Progress in Mathematics
334

Jean-Benoît Bost

Theta Invariants of Euclidean Lattices and Infinite-Dimensional Hermitian Vector Bundles over Arithmetic Curves

Birkhäuser

Birkhäuser

Progress in Mathematics

Volume 334

More information about this series at http://www.springer.com/series/4848

Jean-Benoît Bost

Theta Invariants of Euclidean Lattices and Infinite-Dimensional Hermitian Vector Bundles over Arithmetic Curves

Birkhäuser

Jean-Benoît Bost
Département de Mathématique
Université Paris-Sud
Orsay, France

ISSN 0743-1643 ISSN 2296-505X (electronic)
Progress in Mathematics
ISBN 978-3-030-44328-3 ISBN 978-3-030-44329-0 (eBook)
https://doi.org/10.1007/978-3-030-44329-0

This book is published under the imprint Birkhäuser, www.birkhauser-science.com by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dilectissimae uxori
necnon consilio optimae

Contents

Preface

A. This monograph is dedicated to the construction of suitable categories of *infinite-dimensional Hermitian vector bundles* in the framework of Arakelov geometry and to the study of their *theta invariants*, which are defined in terms of theta series associated to Euclidean lattices and take values in $[0, +\infty]$. Our constructions are developed with a view toward applications to Diophantine geometry: using infinite-dimensional vector bundles and their theta invariants, one may establish diverse results in Diophantine geometry and transcendence theory by arguments that are formally similar to classical algebraization proofs in analytic and formal geometry, as exemplified in the last chapter of this monograph.

A description of our results, intended to arithmetic geometers with a specific interest in Arakelov geometry and its applications to classical Diophantine problems, is given in the general introduction that follows this preface and in the introductions of the successive chapters. Notably the introduction of the final chapter, written to be accessible directly after the general introduction, describes how the general formalism developed in this monograph leads to "concrete" Diophantine applications, concerning, for instance, the construction of isogenies between elliptic curves over $\mathbb{Q}$.

The general form of our results required for their applications to Diophantine geometry, notably the need to work over a base ring that can be the ring of integers $\mathcal{O}_K$ of an arbitrary number field K (that is, an arbitrary extension field of $\mathbb{Q}$ of finite degree), leads to some technicalities in their formulation and may hide their basic simplicity.

In this preface, we try to present them in the simplest possible terms, by sticking to the basic case in which the base ring $\mathcal{O}_K$ is $\mathbb{Z}$, and we refer the reader to the more technical introduction that follows this preface for more complete statements and for references.

B. The basic object of study in this monograph is *Euclidean lattices*. Recall that a Euclidean lattice $\overline{E}$ is defined by the following data:

- a finite-dimensional $\mathbb{R}$-vector space $E_{\mathbb{R}}$;
- a lattice E in $E_{\mathbb{R}}$, namely a subgroup of the additive group $(E_{\mathbb{R}}, +)$ for which there exists some $\mathbb{R}$-basis $(e_i)_{1\leq i\leq n}$ of $E_{\mathbb{R}}$ such that $E = \bigoplus_{1\leq i\leq n} \mathbb{Z}e_i$;
- a Euclidean norm $\|.\|$, associated to some Euclidean scalar product $\langle ., . \rangle$, on $E_{\mathbb{R}}$.

Euclidean lattices traditionally appear in mathematical physics, as mathematical models for crystalline structures, and in number theory, via the so-called *geometry of numbers* (a terminology coined by Minkowski [86]). For the past decades, with the development of lattice-based cryptography, they have also played an important role in computer science.

A Euclidean lattice $\overline{E}$ admits several easily defined classical invariants. The simplest of them are its *rank*, defined in the above notation as

$$\operatorname{rk} E := \dim_{\mathbb{R}} E_{\mathbb{R}} = n,$$

and its *covolume* $\operatorname{covol}\overline{E}$, defined as the Euclidean volume of a fundamental domain for E acting on $E_{\mathbb{R}}$ by translation, for instance, of

$$\Delta := \sum_{1\leq i\leq n} [0,1[\, e_i;$$

it may be expressed in terms of the Gram determinant of the basis $(e_i)_{1\leq i\leq n}$ of the lattice as

$$(\operatorname{covol}\overline{E})^2 = \det(\langle e_i, e_j\rangle)_{1\leq i,j\leq n}.$$

One also classically considers, when the rank of the Euclidean lattice $\overline{E}$ is positive, its *first minimum*

$$\lambda_1(\overline{E}) := \min_{v\in E\setminus\{0\}} \|v\|$$

and its *covering radius*

$$\rho(\overline{E}) := \max_{x\in E_{\mathbb{R}}} \min_{v\in E} \|x - v\|.$$

To every Euclidean lattice $\overline{E}$ is associated the dual Euclidean lattice $\overline{E}^{\vee}$, defined as follows. Its underlying $\mathbb{R}$-vector space is the dual of the $\mathbb{R}$-vector space $E^{\vee}_{\mathbb{R}}$, defined as the space of $\mathbb{R}$-linear forms

$$E^{\vee}_{\mathbb{R}} := \operatorname{Hom}_{\mathbb{R}}(E_{\mathbb{R}}, \mathbb{R}).$$

The lattice $E^{\vee}$ in $E^{\vee}_{\mathbb{R}}$ defining $\overline{E}^{\vee}$ is the subgroup of linear forms that are integral valued on E:

$$E^{\vee} := \{\xi \in E^{\vee}_{\mathbb{R}} \mid \xi(E) \subset \mathbb{Z}\}\,;$$

it may be identified with $\operatorname{Hom}_{\mathbb{Z}}(E, \mathbb{Z})$ by the restriction map $(\xi \mapsto \xi_{|E})$. The Euclidean norm defining $\overline{E}^{\vee}$ is the dual norm $\|.\|^{\vee}$ on $E^{\vee}_{\mathbb{R}}$, defined by the equality

$$\|\xi\|^{\vee} := \max_{x\in E_{\mathbb{R}}, \|x\|\leq 1} |\xi(x)| \quad \text{for every } \xi \in E^{\vee}_{\mathbb{R}}.$$

The ranks of $\overline{E}$ and $\overline{E}^{\vee}$ are clearly equal, and their covolumes are easily seen to be the inverses of each other:

$$\operatorname{covol}(\overline{E}^{\vee}) = (\operatorname{covol}\overline{E})^{-1}.$$

In contrast to the simplicity of these definitions, Euclidean lattices and their invariants lead to difficult problems. Their role in cryptography actually relies on the computational "hardness" of basic questions involving Euclidean lattices when their dimension becomes large. Such difficult problems arise, for instance, when one investigates estimates relating various classical invariants of Euclidean lattices. These estimates involve constants depending on the ranks of the Euclidean lattices under study, and the control of these constants when these ranks become large is often a delicate issue.

This may be illustrated by one of the oldest results in the theory of Euclidean lattices, which goes back to Hermite and Minkowski, namely the existence, for every positive integer n, of some positive constant $C(n)$ such that the first minimum of every Euclidean lattice $\overline{E}$ of rank n satisfies the following upper bound:

$$\lambda_1(\overline{E}) \leq C(n)(\operatorname{covol}\overline{E})^{1/n}. \tag{0.0.1}$$

Hermite first proved this result by induction on the rank n, by developing what is known today as *reduction theory* for Euclidean lattices of arbitrary rank (see [64]). This approach allowed him to establish the estimate (0.0.1) with

$$C(n) = (4/3)^{(n-1)/4}. \tag{0.0.2}$$

Minkowski proved that it actually holds with

$$C(n) = 2\,v_n^{-1/n}, \tag{0.0.3}$$

where v_n denotes the Lebesgue measure of the unit ball in $\mathbb{R}^n$.

The estimate (0.0.1) with the value (0.0.3) for $C(n)$ is the famous Minkowski's first theorem. Its derivation by Minkowski, in his *Geometrie der Zahlen* ([86, pp. 73–76]), admits the following simple physical interpretation. Let us think of the Euclidean lattice as a model for a crystal in the n-dimensional Euclidean space $(E_{\mathbb{R}}, \|.\|)$. The molecules in this crystal are represented by the points v of the lattice E. Since the open balls $\mathring{B}_{\|.\|}(v, \lambda_1(\overline{E})/2)$ of radius $\lambda_1(\overline{E})/2$ centered at these points are mutually disjoint, the density of the crystal — defined as the number of its molecules per unit volume — is at most the inverse of the volume of any of these balls, which is $v_n(\lambda_1(\overline{E})/2)^n$. This density is nothing but the inverse of the covolume of $\overline{E}$. Therefore,

$$\operatorname{covol}(\overline{E})^{-1} \leq [v_n(\lambda_1(\overline{E})/2)^n]^{-1}.$$

This estimate is precisely (0.0.1) with $C(n)$ given by (0.0.3).

Since $v_n = \pi^{n/2}/\Gamma(n/2+1)$, it follows from Stirling's formula that as n goes to $+\infty$, the value (0.0.3) for the constant $C(n)$ obtained from Minkowski's argument admits the following asymptotics:

$$2v_n^{-1/n} \sim \sqrt{2n/e\pi}. \tag{0.0.4}$$

It is much smaller than the value (0.0.2) originally obtained by Hermite.

The square γ_n of the best possible (namely, the minimal) value of the constant $C(n)$ in the estimate (0.0.1) is known as the *Hermite constant* in dimension n. It turns out that Minkowski's upper bound $4v_n^{-2/n}$ on γ_n is of the "correct order of growth" if n goes to infinity. Actually, by combining this upper bound with some further results of Minkowski and Hlawka, one shows that

$$\log \gamma_n = \log n + \varepsilon(n), \tag{0.0.5}$$

where

$$|\varepsilon(n)| = O(1) \quad \text{as } n \longrightarrow +\infty.$$

However, the exact value of γ_n is known only for a small number of values of n, and its precise asymptotic behavior (for instance, the possible convergence of $\varepsilon(n)$ to some limit as n goes to $+\infty$) is still not understood.

C. Another circle of questions involving optimal constants in estimates comparing invariants of Euclidean lattices are the so-called *transference estimates* relating the invariants of a Euclidean lattice $\overline{E}$ and those of its dual $\overline{E}^\vee$.

For instance, consider the first minimum $\lambda_1(\overline{E})$ of some Euclidean lattice $\overline{E}$ of positive rank n, and the covering radius $\rho(\overline{E}^\vee)$ of the dual Euclidean lattice $\overline{E}$. An application of the reduction theory of Euclidean lattices establishes that the product $\lambda_1(\overline{E})\rho(\overline{E}^\vee)$ is bounded from above and from below by positive constants $\tau_1(n)$ and $\tau_2(n)$ depending only on n:

$$\tau_1(n) \leq \lambda_1(\overline{E})\rho(\overline{E}^\vee) \leq \tau_2(n). \tag{0.0.6}$$

One easily sees that for every $n \geq 1$, the optimal value of $\tau_1(n)$ is $1/2$: simply consider the lattice $\mathbb{Z}^n$ in $\mathbb{R}^n$ equipped with the Euclidean norm $\|.\|_\varepsilon$ defined by $\|(x_1, \ldots, x_n)\|_\varepsilon^2 = \varepsilon(x_1^2 + \cdots + x_{n-1}^2) + x_n^2$, with ε a small positive real number.

Concerning $\tau_2(n)$, important progress was obtained in the 1990s by Banaszczyk, who showed in [7] that (0.0.6) holds with

$$\tau_2(n) = n/2,$$

while the best possible (namely the minimal) constant $\tau_2(n)$ satisfies

$$\tau_2(n) \geq (n/2\pi e)(1 + o(n)) \quad \text{as } n \longrightarrow +\infty.$$

To establish the upper bound

$$\lambda_1(\overline{E})\rho(\overline{E}^\vee) \leq n/2,$$

Banaszczyk introduced a new technique, originating in harmonic analysis, based on the consideration of the measures

$$\sum_{v \in E} e^{-\pi\beta\|v\|^2}\, \delta_v, \tag{0.0.7}$$

on the real vector space $E_{\mathbb{R}}$ defined for all $\beta \in \mathbb{R}_+^*$ and supported by the lattice E and their Fourier transforms on the dual space $E_{\mathbb{R}}^{\vee}$. This technique has been especially influential in the development of lattice-based cryptography during the last decades.

The total mass of Banaszczyk's measure (0.0.7) is given by the classical theta series

$$\theta_{\overline{E}}(\beta) := \sum_{v \in E} e^{-\pi\beta\|v\|^2}. \tag{0.0.8}$$

Such theta series have classically played a central role in the study of *integral lattices*, namely of Euclidean lattices whose Euclidean scalar product is $\mathbb{Z}$-valued on $E \times E$. Indeed, the theta series associated to integral lattices turn out to define modular forms, and from Jacobi to Siegel and his followers, the development of the theory of modular forms has led to spectacular applications concerning integral lattices and related integral quadratic forms. Banaszczyk's work has demonstrated the relevance of the theta series (0.0.8) and their measure-theoretic versions (0.0.7) in the investigation of the fine properties of general Euclidean lattices.

D. In the first chapters of this monograph, we investigate in some detail the properties of the invariants of Euclidean lattices defined in terms of these series, their *theta invariants*; the main instance of these is the nonnegative real number:

$$h^0_\theta(\overline{E}) := \log \theta_{\overline{E}}(1) = \log \sum_{v \in E} e^{-\pi\|v\|^2}. \tag{0.0.9}$$

Besides the "technical" motivation to study these theta invariants provided by Banaszczyk's technique, there exists an older and more "conceptual" one, which stems from the classical analogy between number fields and function fields. It is closely related to Arakelov geometry, which itself constitutes an outgrowth of this classical analogy.

Recall that in the analogy between number fields and function fields, the ring of integers $\mathcal{O}_K$ of some number field K, together with its archimedean places[1], appears as the counterpart of a smooth projective (geometrically connected) curve C over some base field k. The field $k(C)$ of rational functions over C, traditionally known as a "function field in one variable" over k, plays the role of the number field K. More generally, one may associate "arithmetic" counterparts over number fields to "geometric" objects over C, such as vector bundles $\mathcal{E}$ over C, and to their invariants, such as the rank $\operatorname{rk}\mathcal{E}$ and the degree $\deg_C \mathcal{E}$ of $\mathcal{E}$, or the dimension

$$h^0(C, \mathcal{E}) := \dim_k \Gamma(C, \mathcal{E})$$

of its space of global regular sections.

Although the special case in which the base field k of the curve C is finite plays an important role in this analogy, readers more inclined toward analytic than

[1] defined by the field embeddings of K in $\mathbb{C}$, up to complex conjugation.

algebraic geometry may focus on the situation in which the base field k is $\mathbb{C}$. Then the data of the curve C (resp., of the algebraic vector bundle $\mathcal{E}$) are equivalent to those of some compact connected Riemann surface C^{an} (resp., of some $\mathbb{C}$-analytic vector bundle $\mathcal{E}^{\mathrm{an}}$ over C^{an}); the degree $\deg_C \mathcal{E}$ of $\mathcal{E}$ coincides with its topological degree defined by its first Chern class $c_1(\mathcal{E}^{\mathrm{an}})$ in $H^2(C^{\mathrm{an}}, \mathbb{Z}) \simeq \mathbb{Z}$, and the finite-dimensional $\mathbb{C}$-vector space $\Gamma(C, \mathcal{E})$ with the space $\Gamma(C^{\mathrm{an}}, \mathcal{E}^{\mathrm{an}})$ of global analytic sections of $\mathcal{E}^{\mathrm{an}}$.

We will concentrate on the case $K = \mathbb{Q}$, and therefore $\mathcal{O}_K = \mathbb{Z}$. Then in the above analogy, *the counterpart of a vector bundle $\mathcal{E}$ over C is precisely a Euclidean lattice $\overline{E}$*. For instance, the role of the trivial line bundle $\mathcal{O}_C$ over C is played by the Euclidean line bundle $\overline{\mathbb{Z}}$, defined by the $\mathbb{R}$-vector space $\mathbb{R}$, the lattice $\mathbb{Z}$ in $\mathbb{R}$, and the Euclidean norm equal to the usual absolute value $|.|$.

To every pair $(\mathcal{E}, \mathcal{F})$ of vector bundles over C are associated the vector bundle $\mathcal{E} \oplus \mathcal{F}$ and the finite-dimensional k-vector space $\mathcal{H}om_{\mathcal{O}_C}(\mathcal{E}, \mathcal{F})$ of morphisms from $\mathcal{E}$ to $\mathcal{F}$. These constructions admit counterparts in the arithmetic side.

Let us indeed consider two Euclidean lattices $\overline{E}$ (resp., $\overline{F}$), defined by the $\mathbb{R}$-vector space $E_{\mathbb{R}}$ (resp., $F_{\mathbb{R}}$), the lattice E (resp., F), and the Euclidean norm $\|.\|_{\overline{E}}$ on $E_{\mathbb{R}}$ (resp., $\|.\|_{\overline{F}}$ on $F_{\mathbb{R}}$). Then their direct sum $\overline{E} \oplus \overline{F}$ is the Euclidean lattice defined by the $\mathbb{R}$-vector space $E_{\mathbb{R}} \oplus F_{\mathbb{R}}$, its lattice $E \oplus F$, and the Euclidean norm $\|.\|$ on $E_{\mathbb{R}} \oplus F_{\mathbb{R}}$ defined by the equality

$$\|x \oplus y\|^2 := \|x\|^2_{\overline{E}} + \|y\|^2_{\overline{F}} \quad \text{for all } (x, y) \in E_{\mathbb{R}} \times F_{\mathbb{R}}.$$

Moreover, $\mathcal{H}om_{\mathcal{O}_C}(\mathcal{E}, \mathcal{F})$ is replaced by the finite set $\mathcal{H}om(\overline{E}, \overline{F})$ of $\mathbb{R}$-linear maps

$$\varphi : E_{\mathbb{R}} \longrightarrow F_{\mathbb{R}}$$

such that $\varphi(E) \subseteq F$ and

$$\|\varphi(v)\|_{\overline{F}} \leq \|v\|_{\overline{E}} \quad \text{for all } v \in E_{\mathbb{R}}.$$

One may also introduce the analogue of a short exact sequence

$$0 \longrightarrow \mathcal{E} \overset{i}{\longrightarrow} \mathcal{F} \overset{p}{\longrightarrow} \mathcal{G} \longrightarrow 0$$

of vector bundles over C. It is a so-called *admissible short exact sequence* of Euclidean lattices:

$$0 \longrightarrow \overline{E} \overset{i}{\longrightarrow} \overline{F} \overset{p}{\longrightarrow} \overline{G} \longrightarrow 0, \tag{0.0.10}$$

defined by the data of Euclidean lattices $\overline{E}$, $\overline{F}$, and $\overline{G}$, and of elements i and p in $\mathcal{H}om(\overline{E}, \overline{F})$ and $\mathcal{H}om(\overline{F}, \overline{G})$ such that the following conditions are satisfied:

- the diagram

  $$0 \longrightarrow E \overset{i}{\longrightarrow} F \overset{p}{\longrightarrow} G \longrightarrow 0$$

  is an exact sequence of $\mathbb{Z}$-modules; this is easily seen to imply that

  $$0 \longrightarrow E_{\mathbb{R}} \overset{i}{\longrightarrow} F_{\mathbb{R}} \overset{p}{\longrightarrow} G_{\mathbb{R}} \longrightarrow 0$$

  is an exact sequence of $\mathbb{R}$-vector spaces;

- the map i is an isometry from the Euclidean $\mathbb{R}$-vector space $(E_{\mathbb{R}}, \|.\|_{\overline{E}})$ to $(F_{\mathbb{R}}, \|.\|_{\overline{F}})$, and the Euclidean norm $\|.\|_{\overline{G}}$ on $G_{\mathbb{R}}$ that defines $\overline{G}$ is the quotient norm induced from the norm $\|.\|_{\overline{F}}$ on $F_{\mathbb{R}}$ by means of the surjective $\mathbb{R}$-linear map $p : F_{\mathbb{R}} \to G_{\mathbb{R}}$.[2]

In this dictionary between vector bundles and Euclidean lattices, the rank $\mathrm{rk}\,\mathcal{E}$ of the vector bundle $\mathcal{E}$ is replaced by the rank $\mathrm{rk}\,E$ of $\overline{E}$, and the degree $\deg_C \mathcal{E}$ by the *Arakelov degree* of $\overline{E}$, defined as

$$\widehat{\deg}\,\overline{E} := -\log \mathrm{covol}\,\overline{E}.$$

Instead of being $\mathbb{Z}$-valued like $\deg_C \mathcal{E}$, the Arakelov degree $\widehat{\deg}\,\mathcal{E}$ is $\mathbb{R}$-valued. However, it satisfies properties formally similar to those satisfied by $\deg_C \mathcal{E}$. For instance,

$$\widehat{\deg}\,(\overline{E} \oplus \overline{F}) = \widehat{\deg}\,\overline{E} + \widehat{\deg}\,\overline{F},$$

and more generally, for every admissible short exact of Euclidean lattices (0.0.10),

$$\widehat{\deg}\,\overline{G} = \widehat{\deg}\,\overline{E} + \widehat{\deg}\,\overline{F}.$$

It turns out that the invariant $h^0(C, \mathcal{E})$ attached to some vector bundle $\mathcal{E}$ over C admits *two* distinct counterparts in the classical literature.

The first one, already considered in substance by Weil in [117], is the non-negative real number

$$h^0_{\mathrm{Ar}}(\overline{E}) := \log |\{v \in E | \|v\| \leq 1\}|,$$

defined in terms of the number of points of the lattice E in the unit ball of the Euclidean vector space $(E_{\mathbb{R}}, \|.\|)$.

We have a bijection

$$\mathcal{H}om(\mathbb{Z}, \overline{E}) \xrightarrow{\sim} \{v \in E | \|v\| \leq 1\},$$

defined by mapping an element φ in $\mathcal{H}om(\mathbb{Z}, \overline{E})$ to $\varphi(1)$, and accordingly, the definition of $h^0_{\mathrm{Ar}}(\overline{E})$ may also be written

$$h^0_{\mathrm{Ar}}(\overline{E}) := \log |\mathcal{H}om(\overline{\mathbb{Z}}, \overline{E})|. \tag{0.0.11}$$

Actually, for every vector bundle $\mathcal{E}$ over the curve C, we have a bijection of k-vector spaces

$$\mathcal{H}om_{\mathcal{O}_C}(\mathcal{O}_C, \mathcal{E}) \xrightarrow{\sim} \Gamma(C, \mathcal{E}),$$

[2] This condition on p, $\|.\|_{\overline{F}}$, and $\|.\|_{\overline{G}}$ may be rephrased as follows: the transpose $p^t : G_{\mathbb{R}} \to F_{\mathbb{R}}$ of $p : F_{\mathbb{R}} \to G_{\mathbb{R}}$, defined using the Euclidean structures on $F_{\mathbb{R}}$ and $G_{\mathbb{R}}$, is an isometry from $(G_{\mathbb{R}}, \|.\|_{\overline{G}})$ to $(F_{\mathbb{R}}, \|.\|_{\overline{F}})$.

also defined by mapping φ in $\mathcal{H}om_{\mathcal{O}_C}$ to $\varphi(1)$, and consequently, when the base field k is finite of order q, the integer $h^0(C,E)$ admits an expression similar to (0.0.11):

$$h^0(C,\mathcal{E}) = \dim_k \Gamma(C,\mathcal{E}) = \dim_k \mathcal{H}om_{\mathcal{O}_C}(\mathcal{O}_C,\mathcal{E}) = \frac{\log|\mathcal{H}om_{\mathcal{O}_C}(\mathcal{O}_C,\mathcal{E})|}{\log q}.$$

The second counterpart of the invariant $h^0(C,\mathcal{E})$ is the theta invariant already defined in (0.0.9):

$$h^0_\theta(\overline{E}) := \log \sum_{v\in E} e^{-\pi\|v\|^2}.$$

The fact that it is an arithmetic analogue of $h^0(C,\mathcal{E})$ goes back to the work of the German school of number theory, in particular to the proofs by Hecke and Schmidt of the meromorphic continuation and the functional equation of the zeta function of some global field. Hecke [61] first treated the case of a number field, and later, Schmidt [97] the case of a function field, defined as above as $k(C)$ with k a base field of finite order $q := |k|$. The comparison of these proofs shows that in the function field case,

$$|\Gamma(C,\mathcal{E})| = q^{h^0(C,\mathcal{E})}$$

plays a role parallel to that of

$$\theta_{\overline{E}}(1) = e^{h^0_\theta(\overline{E})}$$

in the number field case.

Moreover the Riemann–Roch formula on the curve C plays, in Schmidt's proof, a role parallel to that of the Poisson formula for theta series in Hecke's proof. The Poisson formula indeed relates the theta functions $\theta_{\overline{E}}$ and $\theta_{\overline{E}^\vee}$ attached to some Euclidean lattice and to its dual lattice $\overline{E}^\vee$:

$$\theta_{\overline{E}}(\beta) = (\operatorname{covol}\overline{E})^{-1}\beta^{-\operatorname{rk}\overline{E}/2}\,\theta_{\overline{E}^\vee}(\beta^{-1}) \quad \text{for every } \beta\in\mathbb{R}^*_+.$$

When $\beta = 1$, after taking logarithms, it reads

$$h^0_\theta(\overline{E}) - h^0_\theta(\overline{E}^\vee) = \widehat{\deg}\,\overline{E}. \tag{0.0.12}$$

This is formally similar to the Riemann–Roch formula for a vector bundle $\mathcal{E}$ over a smooth projective curve C of genus $g = 1$, which takes the form

$$h^0(C,\mathcal{E}) - h^0(C,\mathcal{E}^\vee) = \deg_C \mathcal{E}.$$

In the same vein, for all $t\in\mathbb{R}$, we may consider the Euclidean lattice $\overline{E}\otimes\overline{\mathcal{O}}(t)$ induced from some Euclidean lattice $\overline{E}$ by scaling its Euclidean norm by e^{-t}. Then, from the asymptotic behavior of $\theta_{\overline{E}}(\beta)$ as β goes to 0, we obtain

$$h^0_\theta(\overline{E}\otimes\overline{\mathcal{O}}(t)) = \operatorname{rk} E\cdot t + \widehat{\deg}\,\overline{E} + o(1) \quad \text{as } t \longrightarrow +\infty.$$

This may be seen as a counterpart of the relation

$$h^0(C, \mathcal{E} \otimes \mathcal{O}_C(k \cdot O) = \mathrm{rk}\,\mathcal{E} \cdot k + \deg_C \mathcal{E} \quad \text{when } k \in \mathbb{N} \text{ is large enough,}$$

valid for an arbitrary vector bundle $\mathcal{E}$ over an elliptic curve C of origin O.

The two invariants $h^0_{\mathrm{Ar}}(\overline{E})$ and $h^0_\theta(\overline{E})$ are actually closely related. For instance, using Banaszczyk's techniques, one may establish the comparison estimates

$$-\pi \leq h^0_\theta(\overline{E}) - h^0_{\mathrm{Ar}}(\overline{E}) \leq (n/2)\log n - \log(1 - 1/2\pi), \quad \text{where } n = \mathrm{rk}\, E. \tag{0.0.13}$$

However, the properties of $h^0_\theta(\overline{E})$ make it a better analogue of the number $h^0(C, \mathcal{E})$ than $h^0_{\mathrm{Ar}}(\overline{E})$. For instance, one easily sees that it is additive for direct sums; namely, for every two Euclidean lattices $\overline{E}$ and $\overline{F}$,

$$h^0_\theta(\overline{E} \oplus \overline{F}) = h^0_\theta(\overline{E}) + h^0_\theta(\overline{F}). \tag{0.0.14}$$

Moreover, as already observed by Quillen and Groenewegen, it is subadditive for short exact sequences; namely, for every admissible short exact sequences of Euclidean lattices (0.0.10), we have

$$h^0_\theta(\overline{F}) \leq h^0_\theta(\overline{E}) + h^0_\theta(\overline{G}). \tag{0.0.15}$$

This is again a consequence of (a suitable version of) Poisson's formula. The relations (0.0.14) and (0.0.15) are easily seen *not* to hold when h^0_θ is replaced by h^0_{Ar}.

Another illustration of the closer similarity of $h^0_\theta(\overline{E})$ to $h^0(C, \mathcal{E})$ is the following observation.

From the Poisson–Riemann–Roch formula (0.0.12) and the nonnegativity of $h^0_\theta(\overline{E})$, we immediately derive the lower bound

$$h^0_\theta(\overline{E}) \geq \widehat{\deg}\, \overline{E}, \tag{0.0.16}$$

which is similar to the lower bound

$$h^0(C, \mathcal{E}) \geq \deg_C E,$$

valid for every vector bundle over a smooth projective curve C of genus $g = 1$.

In turn, combined with (0.0.13), the lower bound (0.0.16) implies

$$h^0_{\mathrm{Ar}}(\overline{E}) \geq \widehat{\deg}\, \overline{E} - c(n), \tag{0.0.17}$$

where

$$c(n) = (n/2)\log n - \log(1 - 1/2\pi).$$

As n approaches infinity, this value of $c(n)$ is equivalent to the best possible (that is, the smallest) constant $c(n)$ in (0.0.17).[3]

[3] Indeed, this best constant is easily seen to satisfy $c(n) \geq (n/2)\log \gamma_n$, where γ_n denotes the Hermite contant in dimension n, introduced in paragraph **B** as the square of the best constant $C(n)$ in the Hermite–Minkowski inequality (0.0.1). From the asymptotics (0.0.5) on γ_n and the above value for $c(n)$, we derive that the best constant $c(n)$ in (0.0.17) satisfies: $c(n) = (n/2)\log n + O(n)$.

A remarkable feature of the estimates (0.0.15) and (0.0.16) concerning the theta invariant h^0_θ is that the ranks of the Euclidean lattices under consideration do *not* appear in them, while analogous relations concerning h^0_{Ar}, such as (0.0.17), would necessarily involve these ranks.

E. This last observation constitutes the starting point of the main constructions in this monograph: the fact that the theta invariants of Euclidean lattices satisfy analytic properties formally independent of their rank indicates that these invariants should make sense for some infinite-dimensional avatars of Euclidean lattices. This is similar to the following familiar observation: the fact that most constructions in finite-dimensional Euclidean geometry are independent of the dimension points toward the theory of Hilbert spaces.

The main result of this monograph is that it is indeed possible to define a nice class of such "infinite-dimensional Euclidean lattices" for which the theta invariant $h^0_\theta(\overline{E})$ is still well defined and satisfies natural continuity properties. Moreover, such infinite-dimensional Euclidean lattices naturally appear in arithmetic geometry, and the consideration of their theta invariants leads to natural proofs in Diophantine geometry and transcendence theory.

Let us describe in elementary terms the class of Euclidean lattices of infinite rank that constitute the main object of study in this monograph. In the terminology introduced in Chapter 5, they are the objects of the category $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$ of "pro-Hermitian vector bundles over $\operatorname{Spec}\mathbb{Z}$" that have infinite rank. They are defined by the following data:

- a topological $\mathbb{R}$-vector space $\widehat{E}_{\mathbb{R}}$ and a $\mathbb{Z}$-submodule $\widehat{E}$ of $\widehat{E}_{\mathbb{R}}$ such that there exists an isomorphism of topological $\mathbb{R}$-vector spaces
$$\varphi : \widehat{E}_{\mathbb{R}} \xrightarrow{\sim} \mathbb{R}^{\mathbb{N}}$$
such that
$$\varphi(\widehat{E}) = \mathbb{Z}^{\mathbb{N}}.$$
Here the space $\mathbb{R}^{\mathbb{N}}$ of $\mathbb{R}$-valued sequences is equipped with the topology of simple convergence, or equivalently, with the product topology derived from the usual topology on each factor $\mathbb{R}$.

- a real Hilbert space $(E^{\mathrm{Hilb}}_{\mathbb{R}}, \|.\|)$ and a continuous injective $\mathbb{R}$-linear map with dense image
$$i : E^{\mathrm{Hilb}}_{\mathbb{R}} \longrightarrow \widehat{E}_{\mathbb{R}}.$$

These data
$$\widehat{E} \subset \widehat{E}_{\mathbb{R}} \xhookleftarrow{i} E^{\mathrm{Hilb}}_{\mathbb{R}},\ \|.\| \tag{0.0.18}$$
will play the role of the data
$$E \subset E_{\mathbb{R}},\ \|.\|$$

defining a Euclidean lattice. The data (0.0.18) defining a Euclidean lattice of infinite rank $\widehat{\overline{E}}$ — or with the terminology of this monograph, an object in the category $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$ — may look rather intricate. However, this definition arises naturally, from both a practical and a conceptual point of view. Let us try to explain how.

E.a. In many Diophantine problems, one encounters a combination of formal geometry over the integers and complex analytic geometry. It turns out that such a combination may often be encoded in data of the type (0.0.18). Let us give a specific example.

Let Ω be an open neighborhood of 0 in $\mathbb{C}$, which will be assumed to be connected, bounded, and invariant under complex conjugation. We may consider the complex Hilbert space $\mathcal{O}_{L^2}(\Omega)$ of square integrable holomorphic functions on Ω, equipped with the L^2-norm defined by

$$\|f\|^2_{L^2(\Omega)} := \int_\Omega |f(x+iy)|^2 \, dx \, dy.$$

It is equipped with a natural $\mathbb{C}$-antilinear "complex conjugation", which maps a function f in $\mathcal{O}_{L^2}(\Omega)$ to $\overline{f}$ defined by

$$\overline{f}(z) := \overline{f(\overline{z})}.$$

The fixed points of this involution define a real Hilbert space $E_{\mathbb{R}}^{\mathrm{Hilb}}$. Its elements are the square integrable holomorphic functions on Ω whose Taylor expansions at 0 have real coefficients.

Then we may consider:

- $\widehat{E} := \mathbb{Z}[[X]]$ and $\widehat{E}_{\mathbb{R}} := \mathbb{R}[[X]]$, equipped with the topology of simple convergence of coefficients;
- $i : E_{\mathbb{R}}^{\mathrm{Hilb}} \longrightarrow \widehat{E}_{\mathbb{R}} = \mathbb{R}[[X]]$, defined as the map sending some holomorphic function f in $E_{\mathbb{R}}^{\mathrm{Hilb}}$ to its Taylor expansion at 0:

$$i(f) := \sum_{n \in \mathbb{N}} \frac{1}{n!} f^{(n)}(0) \, X^n.$$

The map i is injective, since Ω is connected. It is continuous by Cauchy estimates, and its image is dense in $\mathbb{R}[[X]]$, since it contains $\mathbb{R}[X]$, since Ω is bounded. Therefore, these data define an object of the category $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$, which will be denoted by $\widehat{\overline{\mathcal{H}}}(\Omega)$.

E.b. Let us consider a projective system

$$\overline{E}_\bullet : \overline{E}_0 \xleftarrow{q_0} \overline{E}_1 \xleftarrow{q_1} \cdots \xleftarrow{q_{k-1}} \overline{E}_k \xleftarrow{q_k} \overline{E}_{k+1} \xleftarrow{q_{k+1}} \cdots . \tag{0.0.19}$$

of Euclidean lattices, defined by a sequence $(\overline{E}_k)_{k \in \mathbb{N}}$ of Euclidean lattices and a sequence $(q_k)_{k \in \mathbb{N}}$ of morphisms q_k in $\mathcal{H}om(\overline{E}_{k+1}, \overline{E}_k)$. Let us assume that it satisfies the following admissibility conditions, for all $k \in \mathbb{N}$:

- the morphism of $\mathbb{Z}$-modules $q_k : E_{k+1} \to E_k$ — and therefore the $\mathbb{R}$-linear map $q_k : E_{k+1,\mathbb{R}} \to E_{k,\mathbb{R}}$ — is surjective;
- the Euclidean norm $\|.\|_k$ on $E_{k,\mathbb{R}}$ that defines $\overline{E}_k$ is the quotient norm induced from the norm $\|.\|_{k+1}$ on $E_{k+1,\mathbb{R}}$ by means of $q_k : E_{k+1,\mathbb{R}} \longrightarrow E_{k,\mathbb{R}}$.

These conditions may be rephrased as follows: for all $k \in \mathbb{N}$, the morphism q_k fits into an admissible short exact sequence of Euclidean lattices, as defined in paragraph **D** above (see (0.0.10)):

$$0 \longrightarrow \overline{S}_k \xrightarrow{i_k} \overline{E}_{k+1} \xrightarrow{q_k} \overline{E}_k \longrightarrow 0. \tag{0.0.20}$$

(Indeed, the Euclidean lattice $\overline{S}_k$ may be constructed from q_k by considering the lattice $\ker q_{k|E_{k+1}} : E_{k+1} \to E_k$ inside $\ker q_k : E_{i+k,\mathbb{R}} \to E_{k,\mathbb{R}}$, equipped with the restriction of the Euclidean norm $\|.\|_{k+1}$; the morphism i_k is then the inclusion map.)

We shall also assume that the nondecreasing sequence $(\operatorname{rk} E_k)_{k\in\mathbb{N}}$ is unbounded. (Otherwise, the morphisms q_k are isometric isomorphisms for k large enough.)

To any admissible projective system $\overline{E}_\bullet$ of Euclidean lattices as above we may associate data (0.0.18) defining some Euclidean lattice of infinite rank by the following construction.

We may consider the projective limits

$$\widehat{E} := \varprojlim_k E_k := \left\{ (v_k)_{k\in\mathbb{N}} \in \prod_{k\in\mathbb{N}} E_k \mid \forall k \in \mathbb{N}, q_k(v_{k+1}) = v_k \right\}$$

and

$$\widehat{E}_{\mathbb{R}} := \varprojlim_k E_{k,\mathbb{R}} := \left\{ (v_k)_{k\in\mathbb{N}} \in \prod_{k\in\mathbb{N}} E_{k,\mathbb{R}} \mid \forall k \in \mathbb{N}, q_k(v_{k+1}) = v_k \right\}.$$

They are endowed with a natural topology, defined as the topology induced by the product topology on $\prod_{k\in\mathbb{N}} E_k$ (resp., on $\prod_{k\in\mathbb{N}} E_{k,\mathbb{R}}$), when each space E_k (resp., $E_{k,\mathbb{R}}$) is endowed with the discrete topology (resp., with its natural topology of a finite-dimensional $\mathbb{R}$-vector space).

The surjective morphisms of $\mathbb{Z}$-modules $q_k : E_{k+1} \to E_k$ admit $\mathbb{Z}$-linear splittings, and therefore we may construct a sequence $(\varphi_k)_{k\in\mathbb{N}}$ of isomorphisms of $\mathbb{Z}$-modules

$$\varphi_k : E_k \xrightarrow{\sim} \mathbb{Z}^{\operatorname{rk} E_k}$$

such that the diagrams

$$\begin{array}{ccc} E_{k+1} & \xrightarrow{\varphi_{k+1}} & \mathbb{Z}^{\operatorname{rk} E_{k+1}} \\ {\scriptstyle q_k}\downarrow & & \downarrow{\scriptstyle \operatorname{pr}_k} \\ E_k & \xrightarrow{\varphi_k} & \mathbb{Z}^{\operatorname{rk} E_k} \end{array} \tag{0.0.21}$$

are commutative, where pr_k denotes the projection

$$\mathrm{pr}_k : (x_i)_{1 \leq i \leq \mathrm{rk}\, E_{k+1}} \longmapsto (x_i)_{1 \leq i \leq \mathrm{rk}\, E_k}.$$

The maps φ_k induce isomorphisms of finite-dimensional $\mathbb{R}$-vector spaces

$$\varphi_{k,\mathbb{R}} : E_{k,\mathbb{R}} \xrightarrow{\sim} \mathbb{R}^{\mathrm{rk}\, E_k}$$

and, by going to the projective limit, an isomorphism of topological $\mathbb{R}$-vector spaces

$$\widehat{\varphi} : \widehat{E}_{\mathbb{R}} \xrightarrow{\sim} \mathbb{R}^{\mathbb{N}}$$

such that

$$\widehat{\varphi}(\widehat{E}) = \mathbb{Z}^{\mathbb{N}}.$$

Every element v in $\widehat{E}_{\mathbb{R}}$ is defined by a sequence $(v_k)_{k\in\mathbb{N}}$ in $\prod_{k\in\mathbb{N}} E_{k,\mathbb{R}}$ satisfying the coherence conditions:

$$q_k(v_{k+1}) = v_k, \quad \text{for every } k \in \mathbb{N}.$$

The morphisms q_k are norm decreasing, and therefore

$$\|v_k\|_k \leq \|v_{k+1}\|_{k+1}, \quad \text{for every } k \in \mathbb{N}.$$

Consequently, the limit

$$\|v\| := \lim_{k\to+\infty} \|v_k\|_k$$

exists in $[0, +\infty]$, and we may therefore define

$$E_{\mathbb{R}}^{\mathrm{Hilb}} := \{v \in E_{\mathbb{R}}^{\mathrm{Hilb}} \mid \|v\| < +\infty\}.$$

Using that each Euclidean norm $\|.\|_k$ is the quotient norm (via q_k) of the Euclidean norm $\|.\|_{k+1}$, one easily sees that $(E_{\mathbb{R}}^{\mathrm{Hilb}}, \|.\|)$ is actually a real Hilbert space, and that the inclusion morphism

$$i : E_{\mathbb{R}}^{\mathrm{Hilb}} \hookrightarrow \widehat{E}_{\mathbb{R}},$$

is continuous with dense image. Indeed, by considering the orthogonal splittings of the surjective $\mathbb{R}$-linear maps $q_k : E_{k+1,\mathbb{R}} \to E_{k,\mathbb{R}}$, the topological $\mathbb{R}$-vector space $\widehat{E}_{\mathbb{R}}$ may be identified with the product

$$E_{0,\mathbb{R}} \times \prod_{k\in\mathbb{N}} S_{k,\mathbb{R}}$$

and $(E_{\mathbb{R}}^{\mathrm{Hilb}}, \|.\|)$ with the completed infinite direct sum

$$E_{0,\mathbb{R}} \oplus \widehat{\bigoplus}_{k\in\mathbb{N}} S_{k,\mathbb{R}}$$

of finite-dimensional Euclidean $\mathbb{R}$-vector spaces.

The topological $\mathbb{R}$-vector space $\widehat{E}_{\mathbb{R}}$, its submodule $\widehat{E}$, the Hilbert space $(E_{\mathbb{R}}^{\mathrm{Hilb}}, \|.\|)$, and the inclusion morphism $i : E_{\mathbb{R}}^{\mathrm{Hilb}} \hookrightarrow \widehat{E}_{\mathbb{R}}$ so constructed from the admissible projective system $\overline{E}_{\bullet}$ define an object of the category $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$, which will be denoted by $\varprojlim \overline{E}_{\bullet}$.

F. It turns out that this construction of Euclidean lattices of infinite rank as projective limits allows one to recover (up to isomorphism) any object of $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$.

F.a. The central point behind this fact is the construction of *quotient* (finite-dimensional) *Euclidean lattices* of an object $\overline{\widehat{E}}$ of $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$ defined by data as in (0.0.18) above, associated to saturated open submodules of the topological $\mathbb{Z}$-module $\widehat{E}$.

Let U be an open submodule of $\widehat{E}$. By the definition of the topology of $\widehat{E}$ (which is assumed to be topologically isomorphic to $\mathbb{Z}^{\mathbb{N}}$ equipped with the product topology), the quotient $\mathbb{Z}$-module

$$E_U := \widehat{E}/U$$

is then finitely generated. When it is torsion-free, hence isomorphic to $\mathbb{Z}^r$ for some r in $\mathbb{N}$, the submodule U is called saturated. Then the quotient map

$$q : \widehat{E} \longrightarrow E_U \simeq \mathbb{Z}^r$$

is continuous (when E_U is equipped with the discrete topology), and is easily seen to extend uniquely to a continuous $\mathbb{R}$-linear map

$$q_{\mathbb{R}} : \widehat{E}_{\mathbb{R}} \longrightarrow E_{U,\mathbb{R}} := E_U \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{R}^r,$$

which is actually open and surjective.

Let us consider the composite $\mathbb{R}$-linear map

$$q_{\mathbb{R}} \circ i : E_{\mathbb{R}}^{\mathrm{Hilb}} \overset{i}{\hookrightarrow} \widehat{E}_{\mathbb{R}} \overset{q_{\mathbb{R}}}{\longrightarrow} E_{U,\mathbb{R}}.$$

Since $i(E_{\mathbb{R}}^{\mathrm{Hilb}})$ is dense in $\widehat{E}_{\mathbb{R}}$ and $q_{\mathbb{R}}$ is continuous and surjective, its image is dense in $E_{U,\mathbb{R}}$, hence *equals* $E_{U,\mathbb{R}}$, since $E_{U,\mathbb{R}}$ is a finite-dimensional $\mathbb{R}$-vector space.

We may therefore consider the Euclidean norm $\|.\|_U$ of $E_{U,\mathbb{R}}$ defined as the quotient norm induced from the Hilbert norm $\|.\|$ on $E_{\mathbb{R}}^{\mathrm{Hilb}}$ by means of the continuous surjective map $q_{\mathbb{R}} \circ i$. Finally, we may define a Euclidean lattice (of finite rank) $\overline{E}_U$ by the lattice E_U in the $\mathbb{R}$-vector space $E_{U,\mathbb{R}}$ equipped with the Euclidean norm $\|.\|_U$:

$$\overline{E}_U : \quad E_U \subset E_{U,\mathbb{R}}, \ \|.\|_U.$$

For instance, let us consider the Euclidean lattice of infinite rank $\varprojlim \overline{E}_{\bullet}$, constructed above from the admissible projective system $\overline{E}_{\bullet}$. For every $k \in \mathbb{N}$, we may consider the canonical projection

$$\mathrm{pr}_k : \widehat{E} \longrightarrow E_k$$

that maps an element $v = (v_i)_{i\in\mathbb{N}}$ of $\widehat{E}$ seen as a submodule of $\prod_{i\in\mathbb{N}} E_i$ to its kth component v_k. Its kernel U_k is a saturated open submodule of $\widehat{E}$, and the quotient $E_{U_k} := \widehat{E}/U_k$ is easily seen to be canonically isomorphic to E_k, and the Euclidean lattice $\overline{E}_{U_k}$ to be isomorphic to $\overline{E}_k$.

In general, if $\widehat{\overline{E}}$ is an arbitrary object in $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$, then we may choose a decreasing sequence

$$U_0 \supset U_1 \supset \cdots \supset U_k \supset U_{k+1} \supset \cdots$$

of saturated open submodules of $\widehat{E}$ that constitutes a basis of neighborhoods of 0 in $\widehat{E}$, and we may consider the associated Euclidean lattices $\overline{E}_{U_k}$ and the quotient morphisms

$$q_k : E_{U_k,\mathbb{R}} \longrightarrow E_{U_{k+1},\mathbb{R}}.$$

They define a projective system of Euclidean lattices

$$\overline{E}_{U_0} \xleftarrow{q_0} \overline{E}_{U_1} \xleftarrow{q_1} \cdots \xleftarrow{q_{k-1}} \overline{E}_{U_k} \xleftarrow{q_k} \overline{E}_{U_{k+1}} \xleftarrow{q_{k+1}} \cdots$$

that satisfies the admissibility condition introduced in **E.b**. Accordingly, we may construct the object $\varprojlim_k \overline{E}_{U_k}$ in $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$, and there exists a canonical isomorphism:

$$\widehat{\overline{E}} \xrightarrow{\sim} \varprojlim_k \overline{E}_{U_k}.$$

F.b. Let us apply this construction to the Euclidean lattice of infinite rank $\widehat{\overline{E}} := \mathcal{H}(\Omega)$ introduced in **E.a**. Then a natural choice for the decreasing sequence $(U_k)_{k\in\mathbb{N}}$ of saturated open submodules of $\widehat{E} := \mathbb{Z}[[X]]$ is

$$U_k := \left\{ \sum_{n\in\mathbb{N}} a_n X^n \mid a_0 = \cdots = a_{k-1} = 0 \right\} = X^k\,\mathbb{Z}[[X]] \quad \text{for all } k \in \mathbb{N}.$$

Then

$$E_{U_k} = \mathbb{Z}[[X]]/X^k\,\mathbb{Z}[[X]] \simeq \mathbb{Z}[X]_{<k},$$

where for a ring A, we denote by $A[X]_{<k}$ the submodule $\bigoplus_{0\leq i<k} A\cdot X^i$ of $A[X]$, and the Euclidean norm $\|.\|_k$ on

$$E_{U_k,\mathbb{R}} \xrightarrow{\sim} \mathbb{R}[X]_{<k}$$

is (the restriction of) the quotient norm induced from the L^2-norm $\|.\|_{L^2(\Omega)}$ on $\mathcal{O}_{L^2}(\Omega)$ by the truncated Taylor expansion map

$$\begin{array}{rcl} \mathcal{O}_{L^2}(\Omega) & \longrightarrow & \mathbb{C}[X]_{<k}, \\ f & \longmapsto & \sum_{0\leq i<k} \frac{1}{i!} f^{(i)}(0) X^i. \end{array}$$

We may also consider the admissible short exact sequences of Euclidean lattices

$$0 \longrightarrow \overline{S}_k \xrightarrow{i_k} \overline{E}_{U_{k+1}} \xrightarrow{q_k} \overline{E}_{U_k} \longrightarrow 0$$

associated to the quotient maps q_k. The "subquotient" Euclidean lattices $\overline{S}_k$ admit the following description. Clearly, $S_{k,\mathbb{R}}$ (resp., S_k) may be identified with $\mathbb{R}.X^k$ (resp., $\mathbb{Z}.X^k$). Moreover, according to the above discussion, the norm of the generator X^k of S_k is given by

$$\|X^k\|_{\overline{S}_k} = \inf\left\{\|z^k + \rho\|_{L^2(\Omega)}; \rho \in \mathcal{O}_{L^2}(\Omega) \text{ and } \rho(0) = \cdots = \rho^{(k)}(0) = 0\right\}. \tag{0.0.22}$$

Observe that according to Cauchy estimates, for every $k \in \mathbb{N}$, there exists C_k in $\mathbb{R}_+^*$ such that the following inequality holds:

$$\left|f^{(k)}(0)/k!\right| \leq C_k \|f\|_{L^2(\Omega)}, \quad \text{for all } f \in \mathcal{O}_{L^2}(\Omega) \text{ such that}$$
$$f(0) = \cdots = f^{(k-1)}(0) = 0. \tag{0.0.23}$$

It is straightforward that the smallest possible constant C_k in (0.0.23) coincides with the inverse $\|X^k\|_{\overline{S}_k}^{-1}$ of the norm (0.0.22).

It is possible to give upper bounds on the constants C_k — or equivalently, lower bounds on the norms $\|X^k\|_{\overline{S}_k}$ — in terms of invariants of Ω defined by a classical construction from potential theory. Since this type of estimates plays a key role in the applications of the formalism in this monograph to Diophantine geometry, we want to discuss them more closely.

Let us, for instance, assume that the boundary of Ω is regular enough — say that Ω is the interior of some compact C^1-submanifold with boundary $\overline{\Omega}$ of $\mathbb{C} \simeq \mathbb{R}^2$. Then we may introduce the Green's function attached to the point 0 in Ω, namely the unique function $g_{\Omega,0}$ on $\overline{\Omega} \setminus \{0\}$ with values in $\mathbb{R}_+^*$ such that:

- $g_{\Omega,0}$ vanishes on $\partial\Omega := \overline{\Omega} \setminus \Omega$;
- $g_{\Omega,0}$ is harmonic on $\Omega \setminus \{0\}$;
- $g_{\Omega,0}$ has a logarithmic singularity at 0; in other words, the harmonic function

  $$h(z) := g_{\Omega,0}(z) - \log|z|^{-1}$$

  of $z \in \Omega \setminus \{0\}$ remains bounded as z goes to 0, and therefore extends to some harmonic function h on Ω.

The real number

$$C(\Omega) := e^{h(0)}$$

provides a potential theoretic measure of the size of Ω. If, for instance, Ω is the open disk $\mathring{D}(0, R)$ of center 0 and positive radius R, then $C(\Omega) = R$. In general, if K denotes the compact subset of $\mathbb{C}$ defined as

$$K := \{0\} \cup \{z^{-1}; z \in \mathbb{C} \setminus \Omega\},$$

then $h(0)$ is the so-called Robin constant of K, and $C(\Omega)$ is the inverse of the capacity of K.

For all $\varepsilon \in \mathbb{R}_+^*$, we may consider the following relatively compact open subset of Ω:

$$\Omega_\varepsilon := \{0\} \cup \{z \in \Omega \setminus \{0\} \mid g_{\Omega,0}(z) > \varepsilon\}.$$

By Cauchy estimates, there exists $A(\varepsilon)$ in $\mathbb{R}_+^*$ such that for every function f in $\mathcal{O}_{L^2}(\Omega)$,

$$\|f\|_{L^\infty(\partial\Omega_\varepsilon)} \leq A(\varepsilon)\|f\|_{L^2(\Omega)}. \tag{0.0.24}$$

When, moreover, f satisfies $f(0) = \cdots = f^{(k-1)}(0) = 0$, the maximum modulus principle applied to the function $\log|f| + n.g_{\Omega,0}$, together with the inequality (0.0.24), leads to the estimates

$$\begin{aligned}\log\left|f^{(k)}(0)/k!\right| &\leq -nh(0) + \log\|f\|_{L^\infty(\partial\Omega_\varepsilon)} + n\varepsilon \\ &\leq -n(h(0) - \varepsilon) + \log A(\varepsilon) + \log\|f\|_{L^2(\Omega)}.\end{aligned}$$

This shows that the estimate (0.0.23) holds with some constant C_k that satisfies

$$\log C_k \leq -n(\log C(\Omega) - \varepsilon) + \log A(\varepsilon),$$

and finally establishes the following asymptotic lower bound on $\|X^k\|_{\overline{S}_k}$:

$$\liminf_{k\to+\infty} k^{-1} \log\|X^k\|_{\overline{S}_k} \geq \log C(\Omega). \tag{0.0.25}$$

Estimates like (0.0.23), together with some control on the constant C_k, classically appear in Diophantine approximation and transcendence proofs under the name of *Schwarz lemma.* As exemplified by the previous discussion, they may be seen as *lower bounds* on the norms of Euclidean lattices defined as subquotients of the Euclidean lattices of infinite rank encoding the arithmetic and complex analytic data under investigation. These lower bounds are relevant for providing *upper bounds on the theta invariants* of these subquotients, and consequently, as we will see, to control the theta invariants of these Euclidean lattices of infinite rank.

G. Let us now return to the theta invariants of Euclidean lattices and their possible generalizations concerning Euclidean lattices of infinite rank.

A naive guess would be that to an object $\widehat{\overline{E}}$ of the category $\mathbf{pro}\overline{\mathbf{Vect}}_{\mathbb{Z}}^{\leq 1}$ constructed as the projective limit $\varprojlim \overline{E}_\bullet$ of some admissible projective system $\overline{E}_\bullet$ as in **E.b**, one could associate a well-defined and significant theta invariant by the rule

$$h^0_\theta(\widehat{\overline{E}}) := \lim_{k\to+\infty} h^0_\theta(\overline{E}_k).$$

This is grossly wrong. Actually, for every Euclidean lattice of infinite rank $\widehat{\overline{E}}$, there always exists an admissible projective system $\overline{E}_\bullet$ such that $\varprojlim \overline{E}_\bullet$ is isomorphic to $\widehat{\overline{E}}$ and

$$\lim_{k\to+\infty} h^0_\theta(\overline{E}) = +\infty.$$

Equivalently, if $\mathcal{U}(\widehat{E})$ denotes the filter basis of saturated open submodules of $\widehat{E}$, we have

$$\limsup_{U\in\mathcal{U}(\widehat{E})} h^0_\theta(\overline{E}_U) = +\infty.$$

It may, however, happen that for some other realization of $\widehat{\overline{E}}$ as $\varprojlim \overline{E}_\bullet$, the limit $\lim_{k\to+\infty} h^0_\theta(\overline{E})$ exists in $\mathbb{R}$, or does not exist in $[0,+\infty]$.

Among the possible candidates for a definition of $h^0_\theta(\widehat{\overline{E}})$, two natural ones, both taking values in $[0,+\infty]$, may be defined as follows.

Firstly, we can simply mimic the definition of $h^0_\theta(\overline{E})$ of a (finite-dimensional) Euclidean lattice by letting

$$\underline{h}^0_\theta(\widehat{\overline{E}}) := \log \sum_{v\in\widehat{E}\cap i(E^{\mathrm{Hilb}}_{\mathbb{R}})} e^{-\pi\|i^{-1}(v)\|^2}.$$

An immediate drawback of this definition is that it involves the intersection $\widehat{E}\cap i(E^{\mathrm{Hilb}}_{\mathbb{R}})$, which in general may be uncountable.

Secondly, we may try a definition "by approximation", which would avoid the lack of convergence of the theta invariants $h^0_\theta(\overline{E}_U)$ discussed above, by letting

$$\overline{h}^0_\theta(\widehat{\overline{E}}) := \liminf_{U\in\mathcal{U}(\widehat{E})} h^0_\theta(\overline{E}_U).$$

A drawback of this definition is that contrary to $\underline{h}^0_\theta(\widehat{\overline{E}})$, it is not obviously compatible with direct sums of Euclidean lattices of infinite rank.

These two invariants satisfy the estimate

$$\underline{h}^0_\theta(\widehat{\overline{E}}) \leq \overline{h}^0_\theta(\widehat{\overline{E}}),$$

which may actually be strict in general.

It turns out that there exists a class of "tame" Euclidean lattices of infinite rank for which these two invariants are finite and coincide, and which, moreover, is quite convenient for applications to Diophantine geometry.

In order to introduce this class, let us return to the construction of the object $\varprojlim \overline{E}_\bullet$ in $\mathbf{pro}\overline{\mathbf{Vect}}^{\leq 1}_{\mathbb{Z}}$ from some admissible projective system $\overline{E}_\bullet$ in $\mathbf{E.b}$. As already observed, by the definition of such a system, the morphisms q_k may be inserted into admissible short exact sequences of Euclidean lattices:

$$0 \longrightarrow \overline{S}_k \xrightarrow{i_k} \overline{E}_{U_{k+1}} \xrightarrow{q_k} \overline{E}_{U_k} \longrightarrow 0.$$

From the subadditivity (0.0.15) of h^0_θ in admissible short exact sequences, we get the sequence of inequalities

$$h^0_\theta(\overline{E}_{k+1}) - h^0_\theta(\overline{E}_k) \leq h^0_\theta(\overline{S}_k).$$

This implies that the sequence with kth term

$$h^0_\theta(\overline{E}_k) - \sum_{0 \leq i < k} h^0_\theta(\overline{S}_i)$$

is nonincreasing. When, moreover, the condition

$$\textbf{Sum}: \quad \sum_{i \in \mathbb{N}} h^0_\theta(\overline{S}_i) < +\infty$$

holds, it is also bounded from below, hence converges, and therefore the sequence $(h^0_\theta(\overline{E}_k))_{k \in \mathbb{N}}$ itself has a limit in $\mathbb{R}_+$.

A central result of this monograph is that the following minor strengthening[4] of the condition **Sum**,

$$\textbf{Sum}^+: \quad \text{for some } \varepsilon \in \mathbb{R}^*_+, \quad \sum_{i \in \mathbb{N}} h^0_\theta(\overline{S}_i \otimes \overline{\mathcal{O}}(\varepsilon)) < +\infty,$$

is enough to ensure that $\underline{h}^0_\theta(\widehat{\overline{E}})$ *and* $\overline{h}^0_\theta(\widehat{\overline{E}})$ *belong to* $[0, +\infty[$*, coincide, and are actually equal to the limit* $\lim_{k \to +\infty} h^0_\theta(\overline{E}_k)$. In this case, we define:

$$h^0_\theta(\widehat{\overline{E}}) := \underline{h}^0_\theta(\widehat{\overline{E}}) = \overline{h}^0_\theta(\widehat{\overline{E}}) = \lim_{k \to +\infty} h^0_\theta(\overline{E}_k) \in \mathbb{R}.$$

Conversely, for every object $\widehat{\overline{E}}$ in $\mathbf{pro}\overline{\mathbf{Vect}}^{\leq 1}_{\mathbb{Z}}$, one may prove that, if some for $\varepsilon \in \mathbb{R}^*_+$,

$$\underline{h}^0_\theta(\widehat{\overline{E}} \otimes \overline{\mathcal{O}}(\varepsilon)) = \overline{h}^0_\theta(\widehat{\overline{E}} \otimes \overline{\mathcal{O}}(\varepsilon)) < +\infty,$$

then $\widehat{\overline{E}}$ may be realized as $\varprojlim \overline{E}_\bullet$ for some admissible projective system $\overline{E}_\bullet$ satisfying $\mathbf{Sum}^+$.

The Euclidean lattices of infinite dimension $\widehat{\overline{E}}$ such that the Euclidean lattices $\widehat{\overline{E}} \otimes \overline{\mathcal{O}}(t)$ derived from them by scaling their Hilbert norm by e^{-t} satisfy the condition

$$\underline{h}^0_\theta(\widehat{\overline{E}} \otimes \overline{\mathcal{O}}(t)) = \overline{h}^0_\theta(\widehat{\overline{E}} \otimes \overline{\mathcal{O}}(t)) < +\infty$$

for all $t \in \mathbb{R}$ — the *θ-finite pro-Hermitian vector bundles over* $\operatorname{Spec} \mathbb{Z}$ in the terminology of Chapter 7 — satisfy convenient permanence properties. Moreover, the properties of the theta invariants of finite-dimensional Euclidean lattices naturally extend to these Euclidean lattices of infinite dimension.

[4]Recall that $\overline{S}_i \otimes \overline{\mathcal{O}}(\varepsilon)$ is the Euclidean lattice derived from $\overline{S}_i$ by scaling its Euclidean norm by $e^{-\varepsilon}$.

The proof of these results relies on several remarkable analytic properties of the theta series attached to Euclidean lattices — especially, on *subadditivity* properties that extend the estimate (0.0.15) satisfied by the theta invariants of Euclidean lattices in admissible short exact sequences, and on the *convexity* of the function $\log \theta_{\overline{E}}(\beta)$ — and on measure-theoretic constructions on the Polish (non locally compact) topological space $\widehat{E}$.

H. It turns out that θ-finite Euclidean lattices (of infinite rank) provide a convenient framework for applications to Diophantine geometry.

To give some hint of these applications, let us return to the object $\widehat{\overline{\mathcal{H}}}(\Omega)$ of $\overline{\mathbf{proVect}}_{\mathbb{Z}}^{\leq 1}$ defined in **E.a** and investigated in **F.b**.

With the notation of **F.b**, it may be realized as the projective limit $\varprojlim_k \widehat{\overline{E}}_{U_k}$. It is therefore θ-finite, provided that for all $t \in \mathbb{R}$, the condition **Sum** is satisfied by the subquotients $\overline{S}_k \otimes \overline{\mathcal{O}}(t)$ of $\widehat{\overline{\mathcal{H}}}(\Omega) \otimes \overline{\mathcal{O}}(t)$, namely when the following condition holds:

$$\text{for all } t \in \mathbb{R}, \quad \sum_{k \in \mathbb{N}} h^0_\theta(\overline{S}_k \otimes \overline{\mathcal{O}}(t)) < +\infty. \tag{0.0.26}$$

Recall that $\overline{S}_k$ is a Euclidean lattice of rank 1 and that the norm $\|X^k\|_{\overline{S}_k}$ of the generator X^k of S_k satisfies the asymptotic lower bound (0.0.25). The latter implies that for all $t \in \mathbb{R}$,

$$\liminf_{k \to +\infty} k^{-1} \log \|X^k\|_{\overline{S}_k \otimes \overline{\mathcal{O}}(t)} = \liminf_{k \to +\infty} k^{-1} (\log \|X^k\|_{\overline{S}_k} - t) \geq \log C(\Omega). \tag{0.0.27}$$

By means of (0.0.27), we easily obtain the following:

If $C(\Omega) > 1$, *then condition* (0.0.27) *holds, and therefore* $\widehat{\overline{\mathcal{H}}}(\Omega)$ *is* θ*-finite.* (0.0.28)

Indeed, we have

$$h^0_\theta(\overline{S}_k \otimes \overline{\mathcal{O}}(t)) = \log \sum_{m \in \mathbb{Z}} e^{-\pi m^2 \log \|X^k\|^2_{\overline{S}_k \otimes \overline{\mathcal{O}}(t)}}.$$

According to (0.0.27), when $C(\Omega) > 1$, we have:

$$\lim_{k \to +\infty} \|X^k\|_{\overline{S}_k \otimes \overline{\mathcal{O}}(t)} = +\infty,$$

and therefore

$$h^0_\theta(\overline{S}_k \otimes \overline{\mathcal{O}}(t)) \sim 2e^{-\pi \|X^k\|^2_{\overline{S}_k \otimes \overline{\mathcal{O}}(t)}} \quad \text{as } k \longrightarrow +\infty.$$

Using (0.0.27) again, we see that the series $\sum_{k \in \mathbb{N}} h^0_\theta(\overline{S}_k \otimes \overline{\mathcal{O}}(t))$ indeed converges when $C(\Omega) > 1$.

As discussed in Chapter 10, the finiteness property (0.0.28) of the infinite-dimensional Euclidean lattice $\widehat{\overline{\mathcal{H}}}(\Omega)$ lies at the heart of the algebraicity and rationality properties of meromorphic functions on Ω with integral Taylor expansions when $C(\Omega) > 1$, which have been investigated by E. Borel, G. Pólya, D. V. and G. V. Chudnovsky, and their followers.

Orsay, November 2019