11

Ideal Lattices

Eva Bayer-Fluckiger

Introduction

An *ideal lattice* is a pair (I, b), where I is an ideal of a number field, and b is a lattice, satisfying an invariance relation (see §1 for the precise definition). Ideal lattices naturally occur in many parts of number theory, but also in other areas. They have been studied in special cases, but, as yet, not much in general. In the special case of integral ideal lattices, the survey paper Bayer-Fluckiger (1999) collects and slightly extends the known results.

The first part of the paper (see §2) concerns integral ideal lattices, and states some classification problems. In §3, a more general notion of ideal lattices is introduced, as well as some examples in which this notion occurs.

The aim of §4 is to define twisted embeddings, generalising the canonical embedding of a number field. This section, as well as the subsequent one, is devoted to positive definite ideal lattices with respect to the canonical involution of the real étale algebra generated by the number field. These are also called Arakelov divisors of the number field. The aim of §5 is to study invariants of ideals and also of the number field derived from Hermite type invariants of the sphere packings associated to ideal lattices. This again gives rise to several open questions.

1 Definitions, notation and basic facts

A *lattice* is a pair (L, b), where L is a free $\mathbf{Z}$-module of finite rank, and $b : L \times L \to \mathbf{R}$ is a non-degenerate symmetric bilinear form. We say that (L, b) is an *integral lattice* if $b(x, y) \in \mathbf{Z}$ for all $x, y \in L$. An integral lattice (L, b) is said to be *even* if $b(x, x) \equiv 0 \pmod 2$ for all $x \in L$.

Let K be an algebraic number field. Let us denote by $\mathcal{O}$ its ring of integers, and by D_K its discriminant. Let n be the degree of K.

Set $K_{\mathbf{R}} = K \otimes_{\mathbf{Q}} \mathbf{R}$. Then $K_{\mathbf{R}}$ is an étale $\mathbf{R}$-algebra (i.e. a finite product of copies of $\mathbf{R}$ and $\mathbf{C}$). Let us denote by $\mathrm{N} = \mathrm{N}_{K_{\mathbf{R}}/\mathbf{R}}$ the norm, and by $\mathrm{Tr} = \mathrm{Tr}_{K_{\mathbf{R}}/\mathbf{R}}$ the trace, of this étale algebra. Let $^- : K_{\mathbf{R}} \to K_{\mathbf{R}}$ be an $\mathbf{R}$-linear involution.

Definition 1 An *ideal lattice* is a lattice (I, b), where I is a (fractional) $\mathcal{O}$-ideal and $b : I \times I \to \mathbf{R}$ is such that

$$b(\lambda x, y) = b(x, \overline{\lambda} y)$$

for all $x, y \in I$ and for all $\lambda \in O$.

Proposition 1 *Let I be an $\mathcal{O}$-ideal and let $b : I \times I \to \mathbf{R}$ be a lattice. Then the following are equivalent:*

(i) *(I, b) is an ideal lattice;*
(ii) *there exists an invertible element $\alpha \in K_{\mathbf{R}}$ with $\overline{\alpha} = \alpha$ such that*

$$b(x, y) = \mathrm{Tr}(\alpha x \overline{y}).$$

Proof This follows from the fact that $\mathrm{Tr} : K_{\mathbf{R}} \times K_{\mathbf{R}} \to \mathbf{R}$ is non-degenerate. □

The *rank* of an ideal lattice is the degree n of the number field K. As we shall see, the other basic invariants – determinant, signature – are also easy to determine. Let $b : I \times I \to \mathbf{R}$, $b(x, y) = \mathrm{Tr}(\alpha x \overline{y})$, be an ideal lattice.

Proposition 2 *We have*

$$|\det(b)| = \mathrm{N}(I)^2 \mathrm{N}(\alpha) D_K.$$

Proof Straightforward computation. □

In order to determine the signature of ideal lattices, we need the notion of *canonical involution* (or complex conjugation) of an étale $\mathbf{R}$-algebra.

Definition 2 Let E be an étale $\mathbf{R}$-algebra. We have $E = E_1 \times \cdots \times E_r \times F_1 \cdots \times F_s$, where $E_i \simeq \mathbf{R}$ and $F_i \simeq \mathbf{C}$. We say that $x = (x_1, \ldots, x_r)$ is *positive*, denoted by $x > 0$, if $x_i \in \mathbf{R}$ and $x_i > 0$ for all $i = 1, \ldots, r$.

Proposition 3 *Let E be an étale $\mathbf{R}$-algebra. and let $* : E \to E$ be an involution. The following properties are equivalent:*

(i) *$xx^* > 0$ for all non-zero $x \in E$;*

(ii) *the the restriction of* $*$ *to* E_i *is the identity for all* $i = 1, \ldots, r$, *and it is complex conjugation on* F_j *for all* $j = 1, \ldots, s$.

Proof This is immediate. □

In particular, this implies that for any étale $\mathbf{R}$-algebra E there is exactly one involution such that xx^* is positive for all non-zero $x \in E$.

Definition 3 Let E be an étale $\mathbf{R}$-algebra, and let $* : E \to E$ be an involution. We say that $*$ is the *canonical involution* of E if and only if $xx^* > 0$ for all non-zero $x \in E$.

Let $C \subset K_{\mathbf{R}}$ be the maximal étale $\mathbf{R}$-subalgebra such that the restriction of $^-$ to C is the canonical involution of C. Set $c = \mathrm{rank}(C)$.

We are now ready to determine the signature of an ideal lattice $b : I \times I \to \mathbf{R}$, $b(x, y) = \mathrm{Tr}(\alpha x\overline{y})$. Let $A \subset C$ be the maximal étale $\mathbf{R}$-subalgebra such that all the components of α in A are negative. Let $a = \mathrm{rank}(A)$.

Proposition 4 *The signature of* (I, b) *is* $c - 2a$.

Proof This follows from the definitions. □

Corollary 1 *We have*

$$\det(b) = (-1)^{\frac{n-c+2a}{2}} \mathrm{N}(I)^2 \mathrm{N}(\alpha) D_K.$$

Proof This follows from Propositions 2 and 4. □

We now define some equivalence relations on the set of ideal lattices.

Definition 4 Let (I, b) and (I', b') be two ideal lattices.

(i) We say that (I, b) and (I', b') are *isomorphic*, denoted by $(I, b) \simeq (I', b')$, if there exists $a \in K^*$ such that $I' = aI$ and that $b'(ax, ay) = b(x, y)$ for all $x, y \in I$.

(ii) We say that (I, b) and (I', b') are *equivalent*, denoted by $(I, b) \equiv (I', b')$ (or simply $b \equiv b'$), if there exists an isomorphism of $\mathbf{Z}$-modules $f : I \to I'$ such that $b'(f(x), f(y)) = b(x, y)$ for all $x, y \in I$.

Recall that two ideals I and I' are said to be equivalent, denoted by $I \equiv I'$, if there exists $a \in K^*$ such that $I' = aI$.

Proposition 5 *Let (I, b) and (I', b') be two ideal lattices. Suppose that $(I, b) \simeq (I', b')$. Then $I \equiv I'$ and $b \equiv b'$.*

Proof This is clear from the definitions. □

2 Integral ideal lattices

We keep the notation of §1. In particular, K is an algebraic number field, and $\mathcal{O}$ the ring of integers of K. Let $\mathcal{D}_K$ be the different of K, and let D_K be its discriminant.

In this section we suppose that the chosen involution $^-$ preserves K. Let F be the fixed field of this involution. Then either $K = F$ or K is a quadratic extension of F.

The aim of this section is to study *integral* ideal lattices. Recall that a lattice (L, b) is *integral* if $b(x, y) \in \mathbf{Z}$ for all $x, y \in L$; it is said to be *even* if $b(x, x) \in 2\mathbf{Z}$ for all $x \in L$.

Proposition 6 *Let $b : I \times I \to \mathbf{R}$, $b(x, y) = \mathrm{Tr}(\alpha x\overline{y})$, be an ideal lattice. Then (I, b) is integral if and only if*

$$\alpha I\overline{I} \subset \mathcal{D}_K^{-1}.$$

Proof This follows immediately from the definition. □

For any non-zero integer d, let us denote by $\mathcal{L}_d$ the set of integral ideal lattices of determinant d. Set $\mathcal{C}_d(K,^-) = \mathcal{L}_d/\simeq$, and $\mathcal{C}_d(^-) = \mathcal{L}_d/\equiv$. As usual, we denote by $\mathcal{C}(K)$ the ideal class group of K.

We have two projection maps

$$p_1 : \mathcal{C}_d(K,^-) \to \mathcal{C}(K),$$

$$p_2 : \mathcal{C}_d(K,^-) \to \mathcal{C}_d(^-).$$

Several natural questions concerning ideal lattices can be formulated in terms of the sets $\mathcal{C}_d(K,^-)$, $\mathcal{C}_d(^-)$, and of the the projection maps p_1 and p_2. In particular, it is interesting to determine the images and the fibres of these maps. As we will see below, the results are far from complete, especially concerning the map p_2.

Note that if an ideal lattice (I, b) given by $b(x, y) = \mathrm{Tr}(\alpha x\overline{y})$ belongs to $\mathcal{L}_d$, then $\mathrm{N}(\alpha I\overline{I}\mathcal{D}_K) = |d|$. Rather than fixing $|D|$, it turns out that it is more convenient to fix the $\mathcal{O}$-ideal $\alpha I\overline{I}$. The $\mathcal{O}$-ideal $\alpha I\overline{I}$ will be called the *norm* of the ideal lattice (I, b).

For any ideal $\mathcal{A}$, let $\mathcal{L}_{\mathcal{A}}$ be the set of ideal lattices of norm $\mathcal{A}$. Set $\mathcal{C}_{\mathcal{A}}(K,^-) = \mathcal{L}_{\mathcal{A}}/\simeq$, and $\mathcal{C}_{\mathcal{A}}(^-) = \mathcal{L}_{\mathcal{A}}/\equiv$. Again, we have the projection maps

$$p_1 : \mathcal{C}_{\mathcal{A}}(K,^-) \to \mathcal{C}(K),$$

$$p_2 : \mathcal{C}_{\mathcal{A}}(K,^-) \to \mathcal{C}_{\mathcal{A}}(^-).$$

Let us denote by $\mathcal{C}_{\mathcal{A}}(K)$ the image of p_1.

The case where $\mathcal{A}$ is the ring of integers $\mathcal{O}$ of K is especially interesting. If (I, b) and (I', b') are two ideal lattices given by $b(x, y) = \mathrm{Tr}(\alpha x\overline{y})$ and $b'(x, y) = \mathrm{Tr}(\alpha' x\overline{y})$, then we define their product $(I, b)(I', b') = (II', bb')$ by setting II' to be the product of the ideals I and I', and $(bb')(x, y) = \mathrm{Tr}(\alpha.\alpha' x\overline{y})$. If (I, b) and (I', b') have norm $\mathcal{O}$, then their product is again an ideal lattice of norm $\mathcal{O}$, hence we obtain a product on $\mathcal{C}_O(K,^-)$.

Proposition 7 *$\mathcal{C}_O(K,^-)$ is a group with respect to the above product.*

Proof This is clear. □

Proposition 8 *For any ideal $\mathcal{A}$, the set $\mathcal{C}_{\mathcal{A}}(K,^-)$ is either empty, or a principal homogeneous space over the group $\mathcal{C}_O(K,^-)$.*

Proof If (I, b) has norm $\mathcal{A}$ and (I', b') norm $\mathcal{O}$, then the product (II', bb') has norm $\mathcal{A}$. Hence we obtain a structure of homogeneous space of $\mathcal{C}_{\mathcal{A}}(K,^-)$ over $\mathcal{C}_O(K,^-)$. Let us check that it is a principal homogeneous space. This follows from the fact that if $\alpha I\overline{I} = \beta J\overline{J}$, then $\alpha\beta^{-1}(IJ^{-1})\overline{(IJ^{-1})} = O$. □

We denote by U_K be the group of units of K, by U_F the group of units of F, and by $\mathrm{N}_{K/F}$ the norm from K to F.

Proposition 9 (i) *If the involution is trivial, then we have the exact sequence of groups*

$$1 \to U_K/U_K^2 \to \mathcal{C}_O(K,^-) \xrightarrow{p_1} \mathcal{C}_O(K) \to 0.$$

(ii) *If the involution is non-trivial, then we have the exact sequence of groups*

$$1 \to U_F/\mathrm{N}_{K/F}(U_K) \to \mathcal{C}_O(K,^-) \xrightarrow{p_1} \mathcal{C}_O(K) \to 0.$$

Some results about the order of $U_F/\mathrm{N}_{K/F}(U_K)$ are given in Bayer (1982), §2.

Note that if $K = F$, then $\mathcal{C}_O(K)$ is the set of elements of order at most 2 in $\mathcal{C}(K)$. If $K \neq F$, then $\mathcal{C}_O(K)$ is the *relative class group* $\mathcal{C}(K/F)$, that is the kernel of the norm map $\mathrm{N}_{K/F} : \mathcal{C}(K) \to \mathcal{C}(F)$. It is well-known that $\mathrm{N}_{K/F}$ is

onto if K/F is ramified, and has cokernel of order 2 if K/F is unramified (see for instance Bayer 1982, propostion 1.2).

Quadratic fields

Suppose that K is a quadratic field, $K = \mathbf{Q}(\sqrt{d})$ where d is a square-free integer, and that the involution $^- : K \to K$ is given by $\overline{\sqrt{d}} = -\sqrt{d}$.

Let $b : I \times I \to \mathbf{Z}$, $b(x, y) = \mathrm{Tr}(\alpha x\overline{y})$, be an integral, even ideal lattice. Then $\alpha \in (1/\mathrm{N}(I))\mathbf{Z}$. In other words, b is an integral multiple of $b_I : I \times I \to \mathbf{Z}$, $b_I(x, y) = \mathrm{Tr}((1/\mathrm{N}(I))x\overline{y})$. Note that the quadratic form associated to b_I is $q_I : I \to \mathbf{Z}$, $q_I(x) = \mathrm{N}(x)/\mathrm{N}(I)$. We have $\det(b_I) = -D_K$.

Set $D = -D_K$. Gauss defined a correspondence between ideal classes of K and binary quadratic forms of determinant D, which sends an ideal I to the quadratic form q_I. The precise statement will be given below, as well as a way of deriving it using the notion of ideal lattice.

Let us first note that $\mathcal{C}_O(K,^-) = \mathcal{C}_D(K,^-)$. Indeed, if (I, b) is an ideal lattice of norm $\mathcal{O}$, then $b = \pm b_I$, hence it has determinant D. Conversely, an ideal lattice of determinant D has norm $\mathcal{O}$.

We can apply the results of the first part of this section to $\mathcal{C}_D(K,^-)$. In particular, by Proposition 7, it is a group. Any ideal I satisfies $(1/\mathrm{N}(I))I\overline{I} = O$, hence $\mathcal{C}_O(K) = \mathcal{C}(K)$. The involution is non-trivial, so we can apply Proposition 9(ii), and obtain the exact sequence

$$1 \to \{\pm\}/\mathrm{N}(U_K) \to \mathcal{C}_D(K,^-) \xrightarrow{p_1} \mathcal{C}(K) \to 0. \qquad (*)$$

We now need information concerning the set $\mathcal{C}_D(^-)$ and the map

$$p_2 : \mathcal{C}_d(K,^-) \to \mathcal{C}_d(^-).$$

Proposition 10 *Let b be an even, binary lattice with determinant D. Then*

(i) *There exists an ideal I in $K = \mathbf{Q}(\sqrt{d})$ such that (I, b) is an ideal lattice.*
(ii) *If I' is another ideal such that (I', b) is an ideal lattice, then $I' \equiv I$ or $I' \equiv \overline{I}$.*
(iii) *K is the only quadratic field over which b is an ideal lattice.*

Proof Let (L, b) be an even binary lattice with determinant D. Let R be the $\mathbf{Z}$-algebra associated to (L, b), that is,

$$R = \{(e, f) \in \mathrm{End}(L) \times \mathrm{End}(L) \mid b(ex, y) = b(x, fy)\}$$

(cf. Bayer-Fluckiger 1987). Recall that the product of R is given by $(e, f)(e'.f') = (ee', f'f)$, and that R is endowed with the involution $(e, f) \mapsto$

(f, e). If (L, b) is an ideal lattice over a quadratic field $K' = \mathbf{Q}(\sqrt{\delta})$, then by definition $b(\sqrt{\delta}x, y) = -b(x, \sqrt{\delta}y)$. Hence there exists $e \in \mathrm{End}(L)$ such that $(e, -e) \in R$.

Let us fix a $\mathbf{Z}$-basis of L, and let

$$\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix}$$

be the matrix of b in this basis. A straightforward computation shows that the matrix of e in this basis is an integral multiple of

$$E = \begin{pmatrix} B & 2C \\ -2A & -B \end{pmatrix}.$$

As the determinant of this matrix is D, the field K' has discriminant $-D$, hence $K' = K$. This proves (iii).

Let $O = \mathbf{Z}[w]$ be the ring of integers of K, with $w = \sqrt{d}$ if $d \equiv 2,\ 3 \pmod 4$, and $w = (1 - \sqrt{d})/2$ if $d \equiv 1 \pmod 4$. Letting w act by multiplication with E if $d \equiv 2,\ 3 \pmod 4$, and by multiplication with $(1 - E)/2$ if $d \equiv 1 \pmod 4$ provides L with a structure of $\mathcal{O}$-module. This proves that b is an ideal lattice over K, hence assertion (i). Moreover, we see that the only other way of making w act on L is by replacing E with $-E$. This proves (ii). □

Remark 6 Note that the proof of Proposition 10 is constructive: given an even, binary lattice b one constructs the ideals I and $\overline{I}$ over which b is an ideal lattice.

The following are immediate consequences of Proposition 10:

Corollary 2 *The set $\mathcal{C}_D(^-)$ is equal to the set of similarity classes of even binary lattices with determinant D.*

Corollary 3 *If (I, b) and (I', b') are two ideal lattices over K such that $b \simeq b'$, then either $I' \equiv I$ or $I' \equiv \overline{I}$.*

In order to recover the usual statement of Gauss' correspondence between classes of binary quadratic forms and lattices, we need slightly different equivalence relations.

Definition 5 (i) We say that two ideal lattices (I, b) and (I', b') are *strictly isomorphic* if there exists $a \in K^*$ with $\mathrm{N}(a) > 0$ such that $I' = aI$ and $b'(ax, ay) = b(x, y)$.

(ii) We say that two lattices (L, b) and (L', b') with $L \otimes_{\mathbf{Z}} \mathbf{Q} = L' \otimes_{\mathbf{Z}} \mathbf{Q}$ are *strictly equivalent* if there exists a $\mathbf{Z}$-linear isomorphism $f : L \to L'$ with $\det(f) > 0$ such that $b'(fx, fy) = b(x, y)$.

(iii) We say that two ideals I and I' are *strictly equivalent* if there exists $a \in K^*$ with $\mathrm{N}(a) > 0$ such that $I' = aI$.

Let us denote by $\mathcal{C}_D^s(K,^-)$, respectively $\mathcal{C}_D^s(^-)$, the set of strict isomorphism classes, respectively the set of strict equivalence classes, of ideal lattices of determinant D. Let us denote by $\mathcal{C}^s(K)$ the strict (or narrow) ideal class group.

Let us denote by $\mathcal{L}_D^+$ be the set of positive-definite ideal lattices of determinant D, and set $\mathcal{C}_D^+(K,^-) = \mathcal{L}/\simeq$, $\mathcal{C}_D^+(^-) = \mathcal{L}/\equiv$.

If K is an imaginary quadratic field, then the exact sequence (*) yields the isomorphism

$$\mathcal{C}_D^+(K,^-) \simeq \mathcal{C}(K).$$

On the other hand, if K is a real quadratic field, then we obtain from (*) the isomorphism

$$\mathcal{C}_D^s(K,^-) \simeq \mathcal{C}^s(K).$$

Note that if two ideal lattices are strictly isomorphic, then the corresponding ideals are strictly equivalent. This follows from the proof of Proposition 10.

Using this, we obtain the well-known fact that the ideal class group $\mathcal{C}(K)$ is isomorphic to the set of strict equivalence classes of positive-definite, even binary lattices of determinant D if K is imaginary; the strict ideal class group $\mathcal{C}^s(K)$ is isomorphic to the set of strict equivalence classes of even binary lattices of determinant D if K is real.

Cyclotomic fields of prime power conductor

Let p be a prime number, $r \geq 1$ an integer, and let ζ_{p^r} be a primitive p^rth root of unity. Suppose that $K = \mathbf{Q}(\zeta_{p^r})$, the corresponding cyclotomic field, and that the involution is complex conjugation. Recall that $O = \mathbf{Z}[\zeta_{p^r}]$, that there is exactly one ramified ideal P in the extension $K/\mathbf{Q}$, and that $\mathrm{N}(P) = p$. Hence the different $\mathcal{D}_K$ is a power of P. Let $D = |D_K|$.

Proposition 11 *We have* $\mathcal{C}_O(K,^-) = \mathcal{C}_D(K,^-)$.

Proof Let (I, b) be an integral ideal lattice with norm $\alpha I\overline{I}$ and determinant D. Then $\mathrm{N}(\alpha I\overline{I}) = 1$, and $\alpha I\overline{I} \subset \mathcal{D}_K^{-1}$. As $\mathcal{D}_K$ is a power of the single prime ideal P, this implies that $\alpha I\overline{I} = O$. This shows that $\mathcal{C}_D(K,^-) \subset \mathcal{C}_O(K,^-)$. Conversely, if (I, b) is an ideal lattice with norm $\mathcal{O}$, then the determinant of

(I, b) is $\pm D$. By Corollary 1, the determinant is positive, hence $\det(b) = D$. This proves the other inclusion, hence the proposition is proved. □

The fixed field of the involution is the maximal totally real subfield F of K. Applying Proposition 9(ii) and the remarks following, we have the exact sequence

$$1 \to U_F/\mathrm{N}_{K/F}(U_K) \to \mathcal{C}_D(K,^-) \xrightarrow{p_1} \mathcal{C}(K/F) \to 0.$$

The order of $U_F/\mathrm{N}_{K/F}(U_K)$ is 2^n, where $n = [K : \mathbf{Q}]$, cf. Bayer (1982), proposition 2.3. and example 2.5. The order of $\mathcal{C}(K/F)$, called the *relative class number of* K, is known in many cases, see for instance Washington (1982).

Let $\mathcal{L}_D^+$ be the set of positive-definite ideal lattices of determinant D, and let $\mathcal{C}_D^+(K,^-)$ be the set of isomorphism classes of these lattices, that is $\mathcal{C}_D^+(K,^-) = \mathcal{L}_D^+/\simeq$.

Let us denote by U_F^+ the set of totally positive units of F. Then we have the exact sequence

$$1 \to U_F^+/\mathrm{N}_{K/F}(U_K) \to \mathcal{C}_D^+(K,^-) \xrightarrow{p_1} \mathcal{C}(K/F).$$

If moreover the relative class number of K is odd, then $U_F^+ = \mathrm{N}_{K/F}(U_K)$ (cf. Shimura 1977, proposition A2), and we have the isomorphism $\mathcal{C}_D^+(K,^-) \simeq \mathcal{C}(K/F)$.

Examples over cyclotomic fields

Let m be an integer, ζ_m a primitive mth root of unity, and suppose that $K = \mathbf{Q}(\zeta_m)$ is the corresponding cyclotomic field. It is not known in general which are the ideal lattices over K, but many examples are available. For instance, the root lattices A_{p-1} (where p is a prime) are ideal lattices for $m = p$, the root lattice E_6 is an ideal lattice for $m = 9$ and E_8 for $m = 15, 20, 24$. A complete description of root lattices that are ideal lattices over cyclotomic fields is given in Bayer-Fluckiger & Martinet (1994), A2. Moreover, the Coxeter–Todd lattice is an ideal lattice for $m = 21$, and the Leech lattice for $m = 35, 39, 52, 56, 84$ (cf. Bayer-Fluckiger 1984, 1994 and the survey in Bayer-Fluckiger 1999). Let us also point out the computations in higher rank cases of Bachoc & Batut (1992), of Batut, Quebbemann & Scharlau (1995), as well as the construction by Nebe (1998) of a unimodular rank-48 lattice with minimum 6 that is an ideal lattice for $m = 65$. Finally, in Bayer-Fluckiger (2000) examples of *modular* ideal lattices are given when m is not a power of a prime p with $p \equiv 1 (\mathrm{mod}\, 4)$.

3 Generalization and examples

The aim of this section is to indicate a possible generalization of the notion of integral ideal lattice, and the usefulness of this notion in some parts of algebra and topology.

Let A be a finite dimensional $\mathbf{Q}$-algebra with a $\mathbf{Q}$-linear involution $^- : A \to A$. Let $\mathcal{O}$ be an order of A which is invariant under the involution. In this context, an *integral ideal lattice* will be a pair (I, b), where I is a (left) $\mathcal{O}$-ideal and $b : I \times I \to \mathbf{Z}$ is a lattice such that

$$b(\lambda x, y) = b(x, \overline{\lambda} y)$$

for all $x, y \in I$ and for all $\lambda \in O$. This is clearly a generalization of the notion of §2, where $A = K$ was a number field and $\mathcal{O}$ the ring of integers of K.

Proposition 12 *Suppose that A is semi-simple. Let (I, b) be an ideal lattice. Then there exists $\alpha \in A$ such that $b(x, y) = \mathrm{Tr}(x\alpha\overline{y})$.*

Proof This follows from the fact that, as A is semi-simple, $\mathrm{Tr} : A \times A \to \mathbf{Q}$ is non-degenerate. □

Integral ideal lattices naturally appear in several parts of mathematics. In the two examples below A is commutative. However, there are also very interesting examples where A is non-commutative, for instance in the study of polarized abelian varieties.

Knot theory

This example concerns odd-dimensional knots and their algebraic invariants. See Kearton (2000) or Kervaire & Weber (1978) for surveys of the relevant definitions and properties.

Let k be a positive integer, $k \equiv 3 \pmod 4$. Let $\Sigma^k \subset S^{k+2}$ be a fibred knot, and let $\Delta \in \mathbf{Z}[X]$ be the Alexander polynomial of Σ^k. Then Δ is monic, we have $\Delta(X) = X^{\deg(\Delta)}\Delta(X^{-1})$ and $\Delta(1) = \pm 1$. Suppose moreover that Δ has no repeated factors.

Let $A = \mathbf{Q}[X]/(\Delta) = \mathbf{Q}(\tau)$. Then A is a finite-dimensional, semi-simple $\mathbf{Q}$-algebra. Let $^- : A \to A$ be the $\mathbf{Q}$-linear involution induced by $\overline{\tau} = \tau^{-1}$. Set $O = \mathbf{Z}[X]/(\Delta) = \mathbf{Z}[\tau]$. Then $\mathcal{O}$ is an order of A.

Let M^{k+1} be a minimal Seifert surface of Σ^k. Set $r = k + 1/2$, and set

$$I = H_r(M^{k+1}, \mathbf{Z})/(\text{torsion}).$$

Then I is a rank one $\mathcal{O}$-module, hence isomorphic to an $\mathcal{O}$-ideal. The intersection form $b : I \times I \to \mathbf{Z}$ is a symmetric bilinear form of determinant $\Delta(1) = \pm 1$. Moreover, (I, b) is an ideal lattice. Indeed, the monodromy of the fibration induces an isomorphism $t : I \to I$ that preserves the intersection form. In other words, we have $b(tx, ty) = b(x, y)$ for all $x, y \in I$. The Alexander polynomial is also the characteristic polynomial of t, hence t acts as τ on I. We get $b(\tau x, y) = b(x, \tau^{-1}y)$. Noting that $\tau^{-1} = \overline{\tau}$, we see that $b(\lambda x, y) = b(x, \overline{\lambda}y)$ for all $x, y \in I$ and all $\lambda \in O$. Hence (I, b) is an ideal lattice.

We define the sets $\mathcal{C}_{\Delta(1)}(O,^-)$, $\mathcal{C}_{\Delta(1)}(^-)$ and $\mathcal{C}_{\Delta(1)}(O)$, as well as the projection maps $p_1 : \mathcal{C}_{\Delta(1)}(O,^-) \to \mathcal{C}_{\Delta(1)}(O)$, $p_2 : \mathcal{C}_{\Delta(1)}(O,^-) \to \mathcal{C}_{\Delta(1)}(^-)$ as in §2.

These have topological significance. Indeed, the class of (I, b) in $\mathcal{C}_{\Delta(1)}(O,^-)$ is an invariant of the isotopy class of the knot. Its image by p_1 is the Alexander module of the knot, and its image by p_2 is an invariant of the homeomorphism class of the minimal Seifert surface.

Moreover, if we suppose that the knot is simple, then these invariants are complete. The usefulness of this approach to solve concrete problems in knot theory is illustrated by several examples in Kearton (2000) and Bayer-Fluckiger (1999).

Symmetric, skew-symmetric and orthogonal matrices with a given characteristic polynomial

Let $f \in \mathbf{Z}[X]$ be a monic polynomial, and set $A = \mathbf{Q}[X]/(f)$, $O = \mathbf{Z}[X]/(f)$. Then A is a finite-dimensional $\mathbf{Q}$-algebra, and $\mathcal{O}$ is an order of A. The involution $^- : A \to A$. will be the *identity* (trivial involution).

Let $b_0 : L \times L \to \mathbf{Z}$ be the *unit lattice*. In other words, there exists a basis of L in which the matrix of b_0 is the identity matrix.

The following proposition is (essentially) due to Bender (1968):

Proposition 13 *There exists an integral symmetric matrix with characteristic polynomial f if and only if b_0 is an ideal lattice.*

Proof Let $M \in \mathrm{M}_n(\mathbf{Z})$ such that $M^t = M$ and that the characteristic polynomial of M is f. Let L be a free $\mathbf{Z}$-module of rank n, and let $(e_1, \ldots, e_n)$ be a basis of L in which b_0 is the identity matrix. Let $m : L \to L$ be the endomorphism given by the matrix M in this matrix. Let us endow L with the $\mathcal{O}$-module structure induced by m (that is, the action of X is given by m). As

M is symmetric, we have $b_0(mx, y) = b_0(x, my)$ for all $x, y \in L$. This proves that b_0 is an ideal lattice.

Conversely, suppose that $b_0 : I \times I \to \mathbf{Z}$ is an ideal lattice. Let us denote by $m : I \to I$ the endomorphism given by the image of X in $\mathcal{O}$. Then the characteristic polynomial of m is f. As (I, b_0) is an ideal lattice, we have

$$b_0(mx, y) = b_0(x, my) \qquad (**)$$

for all $x, y \in I$. Let $(e_1, \ldots, e_n)$ be a basis with respect to which the matrix of b_0 is the identity matrix. The relation $(**)$ then shows that $M^t = M$. This concludes the proof of the proposition. □

Similar results can be proved for skew-symmetric and orthogonal matrices with given characteristic polynomial. In these cases, the involution is non-trivial. It is induced by $X \mapsto -X$ in the first case, and by $X \mapsto X^{-1}$ in the second.

4 Real ideal lattices

So far, we have considered lattices up to isomorphism, rather than embedded in an euclidian space. However, it is often important to find suitable embeddings, and this will be the subject matter of this section.

Let K be a number field of degree n, and let $\mathcal{O}$ be its ring of integers. Let $\bar{} : K_{\mathbf{R}} \to K_{\mathbf{R}}$ be the canonical involution (cf. Proposition 4). In this section and the next, all lattices will be supposed *positive-definite*.

Suppose that the number field K has r_1 real embeddings, and r_2 pairs of imaginary embeddings. We have $n = r_1 + 2r_2$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings, and let $\sigma_{r_1+1}, \ldots, \sigma_{r_2}$ be non-conjugate imaginary embeddings.

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be a positive element of $K_{\mathbf{R}}$, in other words α_i is real and positive for all i. Let $\sigma_\alpha : K \to \mathbf{R}^n$ be the embedding defined by

$$\begin{aligned}\sigma_\alpha(x) \quad = \quad & \Big(\sqrt{\alpha_1}x_1, \ldots, \sqrt{\alpha_{r_1}}x_{r_1}, \sqrt{2\alpha_{r_1+1}}\Re(x_{r_1+1}), \sqrt{2\alpha_{r_1+1}}\Im(x_{r_1+1}), \\ & \ldots, \sqrt{2\alpha_{r_2}}\Re(x_{r_2}), \sqrt{2\alpha_{r_2}}\Im(x_{r_2})\Big),\end{aligned}$$

where $x_i = \sigma_i(x)$, $\Re$ denotes the real part and $\Im$ the imaginary part. Note that this definition differs slightly from the one in Bayer-Fluckiger 1999, Definition 5.1).

Proposition 14 *For any ideal I of K and any positive $\alpha \in K_{\mathbf{R}}$, the lattice $\sigma_\alpha(I) \subset \mathbf{R}^n$ is an ideal lattice. Conversely, for any ideal lattice (I, b) there exists an $\alpha \in K_{\mathbf{R}}$ such that the ideal lattice $\sigma_\alpha(I)$ is isomorphic to (I, b).*

Proof It is clear that $\sigma_\alpha(I) \subset \mathbf{R}^n$ is a lattice. A straightforward computation shows that $\sigma_\alpha(I)$ is isomorphic to the lattice $b : I \times I \to \mathbf{R}$ given by $b(x, y) = \mathrm{Tr}(\alpha x \overline{y})$. Hence it is an ideal lattice. Conversely, let (I, b) be an ideal lattice given by $b(x, y) = \mathrm{Tr}(\alpha x \overline{y})$, Then $\sigma_\alpha(I)$ is isomorphic to (I, b). □

The above proposition is useful in information theory. Indeed, let us recall that if $x = (x_1, \ldots, x_n) \in \mathbf{R}^n$, then the *diversity* of x, denoted by $\mathrm{div}(x)$, is the number of non-zero x_is. Let $L \subset \mathbf{R}^n$ be a lattice. One defines the *diversity* of L, denoted $\mathrm{div}(L)$, by

$$\mathrm{div}(L) = \min\{\mathrm{div}(x) \mid x \in L, x \neq 0\}.$$

Lattices of high diversity tend to perform better than the Rayleigh fading channel (see Boutros *et al*. 1996, Boutros & Viterbo 1998). The following proposition is proved in Bayer-Fluckiger (1999) in some special cases:

Proposition 15 *Any ideal lattice can be embedded in an euclidean space with diversity* $r_1 + r_2$.

Proof Let I be an ideal and let $\alpha \in K_{\mathbf{R}}$ be totally real and totally positive. It is easy to see that the lattice $\sigma_\alpha(I)$ has diversity $r_1 + r_2$. By Proposition 14, any ideal lattice can be realised under this form, so the proposition is proved. □

5 Arakelov invariants

We keep the notation of §4. In particular, K is a number field of degree n, and $\mathcal{O}$ its ring of integers. The involution $^- : K_{\mathbf{R}} \to K_{\mathbf{R}}$ is again the canonical involution, and all lattices in this section are supposed positive-definite.

A positive-definite ideal lattice with respect to the canonical involution is also called an *Arakelov divisor* of the number field K. Such a lattice defines a sphere packing in $\mathbf{R}^n$, and the density and thickness of this packing are natural invariants of the lattice. We call these here *Arakelov invariants*.

Definition 6 Let (L, b) be a lattice, and set $q(x) = b(x, x)$. Let $V = L \otimes_{\mathbf{Z}} \mathbf{R}$.

(i) The *minimum* of b is defined by $\min(b) = \inf\{q(x) \mid x \in L, x \neq 0\}$.
(ii) The *maximum* of b is by definition

$$\max(b) = \sup\{\lambda \in \mathbf{R} \mid \forall x \in V, \ \exists y \in L \text{ with } q(x - y) \leq \lambda\}.$$

Note that $R = \sqrt{\max(b)}$ is the *covering radius* of b, and $r = \sqrt{\min(b)}/2$ is

its *packing radius*. The thickness and the density of the sphere packing associated to b are defined in terms of these quantities (see Conner & Perlis 1984, chapters I and II). We will here use the related notions of *Hermite invariants*.

Definition 7 Let (L, b) be a lattice. The *Hermite invariants* are defined as follows:

(i) $\gamma(b) = \dfrac{\min(b)}{\det(b)^{1/n}}$.

(ii) $\tau(b) = \dfrac{\max(b)}{\det(b)^{1/n}}$.

Note that the invariant $\gamma(b)$ is classical, but $\tau(b)$ is not. However, it is a natural invariant, related to the thickness as the γ-invariant is to the density. It is also a useful invariant, as we will see below.

It is also useful to consider the best Hermite invariants for lattices of a given rank.

Definition 8

(i) $\gamma_n = \sup\{\, \gamma(b) \mid \text{rank}(b) = n\}$.

(ii) $\tau_n = \inf\{\, \tau(b) \mid \text{rank}(b) = n\}$.

These notions provide us with invariants of the ideal classes of K, and of K itself.

Definition 9 Let I be an ideal. Set

(i) $\gamma_{\min}(I) = \inf\{\gamma(b) \mid (I, b) \text{ is an ideal lattice }\}$.

(ii) $\gamma_{\max}(I) = \sup\{\gamma(b) \mid (I, b) \text{ is an ideal lattice }\}$.

(iii) $\tau_{\min}(I) = \inf\{\tau(b) \mid (I, b) \text{ is an ideal lattice }\}$.

(iv) $\tau_{\max}(I) = \sup\{\tau(b) \mid (I, b) \text{ is an ideal lattice }\}$.

As equivalent ideals carry isomorphic ideal lattices, these are actually invariants of the ideal classes. It is natural to also use these notions to define invariants of the field K, $\gamma_{\min}(K)$, $\gamma_{\max}(K)$, $\tau_{\min}(K)$, and $\tau_{\max}(K)$. Recall that D_K is the discriminant of K. If I is an ideal, let us denote by $\min(I)$ the smallest norm of an integral ideal equivalent to I.

Proposition 16 *Let I be an ideal. Then*

$$\gamma_{\min}(I) \geq \frac{n}{|D_K|^{1/n}} \min(I)^{2/n}.$$

Proof Let (I, b) be an ideal lattice. Set $q(x) = b(x, x)$. We have $q(x) = \mathrm{Tr}(\alpha x\overline{y})$ for some positive $\alpha \in K_{\mathbf{R}}$. Recall that $\det(b) = \mathrm{N}(\alpha)\mathrm{N}(I)^2|D_K|$.

By the inequality between the arithmetic and geometric means, we have

$$\mathrm{Tr}(\alpha x\overline{x}) \geq n\ \mathrm{N}(\alpha x\overline{x})^{1/n} = n\ \det(b)^{1/n}|D_K|^{-1/n}\ \mathrm{N}(I)^{-2/n}\ \mathrm{N}(x)^{2/n}.$$

Hence

$$\frac{q(x)}{\det(b)^{1/n}} \geq \frac{n}{|D_K|^{1/n}}\ \left(\frac{\mathrm{N}(x)}{\mathrm{N}(I)}\right)^{2/n},$$

and this implies that

$$\frac{\min(b)}{\det(b)^{1/n}} \geq \frac{n}{|D_K|^{1/n}}\ \min(I)^{2/n}.$$

As $\gamma(b) = \min(b)/\det(b)^{1/n}$, the proposition is proved. □

Corollary 4 *We have*

$$\gamma_{\min}(O) = \frac{n}{|D_K|^{1/n}}.$$

Proof By Proposition 16 we have $\gamma_{\min}(O) \geq n/|D_K|^{1/n}$. On the other hand, the ideal lattice $b : O \times O \to \mathbf{Z}$ given by $b(x, y) = \mathrm{Tr}(x\overline{y})$ has minimum n and determinant $|D_K|$. Hence the equality holds. □

Note that this also implies that $\gamma_{\min}(O) = \gamma_{\min}(K)$.

Corollary 5 *For any ideal I we have*

$$\frac{\gamma_{\min}(I)}{\gamma_{\min}(O)} \geq \min(I)^{2/n}.$$

Proof This follows from Definition 9 and Proposition 16. □

The following is an immediate consequence of Corollary 5.

Corollary 6 *Let I be an ideal. If there exists an ideal lattice (I, b) with $\gamma(b) = \gamma_{\min}(O)$, then I is principal.*

Recall that the field K is said to be *Euclidean with respect to the norm* if for every $a, b \in O$, $b \neq 0$, there exist $c, d \in O$ such that $a = bc + d$ and $|\mathrm{N}(d)| < |\mathrm{N}(b)|$.

Proposition 17 *Suppose that $\tau_{\min}(O) < \gamma_{\min}(O)$. Then K is Euclidean with respect to the norm.*

Proof The argument of Bayer-Fluckiger (1999), proposition 4.1 gives the desired result. □

Example 1 Let $K = \mathbf{Q}(\zeta_{15})$. We have $n = 8$, $D_K = 3^4 5^6$. Hence $\gamma_{\min}(O) = 8/3^{1/2}5^{3/4}$. The root lattice E_8 is an ideal lattice over $\mathcal{O}$ (see for instance Bayer-Fluckiger 1999). We have $\det(E_8) = 1$. The covering radius of E_8 is 1 (cf. Conway & Sloane 1988), hence $\max(E_8) = 1$. This implies that $\tau(E_8) = 1$, therefore $\tau_{\min}(O) \leq 1$. This implies that $\tau_{\min}(O) < \gamma_{\min}(O)$, so by Proposition 17, K is Euclidean with respect to the norm. We have $\gamma(E_8) = 2$. It is known that $\gamma(E_8) = \gamma_8$ (see Craif 1978), hence $\gamma_{\max}(O) = 2$. Summarising, we have

$$\tau_{\min}(O) \leq 1 < \gamma_{\min}(O) < \gamma_{\max}(O) = 2.$$

References

Bachoc, C. & C. Batut (1992), Etude algorithmique de réseaux construits avec la forme trace, *J. Exp. Math.* **1**, 184–190.

Batut, C., H.-G. Quebbemann & R. Scharlau (1995), Computations of cyclotomic lattices, *J. Exp. Math.* **4**, 175–179.

Bayer, E. (1982) Unimodular hermitian and skew-hermitian forms, *J. Algebra* **74**, 341–373.

Bayer-Fluckiger, E. (1984), Definite unimodular lattices having an automorphism of given characteristic polynomial, *Comment. Math. Helv.* **59** (1984), 509–538.

Bayer-Fluckiger, E. (1987), Principe de Hasse faible pour les systèmes de formes quadratiques, *J. Reine Angew. Math.* **378**, 53–59.

Bayer-Fluckiger, E. (1989), Réseaux unimodulaires, in *Séminaire de Théorie des Nombres de Bordeaux* **1**, 189–196.

Bayer-Fluckiger, E. (1999), Lattices and number fields, *Contemp. Math.* **241**, 69–84.

Bayer-Fluckiger, E. (2000), Cyclotomic modular lattices, *J. Théorie des Nombres de Bordeaux*, **12**, 273–280.

Bayer-Fluckiger, E. & J. Martinet (1994), Réseaux liés à des algèbres semi-simples, *J. Reine Angew. Math.* **415**, 51–69.

Bender, E. (1968), Characteristic polynomials of symmetric matrices, *Pacific J. Math.* **25**, 433–441.

Boutros, J., E. Viterbo, C. Rastello & J.-C. Belfiore (1996), Good lattice constellations for both Rayleigh fading and Gaussian channels, *IEEE Trans. Information Theory*, **42**, 502–518.

Boutros, J. & E. Viterbo (1998), Signal space diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel, *IEEE Trans. Information Theory*, **44**, 1453–1467.

Conner, P. & R. Perlis (1984), *Survey of Trace Forms of Algebraic Number Fields*, World Scientific.

Conway, J.H. & N.J.A. Sloane (1998), *Sphere Packings, Lattices and Groups*, Springer-Verlag.

Craig, M. (1978), Extreme forms and cyclotomy, *Mathematika* **25**, 44–56.

Craig, M. (1978), A cyclotomic construction of Leech's lattice, *Mathematika* **25**, 236–241.

Ebeling, W. (1994), *Lattices and Codes*, Vieweg.

Feit, W. (1978), Some lattices over $\mathbf{Q}(\sqrt{-3})$, *J. Algebra* **52**, 248–263.

van der Geer, G. & R. Schoof (1999), Effectivity of Arakelov divisors and the theta divisor of a number field, preprint.

Kearton, C. (2000), Quadratic forms in knot theory, in *Contemp. Math.* **272**, 135–154.

Kervaire, M. & C. Weber (1978), A survey of multidimensional knots, in Lecture Notes in Math. **685**, 61–134, Springer-Verlag.

Martinet, J. (1995), Structures algébriques sur les réseaux, in *Actes du Séminaire de Théorie des Nombres de Paris, 1992–1993*, London Mathematical Society Lecture Notes **215**, Cambridge University Press, 167–186.

Martinet, J. (1996)*Les Réseaux Parfaits des Espaces Euclidiens*, Masson.

Nebe, G. (1998), Some cyclo-quaternionic lattices, *J. Algebra* **199**, 472–498.

Neukirch, J. (1999), *Algebraic Number Theory*, Springer-Verlag.

Quebbemann, H.-G. (1981), Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung, *J. Reine Angew. Math.* **326**, 158–170.

Serre, J.-P. (1970), *Cours d'Arithmétique*, P.U.F.

Shimura, G. (1977), On abelian varieties with complex multiplication, *Proc. London Math. Soc.* **34**, 65–86.

Washington, L.C. (1982), *Introduction to Cyclotomic Fields*, Springer-Verlag.

On Ideal Lattices and Learning with Errors Over Rings. â^—. Vadim Lyubashevskyâ€ .Ä Ideal lattices and the canonical embedding. Fix some underlying ring R, e.g., the ring of algebraic. integers in a cyclotomic number eld as above. 1 Ring-LWE and its hardness from ideal lattices. 2 Open questions. Selected bibliography: LPRâ€™10 V. Lyubashevsky, C. Peikert, O. Regev. â€œOn Ideal Lattices and Learning with Errors Over Rings,â€ Eurocryptâ€™10 and JACMâ€™13. LPRâ€™13 V. Lyubashevsky, C. Peikert, O. Regev. â€œA Toolkit for Ring-LWE Cryptography,â€ Eurocryptâ€™13. Ideal lattices of lattices. Ralph freese. This paper shows that any compactly generated lattice is a subdirect product of subdirectly irreducible lattices which are complete and upper continuous.Â 5* Retracts of ideal lattices of dual ideal lattices of free lattices* We let (W) denote the Whitman condition which is free of the generators; that is. (W) a A b <,c V d implies a ^ c V d or b ^ c Vd or a A b ^ c or a A b ^ d . Ideal lattices and the structure of rings(j). By. Robert L. blair. It is well known that the set of all ideals(2) of a ring forms a complete modular lattice with respect to set inclusion. The same is true of the set of all right ideals. Our purpose in this paper is to consider the consequences of imposing certain additional restrictions on these ideal lattices. In particular, we discuss the case in which one or both of these lattices is complemented, and the case in which one or both is distributive. Ideal Lattices: cryptographic applications and open problems. Daniele Micciancio (UCSD). based on joint work with Vadim Lyubashevsky (UCSD). Outline. â— Basing cryptography on lattices â— Average-case vs. worst-case complexity â— Cyclic lattices and generalizations â— Connections to algebraic number theory â— (Implementation issues) â— Open problems.Â Ideal lattices and small conjugates. â— Let q(X)=Xn + 1 â— S: Ideal lattice in Z[X]/q(X). â€“ Goal: Find g(X) in S such that ||g|| is small. â— S(w2n) ideal of Z(w2n) where q(w2n)=0.