerde lijnbundel—dus in het bijzonder een rooster—kunnen we aan alle roosterpunten een waarde toekennen. Als x een punt in het rooster is en $\|x\|$ is zijn lengte, dan kennen we de waarde $e^{-\pi\|x\|^2}$ toe. Als we kijken naar het voorbeeld in figuur 1, dan zien we dat het punt $(0,0)$ de waarde $e^{-\pi\cdot 0} = 1$ toegekend krijgt en dat $(1,1)$ de waarde $e^{-\pi(\sqrt{2})^2} = e^{-2\pi}$ krijgt. Die laatste waarde is afgerond op 4 decimalen gelijk aan 0,0019. Voor langere vectoren wordt deze toegekende waarde al snel klein. Bijvoorbeeld, de waarde die aan $(\sqrt{3}, -\sqrt{3}\,)$ wordt toegekend is al kleiner dan $0{,}66 \times 10^{-8}$ en de waarde die bij $(10,10)$ wordt gegeven is minder dan $0{,}14 \times 10^{-272}$. Het toekennen van deze waarden aan de roosterpunten is weergegeven in figuur 3. Als we alle waarden bij elkaar optellen, krijgen we afgerond 1,00373489 en als we daarvan de logaritme nemen, geeft dat 0,0037279. Die laatste waarde is de h^0 van de gemetriseerde lijnbundel uit figuur 1. In het algemeen is de $h^0(L)$ van een gemetriseerde lijnbundel L gelijk aan de logaritme van de som van alle getallen $e^{-\pi\|x\|^2}$, genomen over alle punten x in het rooster van L. Het eerste artikel in dit proefschrift betreft de functie h^0.



figuur 3: waarde $e^{-\pi\|x\|^2}$ die wordt toegekend aan een roosterpunt x. Punten op één cirkel hebben dezelfde lengte en dus dezelfde waarde.

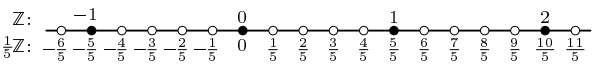
De functie h^0 is geïntroduceerd door de wiskundigen Van der Geer en Schoof als analogon van een belangrijke functie l uit de algebraïsche meetkunde. De functie l is het makkelijkst uit te leggen aan de hand van een voorbeeld. In figuur 4 is plaatje getekend van de algebraïsche kromme gegeven door de vergelijking $y^2 = (x+1)(x-1)(x-2)$. Een divisor op de kromme is een som van punten op de kromme. Bijvoorbeeld, $P_1 = (-1,0)$, $P_2 = (1,0)$ en $P_3 = (2,0)$ zijn drie punten op de kromme en $D = P_1 + P_2 + P_3$ is een voorbeeld van een divisor. Nu bestaat $L(D)$ uit (rationale) functies zonder polen buiten de drie punten P_1, P_2 en P_3 en ten hoogste enkelvoudige polen in deze drie punten. Een functie heeft een pool in een punt als haar inverse daar een nulpunt heeft. Bijvoorbeeld, de functie y die aan een punt op de kromme de y-coördinaat toekent, heeft nulpunten P_1, P_2 en P_3 en dus heeft $1/y$ daar (enkelvoudige) polen. Er geldt dat $1/y$ een functie is in $L(D)$. De functieruimte $L(D)$ is een vectorruimte en $l(D)$ is per definitie de dimensie van $L(D)$. Voor deze D is de dimensie $l(D)$ gelijk aan 3,



figuur 4: de kromme $y^2 = (x+1)(x-1)(x-2)$. De functie y die aan een punt de y-coördinaat toekent heeft nulpunten $P_1 = (-1,0)$, $P_2 = (1,0)$, $P_3 = (2,0)$ en $1/y$ heeft daar polen.

wat precies het aantal punten is waarover D een som is. We zeggen dat D graad n heeft als die een som is van n punten en we schrijven $n = \deg D$. De stelling van *Riemann-Roch* zegt dat er, gegeven een kromme, een geheel getal g bestaat zodat voor alle divisoren D met $\deg D > 2g-2$ geldt $l(D) = \deg D+1-g$. Voor de kromme uit figuur 4 geldt $g = 1$. Dit getal g heet het *geslacht* van de kromme.

Het analogon van een algebraïsche kromme is een getallenlichaam. Het eenvoudigste voorbeeld daarvan is $\mathbb{Q}$. Het analogon van een punt op de kromme is dan een priemgetal. Dus 5 is een 'punt' op de 'kromme' $\mathbb{Q}$. Het analogon van een functie op de kromme is een getal uit het lichaam. Dus $\frac{21}{5}$ is een voorbeeld van een een functie. We kunnen dit getal factoriseren als $\frac{21}{5} = \frac{3\cdot 7}{5}$ en we zeggen dat deze functie nulpunten heeft bij 3 en 7 en een pool bij 5. De getallen in $\mathbb{Z}$ zijn precies de getallen zonder noemers en dus de functies zonder polen. De getallen in de verzameling $\frac{1}{5}\mathbb{Z}$ (zie figuur 5) zijn de functies met op zijn hoogst een pool in 5. In het meetkundegeval kregen we een vectorruimte van functies en konden we de grootte meten door de dimensie te nemen. In onze getaltheoriesituatie krijgen we geen vectorruimte maar een gemetriseerde lijnbundel en in plaats van de dimensie nemen we de h^0. We kunnen ook een graad aan een gemetriseerde lijnbundel toekennen. De graad van de lijnbundel uit figuur 1 is $\log(1) = 0$ en de graad van de lijnbundel uit figuur 2 is $\log(\frac{1}{3})$ omdat daar $\frac{1}{3}$ keer zoveel punten in liggen. De graad van de lijnbundel $\mathbb{Z}$ uit figuur 5 is $\log(1) = 0$ en de graad van $\frac{1}{5}\mathbb{Z}$ is $\log(5)$ omdat daar 5 keer zoveel punten in liggen. Op deze manier krijgen we een analogon van de stelling van Riemann-Roch: er is een getal g zodat voor gemetriseerde lijnbundels L geldt $h^0(L) \approx \deg L+1-g$. Het teken '$\approx$' kan nu niet als gelijkheid worden gelezen, maar het quotiënt van beide kanten gaat naar 1 als de graad naar oneindig gaat. In het eerste artikel in dit proefschrift geven we een analogon van de stelling van Clifford:



figuur 5: de gemetriseerde lijnbundels $\mathbb{Z}$ en $\frac{1}{5}\mathbb{Z}$. De elementen in $\frac{1}{5}\mathbb{Z}$ zijn de functies uit $\mathbb{Q}$ met ten hoogste een pool in het punt 5. De graad van $\mathbb{Z}$ is $\log(1) = 0$ en de graad van $\frac{1}{5}\mathbb{Z}$ is $\log(5)$.

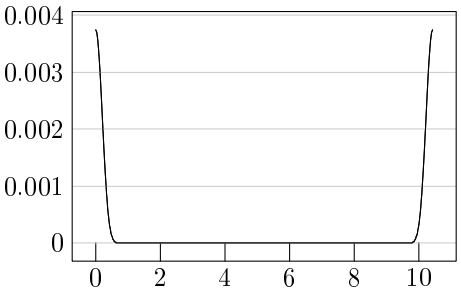
> STELLING (*Clifford*). *Zij D een divisor met $l(D) > 0$ en $l(D^\dagger) > 0$. Dan geldt $l(D) \leq \frac{1}{2}\deg D + 1$.*

De $D^\dagger$ staat voor de duale van D, maar daar zullen we hier geen definitie van geven. Als g het geslacht is van de kromme, zegt de stelling van Clifford dat voor divisoren D met $\deg D$ grofweg tussen 0 en g geldt $l(D) \leq \frac{1}{2}\deg D + 1$. Dus terwijl de stelling van Riemann-Roch met name wat zegt over divisoren met grote graad, gaat Clifford over divisoren met kleine graad. Het arithmetisch analogon dat we bewijzen is het volgende:

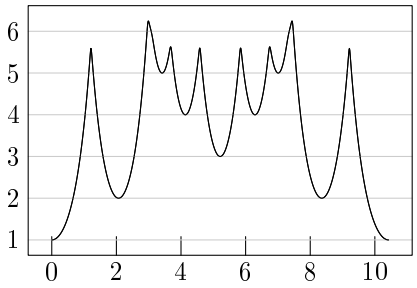
> STELLING. *Er is een constante c die alleen van de graad van het getallenlichaam afhangt, zodat voor gemetriseerde lijnbundels L met $\deg L \geq 0$ en $\deg L^\dagger \geq 0$ geldt $h^0(L) \leq \frac{1}{2}\deg L + c$.*

De constante c wordt in het proefschrift volledig expliciet gegeven.

In het tweede artikel houden we ons bezig met de vraag in hoeverre twee verschillende getallenlichamen dezelfde h^0 kunnen hebben. Laten we eerst kijken naar lichamen van de vorm $\mathbb{Q}(\sqrt{d}\,)$ met d positief. Als voorbeeld nemen we $\mathbb{Q}(\sqrt{129}\,)$. De ring van gehelen is $\mathbb{Z}[\sqrt{129}\,]$ en deze kan als gemetriseerde lijnbundel worden voorgesteld met basis $(1,1)$ en $(\sqrt{129}, -\sqrt{129}\,)$ met het standaard inproduct. Deze gemetriseerde lijnbundel heeft graad 0. Laat nu x een reëel getal zijn en schrijf $y = e^{2x}$. Als we het inproduct in de horizontale richting vermenigvuldigen met een factor y en in de verticale richting met een factor $1/y$, krijgen we een andere gemetriseerde lijnbundel die ook graad 0 heeft. Hiervan kunnen we weer de h^0 nemen. Zo kunnen we een functie maken die aan een reële x de h^0 van de geschaalde lijnbundel toekent. In figuur 6 is deze grafiek getekend. Helaas is aan die grafiek met het blote oog niet zoveel te zien. Een geschaalde, interessantere versie is gegeven in figuur 7. We krijgen zo een functie $\mathbb{R} \to \mathbb{R}$ en als we toestaan dat we in de horizontale richting een totaal andere factor gebruiken dan in de verticale richting, krijgen we een functie $\mathbb{R}^2 \to \mathbb{R}$. De hoofdstelling uit het tweede artikel zegt dat geen twee lichamen aanleiding geven tot dezelfde functie $\mathbb{R}^2 \to \mathbb{R}$. Een vergelijkbare stelling wordt gegeven voor willekeurige getallenlichamen, niet noodzakelijk van de vorm $\mathbb{Q}(\sqrt{d}\,)$.

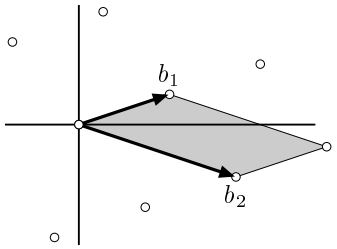


figuur 6: de grafiek van de h^0 van $\mathbb{Q}(\sqrt{129}\,)$ op het graad 0 stuk.



figuur 7: de grafiek van een geschaalde versie van de h^0 van $\mathbb{Q}(\sqrt{129}\,)$.

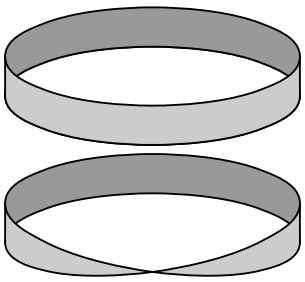
Het derde artikel gaat over vectorbundels en het vinden van 'kleine' punten. We leggen eerst uit wat de stelling van Minkowski zegt. Als we een rooster hebben met basis b_1, b_2, dan is het *volume* van het rooster gelijk aan de oppervlakte van het parallellogram opgespannen door b_1 en b_2 (zie figuur 8). Als we nu een cirkel nemen, gecentreerd om de oorsprong, met oppervlakte 4 keer zo groot als de volume van het rooster, dan zegt de stelling van Minkowski dat er afgezien van de oorsprong nog een ander punt van het rooster in de cirkel zit. De stelling van Minkowski geeft dus een punt ongelijk aan de oorsprong, waarvan de lengte 'klein' is.



figuur 8: het volume van het rooster is de oppervlakte van het grijze vlakje.

We gaan nu het begrip rooster vervangen door *vectorbundel*. Over $\mathbb{Q}$ is een vectorbundel hetzelfde als een rooster. De definitie van vectorbundel over willekeurige getallenlichamen is wat ingewikkelder. Voor ingewijden: het betreft

hier een projectief moduul P van eindige rang over de ring van gehelen met een inproduct op $P \otimes \mathbb{R}$. Even afgezien van het inproduct is een vectorbundel over $\mathbb{Q}$ gelijk aan $\mathbb{Z}^r$ voor een positief geheel getal r. Voor een willekeurig getallenlichamen met ring van gehelen Z is het niet per se zo dat vectorbundels van de vorm Z^r zijn, om dezelfde reden dat een lijnbundel niet altijd gelijk is aan Z met een inproduct. Een lijnbundel is soms een verdraaide versie van de ring van gehelen: Z met een *twist*. Een manier om daar een voorstelling van te maken, is te denken aan een *Möbius band* (zie figuur 9). Een Möbius band krijg je uit een gewone band door die door te knippen, vervolgens één van de eindjes een halve slag te draaien en de eindjes weer aan elkaar te plakken. *Locaal* zijn de gewone band en de Möbius band gelijk aan elkaar: als we een stukje uit een van de twee banden knippen is niet te zien uit welke band dit stukje is gekomen. Alleen *globaal* zijn ze verschillend. In het algemeen is een lijnbundel een getwiste versie van de ring van gehelen met een inproduct. Locaal ziet die er hetzelfde uit als de ring van gehelen, maar globaal niet. Een vectorbundel is een som van getwiste ringen van gehelen met een inproduct. Van een vectorbundel kunnen we ook twists nemen. Voor wie dit wat zegt, betekent dit dat we het tensorproduct nemen met een lijnbundel van graad 0.



figuur 9: de Möbius band onder is een 'twist' van de band boven.

Gegeven een vectorbundel, geeft de stelling van Minkowski een klein punt. In het derde artikel gaan we in op de vraag of *in het algemeen* het minimum van alle kleinste punten over alle twists van een vectorbundel kleiner is dan we op grond van Minkowski zouden mogen verwachten.

Het vierde artikel betreft een onderwerp uit de K-theorie. Dit heeft niet direct te maken met vectorbundels of lijnbundels, hoewel de stelling van Minkowski een veelgebruikt gereedschap is. We geven in dit artikel een grens die gebruikt wordt om de *tamme kern* van een getallenlichaam uit te rekenen. Bovendien tonen we aan dat de tamme kern berekenbaar is. De tamme kern van een getallenlichaam is een *eindige groep* en het uitrekenen ervan betekent dat je een eindig aantal *voortbrengers* opschrijft en een eindig aantal *relaties*. Wanneer we met de computer een tamme kern uitrekenen, zoeken we eerst naar voortbrengers totdat we zekerheid hebben dat we er voldoende hebben gevonden. De grens die we geven, geeft aan tot hoever we moeten zoeken. Vervolgens zoeken we naar de relaties. Daarvoor hebben we geen grens gegeven, maar we kunnen wel bewijzen dat na een eindige zoektocht alle relaties zijn gevonden en ook met zekerheid kan worden gezegd dat ze allemaal gevonden zijn.

De grens uit het vierde artikel verbetert andere grenzen die al in de literatuur in omloop waren. Voor imaginair kwadratische lichamen is de grens omlaag gebracht van $1{,}41|\Delta|^{5/3}$ naar $0{,}234|\Delta|^{3/2}$, waarbij $|\Delta| \geq 631$ de discriminant is van het lichaam. Voor algemene getallenlichamen is $4|\Delta|^{3/2}$ een vereenvoudigde, maar geldige grens. Vóór dit artikel was er voor algemene getallenlichamen nog geen bruikbare grens.

CURRICULUM VITAE

Richard Paul Groenewegen is geboren op 26 februari 1975 te Hoorn. Tijdens zijn jeugd was hij zeer geïnteresseerd in muziek en besteedde hij een groot gedeelte van zijn tijd aan het spelen van accordeon en synthesizer. Hij nam deel aan concoursen en overwoog een opleiding aan het conservatorium te gaan volgen.

Echter, tijdens zijn middelbareschooltijd besloot hij muziek slechts als hobby te houden en verschoof zijn interesse richting de studies wiskunde en informatica. In 1993 rondde hij het Voorbereidend Wetenschappelijk Onderwijs aan de Openbare Scholengemeenschap Hoorn cum laude af. Aansluitend begon hij aan de studie informatica aan de Universiteit van Amsterdam. Na een maand bleek dat er voldoende tijd was om wiskunde als tweede studie te volgen en na een jaar haalde hij de propedeuses voor beide studies cum laude.

Richard vervulde verschillende studentassistentschappen bij zowel wiskunde als bij informatica. Daarnaast hield hij zich actief bezig met inline skaten en was betrokken bij de oprichting van de Amsterdam Friday Night Skate. Zijn afstudeerscriptie *The size function for number fields* betrof een onderwerp uit de algebraïsche getaltheorie en werd begeleid door Peter Stevenhagen. In januari 1999 behaalde hij het doctoraalexamen wiskunde, opnieuw cum laude.

Drie dagen na zijn afstuderen begon hij als Assistent in Opleiding aan het Mathematisch Instituut aan de Universiteit Leiden. Daar werkte hij aan zijn promotieonderzoek onder begeleiding van Hendrik Lenstra en Bart de Smit. Richard bezocht congressen in Nederland, Italië, Frankrijk, Duitsland en de Verenigde Staten. Hij heeft in het najaar van 1999 drie maanden onderzoek uitgevoerd aan de University of California in Berkeley en een jaar later bezocht hij het Mathematical Sciences Research Institute in Berkeley, eveneens voor drie maanden.

Het resultaat van het promotieonderzoek is gebundeld in dit proefschrift. Sinds juni 2003 werkt Richard Groenewegen op de afdeling Credit Risk Modeling van de ABN AMRO in Amsterdam.