



Adelic geometry and polarity

Carsten Thiel

Fakultät für Mathematik, Otto-von-Guericke-Universität Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany

ARTICLE INFO

Article history:

Received 17 November 2011

Accepted 8 February 2012

Available online 4 April 2012

Communicated by Matthias Beck

MSC:

11H06

11R56

52C07

Keywords:

Adelic geometry

Successive minima

Polarity

ABSTRACT

In the present paper we generalise transference theorems from the classical geometry of numbers to the geometry of numbers over the ring of adeles of a number field. To this end we introduce a notion of polarity for adelic convex bodies.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

By a convex body S in the m -dimensional Euclidean space \mathbb{R}^m , we mean a compact and convex set $S \subset \mathbb{R}^m$ with non-empty interior, which we assume to be 0-symmetric, i.e. $S = -S$. A lattice Λ is a free \mathbb{Z} -module of full rank in \mathbb{R}^m .

Given a convex body S and a lattice Λ in \mathbb{R}^m , the i -th successive minimum $\lambda_i(S, \Lambda)$ for $1 \leq i \leq m$ of S with respect to Λ is defined as

$$\lambda_i(S, \Lambda) := \inf\{\lambda > 0 \mid \lambda S \cap \Lambda \text{ contains at least } i \text{ linearly independent elements}\}.$$

With a convex body S and a lattice Λ we can associate the polar body

$$S^* := \{x \in \mathbb{R}^m \mid \langle x, y \rangle \leq 1 \forall y \in S\}$$

E-mail address: carsten.thiel@ovgu.de.

and the polar lattice

$$\Lambda^* := \{x \in \mathbb{R}^m \mid \langle x, y \rangle \in \mathbb{Z} \ \forall y \in \Lambda\},$$

where $\langle \cdot, \cdot \rangle$ denotes the standard scalar product on \mathbb{R}^m . We have $(\mathbb{Z}^m)^* = \mathbb{Z}^m$ and $B_m^* = B_m$ for the Euclidean unit ball.

A classical inequality, first investigated by Mahler, is the transference result

$$1 \leq \lambda_i(S, \Lambda) \lambda_{m-i+1}(S^*, \Lambda^*) \leq m^{3/2}, \quad (1)$$

for $1 \leq i \leq m$. For the easy to prove lower bound see Gruber [9, §5], while the upper bound follows from Banaszczyk [1, Thm. 2.1].

We provide a generalisation of this inequality and of the notion of polarity to the geometry of numbers over the ring of adeles of an algebraic number field.

The theory of adelic geometry of numbers arises in the context of Siegel's Lemma, which asks for a small non-zero integral solution to a system of linear equations with integer coefficients. Answers by Thue, Siegel and others usually involve counting arguments or Minkowski's theorems on successive minima, cf. [15]. In order to allow coefficients and solutions from an algebraic number field, Bombieri and Vaaler in [4] proved an adelic variant of Minkowski's second theorem on successive minima. A comprehensive overview of adelic geometry of numbers can be found in [16].

The theory has been further generalised, as has Siegel's Lemma, with recent results by Fukshansky [5,6] and Gaudron [7] and Gaudron and Rémond [8] on the number of algebraic points in bounded regions. Further work on Siegel's Lemma for the algebraic closure of \mathbb{Q} by Roy and Thunder [14] involves the study of twisted heights. Using these heights they introduce a different notion of adelic polarity and an analogous statement of (1) in terms of these heights, which have been extended by Pekker [12] and Rothlisberger [13].

The present paper however uses a more geometric approach, directly extending the classical notion of polarity to the adelic setting.

To this end we fix an algebraic number field K of degree d over \mathbb{Q} , with field discriminant Δ_K , cf. [11, Kap. I]. We will use geometry of numbers for the module $K_{\mathbb{A}}^n$ of rank $n \in \mathbb{N}$ over the ring of adeles $K_{\mathbb{A}}$ of K .

The definitions of an adelic convex body S and the adelic successive minima $\lambda_i(S)$ for $1 \leq i \leq n$, as introduced by Bombieri and Vaaler [4], will be provided in Section 2. For our definition of polar adelic body see Definition 3.7.

The main results of this paper are the following.

Theorem 1.1. *Let S be an adelic convex body, S^* its polar and let $\lambda_i(S), \lambda_j(S^*)$ ($1 \leq i, j \leq n$) be the successive minima of S and S^* respectively. Then for $1 \leq \ell \leq n$*

$$\lambda_{\ell}(S) \lambda_{n-\ell+1}(S^*) \leq (nd)^{3/2}.$$

In view of the classical result (1) we are also interested in a lower bound. While the classical bound is comparatively easy to prove, this is not the case in the adelic setting and we cannot prove our bound in full generality. For a special class of adelic convex bodies and for K totally real or a CM-field (i.e. a field of complex multiplication) we get the following estimate.

Theorem 1.2. *Let K be totally real or a CM-field and let S be an adelic convex body, with the additional requirement that for all complex places v , we have $S_v = \alpha S_v$ for $\alpha \in \mathbb{C}$ with $|\alpha| = 1$. Let S^* be its polar and let $\lambda_i(S), \lambda_j(S^*)$ ($1 \leq i, j \leq n$) be the successive minima of S and S^* respectively.*

Then for $1 \leq \ell \leq n$

$$\frac{1}{\sqrt[d]{|\Delta_K|}} \leq \lambda_{\ell}(S) \lambda_{n-\ell+1}(S^*).$$

Notice, that in the case $K = \mathbb{Q}$ these results reduce to the classical statement (1). Finally, Example 4.2 shows that the lower bound is sharp, at least for $n = 1$.

2. Adelic geometry of numbers

We start by giving a brief overview of the ring of adeles of an algebraic number field K of degree d over \mathbb{Q} . For more details and proofs we refer to [17, Ch. IV] and [10, Ch. VI]. Let r be the number of real and s the number of pairs of complex embeddings of K into \mathbb{C} . Then $d = r + 2s$. Denote by \mathcal{O} the ring of algebraic integers of K and by Δ_K its field discriminant.

Let $M(K)$ be its set of places. For $v \in M(K)$ we write $v \nmid \infty$ for non-archimedean places and $v \mid \infty$ for the archimedean ones. We write $|\cdot|_v$ for the corresponding absolute value on K . We normalise it to extend either the usual absolute value on \mathbb{Q} for archimedean places or the p -adic absolute value for a prime p . Then the local field K_v is the completion of K with respect to v . For $v \nmid \infty$ let \mathcal{O}_v be the local ring of integers.

Let $K_{\mathbb{A}}$ be the ring of adeles of K and $K_{\mathbb{A}}^n$ the standard module of rank $n \geq 2$, i.e. the n -fold product of adeles. Recall that $K_{\mathbb{A}}$ is the restricted direct product of the K_v with respect to the \mathcal{O}_v . For any $v \in M(K)$ let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree ($\mathbb{Q}_{\infty} \cong \mathbb{R}$). Then for all primes $p \in \mathbb{Z}$

$$d = \sum_{v \mid p} d_v \quad \text{and} \quad d = \sum_{v \mid \infty} d_v, \quad \text{and also} \quad \prod_{v \in M(K)} |a|_v^{d_v} = 1 \quad (2)$$

for all non-zero $a \in K$.

Denote by σ_i , $1 \leq i \leq r$ the embeddings of K into \mathbb{R} and by $\sigma_{r+i} = \overline{\sigma}_{r+i+s}$, $1 \leq i \leq s$ the pairs of embeddings of K into \mathbb{C} , so $d = r + 2s$. We call K *totally real*, if $s = 0$, and we call K a *CM-field*, if it is a quadratic extension of a totally real field with $r = 0$. In the second case there exists a unique non-trivial automorphism τ_K of K , such that $\sigma(\tau_K(x)) = \overline{\sigma(x)}$ for any embedding $\sigma: K \rightarrow \mathbb{C}$, where $\overline{\cdot}$ denotes complex conjugation in \mathbb{C} , cf. [3]. Then

$$\iota: x \mapsto (\sigma_1(x), \dots, \sigma_r(x), \sigma_{r+1}(x), \dots, \sigma_{r+s}(x))$$

and

$$\bar{\iota}: x \mapsto (\sigma_1(x), \dots, \sigma_r(x), \overline{\sigma}_{r+1}(x), \dots, \overline{\sigma}_{r+s}(x))$$

are embeddings of K into $K_{\infty} := \prod_{v \mid \infty} K_v$.

There is a canonical isomorphism $\rho: K_{\infty} \rightarrow \mathbb{R}^d$ with

$$\rho(x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}) = (x_1, \dots, x_r, \Re(x_{r+1}), \Im(x_{r+1}), \dots, \Re(x_{r+s}), \Im(x_{r+s})).$$

Here \Re and \Im denote real and imaginary parts respectively.

Together we get $(\rho \circ \iota): K \hookrightarrow \mathbb{R}^d$,

$$x \mapsto (\sigma_1(x), \dots, \sigma_r(x), \Re(\sigma_{r+1}(x)), \Im(\sigma_{r+1}(x)), \dots, \Re(\sigma_{r+s}(x)), \Im(\sigma_{r+s}(x))).$$

In the rank- n case let $K_{\infty}^n := \prod_{v \mid \infty} K_v^n$,

$$\iota^n := (\sigma_1^n, \dots, \sigma_r^n, \sigma_{r+1}^n, \dots, \sigma_{r+s}^n): K^n \rightarrow K_{\infty}^n, \quad \bar{\iota}^n \text{ respectively,}$$

where the σ_i act componentwise. Similarly $\rho^n: K_{\infty}^n \rightarrow \mathbb{R}^{nd}$. To simplify notation, we usually write ρ and ι in place of ρ^n and ι^n .

Definition 2.1. For each $v \nmid \infty$ let S_v be a free \mathcal{O}_v -module of full rank, where $S_v = \mathcal{O}_v^n$ for all but finitely many v . In other words, for any $v \nmid \infty$ there is an $A_v \in \mathrm{GL}_n(K_v)$ such that $S_v = A_v^{-1} \mathcal{O}_v^n$, where A_v is the identity for all but finitely many v . For $v \mid \infty$ we have $K_v \cong \mathbb{R}$ or $K_v \cong \mathbb{C}$. In this case let $S_v \subset K_v^n$ be a 0-symmetric compact convex body with non-empty interior in \mathbb{R}^n or $\mathbb{C}^n \cong \mathbb{R}^{2n}$ respectively. Then the set

$$S = \prod_{v \nmid \infty} S_v \times \prod_{v \mid \infty} S_v$$

is called a closed symmetric *adelic convex body*. If necessary, we denote $S_\infty = \prod_{v \mid \infty} S_v$.

For $(x_v)_v \in K_{\mathbb{A}}^n$ we define the scalar multiple $(y_v)_v = \lambda(x_v)_v$ for $\lambda \in \mathbb{R}^+$ by

$$y_v := \begin{cases} x_v & \text{if } v \nmid \infty, \\ \lambda x_v & \text{if } v \mid \infty. \end{cases}$$

Definition 2.2. The i -th successive minimum of the adelic convex body S is

$$\lambda_i(S) = \inf \{ \lambda > 0 \mid \exists x_1, \dots, x_i \in K^n \text{ linearly independent over } K \text{ such that } x_j \in \lambda S \text{ for all } j \}$$

for $1 \leq i \leq n$. By construction $\lambda_i(S) \leq \lambda_j(S)$ for $i \leq j$.

Definition 2.3. The *inhomogeneous minimum* of the adelic convex body S is

$$\mu(S) := \inf \left\{ \mu > 0 \mid K_{\mathbb{A}}^n = \bigcup_{\zeta \in K^n} (\mu S + \zeta) \right\}.$$

By construction $\mu(S) = \widehat{\mu}(\rho(S_\infty), \rho(\iota(\mathfrak{M})))$, where

$$\widehat{\mu}(T, \Lambda) := \inf \left\{ \mu > 0 \mid \mathbb{R}^m = \bigcup_{\zeta \in \Lambda} (\mu T + \zeta) \right\}$$

is the classical inhomogeneous minimum of the convex body $T \subset \mathbb{R}^m$ with respect to the lattice $\Lambda \subset \mathbb{R}^m$, cf. [9, §5]. Here $\mathfrak{M} = \bigcap_{v \nmid \infty} (S_v \cap K^n)$.

3. Adelic polarity

In order to define our notion of adelic polarity we first recall some background from Algebraic Number Theory. It is well known [11, Ch. I, (2.8)], that

$$T(x, y) := \mathrm{Tr}_{K/\mathbb{Q}}(xy)$$

is a non-degenerate symmetric \mathbb{Q} -bilinear form on K . Here $\mathrm{Tr}_{K/\mathbb{Q}}$ denotes the field trace. This allows to define

$$^* \mathcal{O} := \{ x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z} \forall y \in \mathcal{O} \}, \quad (3)$$

the *complementary module*, cf. [11, Ch. III, §2]. This is a fractional ideal in K , its inverse is the *different* \mathfrak{d} . On K^n we get a bilinear form given by

$$T_n(x, y) := \sum_{i=1}^n \text{Tr}_{K/\mathbb{Q}}(x_i y_i).$$

By [17, Ch. V, §2, Thms. 2 and 3] for any fractional ideal \mathfrak{m} there is a map $a : M(K) \rightarrow \mathbb{Z}$, such that \mathfrak{m} can be written as

$$\mathfrak{m} = \bigcap_{v \nmid \infty} (K \cap \mathfrak{p}_v^{a(v)}), \quad (4)$$

where almost all $a(v) = 0$ and \mathfrak{p}_v is the unique maximal ideal in \mathcal{O}_v . More concretely, we get the following special case.

Lemma 3.1. *Let $v \nmid \infty$ and define as in the global case*

$${}^*\mathcal{O}_v := \{x \in K_v \mid \text{Tr}_{K_v/\mathbb{Q}_v}(xy) \in \mathbb{Z}_v \ \forall y \in \mathcal{O}_v\}.$$

Then ${}^\mathcal{O} = \bigcap_{v \nmid \infty} ({}^*\mathcal{O}_v \cap K)$. For all but finitely many $v \nmid \infty$ we have ${}^*\mathcal{O}_v = \mathcal{O}_v$.*

Proof. By their definitions (cf. [10, p. 377 (★)]) we have

$${}^*\mathcal{O}_v \cap K = {}^*\mathcal{O}_{(v)} := \left\{ \frac{a}{b} \mid a \in {}^*\mathcal{O}, \ b \in \mathcal{O} \setminus (v) \right\} \supseteq {}^*\mathcal{O},$$

where ${}^*\mathcal{O}_{(v)}$ is the localisation of ${}^*\mathcal{O}$ at the ideal (v) corresponding to v .

For the converse inclusion we follow an idea suggested to us by J. Jahnel. Let $M := \bigcap_{v \nmid \infty} {}^*\mathcal{O}_{(v)}$, $x \in M$ and consider the “ideal of denominators”

$$I := \{b \in \mathcal{O} \mid bx \in M\}.$$

Since $x \in K \cap {}^*\mathcal{O}_v = {}^*\mathcal{O}_{(v)}$, we have $I \not\subseteq (v)$, for the ideal in K corresponding to v . Since this holds for all v , we have $I = \mathcal{O}$. Therefore $x \in {}^*\mathcal{O}$.

The final statement follows from [10, Lemma 6.48], since only finitely many primes are ramified in K . \square

We extend the construction from (3) in a natural way to the rank- n case with the form T_n .

Lemma 3.2. *Let $A \in \text{GL}_n(K)$ and $A_v \in \text{GL}_n(K_v)$ for any finite v . Then*

$${}^*(A\mathcal{O}^n) = A^{-t}({}^*\mathcal{O})^n \quad \text{and} \quad {}^*(A_v\mathcal{O}_v^n) = A_v^{-t}({}^*\mathcal{O}_v)^n,$$

where A^{-t} and A_v^{-t} are the transpose of A^{-1} and A_v^{-1} respectively.

Proof. Notice that

$${}^*(\mathcal{O}^n) := \{x \in K^n \mid T_n(x, y) \in \mathbb{Z} \ \forall y \in \mathcal{O}^n\} \supseteq ({}^*\mathcal{O})^n.$$

Suppose they are not the same, i.e. $\exists a \in {}^*(\mathcal{O}^n) \setminus ({}^*\mathcal{O})^n$. Then for some i : $a_i \notin {}^*\mathcal{O}$, so there is some $b_i \in \mathcal{O}$, such that $\text{Tr}_{K/\mathbb{Q}}(a_i b_i) \notin \mathbb{Z}$ by definition of ${}^*\mathcal{O}$. But then $T_n(a, (0, \dots, 0, b_i, 0, \dots, 0)) \notin \mathbb{Z}$ giving a contradiction.

Now let $(a_{ij})_{ij} = A \in \text{GL}_n(K)$, $x, y \in K^n$. Then

$$\begin{aligned} T_n(x, Ay) &= \sum_i \text{Tr}_{K/\mathbb{Q}}(x_i (Ay)_i) = \sum_i \text{Tr}_{K/\mathbb{Q}}\left(x_i \left(\sum_j a_{ij} y_j\right)\right) \\ &= \sum_i \sum_j \text{Tr}_{K/\mathbb{Q}}(x_i (a_{ij} y_j)) = \sum_j \sum_i \text{Tr}_{K/\mathbb{Q}}((a_{ij} x_i) y_j) \\ &= 7 \sum_j \text{Tr}_{K/\mathbb{Q}}((A^t x)_j y_j) = T_n(A^t x, y). \end{aligned}$$

The second statement is obvious, as the above argument works for $x, y \in K_v^n$ and $A_v \in \text{GL}_n(K_v)$ verbatim using $\text{Tr}_{K_v/\mathbb{Q}_v}$. \square

On the other hand, we can define a scalar product on $\mathbb{R}^d = \mathbb{R}^{r+2s}$ as

$$(x, y) = \sum_{i=1}^r x_i y_i + 2 \sum_{i=r+1}^{2s} x_i y_i, \quad (5)$$

cf. [11, Ch. I, (5.1)]. This gives the scalar product

$$(x, y) := (\rho(x), \rho(y)) = \sum_{v \text{ real}} x_v y_v + \sum_{v \text{ complex}} (x_v \bar{y}_v + \bar{x}_v y_v) \quad (6)$$

on K_∞ , cf. [11, p. 222].

Lemma 3.3. For all $x, y \in K$

$$\text{Tr}_{K/\mathbb{Q}}(xy) = (\rho(\iota(x)), \rho(\bar{\iota}(y))).$$

Proof. Let $x, y \in K$, then

$$\begin{aligned} &(\rho(\iota(x)), \rho(\bar{\iota}(y))) \\ &= \sum_{j=1}^r \sigma_j(x) \sigma_j(y) + \sum_{j=1}^s 2(\Re(\sigma_{r+j}(x)) \Re(\bar{\sigma}_{r+j}(y)) + \Im(\sigma_{r+j}(x)) \Im(\bar{\sigma}_{r+j}(y))) \\ &= \sum_{j=1}^r \sigma_j(x) \sigma_j(y) + 2 \sum_{j=1}^s (\Re(\sigma_{r+j}(x)) \Re(\sigma_{r+j}(y)) - \Im(\sigma_{r+j}(x)) \Im(\sigma_{r+j}(y))). \end{aligned}$$

By [11, Ch. I, (2.6)(ii)], $\text{Tr}_{K/\mathbb{Q}}(x) = \sum_{\sigma} \sigma(x)$, where the sum is over all embeddings $\sigma : K \hookrightarrow \bar{\mathbb{Q}}$. As all complex embeddings appear in conjugate pairs

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(xy) &= \sum_{j=1}^r \sigma_j(xy) + \sum_{j=1}^s \sigma_{r+j}(xy) + \sum_{j=1}^s \overline{\sigma}_{r+j}(xy) \\ &= \sum_{j=1}^r \sigma_j(x)\sigma_j(y) + 2 \sum_{j=1}^s \Re(\sigma_{r+j}(x)\sigma_{r+j}(y)).\end{aligned}$$

The statement follows from $\Re(ab) = \Re(a)\Re(b) - \Im(a)\Im(b)$. \square

Corollary 3.4. For any algebraic number field K with ring of integers \mathcal{O} and embeddings ρ and ι as above, we have

$$\rho(\iota(\mathcal{O}))^* = \rho(\iota^*(\mathcal{O})),$$

where $(\cdot)^*$ is the polar with respect to the form in (5).

The scalar product (\cdot, \cdot) on \mathbb{R}^{nd} is also defined as the sum of the components of each copy of \mathbb{R}^d . Notice that we get the standard scalar product at the real places and the real scalar product multiplied by 2 at the complex places. By direct consequence of Lemma 3.2 and Corollary 3.4 and again [17, Ch. V, §2, Thm. 2], cf. (4), this leads to the following generalisation.

Corollary 3.5. For any algebraic number field K with ring of integers \mathcal{O} and embeddings ρ^n and ι^n as above, we have

$$\rho^n(\iota^n(A^{-1}\mathcal{O}^n))^* = \rho^n(\iota^n(A^t(\mathcal{O}^n)^n))$$

and

$$\rho^n\left(\iota^n\left(\bigcap_{v \nmid \infty} (A_v^{-1}\mathcal{O}_v^n \cap K^n)\right)\right)^* = \rho^n\left(\iota^n\left(\bigcap_{v \nmid \infty} (A_v^t(\mathcal{O}_v^n)^n \cap K^n)\right)\right)$$

for $A \in \mathrm{GL}_n(K)$, $A_v \in \mathrm{GL}_n(K_v)$ for all $n \in \mathbb{N}$.

Remark 3.6. Consider a finite number of 0-symmetric convex bodies $S_i \subset \mathbb{R}^{m_i}$. Then, using the classical notion of polarity, introduced at the beginning of the paper,

$$\left(\prod_i S_i\right)^* \subseteq \prod_i S_i^*. \quad (7)$$

Indeed, let $x \in (\prod_i S_i)^*$, then $\langle x, y \rangle \leq 1$ for all $y \in \prod_i S_i$. So especially for any i we have $\langle x, (0, \dots, 0, y_i, 0, \dots, 0) \rangle \leq 1$ for all $y_i \in S_i$. But that implies $\langle x_i, y_i \rangle \leq 1$ for all i , which defines the right-hand side of (7).

For the scalar product (\cdot, \cdot) instead of $\langle \cdot, \cdot \rangle$ we get $\langle x, (0, \dots, 0, y_i, 0, \dots, 0) \rangle \leq \frac{1}{2}$ and $\langle x_i, y_i \rangle \leq \frac{1}{2}$ for the complex places $(x_i, y_i \in \mathbb{C})$, so (7) holds as well.

Due to Corollary 3.5, we are now in the situation to define our notion of adelic polarity.

Definition 3.7. Let $S = \prod_{v \nmid \infty} A_v^{-1}\mathcal{O}_v^n \times \prod_{v \mid \infty} S_v$ be an adelic convex body. The *polar adelic body* of S is

$$S^* := \prod_{v \nmid \infty} A_v^t({}^* \mathcal{O}_v)^n \times \prod_{v \mid \infty} S_v^*,$$

where S_v^* is the polar body of S_v with respect to the restriction of (5). Since $\mathcal{O}_v = {}^* \mathcal{O}_v$ for almost all $v \nmid \infty$ by Lemma 3.1, S^* is again an adelic convex body.

4. Adelic transference theorems

We now apply the results of the previous section, especially Corollary 3.5, to prove the main results of this paper.

Proof of Theorem 1.1. Let

$$\mathfrak{M} = \bigcap_{v \nmid \infty} (A_v^{-1} \mathcal{O}_v^n \cap K^n) \quad \text{and} \quad \mathfrak{M}^* = \bigcap_{v \nmid \infty} (A_v^t({}^* \mathcal{O}_v)^n \cap K^n).$$

By [16, Lemma] $\rho(\iota(\mathfrak{M}))$ and $\rho(i(\mathfrak{M}^*))$ are lattices of full rank in \mathbb{R}^{nd} . By Corollary 3.5, they are polar to each other.

Denote by S_∞ and S_∞^* the infinite parts of S and S^* respectively. By (7) we have

$$(\rho(S_\infty))^* \subset \rho(S_\infty^*). \quad (8)$$

Denote by $\lambda_\ell(S)$ and $\lambda_\ell(S^*)$ the adelic successive minima of S and S^* respectively and by $\widehat{\lambda}_i(T, \Lambda)$ the classical successive minima of the convex body T and the lattice Λ in \mathbb{R}^{nd} . Then, by [16, p. 256], for $\ell = 1, \dots, n$

$$\lambda_\ell(S) \leq \widehat{\lambda}_{(\ell-1)d+1}(\rho(S_\infty), \rho(\iota(\mathfrak{M})))$$

and

$$\lambda_\ell(S^*) \leq \widehat{\lambda}_{(\ell-1)d+1}(\rho(S_\infty^*), \rho(i(\mathfrak{M}^*))) \leq \widehat{\lambda}_{(\ell-1)d+1}(\rho(S_\infty)^*, \rho(i(\mathfrak{M}^*))),$$

where the last inequality follows from (8).

Finally, applying (1), we conclude

$$\begin{aligned} \lambda_\ell(S) \lambda_{n-\ell+1}(S^*) &\leq \widehat{\lambda}_{(\ell-1)d+1}(\rho(S_\infty), \rho(\iota(\mathfrak{M}))) \widehat{\lambda}_{((n-\ell+1)-1)d+1}(\rho(S_\infty)^*, \rho(i(\mathfrak{M}^*))) \\ &\leq \widehat{\lambda}_{(\ell-1)d+1}(\rho(S_\infty), \rho(\iota(\mathfrak{M}))) \widehat{\lambda}_{(n-\ell)d+d}(\rho(S_\infty)^*, \rho(i(\mathfrak{M}^*))) \\ &\leq (nd)^{3/2}. \quad \square \end{aligned}$$

Corollary 4.1. Let K , S , S^* and $\lambda_1(S)$ be as in Theorem 1.1 and let $\mu(S^*)$ be the inhomogeneous minimum of S^* . Then

$$\lambda_1(S) \cdot \mu(S^*) \leq Cnd(1 + \log nd),$$

where C is a universal constant.

Proof. As in the proof of Theorem 1.1, we have $\lambda_1(S) = \widehat{\lambda}_1(\rho(\iota(\mathfrak{M})), \rho(S_\infty))$ and by (8) we get

$$\widehat{\mu}(\rho(S_\infty^*), \Lambda) \leq \widehat{\mu}(\rho(S_\infty)^*, \Lambda)$$

for any lattice $\Lambda \subset \mathbb{R}^{nd}$. Therefore

$$\lambda_1(S) \cdot \mu(S^*) \leq \widehat{\lambda}_1(\rho(S_\infty), \rho(\iota(\mathfrak{M}))) \cdot \widehat{\mu}(\rho(S_\infty)^*, \rho(\iota(\mathfrak{M}^*))) \leq Cnd(1 + \log nd),$$

by [2, Corollary 1] with some universal constant C . \square

Proof of Theorem 1.2. We use the standard bilinear form on K^n :

$$b(x, y) = \sum_{i=1}^n x_i \bar{y}_i,$$

where $\bar{}$ is the identity for K totally real and if K is a CM-field, it is the unique non-trivial automorphism of K , that corresponds to complex conjugation in \mathbb{C} .

Let u_1, \dots, u_n and v_1, \dots, v_n be K -bases of K^n such that $u_i \in \lambda_i(S)S$ and $v_j \in \lambda_j(S^*)S^*$ for all i, j . Notice that for $u_i \in \mathcal{O}^n$ and $v_j \in (*\mathcal{O})^n$, we have $b(A^{-1}u_j, A^t v_j) = b(u_j, \bar{v}_j) \in *\mathcal{O}$, using that $*\mathcal{O}$ is a fractional ideal in K . By definition of $*\mathcal{O}$ and the different \mathfrak{d} , we have $|x| \leq |\mathfrak{d}|^{-1}$ for $x \in *\mathcal{O}$, [11, Ch. III, §2.1]. This holds for any finite place v as well.

Since b is non-degenerate, there are $i \in \{1, \dots, \ell\}$ and $j \in \{1, \dots, n - \ell + 1\}$ such that $b(u_i, \bar{v}_j) \neq 0$. Then by the product formula in (2)

$$\begin{aligned} 1 &= \prod_v |b(u_i, \bar{v}_j)|_v^{d_v} \cdot \left(\frac{\lambda_i(S) \lambda_j(S^*)}{\lambda_i(S) \lambda_j(S^*)} \right)^d \\ &= \prod_{v \nmid \infty} |b(u_i, \bar{v}_j)|_v^{d_v} \cdot (\lambda_i(S) \lambda_j(S^*))^d \cdot \prod_{v \mid \infty} \left| b\left(\frac{1}{\lambda_i(S)} u_i, \frac{1}{\lambda_j(S^*)} \bar{v}_j \right) \right|_v^{d_v}. \end{aligned}$$

Now for any finite v we have $b(u_i, \bar{v}_j) \in *\mathcal{O}_v$, therefore $|b(u_i, \bar{v}_j)|_v^{d_v} \leq |\mathfrak{d}_v|^{-d_v}$, where \mathfrak{d}_v denotes the local different. Finally $\prod_{v \nmid \infty} |\mathfrak{d}_v|^{-d_v} = |\Delta_K|$, cf. [10, Ch. VI, §8].

To conclude the proof, we consider the factors at the infinite places. By assumption they are either all real or all complex. Fix some $v \mid \infty$. Let $x := \frac{1}{\lambda_i(S)} u_i$ and $y := \frac{1}{\lambda_j(S^*)} v_j$. If K is totally real, i.e. v is real, we have

$$|b(x, \bar{y})|_v^{d_v} = |b(x, y)|_v^1 = \left| \sigma_v \left(\sum_i x_i y_i \right) \right| = \left| \sum_i \sigma_v(x_i) \sigma_v(y_i) \right| \leq 1,$$

by definition of S_v^* .

If K is a CM-field, i.e. v is complex, we get

$$\begin{aligned} |b(x, \bar{y})|_v^{d_v} &= \left| \sigma_v \left(\sum_i x_i \bar{y}_i \right) \right|^2 = \left| \sum_i \sigma_v(x_i) \overline{\sigma_v(y_i)} \right|^2 \\ &\leq \left(\left| \Re \left(\sum_i \sigma_v(x_i) \overline{\sigma_v(y_i)} \right) \right| + \left| \Im \left(\sum_i \sigma_v(x_i) \overline{\sigma_v(y_i)} \right) \right| \right)^2 \leq \left(\left| \frac{1}{2} \right| + 1 \left| \frac{1}{2} \right| \right)^2 = 1, \end{aligned}$$

by definition of S_v^* , since $i\Im(x) = i\Re(ix)$ for all $x \in \mathbb{C}$ and from $(\sigma_v(x_i))_i \in S_v$ we get $i(\sigma_v(x_i))_i \in S_v$ by our additional requirement.

The conclusion follows from the monotonicity of the minima. \square

Example 4.2. Let $n = 1$ and $K = \mathbb{Q}[\sqrt{2}]$, then $\mathcal{O} = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ and the field discriminant is $|\Delta_K| = 8$. Consider $x = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ and $y = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}.$$

Therefore

$$\mathrm{Tr}(xy) = \mathrm{Tr} \begin{pmatrix} ac + 2bd & 2ad + 2bc \\ ad + bc & ac + 2bd \end{pmatrix} = 2ac + 4bd$$

and this is an integer if $a \in \frac{1}{2}\mathbb{Z}$ and $b \in \frac{1}{4}\mathbb{Z}$. Therefore ${}^*\mathcal{O} = \frac{1}{2}\mathbb{Z} + \frac{\sqrt{2}}{4}\mathbb{Z}$.

Now $\rho(\iota(\mathcal{O})), \rho(\iota({}^*\mathcal{O})) \subset \mathbb{R}^2$ are lattices of rank 2, more precisely

$$\rho(\iota(\mathcal{O})) = \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix} \mathbb{Z}^2, \quad \rho(\iota({}^*\mathcal{O})) = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{2}}{4} \\ \frac{1}{2} & -\frac{\sqrt{2}}{4} \end{pmatrix} \mathbb{Z}^2,$$

and we see that $\rho(\iota(\mathcal{O}))^* = \rho(\iota({}^*\mathcal{O}))$. This follows easily from the fact, that the matrices are the inverse transpose of one another.

Taking the 1-dimensional unit ball $[-1, 1]$ at both infinite places for the convex bodies, we see that

$$S = \prod_{v \nmid \infty} \mathcal{O}_v \times \prod_{v \mid \infty} [-1, 1] \quad \text{and} \quad S^* = \prod_{v \nmid \infty} {}^*\mathcal{O}_v \times \prod_{v \mid \infty} [-1, 1]$$

are polar. Obviously $\lambda_1(S) \leq 1$ and since $\frac{\sqrt{2}}{4} < \frac{1}{2}$, we have $\lambda_1(S^*) \leq \frac{\sqrt{2}}{4}$. This gives equality for the lower bound in Theorem 1.2.

Acknowledgments

I would like to thank Martin Henk, Florian Heß, Matthias Henze, Jörg Jahnel, Kristin Stroth and the referees for helpful comments and discussions on the subject.

References

- [1] Wojciech Banaszczyk, New bounds in some transference theorems in the geometry of numbers, *Math. Ann.* 296 (4) (1993) 625–635.
- [2] Wojciech Banaszczyk, Inequalities for convex bodies and polar reciprocal lattices in \mathbb{R}^n . II. Application of K -convexity, *Discrete Comput. Geom.* 16 (3) (1996) 305–311.
- [3] P.E. Blanksby, J.H. Loxton, A note on the characterization of CM-fields, *J. Aust. Math. Soc. Ser. A* 26 (1) (1978) 26–30.
- [4] Enrico Bombieri, Jeffrey D. Vaaler, On Siegel's lemma, *Invent. Math.* 73 (1) (1983) 11–32.
- [5] Lenny Fukshansky, Siegel's lemma with additional conditions, *J. Number Theory* 120 (1) (2006) 13–25.
- [6] Lenny Fukshansky, Algebraic points of small height missing a union of varieties, *J. Number Theory* 130 (10) (2010) 2099–2118.
- [7] Éric Gaudron, Géométrie des nombres adélique et lemmes de Siegel généralisés, *Manuscripta Math.* 130 (2) (2009) 159–182.
- [8] Éric Gaudron, Gaël Rémond, Lemmes de Siegel d'évitement, *Acta Arith.* (2012), in press.
- [9] Peter M. Gruber, Geometry of numbers, in: *Handbook of Convex Geometry*, vols. A, B, North-Holland, Amsterdam, 1993, pp. 739–763.
- [10] Anthony W. Knap, *Advanced Algebra, Cornerstones*, Birkhäuser Boston Inc., Boston, MA, 2007.
- [11] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992.

- [12] Alexander Pekker, On successive minima and the absolute Siegel's lemma, *J. Number Theory* 128 (3) (2008) 564–575, <http://dx.doi.org/10.1016/j.jnt.2007.04.013>.
- [13] Mark Peter Rothlisberger, An analogue of the Korkin–Zolotarev lattice reduction for vector spaces over number fields, Ph.D. thesis, The University of Texas at Austin, 2010.
- [14] Damien Roy, Jeffrey Lin Thunder, An absolute Siegel's lemma, *J. Reine Angew. Math.* 476 (1996) 1–26.
- [15] Wolfgang M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math., vol. 1467, Springer-Verlag, Berlin, 1991.
- [16] Jeffrey Lin Thunder, Remarks on adelic geometry of numbers, in: *Number Theory for the Millennium, III*, Urbana, IL, 2000, A K Peters, Natick, MA, 2002, pp. 253–259.
- [17] André Weil, *Basic Number Theory*, reprint of the second (1973) edition, *Classics Math.*, Springer-Verlag, Berlin, 1995.