THE MINKOWSKI-SIEGEL FORMULA FOR QUADRATIC BUNDLES ON CURVES

Juan Marcos Cerviño

CONTENTS

Introduction 1

1. Quadratic bundles and orthogonal groups 5
1. Valuations and Norms 5
1.1. Valuations 5
1.2. Ramification 6
1.3. Absolute values 6
1.4. (Counting) Norms 7
2. Quadratic bundles and orthogonal groups 9
2.1. Quadratic spaces 9
2.2. Lattices, quadratic forms 10
2.3. Clifford-Algebras, Spinor- norm and group 14
2.4. Quadratic bundles 17
2.5. Orthogonal groups 18

2. Lattices over global rings 23
1. Harder's Theorem 23
1.1. Hermite's Theorem 23
1.2. Harder's Theorem 27
2. Lattice points 29
2.1. Ray and convex bodies 29
2.2. Counting lattice points 31
2.3. Volumes 32
3. Curves in the sense of Chevalley 33
3.1. Abstract curves 33
3.2. Vector bundles and double classes 34
3.3. Extensions 34

3. Orthogonal groups on curves over finite fields 37
1. The group scheme $\mathrm{O}(\mathcal{E})$ 37
1.1. Good models 37
1.2. Reductiveness of the orthogonal group 38
2. Adele Orthogonal Group and Haar-measure 39
2.1. Adele orthogonal group 39
2.2. Congruence subgroups 40
2.3. Haar measure 42
3. Genus Theory 44

3.1. For quadratic bundles 44
3.2. For quadratic bundle representations 45

4. Minkowski-Siegel formula 49
1. Fundamental domains 49
2. Proof of the formula (first part) 53
2.1. Regularization of local Haar-measures 53
3. Quadratic lattices over discrete valuation rings 55
4. Proof of the formula (cont'd.): Volume Computation 57
4.1. The left hand side 58
4.2. The right hand side 63
5. Applications and Consequences 66
5.1. Genus-versal integral quadratic bundles 66
5.2. Deuring-Gekeler Maßformel 70
5.3. Lefschetz trace formula over stacks and Minkowski-Siegel formula 70

Arithmetical semi-groups 71
1. Arithmetical functions. Some properties 72
2. L-functions and asymptotical properties 73

Bibliography 75

INTRODUCTION

The subject of this thesis is the arithmetic theory of (definite) quadratic forms in the language of algebraic geometry. In order to preserve classical arithmetic properties we restricted ourselves to curves over finite fields. Nevertheless, the intention of working over more general schemes should be clear throughout the thesis. In this regard, a general theory of adeles for higher dimensional schemes would be an essential step towards a general theory.

The problem of representability of an integer by an integral quadratic form can be solved locally by the Hasse-principle. Namely, if the quadratic form represents the given number *locally everywhere*, then it represents this number with rational coefficients. This establishes a *qualitative* relation between local and global representability of a number by a given quadratic form. We could ask ourselves for a *quantitative* analogue: does there exist a relation between the number of local representations and the number of global ones? The first concrete and satisfactory attempt to precise this question was done by Gotthold Eisenstein [**Eis47**], where he realized the importance of certain weighted sums for genera of positive definite ternary quadratic forms (nowadays known as the *Maß* of the genus), which could be expressed as an infinite product of *local densities* over the prime numbers. Eisenstein's formula was later proved by Minkowski and Smith. The first general answer to this question, though, was given by Carl Ludwig Siegel in [**Sie35**] and two subsequent papers, where he proved a more general version of Eisenstein's formula: the so called *Minkowski-Siegel formula*.

In the late 1950ies Tsuneo Tamagawa conjectured that the Minkowski-Siegel formula should be equivalent to the fact that certain measure of *a fundamental domain* in an adele group of the special orthogonal group of the quadratic form, is 2. The measure of this fundamental domain is known as the **Tamagawa number** of the orthogonal group (which can be defined for any reductive algebraic group). Tamagawa's "intuition" was confirmed by André Weil in his celebrated lectures [**Wei82**], where he proved that the Tamagawa number of the special orthogonal group of a quadratic form (over a *field* not of characteristic 2) is 2. In the case the group is semi-simple (for example the quadratic form is unimodular), the Tamagawa number is canonically defined; whereas in the case of reductive (non semi-simple) groups some extra normalizations (so called *convergence factors*) must be chosen. A far more abstract interpretation of Siegel's formula was done by A. Weil again, in [**Wei65**]; a more analytical study of the formula with tools from harmonic analysis on topological groups (this kind of formulas are known as the "Siegel-Weil type" formulas). In this direction, [**Har74**] proved a Siegel-Weil type formula in the function field case for dimensions greater or equal to 5 (so the quadratic forms are indefinite in this case). Here we deal, though in a more geometrical context, with *definite*

quadratic forms, so the dimension is at most 4. Even though this is not exactly the complement, since it remains open the study of indefinite forms of dimensions lesser or equal to 4. All these results give a concrete contribution to the rather under-developed situation of the theory of modular forms *in the function field case* (not in the very general frame of automorphic representations). In particular, we are interested in theta functions associated to (definite) quadratic forms defined over function fields.

In an attempt to understand this "analytical world", we started with our very first motivation: integral classification for definite ternary quadratic forms over global function fields of characteristic not 2. I conjecture (based on some facts on supersingular elliptic curves and on its function fields analogues: the *supersingular Drinfeld modules*), that as in the classical case (cf. [**Sch97**]), the integral classes of definite ternary quadratic forms over global function fields are determined by their *"theta series"*, or what amounts the same, by their representation numbers.
It is one of the main aims of this work, to prove the (*arithmetical version* of the) Minkowski-Siegel formula for definite quadratic bundles over curves over finite fields (Theorem 4.4.1), which relates the global representation numbers in the genus with the local representation numbers.

In a joint work with Prof. J. Morales and J. Bureau (Louisiana) we prove Schiemann's result for the rational function field case and quadratic forms of *small* (say prime) discriminant. This result, is again a step towards an attempt to give an explicit algorithm to compute endomorphism rings of rank 2 supersingular Drinfeld modules (cf. [**Cer**]), and gives some understanding to the analytical problem depicted above.

We shortly summarize the contents of the thesis after the first introductory chapter, where we settle notation of basic facts and some proofs, as for example the representability of the orthogonal group of a quadratic bundle over any scheme.
We proceed with Chapter 2. One first attempt to study the Minkowski-Siegel formula in a more geometric language (on curves over finite fields), is the study of the *geometry of numbers* for completions of global fields of positive characteristic. This non-archimedian geometry is pretty much different from the classical one (for example all triangles are isosceles), something which has pros but also cons. The main tool in the study of the geometry of numbers in this context is the basic theorem of Riemann-Roch (Theorem 2.2.6). With a more classical approach, we found a new version of the well known Hermite's Lemma (Theorem 2.1.6) which gives a proof of a theorem of Harder (Theorem 2.1.12). Unaware of this at the time of my investigations, I found this approach for the proof of Harder's theorem was already taken in [**Ger79**] (found after reading a book of Lam on Serre's Conjecture).

The studies in §2.2 were done with the intention of obtaining sufficient information to prove a step (the *left hand side*) of the Minkowski-Siegel formula. In this direction the Proposition 2.2.10 (after which I got to know it existed already in the literature: [**GI63**]) seems to shed some positive light. Instead, we use more traditional methods of elementary analytic number theory (in the framework of arithmetical semi-groups, cf. [**Kno75**]).

At the end, we study the extension property of quadratic bundles defined over an affine, Zariski open subset of a projective *curve* (see later for some restrictions) to the whole.

In the third chapter we study some properties of the adele orthogonal groups, of its Haar measures, and define the necessary ingredients for the proof of the main formula. We give also a proof of the well known fact, that the Hasse principle holds for orthogonal groups over global function fields.

In the last chapter, we prove the Minkowski-Siegel formula for definite (and integral, which is not an essential restriction) quadratic bundles on curves over finite fields (Theorem 4.4.1). We follow the lines of the original proof in [**Sie35**] and also the very nice exposition of it in M. Kneser's [**Kne92**]. In [**Sie37**] Siegel gives a proof of his formula for the case of number fields. We prove a function field counterpart of this last result, and hence the ideas contained in it are also of help.
At the end, we explain some consequences of the Minkowski-Siegel formula, and a suggestion (of Prof. Stuhler) to derive this formula from the Lefschetz trace formula, as recently appeared in [**BD05**]. An interesting application is Theorem 4.5.2, which states that there are finitely many isomorphism classes of definite integral quadratic forms $\mathfrak{q}$ over global rings (of positive characteristic) with the following property: any one dimensional quadratic form represented by some form in the genus of $\mathfrak{q}$ is indeed represented by $\mathfrak{q}$. This result generalizes the analogue of Watson's result over $\mathbb{Z}$ (cf. [**Wat53**] and [**Wat76**]). In the function field case, and only for the special case of the ring $\mathbb{F}_q[T]$, this result was recently proved in [**CD05**].

Some words about the numeration used throughout. The thesis is divided, in this order, in chapters, sections, subsections, subsubsections and deeper logical units*. By abuse of terminology, I will call by* **section** *any section or deeper (subsection, subsubsection, paragraph). When refering to a section we use the numbering: Chapter.Section.Subsection.Subsubsection.Paragraph.Subparagraph (for example 2.3.4.2). The sections (and deeper) do not have "absolute coordinates" when declared (i.e.* **2.3 Hermite's theorem** *is subsection 3 of section 2, but there is no information about the chapter in the declaration). Similarly, the subparagraph:* [2.3.4] *Lattice reduction, is the fourth subparagraph of the third paragraph of the second subsection, but one cannot extract* from the declaration itself *the chapter and section to which it corresponds (other than directly from the text). The goal of this numeration, is to avoid nasty numberings such as: (1.3.2.3.4) Lattice reduction, as it would instead appear.*
This thesis was typeset with `smfbook.cls`.

Acknowledgement
I would like to thank my thesis supervisor, Prof. Dr. Ulrich Stuhler, for his suggestions, comments and corrections, and his support throughout these years. I thank also very much Prof. Dr. Yuri Tschinkel for his support from early days on. During my studies here in Göttingen I had the opportunity to receive much encouragement also from Prof. Dr. Samuel Patterson, Prof. Dr. Pilar Bayer (Barcelona, visiting Göttingen as Emmy-Noether-Professorin), Dr. Venkata Balaji, Prof. Dr. Jorge Morales (Louisiana), Prof. Dr. Preda Mihăilescu and specially from Prof. Dr. Gebhard Böckle (Duisburg-Essen). I thank Benoît Louvel for interesting discussions through these years, for his critical reading and listening of part of this thesis, and mostly for his friendship.

This work would not have been possible without the DAAD scholarship (Kennziffer A/01/17917), which supported me throughout and also the support of Mathematisches Institut at Göttingen and its *Graduiertenkolleg* "Groups and Geometry". I would also like to thank very much PD Dr. Hartje Kriete and Ms. Carmen Barann for their help and engagement in making possible for students from abroad to do research at the *Mathematisches Institut der Universität Göttingen.*

CHAPTER 1

QUADRATIC BUNDLES AND ORTHOGONAL GROUPS

In this chapter we collect basic definitions and elementary results to be used throughout the thesis, most of which is well known.

Some notation:

– $A^\times$ is the multiplicative subgroup of A, and $A^\vee$ is the dual (with A having the necessary structure).
– The star $\star$ will be used to denote an arbitrary/indeterminate charachter/word, which will be understood from the context.
– All schemes are taken in the sense of Grothendieck; i.e. *separated* pre-schemes.
– Unless otherwise stated, all rings will be supposed to be associative, commutative and with unit.

1. Valuations and Norms

Let R be a ring (which we suppose throughout to be associative, commutative and with unit), Γ_0 a totally ordered commutative group, written additively. We denote by $\Gamma := (\Gamma_0)_\infty$ the commutative monoid obtained by adjoining an extra element, ∞, to Γ. We define on Γ a commutative monoid law and a total order, by simply extending the given ones as follows.
For the monoid law, we define $x + y$ to be ∞ if any of the summands is ∞, otherwise the sum is already in $\Gamma_0 \subset \Gamma$. This gives a commutative monoid structure on Γ. The total order is extended by declaring $x < \infty$ for any $x \in \Gamma_0$. We can instead give an intrinsic construction, requiring Γ to be a totally ordered commutative monoid with a unique maximal element ∞, such that the induced monoid law on $\Gamma_0 := \Gamma \setminus \{\infty\}$ gives indeed a (commutative) group structure.

1.1. Valuations. — A **valuation on R with values in** Γ is a map $v : R \to \Gamma$ satisfying the following properties:

Val.1) $v(1_R) = 0$, $v(0) = +\infty$;
Val.2) $v(xy) = v(x) + v(y)$, $\forall x, y \in R$;
Val.3) $v(x + y) \geq \inf(v(x), v(y))$.

In the case, that R is an integral domain, there exists a unique valuation taking only the values 0 and ∞. This valuation is called the **trivial valuation**, and will be left out from our considerations.

Before we give some examples, let us introduce elementary concepts related to valuations on fields, in which we are mainly interested. Let K be a field, and v a valuation on it (with values in Γ). The subset

$$R := R(v) := \{x \in K \mid v(x) \geq 0\} \subset K,$$

is a subring, called the **valuation ring of** v, and

$$\mathfrak{M} := \mathfrak{M}(v) := \{x \in K \mid v(x) > 0\} \subset R,$$

is a maximal R-ideal, called the **(maximal) ideal associated with** v. The field $\kappa := \kappa(v) := R/\mathfrak{M}$ is the **residue field of** v. Finally, $\Gamma_v := v(K^\times)$ is a subgroup of Γ_0, called the **value group of** v.

Whenever we do not mention the group Γ_0, we assume it is the additive group of the rational integers $\mathbb{Z}$. In this case, the valuation of K is called **discrete** (cf. Remark 1.1.2); or equivalently, v is discrete when the valuation ring $R(v)$ is principal (see [**Bou98**, Chapter VI, page 392]).

Example 1.1.1. — (1) Let $K = \mathbb{F}_q$ be any finite field, and v a valuation on it. Then $v(x) = 0$ for any $0 \neq x \in K$, since $K^\times$ is a finite group ([**Wei95**, Lemma 1, page 2]) and $1_K \in K^\times$, for which $v(1_K) = 0$, by definition. So, v is the trivial valuation.

(2) If $K = \mathbb{Q}$, we can define for each (rational) prime number p a valuation as follows. For an integer $a \in \mathbb{Z}$ define $v_p(a)$ as the power of p appearing in the prime decomposition of a (it can be 0). Then we extend this to the rationals: $x = a/b \in \mathbb{Q}^\times$ by defining $v_p(x) := v_p(a) - v_p(b)$. This is a valuation, called the *p-adic valuation*.

(3) For the rational function field $K = \mathbb{F}_q(T)$, we proceed as for $\mathbb{Q}$. We take any irreducible polynomial $P \in \mathbb{F}_q[T]$, and define for the elements in the ring $\mathbb{F}_q[T]$ the *P-adic-valuation*. Since $\mathbb{F}_q[T]$ is a Dedekind (and Euclidean) ring, we can argue as before, by setting $v_P(Q)$ to be the highest power of P in the prime decomposition of $Q \in \mathbb{F}_q[T]$. This extends as before to a valuation in the function field $\mathbb{F}_q(T)$. One figures out what the valuation rings and residue fields are.

Remark 1.1.2. — For a given valuation v on K, one introduces the $\mathfrak{M}$-adic topology on R (see [**Bou98**, Chapter III]), induced from the basis of open sets of $0 \in R$ given by the powers $\mathfrak{M}^n$ of the maximal ideal $\mathfrak{M}$, for $n \in \mathbb{N}$. We say that any two valuations v and v' on K are **equivalent**, if the filtrations $\{\mathfrak{M}(v)\}$ and $\{\mathfrak{M}(v')\}$ define the same topology on R.

1.2. Ramification. — Let K'/K be a finite field extension, and v' be a valuation with values in Γ (not necessarily discrete, i.e. $v'((K')^\times)$ may not be isomorphic, as group, to $\mathbb{Z}$). Then the restriction $v' \mid_K$ gives a valuation on K. It is easy to see, that $R := R(v) = R' \cap K$, where $R' := R(v')$, so we have a group inclusion $\Gamma_v \subset \Gamma_{v'}$. The index $[\Gamma_{v'} : \Gamma_v]$ will be denoted by $e(v'/v)$ and called the **ramification index of** v' **over** v (it can be ∞). We have also, $\kappa(v) \subset \kappa(v')$, and hence we define the degree of this extension to be $f(v'/v)$, the **residue class degree**. In the case of number/function fields, these concepts coincide with the better known definitions of $e_{\mathfrak{P}}$ and $f_{\mathfrak{P}}$ (for $\mathfrak{P}$ a prime ideal *above*, i.e. in R'), using prime ideals and decompositions of ideals (cf. [**Has02**, Chapter 14]).[I]

1.3. Absolute values. — Let $\phi : K^\times \to \mathbb{R}_+^\times$ be a homomorphism of multiplicative groups which satisfies $\phi(x + y) \leq \phi(x) + \phi(y)$. Extend it by setting $\phi(0) := 0$. Such a map is called an **absolute value** on K.

An absolute value ϕ induces a topology on $K^\times$, namely the coarsest topology for which this map is continuous, or what is the same, the topology generated by the basis of open sets given by $\phi^{-1}(U)$, where U is any open interval in $\mathbb{R}_+^\times$. Two absolute values are said to be **equivalent**, if their induced topologies are the same.

Remark 1.1.3. — Two absolute values ϕ and ϕ' are equivalent if and only if $\phi(x) < 1 \Leftrightarrow \phi'(x) < 1 \; \forall x \in K^\times$ (see Bourbaki loc. cit.).

Example 1.1.4. — Suppose we have a valuation v on a field K. Pick a real number $0 < c < 1$. We can define an **absolute value (corresponding to v)** $\phi := \phi_v : K^\times \to \mathbb{R}_+^\times$ as $\phi(x) := c^{v(x)}$. Note that in this case ϕ satisfies the stronger inequality $\phi(x+y) \leq \min\{\phi(x), \phi(y)\}$; i.e. it is a **non-archimedian absolute value**, and its associated valuation is also called non-archimedian.

An equivalence class of absolute values is called a **place**, and when there is no confusion, we work with a representative absolute value (or valuation) in the class.

If ϕ is not non-archimedian, it is said to be **archimedian**, and the map given by $-\log_c(\phi(\star)) : K \to \mathbb{R}$ (any $0 < c < 1$) is called (by abuse of notation) an (archimedian) **valuation associated with** ϕ (though they are not valuations in the sense of section 1.1.1). Any two such archimedian valuations are **equivalent** if and only if their corresponding absolute values belong to the same place. The absolute value corresponding to the trivial valuation on K, is called the trivial absolute value.

We give now the classification of places for the fields in the example 1.1.1.

(1) For the first case, there is only one valuation, hence only one place.

(2) For $K = \mathbb{Q}$, the classification is due to Ostrowski, and besides the p-adic valuations (places) explained in example 1.1.1, there exists also the place corresponding to the valuation associated with the absolute value, say, $v(x) := -\log(|x|)$ (observe that this valuation is *not* discrete).

(3) In the function field case, besides the P-adic valuations given above, there is also one missing, namely the so called *valuation at infinity*, given by $v_\infty(Q/Q') := \deg(Q) - \deg(Q')$, where $Q, Q' \in \mathbb{F}_q[T]$ and deg is the degree of a polynomial in T.

Example 1.1.5. — The *ordinary absolute value* $|\cdot| : K^\times \to \mathbb{R}_+^\times$, where K is, say $\mathbb{Q}$, is an archimedian absolute value. The topology in $\mathbb{Q}$ induced by this absolute value, makes $\mathbb{Q}$ into a topological space, whose completion is $\mathbb{R}$. For the other valuations (places) of $\mathbb{Q}$, we define the *normalized p-adic absolute values* as: $|a/b|_p := (p^{-1})^{(v_p(a) - v_p(b))}$, for p a prime. Its completion, $\widehat{\mathbb{Q}}_{v_p}$, is the well known field of p-adic numbers, denoted usually by $\mathbb{Q}_p$ and introduced by Hensel in a more *analytical* context.
When K is the function field of a curve over a finite field $\mathbb{F}_q = \mathbb{F}_{p^r}$, all completions are isomorphic to $\mathbb{F}_q((\xi))$, for ξ a free parameter. In particular, all the characteristics of the residue fields of the completions are the same, p. On the contrary, in the number field case one has all possible characteristics appearing in the residue fields.

1.4. (Counting) Norms. — A **global ring** is the integral closure of either $\mathbb{Z}$ or $\mathbb{F}_q[T]$ in a finite algebraic extension of $\mathbb{Q}$, resp. $\mathbb{F}_q(T)$, the *rational function field* (of the curve $\mathbb{P}^1_{\mathbb{F}_q}$ over a finite field). The quotient field of a global ring is called a **global field**. Whenever no confusion is possible, we refer to a **function field**, meaning a global field of characteristic $p > 0$. In this section, R and K stand for a global ring and its quotient field, respectively.

In chapter 4 we count ideals of a global ring R with certain properties, for which we need a so called *counting norm* (similar to an absolute value, but) on $\mathrm{Pic}(R)$, the group of fractional R-ideals. This counting norm will be given by

$$\boldsymbol{N}(\mathfrak{a}) := [R : \mathfrak{a}] \tag{1.1.1}$$

on the R-ideals, and hence (canonically) extended to the whole $\mathrm{Pic}(R)$, to obtain the **counting norm** $\boldsymbol{N} : \mathrm{Pic}(R) \to \mathbb{R}_+^\times$; in chapter 4, by abuse of notation, also called the **absolute value** on R. The reason for this term, is that actually this function, corresponds to the classical absolute norm of an ideal of a number field, which is the absolute value of an integer.
In the function field case (i.e. R is the ring of (holomorphic) functions on a curve over a finite field with at worst poles supported on a finite fixed set of points, called points at infinity), the absolute norm of the ideal is not sufficient to *count* (since one gets polynomials instead of natural (=cardinal) numbers). In order to get a cardinal number, we take the unique valuation at infinity for $\mathbb{F}_q[T]$ (as in the example above), and take the composition:

(1.1.2)
$$\begin{array}{ccc} \mathrm{Pic}(R) & & \\ \Big\downarrow{\scriptstyle \boldsymbol{N}_{R/\mathbb{F}_q[T]}(\cdot)} & \searrow & \\ \mathrm{Pic}(\mathbb{F}_q[T]) & \xrightarrow{|\cdot|_\infty} & \mathbb{R}_+^\times. \end{array}$$

We can suppose $K = \mathrm{Quot}(R)$ to be separable over $K_0 := \mathbb{F}_q(T)$ (K is perfect), so the residue degrees of the primes in R depend only on the primes below (in R_0), and therefore $\boldsymbol{N}(\mathfrak{a}) = |\boldsymbol{N}_{R/R_0}(\mathfrak{a})|_\infty$ (cf. [**Ser68**, Prop. 10, page 26]).

Remark 1.1.6. — With this (counting) norm at hand, we can develop a form of abstract analytic number theory, in the sense of [**Kno75**], as explained in §4.5.3.

[4.1] *An idele version of the counting norm.* — We first introduce the *adeles* (also for later purposes) and then the adelic version of the counting norm.

[4.1.1] *Adele ring.* — Let $A_\lambda \subset B_\lambda$ be (topological) rings indexed by $\lambda \in \Lambda$. We define the **restricted product** of the family $\{A_\lambda \subset B_\lambda\}_{\lambda\in\Lambda}$ as the ring

$$\prod_{\lambda\in\Lambda}{}' \{A_\lambda, B_\lambda\} := \varinjlim_{S \text{ finite subset of } \Lambda} \prod_{\mu\in S} B_\mu \times \prod_{\lambda\in\Lambda\setminus S} A_\lambda,$$

whose topology is given by the inductive limit topology (see §3.2.1).

Given a global ring R, there are finitely many places such that the valuations restricted to R take negative values. These places are called *places at infinity* with respect to R, and the set of all them is denoted by S_∞, a subset of the set of all valuations on K: $\mathrm{Val}(K)$. We will suppose S_∞ contains all archimedian valuations (if they exist, clear).
Conversely, given any such finite set of valuations S_∞, one can recover the global ring R, with respect to which S_∞ is the set of valuations at infinity defined above.
We write R_v, K_v for the completions of R, resp. K with respect to a valuation v, and set $K_\infty := \prod_{v\in S_\infty} K_v$.

The **ring of adeles of K with respect to S_∞** is the (locally compact topological) ring

$$\mathbb{A}_K := K_\infty \times \prod_{v\in\mathrm{Val}(K)\setminus S_\infty}{}' \{R_v, K_v\},$$

where the last factor is the **ring of finite adeles of** K (with respect to S_∞), denoted by $\mathbb{A}_{\mathrm{f}}$.

[4.1.2] *Idele group.* — The **idele group of** K, $\mathbb{A}_K^\times$, is the multiplicative subgroup of $\mathbb{A}_K$ formed by all invertible adeles, and endowed with the coarsest topology (finer than the induced topology from the adeles) making the homomorphism $x \mapsto x^{-1}$ continuous (which, a priori, is not continuous on the adeles!). Hence, $\mathbb{A}_K^\times$ is a locally compact topological group (cf. [**Wei95**, Chapter IV]).

Let $\alpha = \{\alpha_v\}_{v\in|X|} \in \mathbb{A}_K^\times$ be an idele of K. There exists a surjective map $\mathbb{A}_K^\times \to \mathrm{Pic}(R)$, which sends the idele α to the ideal $\mathfrak{a} := \mathfrak{a}(\alpha) = \cap_{v\notin S_\infty}(K \cap \pi_v^{v(\alpha_v)} R_v)$ [**Wei95**, Ch. V, Theorem 3]. It is easy to compute the kernel of this projection, namely the stabilizer of R in the group of ideles, which is $\mathbb{A}_{S_\infty}^\times = \prod_{v\notin S_\infty} R_v^\times \times \prod_{v\in S_\infty} K_v^\times$. So, the sequence

$$1 \longrightarrow \mathbb{A}_{S_\infty}^\times \longrightarrow \mathbb{A}_K^\times \longrightarrow \mathrm{Pic}(R) \longrightarrow 0 \tag{1.1.3}$$

is exact.

[4.1.3] *Idele norms.* — For each non-archimedian place v on K, we normalize the corresponding absolute value $|\cdot|_v$ so, that $|\pi_v|_v = |\kappa(v)|$; for archimedian places, we choose the absolute value induced by the *standard* absolute value on $\mathbb{C}$. After these normalizations, we define the **idele norm** $|\cdot|_{\mathbb{A}_K} : \mathbb{A}_K^\times \to \mathbb{R}_+^\times$ by

$$|\{x_v\}|_{\mathbb{A}_K} := \prod_{v\in \mathrm{Val}(K)} |x_v|_v.$$

Remark 1.1.7. — The multiplicative group $K^\times$ is diagonally embedded in the idele group, and the norm restricted to it is the constant function 1 (this is the so called *product formula*, cf. [**Wei95**, Chapter IV, Theorem 5]).

Set $\psi : \mathbb{A}_K^\times \to \mathbb{R}_+^\times$ as $\psi(\{x_v\}) := \prod_{v\in \mathrm{Val}(K)\setminus S_\infty} |x_v|_v^{-1}$. This function is trivial on the kernel in the exact sequence (1.1.3), so it lifts to a function $\tilde{\psi} : \mathrm{Pic}(R) \to \mathbb{R}_+^\times$. From the Chinese remainder Theorem, this function coincides with the counting norm $\boldsymbol{N}$ defined in (1.1.1), and will be denoted by $\boldsymbol{N}$ (in chapter 4) or by $|\cdot|_\infty$ (in chapter 2).

2. Quadratic bundles and orthogonal groups

2.1. Quadratic spaces. — We summarize several basic notions. For details we refer to any book about quadratic forms back in the bibliography.

[1.0.1] Let K be any field of characteristic not 2, $\mathbb{V}$ an m dimensional K-vector space. The pair $(\mathfrak{b}, \mathbb{V})$ is called a **quadratic space**, for $\mathfrak{b}$ a symmetric bilinear K-form on $\mathbb{V}$: $\mathfrak{b} : \mathbb{V}\times\mathbb{V} \to K$. Moreover define $\mathfrak{q}_\mathfrak{b} :=: \mathfrak{q} : \mathbb{V} \to K$, by $v \mapsto 2^{-1}\mathfrak{b}(v,v)$. By abuse of notation we may denote by $\mathfrak{q}$ (by $\mathbb{V}$ or also by $\mathfrak{b}$) the quadratic space $(\mathfrak{b}, \mathbb{V})$.

[1.0.2] We write $(\tilde{\mathfrak{b}}, \tilde{\mathbb{V}}) := (\mathfrak{b}, \mathbb{V}) \perp (\mathfrak{b}', \mathbb{V}')$ for the quadratic space over the vector space $\tilde{\mathbb{V}} := \mathbb{V} \oplus \mathbb{V}'$ with bilinear form $\tilde{\mathfrak{b}}$ given by

$$\tilde{\mathfrak{b}}(x\oplus x', y\oplus y') := \mathfrak{b}(x,y) + \mathfrak{b}'(x',y').$$

In this case, one defines $(\mathfrak{b}, \mathbb{V})^\perp := (\mathfrak{b}', \mathbb{V}')$ as the orthogonal complement of $(\mathfrak{b}, \mathbb{V})$ inside $(\tilde{\mathfrak{b}}, \tilde{\mathbb{V}})$.
The **radical** of a quadratic space $(\mathfrak{b}, \mathbb{V})$ is the maximal K-vector subspace $\mathbb{V}_{\mathrm{rad}}$, such that $\mathfrak{b}(\mathbb{V}_{\mathrm{rad}}, \star) : \mathbb{V} \to K$ is the zero map; i.e. the orthogonal complement of $\mathbb{V}$ itself. A non-zero vector $v \in \mathbb{V}$ is called **isotropic** if $\mathfrak{q}(v)$ is zero. If $\mathbb{V}$ has an isotropic vector, then it is called an **isotropic** quadratic space, otherwise it is **anisotropic**.

[1.0.3] A quadratic space is called **non-degenerate** (**semi-simple** after Eichler) if its radical is $\{0\}$; otherwise it is **singular**. The **discriminant of a quadratic space** $\mathfrak{q}$ is $\Delta(\mathfrak{q}) := (-1)^{\frac{m(m-1)}{2}} 2^{-m} \det(\{a_{i,j}\}_{i,j=1}^{m})$, where $a_{i,j} := \mathfrak{b}(e_i, e_j)$, and $\{e_1, \dots, e_m\}$ is a basis of $\mathbb{V}$.
It is easy to see, that this quantity is non-zero only when the quadratic space is non-degenerate. For non-degenerate spaces, if one changes the basis, the discriminant changes by a square of $K^\times$. So, in any case, it is a well defined element of $K^\times/K^{\times 2} \cup \{0\}$ (to be seen as a commutative semi-group).

[1.0.4] A morphism between two quadratic spaces $(\mathfrak{b}, \mathbb{V})$ and $(\mathfrak{b}', \mathbb{V}')$ is a K-linear transformation ϕ from $\mathbb{V}$ to $\mathbb{V}'$, such that $\mathfrak{b}'(\phi(v), \phi(w)) = \lambda(\phi)\mathfrak{b}(v, w)$, for some $\lambda(\phi) \in K^\times$. These morphisms are called **similarity transformations**, and the corresponding factor λ is the **norm** of the transformation. A similarity transformation of norm 1 is an **orthogonal transformation** if it is an isomorphism of vector spaces; in which case the quadratic spaces are said to be **isomorphic** (or also **isometric**). The set of all orthogonal transformations of a quadratic space $\mathbb{V}$ into itself builds a group, $\mathrm{O}(\mathbb{V})$, called the **orthogonal group** of the quadratic space. The subgroup $\mathrm{SO}(\mathbb{V})$ of $\mathrm{O}(\mathbb{V})$ formed by those orthogonal transformations of determinant 1 is called the **special orthogonal group**.

[1.0.5] We close this subsection with a version of *Witt's famous Theorem*:

***Theorem 1.2.1* (Witt).** — *If S_1, S_2 are two isomorphic non-degenerate subspaces of a quadratic space $(\mathfrak{b}, \mathbb{V})$, then their orthogonal complements are also isomorphic.*

A direct consequence of this Theorem is the uniqueness of the factors (up to isometry) in the orthogonal decomposition of a non-degenerate quadratic space $\mathbb{V}$, as $\mathbb{V} \cong \mathbb{V}_0 \perp \mathcal{H}$, where $\mathcal{H}$ is a hyperbolic space (an odd dimensional regular quadratic space with associated diagonal matrix $\mathrm{diag}(1, \overset{d}{\dots}, 1, -1, \overset{d}{\dots}, -1)$) and $\mathbb{V}_0$ is anisotropic. The (well defined) number $\mathrm{ind}(\mathbb{V}) := d$ (i.e. half the dimension of $\mathcal{H}$) is called the **Witt index** and the anisotropic quadratic space $\mathbb{V}_0$ is the **type** of $\mathbb{V}$. For any two types $\mathbb{V}_0, \mathbb{W}_0$ we define $\mathbb{V}_0 \oplus \mathbb{W}_0 := (\mathbb{V}_0 \perp \mathbb{W}_0)_0$. This gives a group structure to the set of isomorphy classes of types over K, denoted by $\mathrm{W}(K)$, the **Witt group** of K. The identity element of this group is the class which corresponds to the zero quadratic space (which is also the class of any hyperbolic quadratic space). The Witt group can be endowed with a ring structure, considering tensor products of quadratic spaces.

2.2. Lattices, quadratic forms. — Before introducing quadratic forms in the language of algebraic geometry (§1.2.4), we recall the classical definitions, and then generalize them to schemes. In this first approach, we avoid the characteristic 2 case, because of its peculiarities, which need a special treatment. See [**Tit68**], for the general definition of a quadratic form, which stems originally from Klingenberg and Witt.

[2.0.1] Let R be any ($2 \in R^\times$) integral domain, and denote by K its quotient field. For a finitely generated (projective) R-module E, the base change $E \otimes_R K$ is a finite dimensional K-vector space. Moreover, if E is endowed with a symmetric bilinear form $\mathfrak{b}_R : E \otimes_R E \to R$ (with values in R), then the base change to the *generic fiber* produces a quadratic space $(\mathfrak{b}_R \otimes_R K, E \otimes_R K)$.
Suppose given any other finitely generated projective module E' with a bilinear R-form $\mathfrak{b}'_R$ on it. It may well happen, that the quadratic spaces $(\mathfrak{b}_R \otimes_R K, E \otimes_R K)$ and $(\mathfrak{b}'_R \otimes_R K, E' \otimes_R K)$ are isometric (see for example [**O'M00**] for a complete classification of quadratic spaces over local/global fields). When this is the case, the two modules E and E' can be thought to be inside the same quadratic space $(\mathfrak{b} := \mathfrak{b}_R \otimes_R K, \mathbb{V} := E \otimes_R K)$.

Definition 1.2.2. — Let $\mathbb{V}$ be a K-vector space. A finitely generated, projective R-submodule E of $\mathbb{V}$ is a **lattice** (with respect to (R, K)) if $E \otimes_R K = \mathbb{V}$.

The condition $E \otimes_R K = \mathbb{V}$ means just $\mathrm{rk}(E) = \dim_K(\mathbb{V})$.

Remark 1.2.3. — Suppose K is a (non-discrete) locally compact field (so called p-field in Weil's [**Wei95**] terminology). In this case, K is a local field with valuation, say v, and a lattice in a finite dimensional K-vector space $\mathbb{V}$ is an $R(v)$-module $L \subset \mathbb{V}$, such that $L \otimes_{R(v)} K = \mathbb{V}$. Topologically, we can define a lattice, as an open $R(v)$-module L in $\mathbb{V}$, which does not contain any sub-vector space other than 0 (cf. [**Wei95**, page 29]).

[2.0.2] We are interested in the study of lattices inside quadratic spaces. Two lattices E_1 and E_2 in a quadratic space $(\mathfrak{b}, \mathbb{V})$ are said to be in the same **(integral) class**, if there exists an orthogonal transformation $u \in \mathrm{O}(\mathbb{V})$, such that $u(E_1) = E_2$. If a similarity transformation u fulfills $u(E_1) = E_2$, we say that E_1 and E_2 are **similar**, and u is a **similarity between E_1 and E_2**. In the case $E := E_1 = E_2$ the similarity transformations are called **units of** E or **automorphisms**. The group of automorphisms will be denoted by $\mathrm{O}(E)$ $(\subset \mathrm{GL}(\mathbb{V}))$.

[2.0.3] For E a lattice in a quadratic space $(\mathfrak{b}, \mathbb{V})$ with respect to $(R, K := \mathrm{Quot}(R))$, we have a map $\mathfrak{q} : E \to \mathfrak{a}$ given by $v \mapsto 2^{-1}\mathfrak{b}(v, v)$, where $\mathfrak{a}$ is the R-ideal (inside K) generated by the values of $\mathfrak{q}$. More generally,

Definition 1.2.4. — Let R be any ring with $2 \in R^\times$, and let E and $\mathfrak{a}$ be projective modules of rank m and 1 respectively. A **quadratic form on E with values in $\mathfrak{a}$**, denoted by $(\mathfrak{q}, E, \mathfrak{a})$, is a map $\mathfrak{q} : E \to \mathfrak{a}$, such that:

QF1) $\mathfrak{q}(\lambda m) = \lambda^2 \mathfrak{q}(m)$, for any $\lambda \in R,\ m \in E$,
QF2) $\mathfrak{b}(m, m') := \mathfrak{q}(m + m') - \mathfrak{q}(m) - \mathfrak{q}(m')$ is R-bilinear.

When $\mathfrak{a} = R$, the quadratic form is called **integral**, for which we simply write $(\mathfrak{q}, E)$.

Conversely, to any symmetric bilinear form $\mathfrak{b}(\cdot,\cdot)$ one can associate a quadratic form $\mathfrak{q}(\cdot)$ given by the equation $2\mathfrak{q}(v) = \mathfrak{b}(v, v)$. So, quadratic forms and symmetric bilinear coincide (for rings with the assumption above). The nice property of the latter, is that their construction is *linear*, hence can be translated into geometry. Therefore, a quadratic form is a symmetric R-linear map $\mathfrak{b} : E \otimes_R E \to \mathfrak{a}$, or equivalently an element of $(\mathrm{Sym}^2_R(E))^* \otimes_R \mathfrak{a}$.

The main problem in the theory of lattices, is the determination of a complete set of invariants for the classes: when may we find an orthogonal transformation u such that $u(E_1) = E_2$? This problem will be referred to, as the *integral classification of quadratic forms*.
It is still unsolved for global rings, and a complete solution for local rings is given in [**O'M00**].

[2.0.4] *Regularity (for lattices).* — From the symmetric R-linear map $\mathfrak{b}$ we obtain the **adjoint map** (cf. section 1.2.4.1) $\mathfrak{b}^* : E \to E^* \otimes \mathfrak{a}$. When this map is an injective homomorphism of R-modules, we say that the quadratic form is **non-degenerate**, if it is moreover bijective, the form will be called **regular**. The quadratic form is said to be **degenerate** if the adjoint is not injective. A non regular quadratic form will be called **singular**[(1)].

[(1)] This may be different from some other references.

Remark 1.2.5. — From the definitions above, a regular quadratic form is also non-degenerate, but it is not *singular*.

[2.0.5] *Discriminant, reduced determinant.* — Let $\mathfrak{q} = (\mathfrak{q}, E, \mathfrak{a})$ be a quadratic form over R (cf. Definition 1.2.4), with $m := \mathrm{rk}(E)$. The **norm** of $\mathfrak{q}$, $\mathfrak{n}(\mathfrak{q})$, is the R-submodule of $\mathfrak{a}$ generated by the image of the associated bilinear form $\mathfrak{b} := \mathfrak{b}_{\mathfrak{q}}$.
For any set of generators of E, resp. of $E^* \otimes \mathfrak{a}$, we have an associated matrix for the adjoint map (maybe not a $m \times m$-matrix, not even square!). This matrix is said to *represent* $\mathfrak{q}$.
We define the **(ideal) discriminant** of $\mathfrak{q}$ as the ideal generated by the $m \times m$ minors of all matrices representing $\mathfrak{b}$. Again, this determines an element of $\mathrm{Pic}(R)$ (see [**Bou98**, Chapter II, §5.6]).

Remark 1.2.6. — In cohomological terms, for a regular integral quadratic form $(\mathfrak{q}, E)$, one defines as usual a 1-cocycle $\xi(\mathfrak{q}) \in \mathrm{H}^1_{\mathrm{fppf}}(R, \boldsymbol{\mu}_2)$, via the isomorphism $\det(E)^{\otimes 2} \cong R$ (cf. [**Knu91**, Chapter III]). By using

$$1 \longrightarrow \boldsymbol{\mu}_2 \xrightarrow{\iota} \mathbb{G}_m \xrightarrow{\wedge 2} \mathbb{G}_m \longrightarrow 1,$$

we get (as $2 \in R^\times$ this sequence is exact in the étale site)

$$1 \to \Gamma(\mathrm{Spec}(R), R^\times / {R^\times}^2) \to \mathrm{H}^1_{\text{ét}}(R, \boldsymbol{\mu}_2) \xrightarrow{\iota_\star} \mathrm{H}^1_{\text{ét}}(R, \mathbb{G}_m) \cong \mathrm{Pic}(R).$$

Therefore, $\iota_\star \xi(\mathfrak{q})$ is an element of $\mathrm{Pic}(R)$, namely the discriminant ideal we have just defined.

Definition 1.2.7. — The **reduced determinant of** $\mathfrak{q}$ is

$$\mathfrak{d}(\mathfrak{q}) := \mathrm{discr}(\mathfrak{q}) \otimes \mathfrak{n}(\mathfrak{q})^{\otimes(-\mathrm{rk}(E))}.$$

Remark 1.2.8. — The idea behind this *decomposition* of the discriminant, in the end, is to *stratify* the quadratic forms, where in each stratum, the forms *behave* like unimodular quadratic forms, hence, loosely speaking, reducing the study of quadratic forms, to the study of the unimodular ones.[IV]

[2.1] *Quadratic forms over local rings.* — Let K be a non discrete locally compact local field ($\mathrm{char}(K) \neq 2$ as always). Denote by R the valuation ring, by π a uniformizer, $\mathfrak{p} := \pi R$, and by k the residue field (which is finite, since K is locally compact).

[2.1.1] Let $\mathfrak{q} : E \to \mathfrak{a}$ be a quadratic form. In this case, the norm of $\mathfrak{q}$ is the ideal $\mathfrak{n}(\mathfrak{q}) := \mathfrak{m}^\delta$, where $\delta := \inf_{e \in E \setminus \{0\}} \{v(\mathfrak{q}(e))\}$. All projective R-modules are free, so we can take a basis of E and of $\mathfrak{a} = aR$, and write the associated matrix. We easily obtain $\mathrm{discr}(\mathfrak{q})$ and hence $\mathfrak{d}(\mathfrak{q})$.

[2.1.2] A lattice $E \subset \mathbb{V}$ is called **maximal**, if there does not exist another lattice E' containing E, with $\mathfrak{n}(E) = \mathfrak{n}(E')$. It is easy to see, that if the reduced determinant of E is either R or $\mathfrak{m}$, then E is maximal (a strictly bigger lattice of the same norm implies $\mathfrak{m}^2 \mid \mathfrak{d}(E)$).

To illustrate the meaning of the norm of a quadratic form, we recall the (local) classification of maximal anisotropic lattices of rank 3 (see [**Eic73**, II.9, page 54] for the proof) and some elementary examples.

Let E be a *maximal* lattice of norm π^l inside an anisotropic quadratic space $(\mathfrak{q}, \mathbb{V})$ of dimension 3. Then

$$(\mathfrak{q}, E) \cong \begin{cases} \langle \pi^{l+1} \epsilon \rangle \perp \pi^l \boldsymbol{N}_{F/K}, & \text{or} \\ \langle \pi^l \epsilon \rangle \perp \pi^{l+1} \boldsymbol{N}_{F/K}; \end{cases}$$

where F is the unramified quadratic extension of K with relative norm $\boldsymbol{N}_{F/K}$, and ϵ is a unit, uniquely determined up to squares of units.

Example 1.2.9. — We set $E = R^m$, the standard lattice in the vector space K^m, so we are able to write a symmetric matrix $M_{\mathfrak{q}}$ with respect to the standard basis of $E = R^m$ for a quadratic form $\mathfrak{q}$.

(1) In the one dimensional case, for the symmetric matrix $M_{\mathfrak{q}} = [\pi^e]$, we have $\mathfrak{n}(\mathfrak{q}) = \langle \pi^e \rangle = \mathrm{discr}(\mathfrak{q})$, so $\mathfrak{d}(\mathfrak{q}) = R$.

(2) Let $M_{\mathfrak{q}} = \begin{bmatrix} \pi & 0 \\ 0 & \pi^2 \end{bmatrix}$, we have $\mathfrak{n}(\mathfrak{q}) = \langle \pi \rangle$, $\mathrm{discr}(\mathfrak{q}) = \langle \pi^3 \rangle$ and $\mathfrak{d} = \langle \pi \rangle$.

(3) if $M_{\mathfrak{q}} = \begin{bmatrix} 1 & \pi^{-1} \\ \pi^{-1} & 1 \end{bmatrix}$, then $\mathfrak{n}(\mathfrak{q}) = \langle \pi^{-1} \rangle$, $\mathrm{discr}(\mathfrak{q}) = \langle 1 - \pi^{-2} \rangle$ and $\mathfrak{d}(\mathfrak{q}) = \langle 1 - \pi^2 \rangle$.

[2.1.3] It is easy to prove, that every lattice E decomposes as the orthogonal sum of 1-dimensional lattices (and maybe also 2-dimensional factors if $\mathrm{char}(R) = 2$):

$$E = E_1 \perp \ldots \perp E_m;\ \mathrm{rk}(E_i) = 1.$$

[2.1.4] A fundamental property of quadratic lattices over complete local fields is

Theorem 1.2.10. — [**Eic73**, §9, Satz 9.5] *Let L, M be two maximal lattices in a fixed quadratic space $\mathbb{V}$ of Witt-index ι. Then there exists an orthogonal R-basis $\{e_1, \ldots, e_r\}$ of L, and integers $f_1, \ldots, f_r$, such that*

$$\{\pi^{f_1} e_1, \ldots, \pi^{f_\iota} e_\iota, \pi^{f_{\iota+1}} e_{\iota+1}, \ldots, \pi^{f_{r-\iota}} e_{r-\iota}, \pi^{-f_1} e_{r-\iota+1}, \ldots, \pi^{-f_\iota} e_r\}$$

is an orthogonal R-basis for M. The norm of the anisotropic parts are $\pi^{\epsilon_L}\mathfrak{n}(L)$ and $\pi^{\epsilon_M}\mathfrak{n}(M)$, respectively, for non-negative exponents $\epsilon_L, \epsilon_M \in \mathbb{N}_0$.

The uniquely determined (up to permutation) exponents $\{f_l\}_{l=1}^r$ are called the **invariant factors of M in L.**

[2.1.5] The following version of Hensel's Lemma given by Kneser [**Kne92**, Satz 15.3] is a very powerful one. It gives, in particular, the cardinality of the possible liftings of orthogonal transformations defined over the ring $\mathbb{R}/\mathfrak{p}^n$ to orthogonal transformations over $R/\mathfrak{p}^{n+1}$ (cf. loc. cit.), which gives in certain sense (see chapter 4) the local densities of the quadratic forms over local fields. .
Let $\mathbb{V}, \mathbb{V}'$ be two quadratic spaces (with forms $\mathfrak{b}$, resp. $\mathfrak{b}'$), E a lattice in $\mathbb{V}$ and G a finitely generated R-submodule of $\mathbb{V}'$, and $u : E \to \mathbb{V}'$ an R-linear map. Denote by $\phi_u : \mathbb{V}' \to E^*$ the map: $y \mapsto \phi_u(y) : x \mapsto \mathfrak{b}'(ux, y)$.

Lemma 1.2.11 **(Kneser's Hensel)**. — *With the notation just introduced, suppose there is $k \in \mathbb{N}$ with:*

(1) $E^* = \phi_u(G) + \mathfrak{p}E^*$, $\mathfrak{p}^k\mathfrak{q}'(G) \subset \mathfrak{p}$,
(2) $\mathfrak{q}'(ux) \equiv \mathfrak{q}(x) \pmod{\mathfrak{p}^k}$.

Then, there exists a linear map $\tilde{u} : E \to \mathbb{V}'$, such that

(1) $\tilde{u}x \equiv ux \pmod{\mathfrak{p}^k G}$,
(2) $\mathfrak{q}'(\tilde{u}x) \equiv \mathfrak{q}(x) \pmod{\mathfrak{p}^{k+1}}$.

The importance of this result lies in the fact, that when the ring R is *complete*, by iterating this Lemma one gets an *orthogonal extension* of u. Namely,

Theorem 1.2.12. — *With assumptions of Lemma 1.2.11, and R a complete valuation ring; there exists an isometry $\tilde{u} : E \to \mathbb{V}'$, such that $\tilde{u}x \equiv ux \pmod{\mathfrak{p}^k G}$.*

[2.2] *Quadratic forms over global rings.* — Chapter 2 deals in detail with these quadratic forms, so in this section we only state a few general facts.
Let R be now a global ring and K its quotient field. For a lattice E in a quadratic space $\mathbb{V}$ over K, we have

$$\mathfrak{n}(E) = \prod_{v \in |\mathrm{Spec}(R)|} \mathfrak{n}(E_v),$$
$$\mathfrak{d}(E) = \prod_{v \in |\mathrm{Spec}(R)|} \mathfrak{d}(E_v).$$

The standard technique to work with in this case, is the well known local to global principle. For example: if we define a lattice M inside $\mathbb{V}$ to be **maximal**, when there is no lattice $E \supset M$ (different from M) with the same norm; then M is maximal if and only if M_v is maximal in the quadratic space $\mathbb{V}_v$ over the complete local field K_v, for all $v \in |\mathrm{Spec}(R)|$.

[2.2.1] *Structure Theorem for projective modules over Dedekind domains.* —

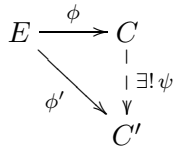
Theorem 1.2.13 **([Bou98**, Chapter VII, §4.10]**).** — *Let M be a finitely generated projective module of rank m over a Dedekind domain R. Then, there exists a unique non-zero R-ideal $\mathfrak{m}$, such that $M \cong R^{m-1} \oplus \mathfrak{m}$.*

The divisor class of $\mathfrak{m}$ is called, by abuse of notation, the **divisor class** of M (which is clearly unique, since $\mathfrak{m} = \det(M) := \wedge^{\mathrm{rk}(M)} M$). Hence, this result tells us that the isomorphy class of finitely generated projective modules is simply given by the *rank* and the *divisor class*.

[2.2.2] *Genus theory.* — One of the basic and most important concepts in the global case, is the *genus theory*, whose aim is to *make clear* the obstruction to the passage from local to global. We refer to section 3.3.

2.3. Clifford-Algebras, Spinor- norm and group. —

[3.1] *The Clifford algebra.* — The idea of constructing the *Clifford algebra of a quadratic form*, relies on the *wish* of taking square roots of the values of a quadratic form. With this in mind, we define a universal *square root* problem for a quadratic form.
Given an integral quadratic form $(\mathfrak{q}, E)$, we look for a unital (i.e. with unit) associative R-algebra C, together with an R-module homomorphism $\phi : E \to C$, such that $\phi(v) \cdot \phi(w) + \phi(w) \cdot \phi(v) = \mathfrak{b}(v, w) \cdot 1_C$, for any v, w in E; where $\cdot$ denotes the product in the algebra C. In particular, for $v = w$, $\mathfrak{q}(v) \cdot 1_C = \phi(v)^2$. The algebra C should moreover fulfill the following universal property: for any other pair (C', ϕ'), with the same properties as (C, ϕ) above, there exists a unique algebra homomorphism $\psi : C \to C'$, such that



commutes. It is well known, that there exists such a universal object, and is therefore unique up to isomorphism ([**Bou59**]), which we denote by $C(E)$ and call the **Clifford algebra** of E.

Remark 1.2.14. — For non integral quadratic bundles $(\mathfrak{q}, E, \mathfrak{a})$ there exists the notion of a Clifford algebra introduced in [**BK94**], which we are not going to use.

Remark 1.2.15. — We refer to [**Bou59**] for the following basic facts.

(1) If $\mathfrak{q} = 0$, then $C(E)$ is just the exterior algebra of E, $\wedge(E)$.
(2) The algebra morphism ϕ is injective.
(3) If E is free, $C(E)$ is a free R-module generated by the products of the form $v_{i_1} \cdot \ldots \cdot v_{i_k}$, for $0 \leq k \leq m$, where $\{v_1, \ldots, v_m\}$ is an R-basis for E (we write $v \cdot w$ for $\phi(v) \cdot \phi(w)$, to simplify notation). Hence, $\dim_R(C(E)) = 2^m$.

The Clifford algebra can be given as a quotient of the tensor algebra $\boldsymbol{T}(E)$ of E, by the two sided ideal generated by the elements of the form $v \otimes v - \mathfrak{q}(v) \cdot 1_{C(E)}$, for all $v \in E$. This algebra possesses a natural $\mathbb{Z}/2\mathbb{Z}$-grading, given by the elements which are linear combinations of products of an odd (even) number of v's. The even part, $C_0(E)$ is still an algebra: the **even Clifford algebra** of E (the odd part has structure of $C_0(E)$-module). The rank of the Clifford algebra (of the even Clifford algebra) is 2^m (2^{m-1}).

[3.2] *The Spinor Norm.* — Define

$$OC(E) := \{\alpha \in C(E)^\times \mid \mathrm{Int}(\alpha)(E) = E\},$$

where $\mathrm{Int}(\alpha)(x) := (-1)^{\deg(\alpha)\deg(x)}\alpha^{-1}x\alpha$, and deg is the function which corresponds to the grading of $C(E)$ (recall the identification of E with $\phi(E) \subset C(E)$). Set also, $OC_0(E) := OC(E) \cap C_0(E)$.
Let $\pi : OC(E) \to O(E)$ the group homomorphism, which sends α to $\mathrm{Int}(\alpha)$. This group homomorphism is a link between *arithmetic* (of algebras) and *geometry* (of the orthogonal group). On the arithmetic side, one has a canonical involution $^-$ defined on the Clifford algebra, given by $\overline{v \cdot w} = w \cdot v$, where v, w are any two degree 1 elements of $C(E)$. This action can be extended to the whole algebra, and gives an involution, which acts trivially on (the image of) E. With it, one can as usual define a norm map $\boldsymbol{N}_C : OC(E) \to R^\times$, which sends v to $\boldsymbol{N}_C(v) := v\bar{v} \in R^\times$.

One would like to define a norm on the side of the orthogonal group. If for example R is a field, every orthogonal transformation can be written as a product of reflexions and we obtain a well defined map $\mathrm{SN} : \mathrm{O}(E) \to R^\times/R^{\times 2}$ (the target is $R^\times/R^{\times 2}$ due to the definition of the homomorphism π); but this is not the generic picture. In order to overcome this situation, we briefly sketch Bass' approach ([**Bas74**]), which constructs a norm on $\mathrm{O}(E)$, for any *regular* E over a commutative ring R.

Let $\mathcal{A} := \mathrm{Aut}_{\text{Gr-Alg}}(C(E))$ be the group of algebra automorphisms of $C(E)$ which preserve degree, and let α be in this group. We define ${}_\alpha C(E)$ as the $C(E) \otimes C(E)^{\mathrm{op}}$-graded algebra $C(E)$ itself with twisted multiplicative structure given by $(a \otimes b) \cdot x := \alpha(a)xb$. Set $L_\alpha := \mathrm{Hom}_{\text{Gr-Alg}}(C(E), {}_\alpha C(E))$, where again $\mathrm{Hom}_{\text{Gr-Alg}}$ stands for the algebra homomorphisms which preserve the grading of the algebras.

Theorem 1.2.16 **(Bass)**. — *There exists a canonically defined isomorphism $\iota_\alpha : L_\alpha \otimes L_\alpha \cong R$.*

Therefore, the pair $\{L_\alpha, \iota_\alpha\}$ is a *discriminant bundle*; i.e. a cocycle in $\mathrm{H}^1_{\mathrm{fppf}}(R, \boldsymbol{\mu}_2)$ (which is $R^\times/R^{\times 2}$ when R is a field). Since $\mathrm{O}(E)$ can be identified with the subgroup $\{u \in \mathcal{A} \mid u(E) = E\}$ (cf. [**Bas74**]), we have a map:

$$\mathrm{SN} : \mathrm{O}(E) \to \mathrm{H}^1_{\mathrm{fppf}}(R, \boldsymbol{\mu}_2),$$

which is in fact a homomorphism of (abelian) groups. This map extends the norm on the Clifford algebra, and therefore, is a correct generalization of the classical spinor norm (cf. (1.2.3.2.1)).

[3.2.1] *Spinor group.* — The **Spinor group** associated with E is

$$\mathrm{Spin}(E) := OC_0(E) \cap \mathrm{Ker}(\boldsymbol{N}_C).$$

Denoting by $\mathrm{O}^+(E)$ the group image $\pi(OC_0(E)) \subset \mathrm{O}(E)$, we may summarize the definitions and facts of this section in the following two diagrams:

$$\begin{array}{ccc} \mathrm{O}(E) & \xrightarrow{\mathrm{SN}} & \mathrm{H}^1_{\mathrm{fppf}}(\mathrm{Spec}(R), \boldsymbol{\mu}_2) \\ \uparrow{\scriptstyle \pi} & & \uparrow \\ OC(E) & \xrightarrow{\boldsymbol{N}} & R^\times/R^{\times 2} \end{array};$$

$$1 \to \boldsymbol{\mu}_2(R) \to \mathrm{Spin}(E) \xrightarrow{\pi} \mathrm{O}^+(E) \xrightarrow{\mathrm{SN}} \mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(R), \boldsymbol{\mu}_2);$$

where the first commutes, and the second is an exact sequence.

[3.3] *An application.* — We will now show, with help of the (even) Clifford algebra, how to compute the Bruhat-Tits building of the special orthogonal group of a non-degenerate, isotropic ternary quadratic form $(\mathfrak{q}, \mathbb{V})$ over a local field K. We refer to [**Ron89**] for basic definitions on buildings.

[3.3.1] As we saw above, the even Clifford algebra $C_0(\mathbb{V})$ is a rank 4 algebra over K, and its associated norm is clearly isotropic, since the quadratic form $\mathfrak{q}$ is isotropic. Therefore, $C_0(\mathbb{V})$ is isomorphic to the matrix algebra $M_2(K)$. Since all automorphisms are inner (Skolem-Noether), $OC_0(\mathbb{V}) = C_0(\mathbb{V})^\times$, and hence

$$\mathrm{PGL}_2(K) = C_0(\mathbb{V})^\times/K^\times = OC_0(\mathbb{V})/K^\times \xrightarrow{\cong} \mathrm{SO}(\mathbb{V}). \tag{1.2.1}$$

More explicitly, if the quadratic form with respect to a suitable basis $\{e_1, e_2, e_3\}$ is $\mathbb{H} \perp a_3$, then the isomorphism of algebras sends the basis of $C_0(\mathbb{V})$, $\{1, e_1 \cdot e_2, e_1 \cdot e_3, e_2 \cdot e_3\}$, to

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -a_3 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & a_3 \\ 1 & 0 \end{bmatrix} \right\}.$$

[3.3.2] Let K now be a complete local field (see section 1.2.2.1 for notation). With isomorphism (1.2.1), the Bruhat-Tits building $\mathcal{X} := \mathcal{X}(\mathrm{SO}(\mathfrak{q}, \mathbb{V}))$ of $\mathrm{SO}(\mathbb{V})$ is simply the affine building of $\mathrm{PGL}_2(K)$, which has a down-to-earth interpretation. Namely, the simplicial complex $\mathcal{X}$ has as vertices, the classes of lattices $L \subset K^2$, where $L_1 \sim L_2 \Leftrightarrow \exists \lambda \in K^\times : L_1 = \lambda L_2$. Since the dimension of the algebraic group $\mathrm{PGL}_2(K)$ is 3 and its K-rank is 1, it follows that the simplicial complex $\mathcal{X}$ is one dimensional. The one simplices are given by flags of R-lattices

$$L_0 \supsetneq L_1 \supsetneq \pi L_0 (\equiv L_0 \pmod{\sim});$$

which after fixing a basis, and recalling the elementary divisor Theorem (a weaker version of Theorem 1.2.10) can be explicitly described. With this, one obtains a complete explicit description of this Bruhat-Tits building.

[3.3.3] When $(\mathfrak{q}, \mathbb{V})$ is anisotropic, we make base change to a quadratic extension K' of K (where we denote by σ the non-trivial automorphism of K' which fixes K) where it is isotropic. There we compute the Bruhat-Tits building for $(\mathfrak{q}, \mathbb{V}) \otimes_K K'$. Then the Bruhat-Tits building of $(\mathfrak{q}, \mathbb{V})$ is simply the set of invariants under the action of σ.

Remark 1.2.17. — The construction of the Bruhat-Tits building above depends on the chosen isomorphism (1.2.1). See [**SP79**] for a direct construction.

2.4. Quadratic bundles. — Let X be a scheme. There exists a one-to-one correspondence between the isomorphism classes of vector bundles on X of rank m, and locally free sheaves of constant rank m ([**EGAII**, §1.7]), given by:

$$\mathcal{E} \mapsto \mathbb{V}(\mathcal{E}) := \mathbf{E} := \mathrm{Spec}(\mathrm{Sym}(\mathcal{E})),$$

and conversely for a vector bundle $\mathbf{V}_X$ over X it associates $\Gamma(\cdot, \mathbf{V}_X)^*$.
We can therefore (and will) interchange *the notation*, whenever it will cause no confusion, vector bundles and locally free sheaves of finite constant rank.
There is also a projective version of $\mathbb{V}(\mathcal{E})$ for $\mathrm{rk}(\mathcal{E}) \geq 2$: $\mathbb{P}(\mathcal{E}) := \mathrm{Proj}(\mathrm{Sym}(\mathcal{E}))$. This is a projective bundle of rank $\mathrm{rk}(\mathcal{E}) - 1$ over X. This functor $\mathbb{P}(\cdot)$, is almost faithful: $\mathbb{P}(\mathcal{E}') \cong \mathbb{P}(\mathcal{E})$ if and only if there exists a line bundle $\mathcal{L}$ on X, such that $\mathcal{E} \cong \mathcal{E}' \otimes \mathcal{L}$.

[4.0.1] Let $\mathcal{E}$ ($\mathbf{E}$) and $\mathcal{L}$ ($\mathbf{L}$) be vector bundles over an S-scheme X of rank m and 1 respectively. As in the affine picture above, we suppose that $2 \in \mathcal{O}_X^\times$.

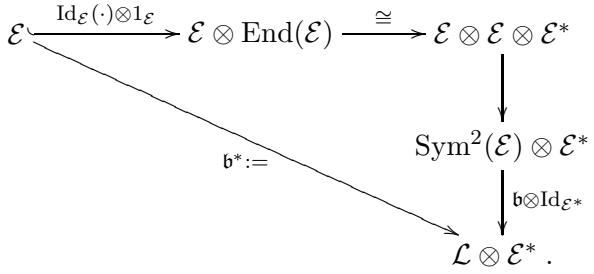
Definition 1.2.18. — A **quadratic form on $\mathcal{E}$ with values in $\mathcal{L}$ (over X)** is a section $\mathfrak{b}$ of $(\mathrm{Sym}^2_{\mathcal{O}_X}(\mathcal{E}))^* \otimes_{\mathcal{O}_X} \mathcal{L}$.

Hence, a quadratic form on X consists of a triple $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$, where

$$\mathfrak{b} \in \Gamma(X, (\mathrm{Sym}^2_{\mathcal{O}_X}(\mathcal{E}))^* \otimes_{\mathcal{O}_X} \mathcal{L}).$$

This triple will be also called a **quadratic bundle**, and it may be written by abuse of notation, as $\mathfrak{q}$ or $\mathcal{E}$. If $\mathcal{L} = \mathcal{O}_X$, the quadratic form is said to be **integral** and $\mathcal{L}$ may be omitted in the triple.

[4.1] *Regularity.* — Given such a quadratic bundle, we define the **adjoint map** $\mathfrak{b}^* : \mathcal{E} \to \mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{E}^*$ as in the following diagram:



One can easily check by trivializing the bundles, that as in the classical case,

Lemma 1.2.19. — *Locally, the morphism $\mathfrak{b}^*$ is such, that $\mathfrak{b}^*(v) = \mathfrak{b}(v, \cdot) \in \mathcal{L} \otimes \mathcal{E}^*$, for local sections v of $\mathcal{E}$.*

Denote by $\mathcal{K}_\mathfrak{q}$ the sheaf defined by the kernel of $\mathfrak{b}^*$, whose support is the Cartier divisor $\mathrm{supp}(\mathcal{K}_\mathfrak{q})$.

Definition 1.2.20. — A quadratic bundle $\mathfrak{q} = (\mathfrak{q}, \mathcal{E}, \mathcal{L})$ over X is called ***s*-degenerate in codimension** c ($s, c \in \mathbb{N}_0$) if and only if the local ranks of $\mathcal{K}_\mathfrak{q}$ are at most s, and the divisor $\mathrm{supp}(\mathcal{K}_\mathfrak{q})$ is supported in codimensions greater than c. $\mathfrak{q}$ is called **degenerate in codimension** c (**non-degenerate**) if it is $\mathrm{rk}(\mathcal{E})$-degenerate in codimension c (0-degenerate in codimension $\dim(X)$).
Finally, $\mathfrak{q}$ is **regular** if and only if $\mathfrak{b}^*$ is a sheaf isomorphism; **singular** if and only if $\mathfrak{q}$ is not regular; and **degenerate** if and only if $\mathfrak{q}$ is not non-degenerate.

For our purposes, we should just keep in mind

$$\mathfrak{q} \text{ is non-degenerate} \iff \mathfrak{b}^* \text{ is injective.}$$

Remark/Example 1.2.21. — In the case X is an integral, geometrically smooth and irreducible curve over a finite field, we have only two possible codimensions, so either degenerate in codimension 1 or 0.

– The first corresponds to the classically known *non-degenerate quadratic forms. These are the forms we are interested in!*

– The latter corresponds to degenerate quadratic forms, which actually (besides the zero form) are non-degenerate on a "big" Zariski open subset of X, but fail to be everywhere non-degenerate.

Nevertheless, it is for higher dimensional schemes, that the Definition 1.2.20 can be of much help. It can be interpreted as a stratification of the singular locus of the "space" of quadratic bundles of a given rank over X.[IIa]

[4.2] *Discriminant and reduced determinant.* — They can be given locally as for quadratic forms (cf. 1.2.2.0.5).

[4.3] *Notational convention.* — Let $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$ be a quadratic bundle over a regular scheme X, and let Y be an irreducible, codimension 1 subscheme of X, such that the local ring $\mathcal{O}_{X,Y}$ is a discrete valuation ring with maximal ideal $\mathfrak{m}$ and local uniformizer $\pi := \pi_Y$ (given locally, as a section of *certain* sheaf: $\mathcal{K}^\times/\mathcal{O}_X^\times$; [**Har97**, Chapter II.6, page 141]). Denote by $\widehat{\mathcal{O}}_{X,Y}$ the completion of $\mathcal{O}_{X,Y}$ with respect to the valuation v associated with π; let $\widehat{\mathcal{O}}_{X,Y,(0)}$ be its quotient field. Therefore, after base change to the completed ring (field), we get an $\widehat{\mathcal{O}}_{X,Y}$-lattice ($\widehat{\mathcal{O}}_{X,Y,(0)}$-quadratic space) endowed with the corresponding base changed quadratic form. We denote the resulting lattice (quadratic space) by $(\widehat{\mathfrak{q}}_Y, \widehat{\mathcal{E}}_Y, \widehat{\mathcal{L}}_Y)$ (resp. $(\widehat{\mathfrak{q}}_{Y,(0)}, \widehat{\mathcal{E}}_{Y,(0)}, \widehat{\mathcal{L}}_{Y,(0)})$).
In chapter 3 and thereafter, we will prescind from the hat to denote completions; that is, $\star_v$ will denote $\hat{\star}_v$, for v a valuation.

[4.4] *Definite quadratic bundles.* — Let D be an effective Cartier divisor on X and $|D|$ its support.

Definition 1.2.22. — A quadratic bundle $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$ on X is called **definite (with respect to** $\operatorname{supp} D$**)** if the quadratic space $(\widehat{\mathfrak{q}}_{Y,(0)}, \widehat{\mathcal{E}}_{Y,(0)}, \widehat{\mathcal{L}}_{Y,(0)})$ is anisotropic for all $Y \in \operatorname{supp} D$. A quadratic bundle which is not definite is called **indefinite**.

Recall the *classical* (i.e. over the rationals) definition of a definite quadratic form: $\mathfrak{q}$ is *definite* (with respect to $\{\infty := |\cdot|\}$), if over $\mathbb{R} = \mathbb{Q}_\infty$ it takes only positive or negative values (with the obvious exception of taking all coordinates equal to zero). This is precisely what the definition above tells in this case: the 0 can be only trivially represented in the completion $\mathbb{R} = \mathbb{Q}_\infty$.

2.5. Orthogonal groups. —

[5.1] *Basic definitions.* — We need to consider also morphisms between quadratic bundles. Let $(\mathfrak{q}_i, \mathcal{E}_i, \mathcal{L}_i)$ for $i = 1, 2$ be two quadratic bundles on X. A **morphism** Φ from $(\mathfrak{q}_1, \mathcal{E}_1, \mathcal{L}_1)$ to $(\mathfrak{q}_2, \mathcal{E}_2, \mathcal{L}_2)$ is a pair of sheaf-morphisms $\Phi = (\varphi_1, \varphi_0)$, with $\varphi_1 : \mathcal{E}_1 \to \mathcal{E}_2$ and $\varphi_0 : \mathcal{L}_1 \to \mathcal{L}_2$, such that the following

diagram commutes:

$$\begin{array}{ccc} \mathrm{Sym}^2(\mathcal{E}_1) & \xrightarrow{\mathrm{Sym}^2(\varphi_1)} & \mathrm{Sym}^2(\mathcal{E}_2) \\ {\scriptstyle \mathfrak{b}_1}\downarrow & & \downarrow{\scriptstyle \mathfrak{b}_2} \\ \mathcal{L}_1 & \xrightarrow{\varphi_0} & \mathcal{L}_2. \end{array} \tag{1.2.2}$$

A morphism Φ as above is a **similarity transformation**, or simply a **similarity**, if both φ_1 and φ_0 are isomorphisms. We denote the set of similarities from $(\mathfrak{q}_1, \mathcal{E}_1, \mathcal{L}_1)$ to $(\mathfrak{q}_2, \mathcal{E}_2, \mathcal{L}_2)$ by $\mathfrak{S}((\mathfrak{q}_1, \mathcal{E}_1, \mathcal{L}_1), (\mathfrak{q}_2, \mathcal{E}_2, \mathcal{L}_2))$. A similarity transformation Φ is an **isomorphism** (or equivalently, an **isometry**) of quadratic bundles if φ_0 is the identity morphism (in particular $\mathcal{L}_1 = \mathcal{L}_2$). In this case, the quadratic bundles are said to be **isomorphic** (=**isometric**), and belong to the same **class (over** X**)** of quadratic bundles.

Definition 1.2.23. — Let $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$ be a quadratic bundle on X. The group of similarities from this bundle to itself is denoted by $\mathfrak{S}(\mathfrak{q}, \mathcal{E}, \mathcal{L})$. Let $\boldsymbol{u} = (u, u_0)$ be a similarity. The homomorphism u_0 can be interpreted as an element in $\Gamma(X, \mathcal{O}_X^\times)$, called the **multiplier** (since an automorphism of $\mathcal{L}$ is an element of $(\mathcal{L}^* \otimes \mathcal{L})^\times \cong \mathcal{O}_X^\times$). An element $\Phi \in \mathfrak{S}(\mathfrak{q}, \mathcal{E}, \mathcal{L})$ is an **orthogonal transformation** or an **automorphism** if $\varphi_0 : \mathcal{L} \to \mathcal{L}$ is the identity morphism, in which case we write simply φ for $\Phi = (\varphi, \mathrm{Id}_{\mathcal{L}})$. The subgroup of the group of similarities given by the orthogonal transformations, $\mathrm{O}(\mathfrak{q}, \mathcal{E}, \mathcal{L})$, is called the **orthogonal group** of the quadratic bundle $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$.

Hence, the orthogonal group of a quadratic bundle $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$ is the subgroup of $\mathrm{Aut}(\mathcal{E}) = GL(\mathcal{E})$, consisting of those $\varphi \in \mathrm{Aut}(\mathcal{E})$ which make the following diagram commutative:

$$\begin{array}{ccc} \mathrm{Sym}^2(\mathcal{E}) & \xrightarrow{\mathrm{Sym}^2(\varphi)} & \mathrm{Sym}^2(\mathcal{E}) \\ & {\scriptstyle \mathfrak{b}}\searrow \quad \swarrow{\scriptstyle \mathfrak{b}} & \\ & \mathcal{L} & \end{array} .$$

As usual, we define the **special orthogonal group** as

$$\mathrm{SO}(\mathfrak{q}, \mathcal{E}, \mathcal{L}) := \{\varphi \in \mathrm{O}(\mathfrak{q}, \mathcal{E}, \mathcal{L}) \mid \det(\varphi) = 1 \in \Gamma(X, \mathcal{O}_X^\times)\},$$

and call its elements **proper automorphisms**. This could be also stated in the language of group schemes, namely, as the connected component of the identity of the orthogonal group, as an algebraic group scheme. For more general purposes, one takes the latter as the definition of the special orthogonal group.

[5.2] *Representability.* — So, we prove now that in fact the groups defined above are indeed group schemes (which we always mean to be affine) representing the corresponding functors on groups. It suffices to prove representability for the orthogonal group itself.

[5.2.1] We will prove that the functor

$$\underline{\mathrm{O}}(\mathcal{E}) : (\boldsymbol{Sch}/X)^{\mathrm{op}} \to \boldsymbol{Groups}$$
$$Y \mapsto \{u \in \underline{\mathrm{GL}}(\mathcal{E})(Y) \mid \mathfrak{b}_Y \circ \mathrm{Sym}^2(u) = \mathfrak{b}_Y\}.$$

is representable, from a general result of Grothendieck on the representability of certain functors [**SGAD**, Exposé VIII, §6], which we briefly sketch for completeness sake. We use Grothendieck's notation when we want to use the fact, that schemes are first of all functors; e.g. GL_n is the group

which represents the functor $\underline{\mathrm{GL}}_n$.
Representability of the functor $\underline{\mathrm{O}}(\mathcal{E})$ means, that there exists a scheme $\mathcal{G}$ over X, such that for any $Y \in \boldsymbol{Sch}/X$

$$\underline{\mathrm{O}}(\mathcal{E})(Y) \cong \mathrm{Hom}_{\boldsymbol{Sch}/X}(Y, \mathcal{G})$$

functorially; that is, the isomorphisms are given through a natural transformation. In this case, the scheme $\mathcal{G}$ will be a group scheme over X.

***Example 1.2.24* (Generic Example).** — Let X, Y, Z be S-schemes, and μ_1, μ_2 be two actions of X on Y with values in Z, i.e.

$$\mu_1, \mu_2 : X \to \underline{\mathrm{Hom}}_S(Y, Z),$$

or what amounts the same,

$$\mu : X \to \underline{\mathrm{Hom}}_S(Y, Z \times_S Z).$$

The subfunctor X' of X defined by $X'(T) := \{x \in X(T) \mid \mu_1(x) = \mu_2(x) : Y_T \to Z_T\}$ for $T \to S$, called the **kernel of** μ is exactly the subfunctor inverse image of $\underline{\mathrm{Hom}}_S(Y, \Delta_Z) \subset \underline{\mathrm{Hom}}_S(Y, Z \times_S Z)$ by μ; with Δ_Z being the diagonal scheme in $Z \times_S Z$. Grothendieck's Theorem on representability (Exposé loc. cit.), gives conditions under which the subfunctor X' is representable.[III]

***Theorem 1.2.25* (Thm. 6.4 loc. cit.).** — *The subfunctor X' defined above is representable by a closed subscheme of X, when Z is separated over S, and Y is* essentially free over S.

We will not introduce in detail the (technical) concept of **essentially freeness**, which in words means, that after *suitable base changes* (faithfully flat, affine), the ring of regular functions on Y, becomes a free module over the base. We use only the following two facts:

– over a field, any scheme is essentially free,
– any scheme is essentially free over itself.

[5.2.2] We want to apply the Theorem above, to prove the representability of the orthogonal group $\underline{\mathrm{O}}(\mathcal{E})$. The group $\mathrm{GL}(\mathcal{E})$ acts on the projective scheme $\mathcal{V} := \mathbb{P}((\mathrm{Sym}^2(\mathcal{E}))^* \otimes \mathcal{L})$, whose sections are precisely the quadratic forms (up to scalars). So, our quadratic form $\mathfrak{b}$ is a section of this projective bundle over X. Now, set $X := \mathrm{GL}(\mathcal{E})$, $Y := \{\mathfrak{b}\}$ and Z the orbit of $\mathfrak{b}$ under $\mathrm{GL}(\mathcal{E})$ in the example above. (Y is a closed subscheme of $\mathcal{V}$ since the latter is projective, hence separated, and therefore any section of the structural morphism is a closed immersion, cf. [**EGAI**, §5.4])
Define two (right) actions $\mu_1, \mu_2 : \mathrm{GL}(\mathcal{E})_X \to \underline{\mathrm{Hom}}_X(\{\mathfrak{b}\}, Z)$ by:

$$\mu_1(g)(\mathfrak{b}) := \mathfrak{b} \cdot g := \mathfrak{b} \circ \mathrm{Sym}^2(g),$$
$$\mu_2(g)(\mathfrak{b}) := \mathfrak{b}.$$

Clearly, the subfunctor defined by the kernel of them, is exactly the orthogonal group. So we need to prove, that $\{\mathfrak{b}\}$ is essentially free and that the orbit is separated. The first is obvious from the definition, since any scheme over itself is essentially free. The second is also clear, since the orbit sits inside a projective bundle. So we have proved

Proposition 1.2.26. — *The functor on groups $\underline{\mathrm{O}}(\mathcal{E}) : (\boldsymbol{Sch}/X)^{op} \to \boldsymbol{Groups}$ is represented by a closed subscheme $\mathrm{O}(\mathcal{E})$ of $\mathrm{GL}(\mathcal{E})_X$,*

$$\begin{array}{ccc} \mathrm{O}(\mathcal{E}) & \hookrightarrow & \mathrm{GL}(\mathcal{E}) \\ & \searrow \quad \swarrow & \\ & X & \end{array} .$$

[5.2.3] Alternatively, one can prove the representability of the orthogonal group over affine patches, and then check the glueings. Even though, the use of Grothendieck's Theorem above seems to be too much for our purposes, its proof is not much more than what one should do, to prove the glueings for the orthogonal group itself, and so, we decided to put it here to show a more versatile fact.

Remark 1.2.27. — The connected component of the identity in $\mathrm{O}(E)$ is the open subgroup scheme of proper automorphisms $\mathrm{O}(\mathcal{E})^\circ = \mathrm{SO}(\mathcal{E}) \subset \mathrm{O}(\mathcal{E})$. This connected group scheme is not flat in general (cf. chapter 3), but when the quadratic form is regular over X, it is indeed reductive. In general, the Lie algebra of $\mathrm{O}(\mathcal{E})$ has trivial nilpotent ideal, so for reductiveness, we need only to check smoothness of the fibers. When the quadratic bundle is not regular, the dimension of the fibers of the orthogonal group jump up at certain "bad points".

CHAPTER 2

LATTICES OVER GLOBAL RINGS

We define a constant which enables a generalization of Hermite's Theorem for global rings, give a proof of Harder's Theorem (Theorem 2.1.12) and study extensions of quadratic bundles on curves (Theorem 2.3.4).

1. Harder's Theorem

1.1. Hermite's Theorem. — In this section, R will be a global ring; i.e. the integral closure of the ring of integers (of $\mathbb{F}_q[T]$) inside a finite degree extension K of $\mathbb{Q}$ ($\mathbb{F}_q(T)$). In the function field case (positive characteristic) K can be seen as the function field of a geometrically smooth, irreducible projective curve X over $\mathrm{Spec}(\mathbb{F}_q)$, with generic point η (so $\kappa(\eta) = K$).

[1.1] $\lambda(R)$. — Let $|\cdot|$ be the absolute value on K, as defined in §1.1.3.

Definition 2.1.1. — The limit

$$\lambda(R) := \text{ess inf}_{x\in K}\, \delta_{|\cdot|}(x, R),$$

where $\delta_{|\cdot|}(x, R) := \inf\{|x - y| \mid y \in R\}$ is called the **Lebesgue number** of R.

Example 2.1.2. — (1) We illustrate the relation with the classical Lebesgue numbers in the case $R = \mathbb{Z}$. Intersect any closed interval $I := [a, a + k] \cap \mathbb{Q} \subset \mathbb{Q} =: K$ for $a \in \mathbb{Q}$ and $k \in \mathbb{N}$. Take for a covering of I the union of the finitely many relative open sets $I \cap (n - 1, n + 1)$ with $n \in \mathbb{Z}$. Then the Lebesgue number of this covering is exactly our $\lambda(\mathbb{Z})$, which is clearly $1/2$.

(2) $R = \mathbb{F}_q[t], K = \mathbb{F}_q(t), |\cdot|_\infty : K^\times \to \mathbb{R}_{\geq 0}$, given by $|x_1/x_2|_\infty = q^{deg(x_1)-deg(x_2)}$. Then $\lambda(\mathbb{F}_q[t]) = 1/q$.
Take $x = x_1/x_2$ and y with $x_1, x_2, y \in R$. Then, we have to compute $\delta_{|\cdot|_\infty} = |x - y|_\infty = |(yx_2 - x_1)/x_2|_\infty$. If $deg(x) \leq -1$ then take $y = 0$ and we obtain $\delta_{|\cdot|_\infty} \leq |x|_\infty \leq 1/q$. If not, $deg(x) \geq 0$, which means $deg(x_1) \geq deg(x_2)$. Since R is an Euclidean domain, we can find $y_0, r_0 \in R : x_1 = y_0x_2 + r_0$ with $deg(r_0) \leq deg(x_2)$. Therefore, $(y_0x_2 - x_1)/x_2 = -r_0/x_2$ has v-norm not greater than $1/q$. It is easy to see, that the limit $1/q$ can be reached (take $x = 1/t$). Hence, $\lambda(\mathbb{F}_q[t]) = 1/q$.

Lemma 2.1.3. — *Let R' be the integral closure of R in a finite extension K' of K, and $|\cdot|_\infty$ denote also the extended absolute value given in §1.1.3. Then $\lambda(R')^{[K':K]} \leq \lambda(R)$.*

Proof. — Combine the example above with the definition of the absolute value (cf. §1.1.3). □

Therefore,

Corollary 2.1.4. — *The Lebesgue number of a global ring of positive characteristic is smaller than* 1.

[1.2] Let $\mathbb{V}$ be an n-dimensional K-vector space, b a non-degenerate bilinear form on it (i.e. $(\mathbb{V}, \mathfrak{b})$ is regular) and E a lattice in $\mathbb{V}$. By scaling the lattice E we may suppose it is integral. Define:

$$m(E) := \inf_{\substack{a \subset E, \\ \text{rank-1 submodule}}} \{|\operatorname{discr}(\mathfrak{a})|_\infty\}, \tag{2.1.1}$$

where $\operatorname{discr}(\mathfrak{a})$ is the discriminant (ideal, cf. §1.2.2.1.1) of $\mathfrak{a}$.

Remark 2.1.5. — (1) The number $m(E)$ is positive, because of the discreteness of R inside K, with respect to $|\cdot|_\infty$.

(2) Denote by $\mathfrak{q}$ the associated quadratic form $\mathfrak{q}(x) := 2^{-1}\mathfrak{b}(x,x)$. Then, if R has class number one, $m(E)$ is the smallest length of a lattice point in E.

(3) In the definition of $m(E)$ for a lattice in a not necessarily regular quadratic space, we restrict the infimum to be taken among the regular submodules. In the case of isotropic (regular) lattices, a bound for the "absolute" minimum (in this case equal to 0) does not give any information. Note that this is not the usual definition, as for example in [**Kne92**].

[1.3] *Hermite's Theorem*. — Let $\mathfrak{a}$ be a rank 1 R-module. We write by $\mathfrak{a} \subset E$ an injective homomorphism of R-modules from $\mathfrak{a}$ into E, and in this case let $\mathfrak{a}$ be identified with its image, such that for example $E/\mathfrak{a}$ makes sense. Take any $\mathfrak{a} \subset E$ such that $m(E) = |\operatorname{discr}(\mathfrak{a})|_\infty$ (which is easily seen to exist).
Claim: *The ideal $\mathfrak{a}$ can be taken to be* **primitive**, *i.e. $E/\mathfrak{a}$ torsion-free.*
Suppose $E/\mathfrak{a}$ is not torsion-free. Then there exist $v \in E \setminus \mathfrak{a}$ and $\lambda \in R \setminus \{0\}$, such that $\lambda v \in \mathfrak{a}$. Set $\mathfrak{a}(v) := \mathfrak{a} + \langle v \rangle_R$. This is again a rank one submodule of E. It is clear that $\operatorname{discr}(\mathfrak{a}(v)) \supset \operatorname{discr}(\mathfrak{a})$, hence $m(E) = |\operatorname{discr}(\mathfrak{a}(v))|_\infty$. If we iterate this process (which finishes because R is Noetherian), we obtain a submodule with the required property.
Claim: *There is a principal ideal $\langle a \rangle \subset \mathfrak{a}$ with the same minimum.*
Clear (because of the discreteness of the absolute norm).

[1.3.1] We return to the vector space $\mathbb{V}$ with its bilinear form $\mathfrak{b}$. Define $\pi_\mathfrak{a}$ to be the projection from $\mathbb{V}$ onto the orthogonal complement of $\mathfrak{a} = \langle a \rangle$. Denote by E' the image of the lattice E under this projection. It is therefore clear that $\operatorname{discr}(E) = \operatorname{discr}(\mathfrak{a}) \operatorname{discr}(E')$. Now take $\mathfrak{a}'$, with $m(E') = |\operatorname{discr}(\mathfrak{a}')|_\infty$. So, by definition of $\lambda(R)$ (and since $\mathfrak{a}$ is principal!) we can find for any $v' \in E'$ a vector $v \in E$ and a $\lambda \in R$ such that $v = v' + \lambda a$ ($\pi_\mathfrak{a}(x) = x - \mathfrak{b}(x,a)/\mathfrak{q}(a)\, a$). Now $\mathfrak{b}(v,v) = \mathfrak{b}(v',v') + \lambda^2 \mathfrak{b}(a,a)$, so we obtain in the archimedian case $m(E) \leq m(E') + \lambda(R)^2 m(E)$, whereas in the non-archimedian case even $m(E) \leq m(E')$, since $\lambda(R) < 1$ (cf. Corollary 2.1.4). The rank of E' is strictly smaller than the rank of E, so we proceed by induction in order to prove

Theorem 2.1.6. — *Let R be a global ring as above, K its quotient field endowed with the valuation $|\cdot|_\infty : K^\times \to \mathbb{R}_{\geq 0}$, for which R is discretely embedded in K. Then, for any non-degenerate integral quadratic lattice $(E, \mathfrak{b})$ of rank n over R holds:*

$$m(E) \leq (1 - \lambda(R)^2)^{-\frac{n-1}{2}} |\operatorname{discr}(E)|_\infty^{\frac{1}{n}}. \tag{2.1.2}$$

If moreover $|\cdot|_\infty$ is non-archimedian, and $\lambda(R) < 1$, then

$$m(E) \leq |\operatorname{discr}(E)|_\infty^{\frac{1}{n}}. \tag{2.1.3}$$

Proof. — Let's handle first the non-archimedian case. Suppose from the inductive hypothesis[(1)]

$$m(E') \leq |\operatorname{discr}(E')|_\infty^{\frac{1}{n-1}}.$$

From this and the relation between the discriminants, we have

$$\begin{aligned} m(E) \leq & m(E') \leq |\operatorname{discr}(E')|_\infty^{\frac{1}{n-1}} = \frac{|\operatorname{discr}(E)|_\infty^{\frac{1}{n-1}}}{m(E)^{\frac{1}{n-1}}}, \\ m(E)^{\frac{n}{n-1}} \leq & |\operatorname{discr}(E)|_\infty^{\frac{1}{n-1}} \Rightarrow m(E) \leq |\operatorname{discr}(E)|_\infty^{\frac{1}{n}}. \end{aligned}$$

If $|\cdot|_\infty$ is archimedian, we suppose

$$m(E') \leq (1-\lambda(R)^2)^{-\frac{n-2}{2}} |\operatorname{discr}(E')|_\infty^{\frac{1}{n-1}},$$

then:

$$\begin{aligned} m(E) \leq & (1-\lambda(R)^2)^{-1} m(E') \leq (1-\lambda(R)^2)^{-\frac{n}{2}} |\operatorname{discr}(E')|_\infty^{\frac{1}{n-1}} = \\ & = (1-\lambda(R)^2)^{-\frac{n}{2}} |\operatorname{discr}(E)|_\infty^{\frac{1}{n-1}} m^{-\frac{1}{n-1}} \\ \Rightarrow m(E)^n \leq & (1-\lambda(R)^2)^{-\frac{n(n-1)}{2}} |\operatorname{discr}(E)|_\infty \\ \Rightarrow m(E) \leq & (1-\lambda(R)^2)^{-\frac{n-1}{2}} |\operatorname{discr}(E)|_\infty^{\frac{1}{n}}. \end{aligned}$$

□

Remark 2.1.7. — For $R = \mathbb{Z}$, if we recall our definition of $\lambda(R)$, we see from (2.1.2) that we recover the classical result :

$$m(E) \leq (2/\sqrt{3})^{n-1} |\operatorname{discr}(E)|^{\frac{1}{n}}. \tag{2.1.4}$$

Remark 2.1.8. — Hermite's Theorem could be said to belong to the realm of *explicit reduction theory*, whose main aim is the explicit construction of fundamental domains (cf. [**God64**], [**Har69**]). Godement says in [**God64**, page 3]:

"Il serait instructif d'étendre si possible la méthode précédente à la charactéristique p, i.e. en prenant pour corps de base $k = \mathbb{F}_p(X)$ au lieu du corps des rationnels."

Our intention for the definition of the *Lebesgue number* of a global ring R was to obtain a generalized version of Hermite's Theorem for characteristic $p > 0$. To extend *"Godement's method"*, one has to generalize a constant c (cf. loc.cit.), which in the case of the rational integers is $2/\sqrt{3}$ and comes from Hermite's Theorem (2.1.4). Hence, for a general global ring R, this constant is $c_R := (1-\lambda(R))^{-1/2}$, where λ is our *Lebesgue number*.[(2)]

[(1)] It is easy to see, that the "right" exponent for $\operatorname{discr}(E')$ in the inductive assumption should be $\frac{1}{n-1}$. Replace the unknown exponent for rank $n-1$ modules by ϵ_n, and then observe, that $\epsilon_n = \frac{\epsilon_{n-1}}{\epsilon_{n-1}+1}$.

[(2)] *Added in edition*: We unfortunately did not know about investigations on *explicit reduction theory* by the time of writing the thesis. See for example [**Thu96**], [**Wat04**] and references therein for generalizations of the so called *Hermite constant*, where the latter also generalizes Thunder's definition (over number fields) for linear algebraic groups over global fields.

[1.4] The finiteness of the class group of a number field follows from Hermite's inequality. A similar statement in this context is the following (cf. [**Kne92**, Satz 20.2])

Proposition 2.1.9. — *For any $n \in \mathbb{N}, d \in |R|_\infty \subset \mathbb{R}_{\geq 0}$ fixed, there exist finitely many isomorphism classes of integral, non-degenerate quadratic lattices $(\mathfrak{b}, E)$ such that E is of rank n and $d = |\operatorname{discr}(E)|_\infty$.*

Proof. — Since the statement is up to isomorphy, we can suppose the lattices to be in the same n-dimensional quadratic space $\mathbb{V}$. Let $n = 1$. Then by Theorem 1.2.13, E is isomorphic to an ideal $\mathfrak{a}$ of R. Let $\mathrm{Cl}(R) = \{\mathfrak{a}_1 = R, \mathfrak{a}_2, \ldots, \mathfrak{a}_h\}$ be the class group of R and $\mathfrak{a}_i = \langle a_{i,1}, \ldots, a_{i,n_i}\rangle$. Then $E \cong \alpha\mathfrak{a}_i$ for some $i = 1, \ldots, h$ and for some $\alpha \in K$. Since the rank of E is one, we can associate to the pair $(\mathfrak{b}, E)$ a $n_i \times n_i$ matrix M with coefficients in K, of the following form:

$$M = \begin{pmatrix} \beta b_{1,1} & \beta b_{1,2} & \ldots & \beta b_{1,n_i} \\ \beta b_{2,1} & \beta b_{2,2} & \ldots & \beta b_{2,n_i} \\ \ldots & & & \\ \beta b_{n_1,1} & \beta b_{n_1,2} & \ldots & \beta b_{n_i,n_i} \end{pmatrix}.$$

The coefficients $b_{k,l}$ belong to K, and are determined by the class of the ideal associated with E. They are obtained from the relations (in K) between the n_i generators of $\mathfrak{a}_i$. The "indeterminate" β is given by the bilinear form $\mathfrak{b}$ on E. Therefore, if we impose a bound for the discriminant of E with respect to the bilinear form $\mathfrak{b}$, this gives a bound on β, since the matrix M/β depends only on the class of the ideal $\mathfrak{a}_i$. But there are h such matrices, so we can bound β uniformly; therefore the claim for rank 1 lattices. (We could have certainly taken $n_i = 2$.)
Suppose the assertion is valid for all modules of rank smaller than n (> 1). Take $\mathfrak{a}_1 \subset E$ such that $|\operatorname{discr}(\mathfrak{a}_1)|_\infty = m(E)$. As we saw before, $\mathfrak{a}_1$ is a primitive sub-module of E of rank 1. So by the inductive hypothesis, since its discriminant is bounded by $\lambda(R)$ and $\operatorname{discr}(E)$ (Theorem 2.1.6), there are finitely many possibilities for $\mathfrak{a}_1$. Set $G := E \cap \mathfrak{a}_1^\perp$. Observe that $G \perp \mathfrak{a}_1 \subset E \subset E^\# \subset G^\# \perp \mathfrak{a}_1^\#$. From this it is clear that we have only to bound the discriminant of G, since $\operatorname{rk}(G) < \operatorname{rk}(E)$. A uniform bound for it follows from next lemma, so the proof is finished. □

Remark 2.1.10. — We can prove also a similar result for quadratic lattices with values in fractional ideals with bounded discriminants, instead of values in R.

For a quadratic form $(M, \mathfrak{q})$ over R, and $\alpha \in K$; set ${}^\alpha M$ to be the quadratic form over M which sends x to $\alpha\mathfrak{q}(x)$. In case it is necessary from the context, we write ${}^\alpha x$ for the element $x \in M$, but M seen with the quadratic form $\alpha\mathfrak{q}$.

Lemma 2.1.11. — *Let E be a lattice in a regular quadratic space $(\mathbb{V}, \mathfrak{b})$, and L a primitive sublattice of E. Then, there exists a divisor δ of $\operatorname{discr}(E)$, such that:*

$$|\delta|_\infty{}^2 |\operatorname{discr}(L^\perp \cap E)|_\infty = |\operatorname{discr}(E)|_\infty |\operatorname{discr}(L)|_\infty.$$

Proof. — It is clear that $|\operatorname{discr}(E \perp^{-1} L)|_\infty = |\operatorname{discr}(E)|_\infty |\operatorname{discr}(L)|_\infty$. We compute this quantity in another way.
Both modules L and $L^\perp \cap E$ are direct summands of E (L is primitive), say

$$E = G \oplus (L^\perp \cap E) = H \oplus L. \tag{2.1.5}$$

Define $L' := \{(x, {}^{-1}x) \mid x \in L\} \subset E \oplus L$. Then $E \perp^{-1} L = E \oplus L' = G \oplus (L^\perp \cap E) \oplus L'$. With respect to this last direct sum, any *matrix representing* (*associated with*, cf. §1.2.2.0.5) the bilinear form on

$E \perp^{-1} L$, $\tilde{\mathfrak{b}}$, has the following shape:

$$\begin{pmatrix} \star & \star & \tilde{\mathfrak{b}}(G, L') \\ \star & \mathfrak{q}(L^\perp \cap E) & 0 \\ \tilde{\mathfrak{b}}(L', G) & 0 & 0 \end{pmatrix}. \tag{2.1.6}$$

The bilinear form $\tilde{\mathfrak{b}}$ on (G, L') can be read off from (2.1.5), where the associated matrix (with respect to $G \oplus (L^\perp \cap E)$ for rows and $H \oplus L$ for columns) is:

$$\begin{pmatrix} \mathfrak{b}(G, L) & \mathfrak{b}(G, H) \\ 0 & \mathfrak{b}(L^\perp \cap E, H) \end{pmatrix}.$$

Now, $\mathfrak{b}(G, L) = \tilde{\mathfrak{b}}(G, L')$, and then $\operatorname{discr}(E) = \operatorname{discr}(G, L') \operatorname{discr}(L^\perp \cap E, H)$; therefore $|\operatorname{discr}(G, L')|_\infty \mid |\operatorname{discr}(E)|_\infty$. Now, from (2.1.6):

$$|\operatorname{discr}(E)|_\infty |\operatorname{discr}(L)|_\infty = |\operatorname{discr}(L^\perp \cap E)|_\infty |\operatorname{discr}(G, L')|_\infty^{\,2},$$

which proves the claim. □

1.2. Harder's Theorem. — In this section we set $R = \mathbb{F}_q[T]$. The restriction is, essentially, to have an euclidean ring with respect to the norm at infinity $|\cdot|_\infty$; something clearly satisfied by $\mathbb{F}_q[T]$.

***Theorem 2.1.12* (Harder).** — *Any unimodular quadratic lattice $E = (\mathfrak{q}, E)$ over R "comes from" $\mathbb{F}_q$; i.e.*

$$(\mathfrak{q}, E) \cong (\mathfrak{q}_0, E_0) \otimes_{\mathbb{F}_q} R,$$

for some quadratic lattice (space) $(\mathfrak{q}_0, E_0)$ over $\mathbb{F}_q$.

This result appeared for the first time in Knebusch's Habilitationsschrift [**Kne69**]. Ours, is naturally based on the geometry of numbers, and in particular on Hermite's result. It is not a coincidence, that already Gerstein [**Ger79**] took this approach; which we did not know before this investigation. *Because I (re)discovered this proof, I feel free to write it down here.*

[2.1] *Lattice reduction.* —

Definition 2.1.13. — A symmetric matrix $B = (b_{i,j})_{i,j=1}^n \in \operatorname{Mat}_n(K)$ is **reduced** if and only if

(1) $|b_{i,i}|_\infty > |b_{i,j}|_\infty$ for any $j \neq i$;
(2) $|b_{1,1}|_\infty \leq |b_{2,2}|_\infty \leq \ldots \leq |b_{n,n}|_\infty$.

For principal ideal domains, the lattices are free, and therefore we can associate matrices to the bases. Let $\{e_1, \ldots, e_n\}$ be a basis for a given lattice E. Then a bilinear form $\mathfrak{b} : E \times E \to R$ has an associated matrix $B \in \operatorname{Mat}_n(R)$. The basis $\{e_1, \ldots, e_n\}$ is called **reduced** if B is reduced. Any subset of E is called reduced, if it is a reduced basis for the lattice it generates.

Proposition 2.1.14. — *If the lattice E is anisotropic, then it possesses a reduced basis.*

For the sake of completeness we repeat the algorithmic proof by Djoković given in [**Ger03**], which can be seen as an application of the Gauss pivoting method for matrices with entries in a polynomial ring over a field.

Algorithm. — Choose any basis $\{e_1, \ldots, e_n\}$ of E. Arrange the vectors of this basis in such a way, that the diagonal of the associated matrix of $\mathfrak{b}$ satisfies $|b_{1,1}|_\infty \leq \ldots \leq |b_{n,n}|_\infty$.

Begin. If this basis is reduced, there is nothing to do, so return $\{e_1, \dots, e_n\}$.
If not, let $r \in \{1, \dots, n-1\}$ be so, that $\{e_1, \dots, e_r\}$ is reduced, but $\{e_1, \dots, e_{r+1}\}$ is not.
Since $\{e_1, \dots, e_{r+1}\}$ is not reduced, $d := \max_{1 \le i \le r} v_\infty(b_{i,r+1}) - v(b_{i,i})$ is non negative. Set $v_i := v_\infty(b_{i,i})$, and $\lambda_i := \mathrm{coeff}_{v_i}(b_{i,i})$, $i = 1, \dots, n$. None of the λ_i's are zero. Write

$$b_{i,r+1} = c_i \xi^{v_i + d} + \{\text{lower term degrees}\},\ i = 1, \dots, r,$$

for some $c_i \in \mathbb{F}_q$ (clearly, $c_i = 0$ when $v_i + d > v_\infty(b_{i,r+1})$). Define

$$e'_{r+1} := e_{r+1} - \sum_{i=1}^{r} \frac{c_i}{\lambda_i} x^d e_i.$$

Now, for $j = 1, \dots, r$ we have that

$$\mathfrak{b}(e_j, e'_{r+1}) = b_{j,r+1} - \frac{c_j}{\lambda_j} x^d b_{j,j} - \sum_{1 \le i \le r, i \ne j} \frac{c_i}{\lambda_i} x^d b_{i,j}$$

has degree smaller than $v_j + d$. If $|\mathfrak{b}(e'_{r+1}, e'_{r+1})|_\infty \ge |b_{r,r}|_\infty$, then replace e_{r+1} by e'_{r+1} in the original basis, and go back to the beginning. Then we can always reduce the degree of the new $b_{i,r+1}$ at least by one and then after at most $d+1$ passes through the beginning, we get a dominant $b_{r+1,r+1}$; i.e. $|b_{r+1,r+1}|_\infty > |b_{i,r+1}|_\infty$, $\forall i = 1, \dots, r$. We might have to arrange the vectors $\{e_1, \dots, e_r, e'_{r+1}, e_{r+2}, \dots, e_n\}$ since $b_{r+1,r+1}$ might have smaller norm as the others $b_{i,i}$, for $i = 1, \dots, r$. After doing this, we have a basis $\{e_1, \dots, e'_{r+1}, \dots, e_r, e_{r+1}, \dots, e_n\}$ (or $\{e_1, \dots, e_r, e'_{r+1}, e_{r+2}, \dots, e_n\}$) where the first $r+1$ elements form a reduced basis. So after repeating the whole process above at most n times, we obtain a reduced basis $\{\tilde{e}_1, \dots, \tilde{e}_n\}$ of E.
End. Return $\{\tilde{e}_1, \dots, \tilde{e}_n\}$. □

[2.2] From this algorithm and Theorem 2.1.6 we can easily derive Harder's Theorem.

Proof of Theorem 2.1.12. — Assume first E to be anisotropic. From (2.1.3), there exists a rank one submodule $\mathfrak{a}$ whose discriminant is a unit in $R^\times$. But R is a principal ideal domain, so there exists $e_1 \in E$ such that $\mathfrak{b}(e_1, e_1)$ is a unit. Moreover we can extend $\{e_1\}$ to a basis $\{e_1, \dots, e_n\}$ of E ($\langle e_1 \rangle_R \subset E$ is primitive). Since E is anisotropic, and $\mathfrak{b}(e_1, e_1)$ is already a unit, the lattice reduction algorithm 2.1.14 produces a reduced basis $\{\tilde{e}_1 = e_1, \tilde{e}_2, \dots, \tilde{e}_n\}$. The diagonal of the associated matrix is dominant, and $\mathfrak{b}(e_1, e_1)$ a unit, hence the free submodule generated by e_1 is indeed an orthogonal summand of E: $\mathfrak{a} \perp E' = E$. It is clear that E' is again unimodular and of smaller rank, so we can reproduce the same arguments as before, and finally obtain a diagonal form for E with entries in the group of units of R, namely $\mathbb{F}_q^\times$.
If E is isotropic, we proceed by induction on the Witt index of E (recall R is an euclidean domain and E is regular). So, any hyperbolic space inside E is an orthogonal summand of it. By induction we are reduced to the case $\mathrm{ind}(E) = 1$. From (2.1.3), there is an ideal $\mathfrak{a} = \langle a \rangle_R \subset E$ such that $\mathfrak{b}(a, a)$ is a unit, and it is also a summand (see the proof of Theorem 2.1.6). $E = \mathfrak{a} \oplus \mathfrak{a}'$, with $\mathfrak{a}' = \langle a' \rangle_R$ a regular lattice. Since $\mathfrak{b}(a, a)$ and $\mathfrak{b}(a', a')$ are both units, it is easy to see, that the associated matrix with respect to the basis $\{a, a'\}$ is $\begin{pmatrix} \mathfrak{b}(a,a) & 0 \\ 0 & \mathfrak{b}(a',a') \end{pmatrix}$. The proof is finished. □

[2.3] *Harder's proof.* — We sketch the original proof.
In our previous proof, modulo lattice reduction (§2.1.2.1), the whole effort consisted in finding a unimodular orthogonal factor of the given (unimodular) lattice. If we found a unimodular sublattice, by reduction theory, we get indeed a unimodular *orthogonal factor*, so it is enough to find a unimodular sublattice. This was done with help of Hermite's Theorem 2.1.6, whose bound guarantees the existence

of such a sublattice. Harder proceeds as follows (recall notation from this section).
Set $U := \mathrm{Spec}(R)$, $X := \mathbb{P}^1_{\mathbb{F}_q}$, and $S := X \setminus U$. Extend (cf. §2.3.3) $(\mathfrak{q}, E)$ to a maybe singular quadratic bundle $(\tilde{\mathfrak{q}}, \tilde{E})$ over X. There is therefore an exact sequence of coherent $\mathcal{O}_X$-sheaves

$$0 \longrightarrow \tilde{E} \xrightarrow{\mathfrak{b}^*} \tilde{E}^* \longrightarrow N \longrightarrow 0.$$

Since N is a skyscraper-sheaf, $\chi(N) = \dim(\mathrm{H}^0(X, N)) = s \deg(T) = s$, where $m - s$ is the dimension of the quadratic space over the residue field of the (regular) local ring of T ($\mathbb{F}_q$). The other two Euler-characteristics are (after Grothendieck-Hirzebruch-Riemann-Roch; cf. [**Har97**, Appendix A, Theorem 4.1] for the statement and notation):

$$\chi(\tilde{E}) = \deg([\mathrm{ch}(\tilde{E}).\,\mathrm{td}(\mathcal{T}_X)]_1) = \deg(\det(\tilde{E})) - \frac{m}{2}\deg(K_X) = \deg(\det(\tilde{E})) + m, \text{ and similarly}$$
$$\chi(\tilde{E}^*) = -\deg(\det(\tilde{E})) + m.$$

The alternating sum of Euler-characteristics $\chi(\tilde{E}) - \chi(\tilde{E}^*) + \chi(N)$ is always zero, which gives $\chi(\tilde{E}) = m - \frac{1}{2}s$, and therefore, since $s \leq m$, $\chi(\tilde{E})$ is positive and consequently $\tilde{E}$ possesses a global section σ. Its norm is hence a global section, and so belongs to $\Gamma(X, \mathcal{O}_X^\times) = \mathbb{F}_q^\times$. The sublattice generated by $\sigma\,|_U$ inside E is unimodular, so the theorem follows.

Remark 2.1.15. — In Harder's proof, one can obviously change $S = \{T^{-1}\}$ for any other set of places at infinity, and the result remains true for $\deg(\mathrm{supp}(S)) \leq 2$ (cf. [**Kne69**, Satz 13.4.4]).

Remark 2.1.16. — Instead of using the very strong Grothendieck-Hirzebruch-Riemann-Roch Theorem, one can directly prove, using the classical Riemann-Roch Theorem 2.2.6, by induction on the rank of the vector bundle (since det behaves additively), that

$$\chi(\mathcal{E}) = \deg(\mathcal{E}) + \mathrm{rk}(\mathcal{E})(1 - g);$$

and use this equation directly in the proof above.

2. Lattice points

For the rest of this chapter, we concentrate ourselves on the function field case.

<u>Convention</u> 1. Unless otherwise stated, a curve from now on is a complete, geometrically irreducible and smooth one dimensional scheme over $\mathrm{Spec}(\mathbb{F}_q)$ (in particular projective).

Let X be a curve, $S_\infty \subset |X|$ finitely many closed points on X, and denote by $\mathrm{Val}(S_\infty)$ the set of their corresponding valuations; set $R := \Gamma(X \setminus S_\infty, \mathcal{O}_X)$ for the global ring of functions holomorphic on $U := X \setminus S_\infty$, K for its quotient field (the function field of X).

2.1. Ray and convex bodies. — Let $\infty \in S_\infty$ and $\mathbb{V}$ be a K-vector space with basis $\mathcal{B} := \{v_1, \ldots, v_m\}$. Denote by $\mathbb{V}_\infty$ the vector space obtained by extension of scalars to K_∞, where ∞ is any valuation ("at infinity"). We can define a norm on it (which depends on the basis $\mathcal{B}$):

$$\|v\|_\infty := \max_{i=1,\ldots,m}\{|\alpha_i|_\infty \mid v = \sum_{k=1}^{m} \alpha_k v_k\}.$$

Choose a lattice $L_\infty \subset \mathbb{V}_\infty$. Our main goal is to relate the number of points of L_∞ inside a given convex or ray-body (see the definition below), with certain quantity associated with it (its *"volume"*).

Definition 2.2.1. — A function $\sigma : \mathbb{V}_\infty \to [0, \infty)$ which satisfies the following properties:

SRF1. $\sigma(\lambda v) = |\lambda|_\infty \sigma(v)\ \forall v \in \mathbb{V},\ \lambda \in K$, and
SRF2. σ is continuous with respect to the (canonical) norm $\|\cdot\|_\infty$

is called a **semi-ray function**; if moreover

RF3. $\sigma(v) = 0 \Leftrightarrow v = 0$

is satisfied, then σ is a **ray-function**. For any ray function σ and a positive number B, the set $\mathbb{V}_\infty(\sigma, B) := \{v \in \mathbb{V}_\infty \mid \sigma(v) \leq B\}$ a is called a **(centered) ray-body**.

If a ray function σ satisfies also the inequality (recall that for the exposition's sake, we restrict to the non-archimedian case) $\sigma(v+w) \leq \max\{\sigma(v)+\sigma(w)\}$, it is a **convex function** and its associated ray-body is called a **convex body**.
We illustrate this definition in two examples, which will be of main interest for us.

Example 2.2.2. — (1) Take $\sigma(\cdot) = \|\cdot\|_\infty$. Then the associated convex bodies are nothing else, but spheres.
(2) Let $F : \mathbb{V}_\infty = K_\infty^m \to K_\infty$ be any homogeneous d-form. Then we can define: $\sigma_F : \mathbb{V}_\infty \to [0, \infty)$ by $\sigma_F(v) := |F(v)|_\infty^{1/d}$. The semi-ray function σ_F is a ray function if and only if the hyper-surface $H_F := Proj(K_\infty[T_1, \ldots, T_m]/\langle F\rangle)$ has no rational points. For our further purposes we should keep in mind the quadratic case ($d = 2$).

Any body (as defined above) will be called **absorbent** if and only if it contains at least one element different from 0 of any 1-dimensional vector subspace of $\mathbb{V}_\infty$.

Remark 2.2.3. — Let σ be any ray function and $S := \{v \in \mathbb{V}_\infty \mid \|v\|_\infty = 1\}$. Since S is a compact set (see below), we have $\sigma(S) \subset [0, \infty)$ is also compact, and therefore it is bounded. Call g, G the lower, respectively the upper bound of the image set. It is clear, that $g > 0$ (from Definition 2.2.1 and the compactness of S). So, we have:

$$\|v - w\|_\infty g \leq \sigma(v - w) \leq \|v - w\|_\infty G,\ \ \forall v, w \in \mathbb{V}_\infty.$$

Although in the archimedian case it is well known that spheres are compact, we must show this easy fact in the non-archimedian case. We will prove that $B := \mathbb{V}_\infty(\|\cdot\|_\infty, 1)$ is compact, from which the claim follows.
Since $\mathbb{V}_\infty$ is locally compact, there exists a neighborhood U of zero which is relatively compact. We can indeed suppose $\bar{U} \subset B$ (B is closed). Since U is absorbent, we have to find $\lambda \in K_\infty^\times : \lambda\bar{U} \supset B$. Fix any $\lambda \in K_\infty^\times$ with $|\lambda|_\infty > 1$ and define $\mu : \bar{U} \to \mathbb{N}$ by $\mu(v) := \min\{n \mid \lambda^n v \notin B\} \cup \{\infty\}$ (see that it never takes the zero value). If we prove that μ is a continuous function, then we are done, since it is defined on a compact set, and therefore the image would be contained in some interval $[1, N]$, and therefore $B \subset \lambda^N \bar{U}$; which proves the claim.
(Our topological spaces satisfy always the second axiom of countability, and hence we may check continuity by sequences.) Let $\|v - v_n\|_\infty \overset{n\to\infty}{\longrightarrow} 0$. We have to relate the numbers $e = \mu(v)$ and $e_n = \mu(v_n)$. $\|\lambda^e v\|_\infty > 1$ and $\|\lambda^{e_n} v_n\|_\infty > 1$. But since v_n tends to v, and $\|\cdot\|_\infty$ is non archimedian, for big n, we have $\|v\|_\infty = \|v_n\|_\infty$, which implies that $e_n = e$; so μ is continuous. Hence we have proved the following

Lemma 2.2.4. — *Any bounded and closed subset of* $\mathbb{V}_\infty$ *is compact.*

2.2. Counting lattice points. — The notation is as in the previous section.

Lemma 2.2.5. — *The pull-back* $(\mathfrak{q}_{\infty,(0)}, \mathcal{E}_{\infty,(0)}, K_\infty)$ *contains* $\Gamma(U,\mathcal{E}) =: M$ *as a discrete sublattice. In particular,* $M \cap \mathcal{E}_{\infty,(0)}(\sigma, B)$ *is a finite set for every ray function* σ *and any* $B \in \mathbb{R}_+$.

Proof. — After Lemma 2.2.4, we have to prove that M is discrete. If M is free, it is clear from the properties of $\|\cdot\|_\infty$ (see §1.1). If not, from the structure theorem it suffices to prove that any fractional ideal $\mathfrak{a}$ is discretely embedded in K_∞, which is also clear once we fix a generating set for it. □

To count the lattice points, say for example of M inside $\mathcal{E}_{\infty,(0)}(\sigma, B)$ as above, one naturally needs the classical theorem of Riemann-Roch.

[2.1] *Riemann-Roch.* — We briefly recall this very basic result for completeness.
Let X be a scheme, and $\mathcal{K}$ be the sheaf associated with the pre-sheaf $U \mapsto S_U^{-1}\Gamma(U, \mathcal{O}_X)$, where S_U is the multiplicative subset of $\Gamma(U, \mathcal{O}_X)$ of non-zero divisors (cf. [**Har97**, page 145]). For a Cartier divisor $D = \{(U_i, f_i)\}$ on X, we define $\mathcal{L}(D)$ as the $\mathcal{O}_X$-submodule of $\mathcal{K}$ generated by f_i^{-1} on U_i (which is well defined, since f_i/f_j is invertible on $U_i \cap U_j$). The invertible sheaf $\mathcal{L}(D)$ (it is coherent and locally of rank 1) is the **sheaf associated** with D. Conversely, any coherent sheaf of local constant rank 1 has an associated Cartier divisor class (a Divisor modulo principal divisors, cf. [**Har97**, Chapter II, §6]).

Take now X an irreducible, smooth, complete curve over an algebraically closed field k. Denote by $g := p_a := \dim_k \mathrm{H}^1(X, \mathcal{O}_X)$ its arithmetic genus, and by K_X the **canonical class** of X; i.e. the Cartier divisor class associated with the invertible sheaf $\det(\Omega_X)$, for Ω_X the sheaf of relative differentials on X over k. For a Cartier divisor D write $l(D)$ for the dimension of the k-vector space $\mathrm{H}^0(X, \mathcal{L}(D))$.

Theorem 2.2.6 **(Riemann-Roch)**. — *With the notation above, if* D *is a Cartier divisor on* X*, then*

$$l(D) - l(K - D) = \deg(D) + 1 - g.$$

[2.2] *Counting.* — When the ray function is the (convex) function which corresponds to the norm, we can compute the cardinal of the set in Lemma 2.2.5, using Riemann-Roch, explicitly:

Proposition 2.2.7. — *The finite set of Lemma 2.2.5 for* $\sigma(\cdot) = \|\cdot\|_\infty$ *and* $\log_q(B) > 2g - 2 + \deg(\det(M))$*, has the following cardinality:*

$$|M \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B)| = q^{-m(g-1-\log_q B)-\deg(\det(M))}. \tag{2.2.1}$$

Proof. — Write $M = \oplus_{i=1}^m \mathfrak{a}_i$. Since the norm $\|\cdot\|_\infty$ is the maximum norm with respect to $|\cdot|_\infty$, the cardinality of $M \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B)$ is multiplicative on the summands of M, and the right hand side of (2.2.1) is also, since $\deg \circ \det$ behaves well additively. Therefore we can suppose $m = 1$, say $M = \mathfrak{a}$.

$$\begin{aligned}\mathfrak{a} \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B) =& \{a \in \mathfrak{a} \mid |a|_\infty \leq B\} = \\ =& \{a \in K^\times \mid |a|_\infty \leq B \text{ and } v_\mathfrak{p}(a) \geq v_\mathfrak{p}(\mathfrak{a})\ \forall \mathfrak{p} \in \Omega_0(K)\} = \\ =& \mathcal{L}(\log_q(B) \cdot (\infty) - \mathfrak{a}).\end{aligned}$$

If B is sufficiently large, as in the hypothesis above, the $l(K - D)$ summand of the Riemann-Roch Theorem 2.2.6 vanishes, so we get:

$$|\mathfrak{a} \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B)| = q^{\dim(\mathcal{L}(\log_q(B)\cdot(\infty)-\mathfrak{a})} = q^{1-g+\log_q(B)-\deg(\mathfrak{a})},$$

as required. □

Note that in the proof we wrote $M = \oplus_{i=1}^{m} \mathfrak{a}_i$ instead of simply $M \cong \oplus_{i=1}^{m} \mathfrak{a}_i$. The difference of these two is illustrated in the following:

Corollary 2.2.8. — *Let $T : \mathcal{E}_\eta \to \mathcal{E}_\eta$ be an invertible linear transformation. Then, for B sufficiently large,*

$$|T(M) \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B)| = |\det(T)|_{\xi^{-1}} |M \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B)|.$$

Proof. — Recall that $T(v_1) \wedge \ldots \wedge T(v_l) = (\det(T)).v_1 \wedge \ldots \wedge v_l$. So, from (2.2.1) we get:

$$\begin{aligned} |T(M) \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B)| &= q^{-m(g-1-\log_q B)-\deg(\det(T(M)))} = \\ &= q^{-m(g-1-\log_q B)-\deg(\det(T)\det(M))} = q^{-m(g-1-\log_q B)-\deg(\det(M))-\deg(\det(T))} = \\ &= |\det(T)|_{\xi^{-1}} |M \cap \mathcal{E}_{\infty,(0)}(\|\cdot\|_\infty, B)|. \end{aligned}$$

□

2.3. Volumes. — As explained in the introduction, we want to relate the number of lattice points inside an "ellipsoid" defined by a definite quadratic form with the volume of the ellipsoid and the volume of the fundamental domain of the lattice.

In the classical case, i.e. $R = \mathbb{Z}$, the situation is as follows. Let $\mathbb{V}$ be a m dimensional $\mathbb{Q}$-vector space, and $M \subset \mathbb{V}$ is a free $\mathbb{Z}$-module of full rank. Endow $\mathbb{V}$ with a (positive) definite integral quadratic form (by abuse of notation, since the characteristic of our fields is different from 2, we use the corresponding bilinear form) $\mathfrak{q} : \mathbb{V} \to \mathbb{Q}$. Then for $m \geq 4$ we have

Theorem 2.2.9. —

$$\begin{aligned} |M \cap \mathbb{V}_{\mathbb{R}}(|\mathfrak{q}(\cdot)|^{1/2}, B)| &= \frac{\pi^m B^m}{\sqrt{|\mathrm{discr}(M)|}\,\Gamma(m+1)} + O(B^{m-2}) = \\ &= \frac{\mathrm{vol}(\mathbb{V}_{\mathbb{R}}(|\cdot|, B))}{\mathrm{vol}(\mathcal{F}_M)} + O(B^{m-2}), \end{aligned}$$

when B tends to infinity.

This formula, essentially due to Landau and Walfisz, though not in its sharpest form, is enough for the computations involved in the Minkowski-Siegel formula [**Kne92**].

In the function field case, we have seen that at least for some particular cases we can *explicitly* compute this asymptotic cardinality without any error term. We want to compute it also for ray functions of the form $\sigma(\cdot) = |\mathfrak{q}(\cdot)|_\infty^{1/2}$, where $\mathfrak{q}$ is any definite quadratic form. This computation will be carried out in chapter 4. The following fact will be of use.[V]

Proposition 2.2.10. — *The semi-ray function associated with a quadratic form is a norm if and only if the quadratic form is anisotropic.*

Proof. — Let $\mathfrak{q} : \mathcal{E}_{\infty,(0)} \to K_\infty$ be a quadratic form, with bilinear form $\mathfrak{b}(\cdot,\cdot)$. The necessity condition is clear, since an isotropic quadratic form represents zero non trivially, and hence the semi-ray function would take the value zero at a non-zero vector, so it is not a norm.
The condition is sufficient. To see this, we need to prove that $\sigma_{\mathfrak{q}}(v+w) \leq \max\{\sigma_{\mathfrak{q}}(v), \sigma_{\mathfrak{q}}(w)\}$. This is easily seen to be equivalent to the claim $|\mathfrak{b}(v,w)|_\infty \leq \max\{|\mathfrak{q}(v)|_\infty, |\mathfrak{q}(w)|_\infty\}$, which is again equivalent to

$$(\star) \qquad v_\infty(\mathfrak{q}(v,w)) \geq \inf\{v_\infty(\mathfrak{q}(v)), v_\infty(\mathfrak{q}(w))\}.$$

We now prove this last inequality, for which there are two cases, depending on whether v and w are linearly dependent or not.
Since the form $\mathfrak{q}$ is anisotropic, $\mathfrak{q}(v+\lambda w) = 0$ only when $v = -\lambda w$, in which case the initial inequality follows directly from the fact that $|1+\lambda|_\infty \leq |\lambda|_\infty$ ($\lambda \in K_\infty$). So suppose v and w are linearly independent. Then $\mathfrak{q}(v+\lambda w) = \mathfrak{q}(x)+\lambda^2\mathfrak{q}(w)+2\lambda\mathfrak{b}(v,w)$ is never zero. By suitable multiplication by a power of a uniformizer π_∞, we can suppose the valuations of the coefficients to be non-negative. From Hensel's Lemma (recall K_∞ is a complete local field, so henselian) the reduced polynomial will not have roots in $R_\infty/\pi_\infty R_\infty$. We have to prove $(\star)$, so suppose $v_\infty(\mathfrak{b}(v,w)) \leq \inf\{v_\infty(\mathfrak{q}(v)), v_\infty(\mathfrak{q}(w))\}$. If $v_\infty(\mathfrak{b}(v,w)) < v_\infty(\mathfrak{q}(w))$, we easily see that the reduced equation will not have solutions, only when $v_\infty(\mathfrak{q}(v)) = v_\infty(\mathfrak{b}(v,w))$, so $(\star)$. On the other hand, if $v_\infty(\mathfrak{b}(v,w)) < v_\infty(\mathfrak{q}(v))$, then we have immediately local solutions, hence global, which is a contradiction to the anisotropicity of $\mathfrak{q}$. □

3. Curves in the sense of Chevalley

The goal of this section is the study of extensions of quadratic bundles defined over Zariski open subsets of projective curves over finite fields. One standard tool to study this kind of problem, is the language of *adeles*. In the following, we will try to explain how the adeles *naturally* (after Chevalley!) arise in algebraic geometry.

3.1. Abstract curves. — We would like to recall some properties of smooth (quasi-) projective curves over a field k [**Har97**, Ch. I, §6]. For any such a curve X, we denote by F its function field. Consider the following set

$$\mathcal{R}(X) := \{R \subset F \mid R \text{ is a valuation ring with quotient field } F\}.$$

Endow this set with the topology given by the closed sets:

$$\{S \subset \mathcal{R}(X) \mid \ S \text{ is finite}\},$$

(i.e. the topology given by the *Fréchet's filter* in Bourbaki's terminology) and with a sheaf of regular functions $\mathcal{O}_{\mathcal{X}}(U) := \cap_{R_\infty \in U} R_\infty$. Then, $\mathcal{R}(X)$ is called the **abstract (non-singular) curve** associated with F. So we know how to associate to a function field of transcendence degree 1, an abstract curve $\mathcal{R}(X)$ (the reverse of which is trivial):

$$F \rightsquigarrow \mathcal{R}(X).$$

Theorem 2.3.1. — [**Har97**, Ch. I, Thm. 6.9] *Any abstract nonsingular curve $\mathcal{R}(X)$ is isomorphic (as a locally ringed space) to a nonsingular projective curve X_F.* □

This correspondence enables us to study vector bundles on abstract curves, where the adeles naturally arise. It is worth to cite, that in [**EGAI**, §8], there is a more general correspondence established, between integral noetherian schemes and *Chevalley schemes* (loc. cit.); so the abstract nonsingular curve $\mathcal{R}(X)$ above is a one dimensional, smooth Chevalley scheme: a **curve in the sense of Chevalley**.
This somehow formal observation of Chevalley enables a concrete interplay between geometry and arithmetic. We illustrate this in more detail in the following section.

3.2. Vector bundles and double classes. — Let $\mathcal{E}$ be a vector bundle on a curve X. Denote by η the generic point of X, and by $K := \kappa(\eta)$ its function field. The vector bundle on the abstract curve $\mathcal{R}(X)$ is given by a collection of *local data* (on the *Chevalley side*) $\{\mathcal{E}_v\}_{v\in \mathrm{Val}(K)}$, where $\mathrm{Val}(K) :=: |X|$ is the set of places of K (i.e. the closed points of X). We can write equivalently $\{\widehat{\mathcal{E}_v}\}_{v\in \mathrm{Val}(K)}$, since $_\otimes_{\mathcal{O}_{X,v}} \widehat{\mathcal{O}_{X,v}}$ is a faithfully flat functor. A vector bundle is a locally trivial sheaf of constant rank, say m; in particular, whenever we choose a trivialization $\mathcal{E}\mid_U \cong (\mathcal{O}_X\mid_U)^{\oplus m}$, it induces on the side of the abstract curve, a trivial collection $\{\widehat{\mathcal{O}_{X,v}}\}_{v\in U}$, where $X\backslash U$ is finite. The bundle $\mathcal{E}$ is obtained by glueing such locally trivial bundles. The group given by the restricted product (cf. §1.1.4.1.1) $\mathrm{GL}_m(\mathbb{A}_K) := \prod'_{v\in \mathrm{Val}(K)} \{\mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}}), \mathrm{GL}_m(\widehat{K_v})\}$ acts on the *Chevalley side*. The stabilizer of the *locally trivial Chevalley bundles* are the integral matrices in $\mathrm{GL}_m(\mathbb{A}_K)$; namely $\mathrm{GL}_m(\mathbb{O}_K) := \prod_{v\in \mathrm{Val}(K)} \mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})$. Therefore, there is a surjection:

$$\tilde{\pi} : \mathrm{GL}_m(\mathbb{A}_K)/\mathrm{GL}_m(\mathbb{O}_K) \twoheadrightarrow \{\text{Rank-}m \text{ vector bundles over } X\}/\cong .$$

In order to establish a bijection, we study the construction of a vector bundle on X from a given compatible family $\{\widehat{\mathcal{E}_v}\}_{v\in \mathrm{Val}(K)}$, i.e. for any $v_0 \in \mathrm{Val}(K)$, there exists a matrix $M_{v_0} \in \prod_{v\in U_{v_0}} \mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})$, such that $M_{v_0}(\widehat{\mathcal{E}_v}) = \widehat{\mathcal{O}_{X,v}}^{\otimes m}$ for all $v \in U_{v_0}$ ($U_{v_0} \subset X$ is Zariski open). From the correspondence between X and $\mathcal{R}(X)$ as locally ringed spaces, we have $\Gamma(U, \mathcal{O}_X) = \cap_{v\in U}\mathcal{O}_{X,v}$, and therefore, for vector bundles: $\Gamma(U, \mathcal{E}) := \cap_{v\in U}\mathcal{E}_v = \cap_{v\in U}(\widehat{\mathcal{E}_v} \cap \mathcal{E}_\eta)$; which from the above, is a locally trivial sheaf of local constant rank m. Moreover, the subgroup $\mathrm{GL}_m(K) \subset \mathrm{GL}_m(\mathbb{A}_K)$ acts on the classes $\mathrm{GL}_m(\mathbb{A}_K)/\mathrm{GL}_m(\mathbb{O}_K)$. Therefore, there exists an induced action of $\mathrm{GL}_m(K)$ on the vector bundles over X, which is trival, since $\Gamma(U, \mathcal{E}) = \cap_{v\in U}(\widehat{\mathcal{E}_v} \cap \mathcal{E}_\eta) = \cap_{v\in U}(\widehat{\mathcal{E}_v} \cap T(\mathcal{E}_\eta))$ for all $T \in \mathrm{GL}(\mathcal{E}_\eta) = \mathrm{GL}_m(K)$. Hence,

$$\pi : \mathrm{GL}_m(K)\backslash \mathrm{GL}_m(\mathbb{A}_K)/\mathrm{GL}_m(\mathbb{O}_K) \twoheadrightarrow \{\text{Rank-}m \text{ vector bundles over } X\}/\cong . \tag{2.3.1}$$

Claim: *The map in* (2.3.1) *is a bijection.*

It remains to see the injectivity of the map. Let $\{\widehat{\mathcal{E}_v}^{\,i}\}_{v\in \mathrm{Val}(K)}$, $i = 1, 2$, be representatives of any two double classes, which have the same image under the map π. From the action of $\mathrm{GL}_m(K)$ we can suppose that all the lattices $\mathcal{E}_v^i = \widehat{\mathcal{E}_v}^{\,i} \cap \mathcal{E}_\eta$ ($i = 1, 2$) are inside the same fixed $K = \kappa(\eta)$-vector space $\mathcal{E}_\eta$ (send $\mathcal{E}_\eta^1$ isomorphically to $\mathcal{E}_\eta^2$). Denote by $\mathcal{E}_i := \pi(\{\widehat{\mathcal{E}_v}^{\,i}\}_{v\in \mathrm{Val}(K)})$, $i = 1, 2$, and by $\varphi : \mathcal{E}_1 \to \mathcal{E}_2$ an isomorphism of vector bundles on X. At the generic point η of X, $\varphi_\eta \in \mathrm{GL}(\mathcal{E}_\eta) = \mathrm{GL}_m(K)$. Locally, vector bundles are trivial, so $\widehat{\varphi_v}(\widehat{\mathcal{E}_{1,v}}) = \widehat{\mathcal{E}_{2,v}}$, and hence $\widehat{\varphi_v} \in \mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})$, which is just a *base change* of φ_η. Therefore, on the Chevalley side, we obtain locally everywhere matrices in $\mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})$, so $\{\widehat{\varphi_v}\}_{v\in X} \in \mathrm{GL}_m(\mathbb{O}_K)$; what proves the claim.
Summarizing,

Proposition 2.3.2. — *The map*

$$\mathrm{GL}_m(K)\backslash \mathrm{GL}_m(\mathbb{A}_K)/\mathrm{GL}_m(\mathbb{O}_K) \longrightarrow \{\textit{Rank-}m \textit{ vector bundles over } X\}/\cong$$

constructed above is bijective.

3.3. Extensions. —

[3.1] *Extensions of vector bundles.* — We return to our problem of extending a given vector bundle on an affine Zariski subset U of X. From the discussion above, it is easy to prove

Proposition 2.3.3. — *The extensions of a given vector bundle $\mathcal{E}$ on U to the whole curve X are parametrized by $\prod_{v\in X\setminus U}\mathrm{GL}_m(K)/\mathrm{GL}_m(\mathcal{O}_{X,v})$.*

Proof. — From the group theoretical interpretation above, this kernel is given by

$$\frac{\mathrm{GL}_m(\mathbb{A}_K)/\mathrm{GL}_m(\mathbb{O}_K)}{\prod'_{v\in U}\mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})/\prod_{v\in U}\mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})}\cong\prod_{v\in X\setminus U}\mathrm{GL}_m(\widehat{K_v})/\mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})\cong$$
$$\cong\prod_{v\in X\setminus U}\mathrm{GL}_m(K_v)/\mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})\cap\mathrm{GL}_m(K_v)\cong$$
$$\cong\prod_{v\in X\setminus U}\mathrm{GL}_m(K_v)/\mathrm{GL}_m(\mathcal{O}_{X,v}).$$

The second isomorphism follows from the observation that

$$\mathrm{GL}_m(\widehat{K_v})=\mathrm{GL}_m(\widehat{\mathcal{O}_{X,v}})\,\mathrm{GL}_m(K_v),$$

which is easy to see, since $\mathrm{GL}_m(K_v)$ is dense in $\mathrm{GL}_m(\widehat{K_v})$. □

[3.2] *Extensions of quadratic bundles.* — Endow $\mathcal{E}$ with a symmetric bilinear form $\mathfrak{b}_U:\mathrm{Sym}^2(\mathcal{E})\to\mathcal{L}$ with values in certain line bundle $\mathcal{L}\in\mathrm{Pic}(U)$. We can ask ourselves for the extensions of this quadratic form to the whole X. From the above proposition, we have extensions for $\mathcal{E}$ and $\mathcal{L}$ to X parametrized by $\prod_{v\in X\setminus U}\mathrm{GL}_r(K)/\mathrm{GL}_r(\mathcal{O}_{X,v})$ for $r=m$ and $r=1$ respectively. Fix extensions $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{L}}$ of the given bundles. We want to study the fibers of

$$\Gamma(X,(\mathrm{Sym}^2(\tilde{\mathcal{E}}))^*\otimes_{\mathcal{O}_X}\tilde{\mathcal{L}})\xrightarrow{\rho_U}\Gamma(U,(\mathrm{Sym}^2(\mathcal{E}))^*\otimes_{\mathcal{O}_X}\mathcal{L}).$$

Theorem 2.3.4. — *Let $U=\mathrm{Spec}(R)$ be an affine Zariski open subset of a curve X over a finite field k, and let $\mathfrak{b}_U:\mathrm{Sym}^2(\mathcal{E})\to\mathcal{L}$ be a quadratic form on $\mathcal{E}$ over U with values on the line bundle $\mathcal{L}$. Then, there exist finitely many isometry classes of quadratic forms $\tilde{\mathfrak{b}}:\mathrm{Sym}^2(\tilde{\mathcal{E}})\longrightarrow\tilde{\mathcal{L}}$, such that $\tilde{\mathfrak{b}}\mid_U=\mathfrak{b}_U$, for given bundle extensions $\tilde{\mathcal{E}}$, $\tilde{\mathcal{L}}$. This number is uniformly bounded.*

Proof. — Denote by S the finitely many (closed) points of $X\setminus U$. Pick any $\mathfrak{p}_\infty\in S$. Write $\mathbb{V}(\mathrm{Sym}^2(\tilde{\mathcal{E}})^*\otimes\tilde{\mathcal{L}})$ for the projective scheme of all quadratic forms up to *scalars*. Over a Zariski open, affine $U_0:=\mathrm{Spec}(R_0)\subset X$

$$\mathbb{V}(\mathrm{Sym}^2(\tilde{\mathcal{E}})^*\otimes\tilde{\mathcal{L}})(U_0):=\mathrm{Proj}(\mathrm{Sym}_{R_0}(\mathrm{Hom}_{R_0}(\mathrm{Sym}^2(\tilde{\mathcal{E}})^*\otimes\tilde{\mathcal{L}},R_0));$$

i.e. the fibers of this vector bundle over the Zariski open, affine subschemes of X are projective schemes of the symmetric algebra of the coherent sheaf $(\mathrm{Sym}^2(\tilde{\mathcal{E}}))^*\otimes\tilde{\mathcal{L}}$ (see §1.2.4). There exists clearly an extension of the quadratic form to the completion of the function field K of X with respect to $\mathfrak{p}_\infty$ (just by base change, which gives a *quadratic space*), and any other possible extension is similar over $\mathrm{Spec}(K_\infty)$ to this one (cf. [**Eic73**, §II]). Hence, we have a uniquely determined section of the projective bundle $\mathbb{V}(\mathrm{Sym}^2(\tilde{\mathcal{E}})^*\otimes\tilde{\mathcal{L}})$. By the valuative criterion of properness ([**Har97**, Ch.II, §4]), we have a unique dotted arrow

$$\begin{array}{ccc}\mathrm{Spec}(K_\infty) & \xrightarrow{\mathfrak{b}_\infty} & \mathbb{P}(\mathrm{Sym}^2(\tilde{\mathcal{E}})^*\otimes\tilde{\mathcal{L}})\\ {\scriptstyle i}\downarrow & \nearrow_{\tilde{\mathfrak{b}}_\infty} & \\ \mathrm{Spec}(R_\infty) & & \end{array},$$

which lifts $\mathfrak{b}_\infty$. Therefore, the extension is unique up to multiplying by a scalar $K_\infty^\times$. We will show, that this scalar has bounded valuation from above and from below. Hence, using that $k^\times/k^{\times 2}$ is finite

and the valuation discrete, we have only finitely many classes which extend $\mathfrak{b}_\infty$. We do this with each point at infinity, and the claim follows.
The valuation is obviously bounded from below, since the bundles $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{L}}$ are fixed. From above is also bounded, since the curve X is projective, hence we consider it as a covering of $\mathbb{P}^1_k$, with $S \subset X$ the support of the fiber over $\infty = (T_1) \in \mathbb{P}^1_k := \mathrm{Proj}(k[T = T_0, T_1])$. An arbitrarily high power of the uniformizer at $\mathfrak{p}_\infty \in X$ would give an arbitrarily negative power of the uniformizer at T, which is impossible, since the values of the quadratic bundle at any point above T are uniformly bounded from below (by $\mathcal{L}$, i.e. the form should take values in $\mathcal{L}$).
The last assertion is now clear from the proof. □

The property of a quadratic bundle of being *definite* depends on the points at infinity. We have just seen that a quadratic bundle on a Zariski open dense subset $U = X \setminus S$ possesses (different) extensions to the points S at infinity. From the proof of Theorem 2.3.4 we obtain the following

Corollary 2.3.5. — *Fix a pair of extensions $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{L}}$ of given vector bundles $\mathcal{E}$ and $\mathcal{L}$ on a Zariski open subset $U \subset X$. Then, if one extension to X of a quadratic bundle on U is definite, then so are all the others.*

CHAPTER 3

ORTHOGONAL GROUPS ON CURVES OVER FINITE FIELDS

In this chapter we set up the language and definitions and prove basic facts before introducing the Minkowski-Siegel formula in a geometrical setting.

Notation. — Let $X/\operatorname{Spec}(\mathbb{F}_q)$ be a smooth, projective, geometrically irreducible curve; $\mathcal{E}$ a vector bundle with a quadratic form on it $\mathfrak{b} : \operatorname{Sym}^2(\mathcal{E}) \to \mathcal{L}$ (recall we assume $2 \in \mathcal{O}_X^\times$), where $\mathcal{L}$ is any line bundle on X. Denote by K the rational function field of X, by $\operatorname{Val}(X)$ the set of all inequivalent places of K (which is in one to one correspondence with the set of all closed rational points of X). For a valuation (place) $v \in \operatorname{Val}(X)$, K_v will denote the completion of K with respect to v. By abuse of notation, let us write $\mathcal{E}$ or simply $\mathfrak{b}$ for $(\mathfrak{b}, \mathcal{E}, \mathcal{L})$. Let $S_\infty \subset \operatorname{Val}(X)$ be a fixed finite set of "points" on X, which we declare to be the *points at infinity*. The subset $U := X \setminus S_\infty$ is affine and Zariski open, say $U = \operatorname{Spec}(R)$.

It is well known, that rank 4 quadratic forms over local fields are universal, therefore

Theorem 3.0.6. — *After base change to* $\operatorname{Spec}(K_v)$*, the quadratic form* $\mathfrak{b}_v$ *is isotropic if* $\operatorname{rk}(\mathcal{E}) \geq 5$*; i.e. there exists a non zero section* v *of* $\mathcal{E} \otimes K_v$*, such that* $\mathfrak{b}_v(v) = 0$.

Remark 3.0.7. — If $rk(\mathcal{E}) \geq 5$, there are no definite quadratic forms on it (recall Definition 1.2.22).

Although it will not be everywhere necessary in this chapter, we restrict to definite quadratic bundles, so in particular $\operatorname{rk}(\mathcal{E}) \leq 4$.

1. The group scheme $\mathrm{O}(\mathcal{E})$

1.1. Good models. — The orthogonal group over X is represented by a subgroup scheme over X (see Proposition 1.2.26)

$$\mathrm{O}(\mathcal{E}) := \mathrm{O}(\mathfrak{q}, \mathcal{E}, \mathcal{L}) := \{\varphi \in \mathrm{GL}(\mathcal{E}) \mid \mathfrak{b} \circ \operatorname{Sym}^2(\varphi) = \mathfrak{b}\} \subset \mathrm{GL}(\mathcal{E}).$$

Denote by $\mathrm{O}(\mathcal{E})_K$ the group scheme over $\operatorname{Spec}(K)$ obtained by base change to the generic point $\eta \in X$.

Definition 3.1.1. — A **good model** of $\mathrm{O}(\mathcal{E})_K$ over a Zariski open, dense $Y \subset X$ is a smooth affine group scheme $\mathcal{G}_Y$ over Y, together with a morphism $\mathrm{O}(\mathcal{E})_K \to \mathcal{G}_Y$ and a map $\mathcal{G}_Y \to \mathrm{O}(\mathcal{E})_Y$ inducing

an isomorphism over the smooth locus of $\mathrm{O}(\mathcal{E})_Y$, and making the following diagram commutative

$$\begin{array}{ccc} & & \mathcal{G}_Y \\ & \nearrow & \downarrow \\ \mathrm{O}(\mathcal{E})_K & \hookrightarrow & \mathrm{O}(\mathcal{E})_Y \\ \downarrow & & \downarrow \\ \eta & \hookrightarrow & Y\,. \end{array}$$

Theorem 3.1.2. — *The orthogonal group* $\mathrm{O}(\mathcal{E})$ *is a good model over an affine, Zariski open subset* $\mathrm{Spec}(A)$ *of* X*, if and only if* $\mathrm{supp}(\mathrm{discr}(\mathcal{E})) \cap \mathrm{Spec}(A) = \emptyset$*.*

Sketch. — The necessity is clear from the classification of anisotropic quadratic forms over local fields (over local rings not of characteristic 2, we can diagonalize the forms!). We easily see also, that the orthogonal group is a smooth scheme over $\mathrm{Spec}(A)$, when the intersection above is empty. Namely, if we denote by $\bar{k}_v$ the algebraic closure of the residue field with respect to the valuation $v \in \mathrm{Val}(\mathrm{Spec}(A))$, the $\bar{k}_v$-algebra $\Gamma(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{O}(\mathcal{E})}) \otimes \bar{k}_v$ should be reduced, which is clear, since the form is similar to the trivial diagonal form. □

The good model obtained from above, with least number of points at infinity, is denoted by $\mathrm{O}(\mathcal{E})_\circ$ and $R_\circ := \cap' \mathcal{O}_{X,\mathfrak{p}}$, where the prime means that the intersection is to be taken over all points $\mathfrak{p}$ at which the group $\mathrm{O}(\mathcal{E})$ has good reduction. These points may be also called **regular primes**. The set of points on the curve outside $\mathrm{Spec}(R_\circ)$ is denoted by $S_\circ$.

Again, from the local classification of quadratic forms we have

Proposition 3.1.3. — *If* $\mathrm{rk}(\mathcal{E})$ *is greater than* 2*, then* $S_\circ$ *is exactly the set of points where the quadratic form is anisotropic.*

Remark 3.1.4. — In the rank 2 case, for example, the assertion of the proposition above is not true. The quadratic form $x^2 - \delta y^2$ is anisotropic over a point of even degree (δ a non-square), whereas the orthogonal group has good reduction.

Therefore, definite quadratic bundles on X of rank 3 or 4 are *never* regular (i.e. $S_\circ \neq \emptyset$). Moreover, the support of the divisor at infinity must be contained in the support of the discriminant of the bundle.

In the classical case, the discriminant of (positive) definite quadratic forms is negative *by convention*. In fact, this is not a mere convention. To be more rigorous, one should actually put, in this case, the point at infinity in the discriminant. For example a positive definite, rational integral, ternary quadratic form of discriminant $-p$, has discriminant $\infty \cdot p$. This can be better understood from the definition of the discriminant of the associated quaternion algebra, via its even Clifford algebra, say.

1.2. Reductiveness of the orthogonal group. — *As far as I know, the following result is well known in the frame of* Bruhat-Tits Theory *(cf.* [**BT87**]*). Instead we give here a simple proof.*

Theorem 3.1.5. — *The special orthogonal group* $\mathrm{SO}(\mathcal{E})_\circ$ *is a reductive group; i.e. affine, smooth with connected and reductive geometric fibers.*

Proof. — Need only to check reductiveness. For rank $1, 2$ it is clear, hence for rank 4. For rank three, our form is locally $y^2 - xz$, since for reductiveness (cf. [**SGAD**, Exposé XIX]) we can pass to the

algebraic closure. The nilradical of $\mathrm{Lie}(\mathrm{O}(\mathcal{E}))$ consists of elements of the form $\begin{bmatrix} a_{11} & a_{12} & 0 \\ 2a_{23} & 0 & 2a_{12} \\ 0 & a_{32} & -a_{11} \end{bmatrix}$ whose square

$$\begin{bmatrix} a_{11}^2 - a_{12}^2 + a_{32}a_{31} & a_{11}a_{12} & 2a_{12}^2 \\ 2a_{11}a_{32} & 4a_{12}a_{32} & -2a_{11}a_{12} \\ 2a_{32}^2 & -a_{11}a_{32} & 2a_{12}a_{32} + a_{11}^2 \end{bmatrix}$$

is zero. This ideal is visibly trivial, so the claim.
Please note, that we have made use of a couple of basic nontrivial results about p-Lie algebras of (unipotent) group schemes. Namely, the unipotent subgroup scheme corresponds to the nilpotent ideal of the Lie-algebra and that for any presentation of the group chosen, unipotent elements go to unipotent ones (a consequence of *Jordan's Theorem*). See for this [**Bor91**, Chapter I, §4]. □

Remark 3.1.6. — The nilpotent ideal of the Lie Algebra of quadratic bundles at anisotropic points is also trivial. We do not include here the rather lengthy computations, since in general, the wanted result, the orthogonal group over X be reductive, is clearly *false*: the orthogonal group over X is *not* even flat for definite forms (non regular), say of rank greater than 2, since the dimensions of the orthogonal groups on the fibers, jump up precisely at the points where the form is not unimodular (cf. Proposition 3.1.3).

2. Adele Orthogonal Group and Haar-measure

2.1. Adele orthogonal group. — We make the following notational

Convention 2. From now on, $*_v$ will denote the completion of $*$ with respect to the valuation v, instead of $\hat{*}_v$.

Pick a divisor *at infinity* $S_\infty \subset X$, and denote $R := \Gamma(X \setminus S_\infty, \mathcal{O}_X)$, $U := \mathrm{Spec}(R)$. The base change of $\mathcal{E}$ to a completion K_v of K with respect to a place/point v will be denoted by $\mathcal{E}_{v,(0)}$; which is a K_v-vector space of dimension $m := \mathrm{rk}(\mathcal{E})$. Any completion $R \hookrightarrow R_v$ induces a map in geometry which enables us to evaluate

$$\mathrm{O}(\mathcal{E})(\mathrm{Spec}(R_v)) =: \mathrm{O}(\mathcal{E}_v).$$

Equivalently we write $\mathrm{O}(\mathcal{E}_{v,(0)})$ or $\mathrm{O}(\mathfrak{b}_{v,(0)}, \mathcal{E}_{v,(0)}, \mathcal{L}_{v,(0)})$ for $\mathrm{O}(\mathcal{E})(\mathrm{Spec}(K_v))$.

Unless otherwise stated, S_* stands for a finite set of places of K containing S_∞, where $*$ is any sequence of characters (possibly empty).
For any (finite set of places) S containing S_∞, we define:

$$\mathrm{O}_S(\mathcal{E}) := \{(u_v) \in \prod_{v \in \mathrm{Val}(X)} \mathrm{O}(\mathcal{E}_{v,(0)}) \mid u_v \in \mathrm{O}(\mathcal{E}_v)\ \forall v \notin S\},\ \text{and}$$

$$\mathrm{O}_{S,\mathrm{f}}(\mathcal{E}) := \{(u_v) \in \prod_{v \notin S_\infty} \mathrm{O}(\mathcal{E}_{v,(0)}) \mid u_v \in \mathrm{O}(\mathcal{E}_v)\ \forall v \notin S\};$$

both endowed with the induced product topology.

Definition 3.2.1. — The group

$$\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}) := \mathrm{O}_{\mathbb{A}_K}(\mathfrak{b}, \mathcal{E}, \mathcal{L}) := \varinjlim_{S_\infty \subset S \subset \mathrm{Val}(X)} \mathrm{O}_S(\mathcal{E})$$

is called the **adele orthogonal group** and

$$\mathrm{O}_{\mathbb{A}_{\mathrm{f}}}(\mathcal{E}) := \mathrm{O}_{\mathbb{A}_{\mathrm{f}}}(\mathfrak{b}, \mathcal{E}, \mathcal{L}) := \varinjlim_{S_\infty \subset S \subset \mathrm{Val}(X)} \mathrm{O}_{S,\mathrm{f}}(\mathcal{E})$$

is the **finite adele orthogonal group** associated with the quadratic bundle $(\mathfrak{b}, \mathcal{E}, \mathcal{L})$.

Remark 3.2.2. — In this chapter we develop the theory for $\mathrm{O}_{\mathbb{A}_K}$, valid without changes for the finite adeles. The results in chapter 4 from here (Propositions 3.3.3 and 3.3.8) are clearly valid for the finite adeles as well.

The topology in $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E})$ is the inductive limit topology, namely the one given by

$$\cup_{S \subset \mathrm{Val}(X)} \mathrm{O}_S(\mathcal{E})/\mathcal{R},$$

where $(\alpha_{S_1}, \alpha_{S_2}) \in \mathcal{R} \iff \iota_{S_1,S_2}(\alpha_{S_1}) = \iota_{S_2,S_1}(\alpha_{S_2})$, for

$$\begin{array}{ccccc} & & \mathrm{O}_{S_1 \cup S_2}(\mathcal{E}) & & \\ & \overset{\iota_{S_1 \cup S_2}}{\nearrow} & & \overset{\iota_{S_2 \cup S_1}}{\nwarrow} & \\ \mathrm{O}_{S_1}(\mathcal{E}) & & & & \mathrm{O}_{S_2}(\mathcal{E})\ . \end{array}$$

Remark 3.2.3. — The adele orthogonal group $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E})$ can be seen also as the group of adelic points $\mathrm{O}(\mathcal{E})(\mathbb{A}_K)$ of the the orthogonal K-group scheme $\mathrm{O}(\mathcal{E})$ (cf. §1.1.4.1.1). The same is valid for $\mathbb{A}_{\mathrm{f}}$ instead of $\mathbb{A}_K$.

We recall some basic facts about orthogonal groups (see [**Eic73**], [**O'M00**] or more generally [**Wei82**]).

(1) A subset $\mathcal{G} \subset \mathrm{O}_{\mathbb{A}_K}(\mathcal{E})$ is open (closed) if and only if $\iota_S^{-1}(\mathcal{G}) \subset \mathrm{O}_S(\mathcal{E})$ is open (closed) for all S.

(2) The subgroups

$$\mathrm{O}_S(\mathcal{E}) = \textstyle\prod_{v \notin S} \mathrm{O}(\mathcal{E}_v) \times \prod_{v \in S} \mathrm{O}(\mathcal{E}_{v,(0)}) \hookrightarrow \mathrm{O}_{\mathbb{A}_K}(\mathcal{E})$$

are open and locally compact. The groups $\mathrm{O}(\mathcal{E}_v)$ are indeed compact.

(3) The adele orthogonal group $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}) = \varinjlim_{S \subset \mathrm{Val}(X)} \mathrm{O}_S(\mathcal{E})$ is locally compact.

2.2. Congruence subgroups. —

[2.1] *Local principal congruence subgroups.* — Let $v \in \mathrm{Val}(X) \setminus S_\infty$ be any "finite" valuation, and $\gamma \in R_v$. Since $\mathcal{E}$ is a vector bundle, the endomorphism of $\mathcal{E}_v$ given by multiplication by γ is injective. Hence we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{E}_v & \xrightarrow{\gamma\cdot} & \mathcal{E}_v & \longrightarrow & \mathcal{E}_v/\gamma\mathcal{E}_v & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_v} & & \downarrow{\scriptstyle \varphi_v} & & & & \\ 0 & \longrightarrow & \mathcal{E}_v & \xrightarrow{\gamma\cdot} & \mathcal{E}_v & \longrightarrow & \mathcal{E}_v/\gamma\mathcal{E}_v & \longrightarrow & 0 \end{array}$$

with exact rows. A simple application of the *snake lemma* shows that we have a homomorphism $\psi_{v,\gamma} : \mathrm{O}(\mathcal{E}_v) \to \mathrm{GL}(\mathcal{E}_v/\gamma\mathcal{E}_v)$ (shortly: the orthogonal group is a functor). We define $\mathrm{O}(\mathcal{E}_v, \gamma)$ to be the

kernel of this homomorphism.

Claim. $\mathrm{O}(\mathcal{E}_v, \gamma) \subset \mathrm{O}(\mathcal{E}_v)$ is a closed and open subgroup.
Set $\mathfrak{a} := \mathrm{ann}_{R_v}(\mathcal{E}_v/\gamma\mathcal{E}_v) = \gamma R_v$, then $\mathcal{E}_v/\gamma\mathcal{E}_v$ has structure of $R_v/\mathfrak{a}$ module of finite rank ($\mathfrak{a}$ is not zero!). Since this last quotient ring is finite, we conclude $\mathrm{GL}(\mathcal{E}_v/\gamma\mathcal{E}_v)$ is finite. This space has the discrete topology, so $\{\mathrm{Id}_{\mathcal{E}_v/\gamma\mathcal{E}_v}\}$ is closed and open; hence the claim.

Another kind of local congruence subgroups can be defined as follows. For a valuation v in $\mathrm{Spec}(R_\circ)$ (i.e. a place of good reduction), we choose a uniformizer element π_v and a natural number $n_v \in \mathbb{N}_0$.

$$\mathrm{O}(\mathcal{E}_v, \pi_v^{n_v}\mathcal{O}_v) := \psi_{v,\gamma}^{-1}(\mathrm{Centr}(\mathrm{O}(\mathcal{E}_v/\pi_v^{n_v}\mathcal{O}_v))),$$

which follows from the formal smoothness of the group functor $\mathrm{O}(\star)$ at v, since at this place the orthogonal group was assumed to be smooth (cf. [**SGAD**, Exposé XI, §1]).

Clearly, $\mathrm{O}(\mathcal{E}_v, \gamma) \subset \mathrm{O}(\mathcal{E}_v, \pi_v^{v(\gamma)}\mathcal{O}_v)$, and

$$\Big[\mathrm{O}(\mathcal{E}_v, \pi_v^{v(\gamma)}\mathcal{O}_v) : \mathrm{O}(\mathcal{E}_v, \gamma)\Big] = |\mathrm{Centr}(\mathrm{O}(\mathcal{E}_v \otimes \mathcal{O}_v/\pi_v^{v(\gamma)}\mathcal{O}_v))|.$$

Remark 3.2.4. — (1) With this second definition in mind, we observe, that we can define congruence subgroups with respect to any (normal) subgroup $\mathcal{Z}_v$ of $\mathrm{O}(\mathcal{E}_v \otimes \mathcal{O}_v/\pi_v^{n_v}\mathcal{O}_v)$. We will suppose this subgroup to be trivial, when the orthogonal group has bad reduction at v.

(2) For a Haar measure μ on the locally compact group $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E})$, we have

$$\mu(\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \gamma R)) = \mu(\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \gamma)) \prod_{\substack{v \in \mathrm{Val}(X) \\ v(\gamma) > 0}} |\mathrm{Centr}(\mathrm{O}(\mathcal{E}_v \otimes R_v/\pi_v^{v(\gamma)}R_v))|.$$

[2.2] *Principal congruence subgroups.* — To an idele α with non-negative valuations at finite places, we can associate the group

$$\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \alpha) := \prod_{v \notin S_\infty} \mathrm{O}(\mathcal{E}_v, \alpha_v) \times \prod_{v \in S_\infty} \mathrm{O}(\mathcal{E}_v).$$

The definition of $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \alpha)$ is naturally invariant by $\mathbb{A}_{S_\infty}^\times$:

$$\text{for } \alpha_0 \in \mathbb{A}_{S_\infty}^\times,\ \mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \alpha_0\alpha) = \mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \alpha).$$

Therefore, this definition descends to the R-ideals (recall (1.1.3)):

Definition 3.2.5. — Let $\mathfrak{a} \subset R$ be an ideal, and α any lifting of $\mathfrak{a}$ to the idele group of K. The subgroup

$$\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \mathfrak{a}) := \prod_{v \notin S_\infty} \mathrm{O}(\mathcal{E}_v, \alpha_v) \times \prod_{v \in S_\infty} \mathrm{O}(\mathcal{E}_v),$$

is called a **principal congruence subgroup** of $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E})$.

Remark 3.2.6. — For the zero ideal of R, the definition makes also sense:

$$\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, 0) := \prod_{v \in \mathrm{Val}(X)} \mathrm{O}(\mathcal{E}_v).$$

With this, $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, \mathfrak{a}) \subset \mathrm{O}_{\mathbb{A}_K}(\mathcal{E}, 0)$.

Lemma 3.2.7. — *Any two principal congruence subgroups are commensurable.*

Proof. — Let $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E},\mathfrak{a})$ and $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E},\mathfrak{b})$ be two principal congruence subgroups, and denote by α, respectively β, any lifting of the ideals to the ideles. It is clearly sufficient to check the claim locally; which follows from the following commutative diagram

$$\begin{array}{ccc} \mathcal{O}_v & \longrightarrow & \mathcal{O}_v/\mathfrak{M}_v^n \\ & \searrow & \downarrow \\ & & \mathcal{O}_v/\mathfrak{M}_v^{n+m} \end{array}$$

for non negative integers $n > 0$, m. Applying the functor of points of the orthogonal group $\mathrm{O}(\mathcal{E})$, we observe, that $\mathrm{O}(\mathcal{E}_v,\pi_v^{n+m})$ is contained in $\mathrm{O}(\mathcal{E}_v,\pi_v^n)$, certainly with finite index (cf. §3.2.2.1). The ideles coincide almost everywhere, so the claim. □

Remark 3.2.8. — We see also from the proof above, that $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E},\mathfrak{a})\cap\mathrm{O}_{\mathbb{A}_K}(\mathcal{E},\mathfrak{b}) = \mathrm{O}_{\mathbb{A}_K}(\mathcal{E},\mathrm{lcm}(\mathfrak{a},\mathfrak{b}))$; since on the side of the ideles (with the previous notation), a lifting of the ideal $\mathrm{lcm}(\mathfrak{a},\mathfrak{b})$ in the ideles is $\prod_{v\notin S_\infty}\pi_v^{\max_{n\in\mathbb{N}}\{v(\alpha_v),v(\beta_v)\}}$, which gives this intersection.

[2.3] *Congruence subgroups.* — Here we define a Haar measure on a certain Borel[VII] algebra, suitable for our computational purposes.

Definition 3.2.9. — A **congruence subgroup** $\mathcal{G}\subset\mathrm{O}_{\mathbb{A}_K}(\mathcal{E})$ is a subgroup which is locally almost everywhere $\mathrm{O}(\mathcal{E}_v)$ (including all $v\in S_\infty$), and for each other place v, it is the pre-image of a normal subgroup of $\mathrm{O}(\mathcal{E}_v\otimes\mathcal{O}_v/\pi_v^{n_v}\mathcal{O}_v)$ under $\psi_{v,n_v} := \psi_{v,\pi_v^{n_v}}$.

Any congruence subgroup $\mathcal{G}$ contains a principal congruence subgroup.

2.3. Haar measure. — Define

$$\mathcal{A}(\mathcal{E}) := \{\cup_{k=1}^n \cap_{l=1}^{m_n} u_{k,l}\,\mathrm{O}(\mathcal{E},\mathfrak{a}_{k,l}) \mid u_{k,l}\in\mathrm{O}_{\mathbb{A}_K}(\mathcal{E}),\ \mathfrak{a}_{k,l}\subset\Gamma(U,\mathcal{O}_X)\}\cup\{\emptyset\}.$$

Proposition 3.2.10. — *The set $\mathcal{A}(\mathcal{E})$ is an* algebra of sets *(in the sense of measure theory); i.e. the following conditions are satisfied*

SR1. $\emptyset\in\mathcal{A}(\mathcal{E})$*;*
SR2. $A,B\in\mathcal{A}(\mathcal{E})\Rightarrow A\cap B\in\mathcal{A}(\mathcal{E})$*;*
SR3. $A,B\in\mathcal{A}(\mathcal{E})\wedge A\subset B\Rightarrow B = A\cup\dot{\bigcup}_{k=1}^n A_k;\ A_k\in\mathcal{A}(\mathcal{E})$;
R1. *finite unions of elements of $\mathcal{A}(\mathcal{E})$ belong again to this set;*
A. *$\mathcal{A}(\mathcal{E})$ has a* **unit** *(set), i.e.*

$$\exists\, E\in\mathcal{A}(\mathcal{E}),\ \text{such that}\ \forall\mathcal{G}\in\mathcal{A}(\mathcal{E}):\ E\cap\mathcal{G} = \mathcal{G}.$$

Proof. — The first condition is satisfied by definition.
Take locally any two translated pre-images of subgroups, say $\mathcal{Z}_v(\alpha)\subset\mathrm{O}(\mathcal{E}_v,\alpha_v)$ and $\mathcal{Z}_v(\beta)\subset\mathrm{O}(\mathcal{E}_v,\beta_v)$, by u_v, $v_v\in\mathrm{O}(\mathcal{E}_v)$ respectively. Suppose, without loss of generality, $n_v := v(\alpha_v)\le m_v := v(\beta_v)$. We have the following diagram

(3.2.1)
$$\begin{array}{ccc} & & \mathrm{O}(\mathcal{E}\otimes\mathcal{O}_v/\mathfrak{M}_v^{n_v})\supset\mathcal{Z}_v(\alpha) \\ & \overset{\pi_{v,n_v}}{\nearrow} & \uparrow \\ \mathrm{O}(\mathcal{E}_v) & & \psi_{m_v,n_v} \\ & \underset{\pi_{v,m_v}}{\searrow} & \\ & & \mathrm{O}(\mathcal{E}\otimes\mathcal{O}_v/\mathfrak{M}_v^{m_v})\supset\mathcal{Z}_v(\beta) \end{array}$$

From the next lemma we obtain

$$u_v\pi_{v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap v_v\pi_{v,m_v}^{-1}(\mathcal{Z}_v(\beta))=$$
$$=\left(\underset{\lambda}{\cup}\, u_vu_\lambda\pi_{v,m_v}^{-1}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta))\right)\cap$$
$$\cap\left(\underset{\rho}{\cup}\, v_vv_\rho\pi_{v,m_v}^{-1}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta))\right)=$$
$$=\underset{\rho'}{\cup}\, w_{\rho'}\pi_{v,m_v}^{-1}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta)),$$

for appropriate $w_{\rho'}$'s; which implies SR2, after pasting the local information. SR3 follows directly from this decomposition and R1 is obvious. With these properties satisfied, we already have a ring of sets. This ring of sets is called and algebra if it additionally has a unit (cf. A). In this case, the unit E is $\mathrm{O}_{\mathbb{A}_K}(\mathcal{E},0)$ (see Remark 3.2.6). □

Lemma 3.2.11. — *Let the notation be as in the proof above (recall $n_v\leq m_v$), we have*

$$\dot\cup\, u_\lambda\pi_{v,m_v}^{-1}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta))=\pi_{v,n_v}^{-1}(\mathcal{Z}_v(\alpha)),$$

and also

$$\dot\cup\, v_\rho\pi_{v,m_v}^{-1}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta))=\pi_{v,m_v}^{-1}(\mathcal{Z}_v(\beta)),$$

for certain finitely many local orthogonal transformations u_λ and $v_\rho\in\mathrm{O}(\mathcal{E}_v)$.

Proof. — From (3.2.1), we observe that $\pi_{v,m_v}^{-1}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta))$ is a subgroup of $\pi_{v,n_v}^{-1}(\mathcal{Z}_v(\alpha))$ and of $\pi_{v,n_v}^{-1}(\mathcal{Z}_v(\beta))$; clearly of finite index in both. The index in the latter is the order of $\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta)\backslash\mathcal{Z}_v(\beta)$, and lifting (when possible) these classes, we get orthogonal transformations $v_\rho\in\mathrm{O}(\mathcal{E}_v)$ which give us the decomposition

$$\pi_{v,m_v}^{-1}(\mathcal{Z}_v(\beta))=\dot\cup\, v_\rho\pi_{v,m_v}^{-1}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta)).$$

For the other decomposition, the "chasing" is almost the same, but for example the number of co-sets covering $\pi_{v,n_v}^{-1}(\mathcal{Z}_v(\alpha))$ is not (necessarily) the cardinality of a quotient group! Take lifts via π_{v,n_v} of the finitely many classes $\psi_{m_v,n_v}(\psi_{m_v,n_v}^{-1}(\mathcal{Z}_v(\alpha))\cap\mathcal{Z}_v(\beta))\backslash\mathcal{Z}_v(\alpha)$. The problem now, is that these lifts may *not* be enough to give a complete covering. The reason is that any two lifts u_λ and u'_λ of a given class $\overline{u_\lambda}$ do not necessarily give the same co-sets. They only do, when $\psi_{m_v,n_v}^{-1}(\pi_{v,n_v}(u_\lambda^{-1}u'_\lambda))$ belongs to $\mathcal{Z}_v(\beta)$. Since there are only finitely many possibilities for $\psi_{m_v,n_v}^{-1}(\pi_{v,n_v}(u_\lambda^{-1}u'_\lambda))$ not to be in $\mathcal{Z}_v(\beta)$, we have again a finite union. The disjointness is clear, so the proof is finished. □

Remark 3.2.12. — The lemma says that any two elements of the algebra (none being empty) are commensurable.

We have also from lemma 3.2.11

Corollary 3.2.13. — *Any element of the algebra $\mathcal{A}(\mathcal{E})$ can be written as $\cup_{k=1}^N u_k\,\mathrm{O}(\mathcal{E},\mathfrak{a}_k)$.*

A semi-ring of sets (in particular an algebra) generates an algebra of sets (itself), and a measure on the semi-ring can be uniquely extended to the algebra (see [**KF75**] for these concepts and proofs). Moreover, since the sets in our algebra are *commensurable* between each other (modulo translations), any measure invariant under translations will be also σ-additive, which allows us to extend the measure to a larger class of measurable sets; namely to the **Borel algebra** $\mathcal{B}(\mathcal{E})$ generated by $\mathcal{A}(\mathcal{E})$. The extended measure to the Borel algebra, known as the **Lebesgue extension** of the former, will be also σ-additive. A Haar measure on $\mathcal{A}(\mathcal{E})$ can be given just by arbitrarily fixing the measure for a principal congruence subgroup: $\mu(\mathrm{O}(\mathcal{E},\mathfrak{a}))=\mu_0\in\mathbb{R}_{>0}$ for some ideal $\mathfrak{a}$.

Namely, since any congruence subgroup contains a principal congruence subgroup, and the last one is of finite index in the first, and any two principal congruence subgroups are commensurable; we can compute the measure of the congruence subgroup from the measure $\mu(\mathrm{O}(\mathcal{E},\mathfrak{a})) = \mu_0$. Also the Borel-measurable sets can be written in such a way, that knowing the measure of a congruence subgroup, one can compute the measure of the Borel set itself.

In symbols, let $\emptyset \neq A = \cup_{\lambda\in\mathbb{N}} u_\lambda \,\mathrm{O}(\mathcal{E},\mathfrak{a}_\lambda) \in \mathcal{B}(\mathcal{E})$. To compute its measure, we write first $A_n := \cup_{\substack{\lambda\in\mathbb{N}\\ \lambda\leq n}} u_\lambda \,\mathrm{O}(\mathcal{E},\mathfrak{a}_\lambda)$, and $\mathcal{I}_n := \cap_{\substack{\lambda\in\mathbb{N}\\ \lambda\leq n}} u_\lambda \,\mathrm{O}(\mathcal{E},\mathfrak{a}_\lambda)$. There exists a rational number ρ_n, such that $\mu(\mathcal{I}_n) = \rho_n\mu_0$ (Remark 3.2.12). The (finite) index of $\mathcal{I}_n$ in A_n is denoted by ι_n; i.e. $A_n = \cup_{k=1}^{\iota_n} v_k\mathcal{I}_n$. Then, from the σ-additivity of the measure, we can compute the measure of A as

$$\mu(A) = \lim_{n\to\infty} \iota_n\rho_n\mu_0,$$

which exists (maybe infinity), since the sequence $\iota_n\rho_n$ is increasing.

Remark 3.2.14. — This construction of the Haar measure is of a rather general nature. One can also define such a measure using a *top degree* non-zero differential form $\omega \in \det(\Omega_{\mathrm{O}(\mathcal{E})})$, as in [**Wei82**]. This form induces, by integration, an invariant measure on $\mathrm{O}(\mathcal{E})_\mathfrak{p}$ for any prime $\mathfrak{p}$. By the product formula, this induces a well defined global measure on $\mathrm{O}_\mathbb{A}(\mathcal{E})$ - the so called *Tamagawa measure* - provided the product over all primes converges. This occurs when the group is semi-simple (so in our case, for example, orthogonal groups of unimodular quadratic forms). For non-semi-simple, reductive groups one can still define a *Tamagawa measure*, for which one has to introduce *convergence factors* (see loc.cit.).

3. Genus Theory

In this section, we repeat the ideas of §2.3, applied to quadratic bundles instead of vector bundles.

3.1. For quadratic bundles. — Again, we fix a line bundle $\mathcal{L}$ over X, where the quadratic bundles take their values and fix also an open, affine subset $U =: \mathrm{Spec}(R) \subset X$. Set $S := S_\infty := X \setminus U$.

Definition 3.3.1. — Two quadratic bundles $(\mathfrak{q}_i,\mathcal{E}_i) := (\mathfrak{q}_i,\mathcal{E}_i,\mathcal{L})$, $i = 1,2$, belong to the same **genus** over $U \subset X$ if and only if $(\mathfrak{q}_{1,v},\mathcal{E}_{1,v}) \cong (\mathfrak{q}_{2,v},\mathcal{E}_{2,v})$, for all $v \in \mathrm{Val}(U)$ and $(\mathfrak{q}_{1,v,(0)},\mathcal{E}_{1,v,(0)}) \cong (\mathfrak{q}_{2,v,(0)},\mathcal{E}_{2,v,(0)})$, for all $v \in S$. The set of quadratic bundles which belong to the genus of $(\mathfrak{q},\mathcal{E})$ over U will be denoted by $\mathrm{gen}_U(\mathfrak{q},\mathcal{E})$, or simply $\mathrm{gen}(\mathfrak{q},\mathcal{E})$.

Remark 3.3.2. — The genus of a given quadratic bundle consists of whole isomorphism classes, since global isomorphisms give rise to local ones. Hence, $\mathrm{gen}(\mathfrak{q},\mathcal{E})$ can be partitioned into isomorphism classes, and we are able to talk about a class belonging to a genus.

Proposition 3.3.3. — *The set of isomorphism classes of quadratic bundles in the genus of $\mathcal{E}$ is parametrized by the double classes*

$$\mathrm{O}(\mathcal{E})(K)\backslash \mathrm{O}_\mathbb{A}(\mathcal{E})/\mathrm{O}_\mathbb{A}(\mathcal{E},0). \tag{3.3.1}$$

Proof. — (cf. Proposition 2.3.2) Let $\mathbb{V}$ be a quadratic space over K. Then, any two lattices $L, L' \subset \mathbb{V}$ coincide almost everywhere, i.e. $L_v = L'_v$ for almost every place $v \in \mathrm{Val}(K)$ ([**Eic73**, Satz 13.1]).
Given two quadratic bundles $\mathcal{E} = (\mathfrak{q},\mathcal{E},\mathcal{L})$ and $\mathcal{E}' = (\mathfrak{q}',\mathcal{E}',\mathcal{L})$ on X, it is easy to see from the remark above, that there exists an automorphism $\phi \in \mathrm{O}(\mathcal{E})(\eta_X) = \mathrm{O}(\mathcal{E})(K)$ such that $\phi(\mathcal{E}_v) = \mathcal{E}'_v$ for almost

all v. for almost all places $\mathcal{E}_v = \mathcal{E}'_v$. Therefore, two such bundles are in the same genus if and only if there exists $\boldsymbol{u} = (u_v) \in \mathrm{O}_{\mathbb{A}}(\mathcal{E})$ such that $\phi u_v \mathcal{E}_v = \mathcal{E}'_v$ for all $v \in \mathrm{Val}(U)$; that is, the co-sets $\mathrm{O}(\mathcal{E})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{E})$ act transitively on $\mathrm{gen}(\mathcal{E})$.
The next natural step, is to compute the stabilizer of $\mathcal{E}$:

$$\mathrm{Stab}_{\mathrm{O}_{\mathbb{A}}(\mathcal{E})}(\mathcal{E}) = \{\boldsymbol{u} = (u_v) \in \mathrm{O}_{\mathbb{A}}(\mathcal{E}) \mid \boldsymbol{u}\mathcal{E} = \mathcal{E}\};$$

which is $= \mathrm{O}_{\mathbb{A}}(\mathcal{E}, 0)$. □

Theorem 3.3.4. — *Every genus contains finitely many isomorphism classes of quadratic bundles on X.*

Proof. — Denote by $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$ the quadratic bundle on X. By local considerations, we can compute the discriminant of the quadratic bundle, which is certainly, over U, an invariant of the genus. Hence, over U, $d := \boldsymbol{N}(\mathrm{discr}(\mathfrak{q}, \mathcal{E}, \mathcal{L}))$ is fixed. Moreover, the genus determines at infinity the quadratic spaces $\mathcal{E}_{\infty,(0)}$. From Proposition 2.1.9 (and Remark 2.1.10) we have finitely many quadratic bundles over U in the genus of $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$. Now, any of these finitely many bundles over U possesses finitely many extensions to X, up to isometry (Theorem 2.3.4). Therefore, we have finitely many isometry classes in the genus, so the proof is finished. □

Corollary 3.3.5. —

$$\mathrm{O}_{\mathbb{A}}(\mathcal{E}) = \bigcup_{k=1}^{h} \mathrm{O}(\mathcal{E})(K)\boldsymbol{u}_k \,\mathrm{O}_{\mathbb{A}}(\mathcal{E}, 0),$$

where $h = |\mathrm{gen}(\mathcal{E})/\,\mathrm{cls}|$. More generally,

$$\mathrm{O}_{\mathbb{A}}(\mathcal{E}) = \bigcup_{k=1}^{h(\gamma)} \mathrm{O}(\mathcal{E})(K)\boldsymbol{u}_k \,\mathrm{O}_{\mathbb{A}}(\mathcal{E}, \gamma),$$

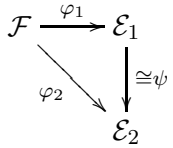
for any $\gamma \in \Gamma(X \setminus S_\infty, \mathcal{O}_X)$.

3.2. For quadratic bundle representations. — We finish this section with a result similar to (3.3.1), in the context of *representation of quadratic bundles by quadratic bundles*. It resembles the classical notion of representation of a number by a quadratic forms, or more accurately the representation of a quadratic form by another. As said in the beginning of this section, again this reasoning is similar to the ones cited above, and therefore will not be repeated again. Instead, we state the analogous definitions and results.

[2.1] *Definitions.* —

Definition 3.3.6. — (1) Let $\mathcal{E}_i := (\mathfrak{q}_i, \mathcal{E}_i, \mathcal{L})$ $(i = 1, 2)$ be two quadratic bundles on X. We say that $\mathcal{E}_2$ **represents** $\mathcal{E}_1$ if there exists an injective morphism $\varphi : \mathcal{E}_1 \to \mathcal{E}_2$ such that $\mathfrak{b}_2 \circ \mathrm{Sym}^2(\varphi) = \mathfrak{b}_1$. This morphism is called a **representation of $\mathcal{E}_1$ by $\mathcal{E}_2$**. The set of all such representations will be denoted by $\mathfrak{R}((\mathfrak{q}_2, \mathcal{E}_2, \mathcal{L}), (\mathfrak{q}_1, \mathcal{E}_2, \mathcal{L}))$, or shortly $\mathfrak{R}(\mathcal{E}_2, \mathcal{E}_1)$ $(= \mathfrak{R}(\mathfrak{q}_2, \mathfrak{q}_1))$.

(2) Any two representations $\varphi_i : \mathcal{F} \to \mathcal{E}_i$ $(i = 1, 2)$ belong to the same **class** if there exists an isomorphism $\psi : \mathcal{E}_1 \to \mathcal{E}_2$ such that the diagram



commutes.

(3) Two representations $\varphi_i : \mathcal{F} \to \mathcal{E}_i$ $(i = 1, 2)$ are in the same **genus (w.r.t. U)** if there exist isomorphisms $\psi_{v,(0)} : \mathcal{E}_{1,v,(0)} \to \mathcal{E}_{2,v,(0)}$ for all v, with

$$\begin{array}{ccc} \mathcal{F}_v & \xrightarrow{\varphi_{1,v}} & \mathcal{E}_{1,v,(0)} \\ & \searrow^{\varphi_{2,v}} & \downarrow \cong \psi_{v,(0)} \\ & & \mathcal{E}_{2,v,(0)} \end{array}$$

commutative and for all $v \in \mathrm{Val}(U)$ $\psi_{v,(0)} \mid_{\mathcal{E}_{1,v}} : \mathcal{E}_{1,v} \xrightarrow{\cong} \mathcal{E}_{2,v}$.

Remark 3.3.7. — – By definition, if two representations $\varphi_i : \mathcal{F} \to \mathcal{E}_i$ $(i = 1, 2)$ belong to the same class (genus), then the quadratic bundles $\mathcal{E}_1$, $\mathcal{E}_2$ belong to the same class (genus).

– In the next chapter, we are going to consider only definite bundles. For these in particular, the conditions at infinity disappear, since over complete local fields there exists only one anisotropic quadratic space (up to isomorphism), when the rank is $1, 3, 4$. In the rank 2 case, the class is also determined outside the points at infinity (cf. [**Eic73**, §II]).

[2.2] Let $\mathcal{F} \hookrightarrow \mathcal{E}$ be a representation. Over the affine, Zariski open subset $U = \mathrm{Spec}(R)$ it is just an injective R-homomorphism of the corresponding projective modules, which respects the quadratic forms. Over the generic point, we can write $\mathcal{F}_\eta \perp \mathcal{F}_\eta^\perp = \mathcal{E}_\eta$. Take an R-lattice G inside the vector space $\mathcal{F}_\eta^\perp$. Choose any extension $\mathcal{G}$ of the quadratic bundle $\tilde{G}$ on U to X, such that $\mathcal{F}_v \perp \mathcal{G}_v \subset \mathcal{E}_v$ for all $v \in \mathrm{Val}(X)$. Almost everywhere, $\mathcal{F}_v \perp \mathcal{G}_v = \mathcal{E}_v$, and at some other places the quotient module $\mathcal{E}_v/(\mathcal{F}_v \perp \mathcal{G}_v)$ is a non-trivial finite (torsion) module. In any case, for a given $u_v \in \mathrm{O}(\mathcal{G}_v)$, the orthogonal transformation $\mathrm{Id}_{\mathcal{F}_v} \perp u_v \in \mathrm{O}(\mathcal{F}_v \perp \mathcal{G}_v)$ can be extended in a canonical way to an orthogonal transformation $\tilde{u}_v$ on the local *vector space* $\mathcal{E}_{v,(0)}$, which almost always lies in $\mathrm{O}(\mathcal{E}_v)$.
For example, if $\mathrm{rk}(\mathcal{G}) = 1$, we illustrate the canonical extensions referred to above. Choose an adapted orthogonal basis $\mathcal{B}_v$ of $\mathcal{E}_v$, with $\langle v_v \rangle \cap \mathcal{G}_v \neq \emptyset$. Then, there exists $n_0 \in \mathbb{N}$ such that $\pi_v^{n_0} v$ generates $\mathcal{G}_v$. Any linear (orthogonal) transformation of $\mathcal{G}_v$ extends by linearity to $\langle v \rangle$.
In this manner we obtain an injection

$$\begin{aligned} \mathrm{O}_{\mathbb{A}}(\mathcal{G}) &\hookrightarrow \mathrm{O}_{\mathbb{A}}(\mathcal{E}) \\ \boldsymbol{u} := (u_v) &\mapsto \tilde{\boldsymbol{u}} := (\tilde{u}_v). \end{aligned}$$

Using this injection, we define

$$\mathrm{O}_{\mathbb{A}}(\mathcal{G}, \mathcal{E}) := \mathrm{Stab}_{\mathrm{O}_{\mathbb{A}}(\mathcal{G})}(\mathcal{E}).$$

Let us state the analogue result to Proposition 3.3.3, which follows by repeating similar arguments of Proposition 3.3.3, or as in [**BD05**], since the Hasse principle holds for the orthogonal group (ff. §3.3.2.3).

Proposition 3.3.8. — *Fix a representation $\mathcal{F} \hookrightarrow \mathcal{E}$. There exists a bijection*

$$\mathrm{O}(\mathcal{G})(K) \backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G}) / \mathrm{O}_{\mathbb{A}}(\mathcal{G}, \mathcal{E}) \overset{1\text{-}1}{\longleftrightarrow} \{ j' : \mathcal{F} \hookrightarrow \mathcal{E}' \mid j' \in \mathrm{gen}(j : \mathcal{F} \hookrightarrow \mathcal{E}) \} / \mathrm{cls}\,. \tag{3.3.2}$$

Theorem 3.3.9. — *Let $\mathcal{F}$ be a non-degenerate quadratic bundle. Then there exist finitely many isomorphism classes of representations $\mathcal{F} \to \mathcal{E}$, such that $\mathcal{E}$ has fixed rank and discriminant (say m and $\mathfrak{a}$, respectively).*

This theorem combined with Proposition 3.3.8 gives, as in the case of genera of quadratic bundles (cf. Corollary 3.3.5),

$$\boxed{\mathrm{O}_{\mathbb{A}}(\mathcal{G}) = \bigcup_{k=1}^{h(\rho)} \mathrm{O}(\mathcal{G})(K)\boldsymbol{u}_k\,\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E})}, \tag{3.3.3}$$

where $\rho : \mathcal{F} \hookrightarrow \mathcal{E}$ is a (special) representation of the quadratic bundle $\mathcal{F}$ though $\mathcal{E}$.

Remark 3.3.10. — This statement is nothing else, than the finiteness of the measure $\mu(\mathrm{O}(\mathcal{G})(K)\backslash\,\mathrm{O}_{\mathbb{A}}(\mathcal{G}))$. It is the computation of this Haar-measure in two different ways, what gives the Minkowski-Siegel formula. A further computation gives also the constants appearing in the formula. All this is the topic of the next chapter.

[2.3] *Hasse principle for orthogonal groups.* — The results of §3.3.2.2 are indeed a consequence of the Hasse principle for orthogonal groups over function fields (see, for example, [**BD05**, §7]). We briefly recall here the Hasse principle in our case.

The formulation of the Hasse principle for algebraic groups is a direct generalization of the local to global principle for quadratic forms over global fields. For an algebraic group G over a global field K, we say that G **satisfies the Hasse principle** if the map between Galois cohomology sets

$$\mathrm{H}^1(K,G) \to \prod_{v\in\mathrm{Val}(K)} \mathrm{H}^1(K_v,G)$$

(given by restriction and extension of scalars; cf. [**Kne67**] or [**Ser97**, III.§4]) is injective.
With the notation as above, let $1 < m = \mathrm{rk}(\mathcal{E})$.

Proposition 3.3.11. — *The generic fiber of the orthogonal group of $\mathcal{E}$, $G := \mathrm{O} := \mathrm{O}(\mathcal{E})_\eta$, satisfies the Hasse principle.*

Proof. — Claim: *If* $\mathrm{SO} := \mathrm{SO}(\mathcal{E})_\eta$ *satisfies the Hasse principle, then so does* O.

From the exact sequence

$$1 \longrightarrow \mathrm{SO} \longrightarrow \mathrm{O} \longrightarrow \boldsymbol{\mu}_2 \longrightarrow 1,$$

we get

$$\begin{array}{ccccc}
\mathrm{H}^1(K,\mathrm{SO}) & \longrightarrow & \mathrm{H}^1(K,\mathrm{O}) & \longrightarrow & \mathrm{H}^1(K,\boldsymbol{\mu}_2) = K^\times/K^{\times 2} \\
\downarrow & & \downarrow & & \downarrow \\
\prod_{v\in\mathrm{Val}(K)} \mathrm{H}^1(K_v,\mathrm{SO}) & \longrightarrow & \prod_{v\in\mathrm{Val}(K)} \mathrm{H}^1(K_v,\mathrm{O}) & \longrightarrow & \prod_{v\in\mathrm{Val}(K)} K_v^\times/K_v^{\times 2}\ .
\end{array}$$

Take a cycle $\xi \in \mathrm{H}^1(K,\mathrm{O})$ in the kernel of the middle vertical map. Since an element in $K^\times$ which is locally everywhere a square is indeed a square (injectivity of the right vertical map), we have that ξ comes from a cocycle, say ξ^0, of $\mathrm{H}^1(K,\mathrm{SO})$. Now the bottom-left map is injective, since the maps $\mathrm{H}^0(K_v,\mathrm{O}) \to \mathrm{H}^0(K_v,\boldsymbol{\mu}_2)$ are surjective; so ξ^0 is in the kernel of the left vertical map. From the assumption of the Hasse principle for SO, ξ^0 is trivial, hence ξ is trivial.
Claim: *The special orthogonal group* SO *over K satisfies the Hasse principle.*

Using the exact sequence

$$1 \longrightarrow \boldsymbol{\mu}_2 \longrightarrow \mathrm{Spin} \longrightarrow \mathrm{SO} \longrightarrow 1,$$

and the fact that $\mathrm{H}^2(K_v, \boldsymbol{\mu}_2)$ is the kernel of multiplication by 2, $\mathrm{Br}(K_v)_2$, in the Brauer group of K_v, we obtain

$$\mathrm{H}^1(K, \mathrm{SO}) \xrightarrow{\varphi} \prod_{v \in \mathrm{Val}(K)} \mathrm{H}^1(K_v, \mathrm{SO}) \hookrightarrow \prod_{v \in \mathrm{Val}(K)} \mathrm{Br}(K_v)_2.$$

But $\mathrm{H}^1(K, \mathrm{SO}) \hookrightarrow \mathrm{Br}(K)_2$ (since Spin is simply-connected), so any cycle on the kernel of φ, corresponds to an element of the Brauer group over K with trivial local invariants everywhere, so by Brauer-Hasse-Noether, it is itself trivial. This completes the proof. □

CHAPTER 4

MINKOWSKI-SIEGEL FORMULA

We prove the geometrical version of the Minkowski-Siegel formula, which consists of an explicit computation of *certain* fundamental volumes (Theorem 4.4.1). At the end, as an application, we prove a theorem on definite regular (in the sense of Dickson, see §4.5) quadratic forms over global rings (Theorem 4.5.2). We explain some other consequences of this formula, as well as relations with other topics and possible future work.

Notation. — Let $X/\operatorname{Spec}(\mathbb{F}_q)$ be a smooth, projective, geometrically irreducible curve; $\mathcal{E}$ a definite (with respect to a fixed set S_∞ of places at infinity) vector bundle of rank $m \leq 4$ with a quadratic form on it $\mathfrak{b} : \operatorname{Sym}^2(\mathcal{E}) \to \mathcal{L}$ (recall we assume $2 \in \mathcal{O}_X^\times$), where $\mathcal{L}$ is any line bundle on X; and also $\mathcal{F}$ will denote a positive definite vector bundle of rank n, with values in $\mathcal{L}$.
We set $U := X \setminus S_\infty$ and $\mathbb{A} := \mathbb{A}_{\mathrm{f}}$.

1. Fundamental domains

We need to show the existence of fundamental domains for the action of $\mathrm{O}(\mathcal{E})(K)$ on $\mathrm{O}_{\mathbb{A}}(\mathcal{E})$.[VIII] For any Borel-measurable $\boldsymbol{A} \subset \mathrm{O}_{\mathbb{A}}(\mathcal{E})$, we would like to write $\mathrm{O}(\mathcal{E})(K) \cdot \boldsymbol{A}$ as a disjoint union of translates of a **fundamental domain for** $\boldsymbol{A}$, namely $\mathrm{O}(\mathcal{E})(K) \cdot \boldsymbol{A} = \cup_{k=1}^{n} \boldsymbol{v}_k \mathfrak{F}_{\boldsymbol{A}}$, for certain $\mathfrak{F}_{\boldsymbol{A}} \subset \mathrm{O}_{\mathbb{A}}(\mathcal{E})$.

Proposition 4.1.1. — *Let $\mathcal{E}$ be a quadratic bundle, $\mathcal{B}(\mathcal{E})$ its Borel algebra (cf. §3.2.3). Then for any $\boldsymbol{A} \in \mathcal{B}(\mathcal{E})$, there exists a fundamental domain $\mathfrak{F}_{\boldsymbol{A}} \subset \mathrm{O}_{\mathbb{A}}(\mathcal{E})$. If $\mathfrak{F}'_{\boldsymbol{A}}$ is another fundamental domain for $\boldsymbol{A}$, then $\mu(\mathfrak{F}_{\boldsymbol{A}}) = \mu(\mathfrak{F}'_{\boldsymbol{A}})$.*

The following result will be used in the proof of the above proposition. Recall p is always ≥ 3.

Lemma 4.1.2. — *For any non-trivial ideal $\mathfrak{a} \subset R = \Gamma(U, \mathcal{O}_X)$, the intersection $\mathrm{O}(\mathcal{E})(K) \cap \mathrm{O}_{\mathbb{A}}(\mathcal{E}, \mathfrak{a})$ is trivial.*

Proof. — Let $\boldsymbol{u} \in \mathrm{O}(\mathcal{E})(K) \cap \mathrm{O}_{\mathbb{A}}(\mathcal{E}, \mathfrak{a}) \subset \mathrm{O}(\mathcal{E})(U)$. Since $\mathcal{E}$ is definite, $\boldsymbol{u}$ has finite order e.
Assume $p \mid e$, say without loss of generality, $p = e$. From remark 3.1.6, we know that $\mathrm{SO}(\mathcal{E})(U)$ has no non-trivial unipotents. If $\boldsymbol{u} \in \mathrm{O}(\mathcal{E})(U)$ is unipotent of order $e \geq 2$, denote by δ its determinant over U. Then $\delta^p = 1$, which implies $\delta = 1$ and therefore $\boldsymbol{u} \in \mathrm{SO}(\mathcal{E})(U)$, so the identity.
Suppose $p \nmid e$ and $\boldsymbol{u} \neq \mathrm{Id}$. Write $\boldsymbol{v} := \boldsymbol{u} - \mathrm{Id} \in \mathrm{End}(\mathcal{E})$.

$$\boldsymbol{u}^e = (\boldsymbol{v} + \mathrm{Id})^e = \mathrm{Id} + e\boldsymbol{v} + \ldots + e\boldsymbol{v}^{e-1} + \boldsymbol{v}.$$

Take a prime $\mathfrak{p} \mid \mathfrak{a}$ (here comes the assumption on the non-triviality of $\mathfrak{a}$). Then for a certain $n_\mathfrak{p} \in \mathbb{N}$, $\boldsymbol{u} \equiv \mathrm{Id} \pmod{\mathfrak{p}^{n_\mathfrak{p}}}$ (take the greatest such $n_\mathfrak{p}$, which exists, since $\boldsymbol{v} \neq 0$). Hence $\boldsymbol{u}^e = \mathrm{Id} \equiv \mathrm{Id} + e\boldsymbol{v} \pmod{\mathfrak{p}^{2n_\mathfrak{p}}}$, which contradicts the maximality of $n_\mathfrak{p}$. □

Proof of Proposition 4.1.1. — Let $\boldsymbol{A} = \cup_{k=1}^{n} \boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{E}, \mathfrak{a})$, so $\mathrm{O}(\mathcal{E})(K) \cdot \boldsymbol{A} = \cup_{l=1}^{d} \mathrm{O}(\mathcal{E})(K)\boldsymbol{v}_l \,\mathrm{O}_\mathbb{A}(\mathcal{E}, \mathfrak{a})$. Set $\mathfrak{F} := \cup_{l=1}^{d} \boldsymbol{v}_l \,\mathrm{O}_\mathbb{A}(\mathcal{E}, \mathfrak{a})$; then $\mathrm{O}(\mathcal{E})(K) \cdot \boldsymbol{A} = \cup_k \boldsymbol{w}_k \mathfrak{F}$. Is this union disjoint?
Assume, $\boldsymbol{w}_l \boldsymbol{v}_k \rho = \boldsymbol{w}_{l'} \boldsymbol{v}_{k'} \rho'$. From one disjoint union above, we have $k = k'$, that is $\boldsymbol{w}_l \boldsymbol{v} \rho = \boldsymbol{w}_{l'} \boldsymbol{v} \rho'$, for $\boldsymbol{v} := \boldsymbol{v}_k$. But then,

$$\begin{aligned} \boldsymbol{v}\rho\rho'^{-1}\boldsymbol{v}^{-1} = \boldsymbol{w}_l^{-1}\boldsymbol{w}_{l'} \in \mathrm{O}(\mathcal{E})(K) \cap \boldsymbol{v}\,\mathrm{O}_\mathbb{A}(\mathcal{E}, \mathfrak{a})\boldsymbol{v}^{-1} = \\ = \mathrm{O}(\mathcal{E})(K) \cap \mathrm{O}_\mathbb{A}(\boldsymbol{v}\mathcal{E}, \mathfrak{a}) = \{\mathrm{Id}\}; \end{aligned}$$

where the last equality is given by the previous lemma. Hence $\boldsymbol{w}_l = \boldsymbol{w}_{l'}$ and $\rho = \rho'$, which proves the first assertion.
Let $\mathfrak{F} = \cup_{k=1}^{n} \boldsymbol{u}_k B$ and $\mathfrak{F}' = \cup_{k=1}^{m} \boldsymbol{u}'_k B'$ be two fundamental domains for $\boldsymbol{A}$. Without loss of generality, we may assume $B = B'$ (by taking the intersection, cf. Lemma 3.2.7). To show: $n = m$.
By definition $\mathrm{O}(\mathcal{E})(K) \cdot \mathfrak{F} = \mathrm{O}(\mathcal{E})(K) \cdot \mathfrak{F}' = \cup_{k=1}^{m} \mathrm{O}(\mathcal{E})(K)\boldsymbol{u}'_k B$. So each $\mathrm{O}(\mathcal{E})(K)\boldsymbol{u}_{k_0} B$ must be included in only one $\mathrm{O}(\mathcal{E})(K)\boldsymbol{u}'_{\sigma(k_0)} B$, and vice versa: $\mathrm{O}(\mathcal{E})(K)\boldsymbol{u}_{k_0} B = \mathrm{O}(\mathcal{E})(K)\boldsymbol{u}_{\sigma(k_0)} B$; where σ is a permutation in the set of n elements. In particular, $n = m$, which implies $\mu(\mathfrak{F}) = \mu(\mathfrak{F}')$. □

It follows from the proposition that the volume of any fundamental domain of a fixed $\boldsymbol{A} \in \mathcal{B}(\mathcal{E})$ is the same. Therefore we define

$$\mu(\mathrm{O}(\mathcal{E})(K) \backslash \mathrm{O}(\mathcal{E})(K) \cdot \boldsymbol{A}) := \mu(\mathfrak{F}_{\boldsymbol{A}}),$$

for some (and hence for any) fundamental domain $\mathfrak{F}_{\boldsymbol{A}}$ of $\boldsymbol{A}$.

Recall definitions and notation from §3.3.2. Equation (3.3.3) gives

$$\mu(\mathrm{O}(\mathcal{G})(K) \backslash \mathrm{O}_\mathbb{A}(\mathcal{G})) = \sum_{k=1}^{h(j)} \mu(\mathrm{O}(\mathcal{G})(K) \backslash \mathrm{O}(\mathcal{G})(K)\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})). \tag{4.1.1}$$

Remark 4.1.3. — A fundamental domain $\mathfrak{F} \subset \boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})$ for $\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})$ under the action of $\mathrm{O}(\mathcal{G})(K)$ is also a fundamental domain for $\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})$ under the action of $\mathrm{O}(\mathcal{G})(K) \cap \boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})\boldsymbol{u}_k^{-1}$ (by which we actually refer to the action of $\mathrm{O}(\mathcal{G})(K)$ on $\mathrm{O}(\mathcal{G})(K)\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})$; cf. (4.1.2)), and conversely.

The converse is trivial. For the other way, we must show that for any representation

$$\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E}) = \bigcup_{l=1}^{n} h_l \mathfrak{F}, \tag{4.1.2}$$

the h_l's belong to $\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})\boldsymbol{u}_k^{-1}$. Since there exists a $\boldsymbol{v} \in \mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})$ such that $h_l \boldsymbol{u}_k \boldsymbol{v} \in \boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})$, $h_l \boldsymbol{u}_k$ belongs also to this coset, and so $h_l \in \boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})\boldsymbol{u}_k^{-1}$.

This fact does not use any property of orthogonal groups or whatsoever; it is a simple abstract statement (cf. [**Kne92**, §30]).

Pick a fundamental domain $\mathfrak{F}_k$ of $\mathrm{O}(\mathcal{G})(K) \backslash \mathrm{O}(\mathcal{G})(K)\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E})$ for each $k = 1, \ldots, h(j)$. Then

$$\boldsymbol{u}_k \,\mathrm{O}_\mathbb{A}(\mathcal{G}, \mathcal{E}) = \bigcup_{u_l \in \mathrm{O}(\mathcal{G}, \boldsymbol{u}_k \mathcal{E})(U)} u_l \mathfrak{F}_k,$$

since remark 4.1.3 asserts that the same $\mathfrak{F}_k$ is a fundamental domain for the action of

$$\mathrm{O}(\mathcal{G})(K) \cap \boldsymbol{u}_k \,\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E})\boldsymbol{u}_k^{-1} = \mathrm{O}(\mathcal{G})(K) \cap \mathrm{O}_{\mathbb{A}}(\mathcal{G},\boldsymbol{u}_k\mathcal{E}) = \\ = \mathrm{O}(\mathcal{G},\boldsymbol{u}_k\mathcal{E})(U).$$

The summands of (4.1.1) can be written as

$$\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}(\mathcal{G})(K)\boldsymbol{u}_k \,\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E})) = \mu(\mathfrak{F}_k) = \mu(\boldsymbol{u}_k \,\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E}))\cdot \\ \cdot |\mathrm{O}(\mathcal{G},\boldsymbol{u}_k\mathcal{E})(U)|^{-1} = \mu(\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E}))\frac{[\mathrm{O}(\boldsymbol{u}_k\mathcal{E})(U) : \mathrm{O}(\mathcal{G},\boldsymbol{u}_k\mathcal{E})(U)]}{|\mathrm{O}(\boldsymbol{u}_k\mathcal{E})(U)|};$$

and hence the total volume

$$\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G})) = \sum_{k=1}^{h(j)} \mu(\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E}))\frac{[\mathrm{O}(\boldsymbol{u}_k\mathcal{E})(U) : \mathrm{O}(\mathcal{G},\boldsymbol{u}_k\mathcal{E})(U)]}{|\mathrm{O}(\boldsymbol{u}_k\mathcal{E})(U)|} = \\ = \mu(\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E}))\sum_{k=1}^{h(j)} \frac{[\mathrm{O}(\boldsymbol{u}_k\mathcal{E})(U) : \mathrm{O}(\mathcal{G},\boldsymbol{u}_k\mathcal{E})(U)]}{|\mathrm{O}(\boldsymbol{u}_k\mathcal{E})(U)|} = \mu(\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E}))\cdot \\ \cdot \sum_{\mathrm{cls}(\mathcal{E}')\in\mathrm{gen}(\mathcal{E})} \frac{\sum_{\substack{j':\mathcal{F}\hookrightarrow\mathcal{E}' \\ \mathrm{cls}(j')\in\mathrm{gen}(j)}} [\mathrm{O}(\mathcal{E}')(U) : \mathrm{O}(\mathcal{G},\mathcal{E}')(U)]}{|\mathrm{O}(\mathcal{E}')(U)|}.$$

Setting

$$\mathsf{r}_j(\mathcal{E}',\mathcal{F}) := \sum_{\substack{j':\mathcal{F}\hookrightarrow\mathcal{E}' \\ \mathrm{cls}(j')\in\mathrm{gen}(j)}} \big[\mathrm{O}(\mathcal{E}')(U) : \mathrm{O}(\mathcal{G},\mathcal{E}')(U),\big]$$

we have

$$\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G})) = \mu(\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E})) \sum_{\mathrm{cls}(\mathcal{E}')\in\mathrm{gen}(\mathcal{E})} \frac{\mathsf{r}_j(\mathcal{E}',\mathcal{F})}{|\mathrm{O}(\mathcal{E}')(U)|} = \mu(\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E})) \sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{r}_j(\mathcal{E}_l,\mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|}.$$

Note, over what the initial and the latter sum indices run. Precisely this difference is what this computation is for!
Writing together, we obtain

$$\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G})) = \mu(\mathrm{O}_{\mathbb{A}}(\mathcal{G},\mathcal{E})) \sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{r}_j(\mathcal{E}_l,\mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|}. \tag{4.1.3}$$

Lemma 4.1.4. — *Let μ_v and μ be Haar-measures on $\mathrm{O}(\mathcal{E}_{v,(0)})$, on $\mathrm{O}_{\mathbb{A}}(\mathcal{E})$ respectively, such that $\prod_{v\notin S_\infty} \mu_v(A_v)$ is convergent for some $\boldsymbol{A} \in \mathcal{B}(\mathcal{E})$. Then, there exists a constant $c \in \mathbb{R}_{>0}$, such that for any congruence subset $\boldsymbol{C} = \prod_{v\notin S_\infty} C_v \subset \mathrm{O}_{\mathbb{A}}(\mathcal{E})$,*

$$\mu(\boldsymbol{C}) = c \prod_{v\notin S_\infty} \mu_v(C_v).$$

Proof. — From Corollary 3.2.13 and remark afterwards, it suffices to show the statement for the algebra of sets $\mathcal{A}(\mathcal{E})$ instead of $\mathcal{B}(\mathcal{E})$ (a simple limit process passes from the algebra of sets to its *Borel completion*). So, we suppose that the congruence subset $\boldsymbol{A}$, as well as $\boldsymbol{C}$ are in $\mathcal{A}(\mathcal{E})$; i.e. they are finite disjoint union of translates of congruence groups (cf. Corollary op.cit.).
Since any two congruence groups differ at most, at finitely many places, we show the statement by induction on the number of coordinates where they differ. Namely, we can suppose that the formula

is true for some congruence subset $\boldsymbol{B}$ (for instance $\boldsymbol{A}$), and then have to show that it is true also for any congruence subset $\boldsymbol{C}$, which differs from $\boldsymbol{B}$ in at most 1 place.
Without loss of generality (see Definition 3.2.9), we can take $\boldsymbol{B} := \prod_{v\notin S_\infty} \mathrm{O}(\mathcal{E}_v)$, and $\boldsymbol{C} := \prod_{v\neq v_0} \mathrm{O}(\mathcal{E}_v) \times C_{v_0}$, for some measurable $C_{v_0} \subset \mathrm{O}(\mathcal{E}_{v_0,(0)})$. By assumption we can find $c \in \mathbb{R}_{>0}$ such that $\mu(\boldsymbol{B}) = c\prod_{v\notin S_\infty} \mu_v(B_v)$ ($B_v = \mathrm{O}(\mathcal{E}_v)$). Define $\tilde{\mu}_{v_0} : \mathcal{B}(\mathcal{E}_{v_0}) \to \mathbb{R}_{\geq 0}$, by $C_{v_0} \mapsto \mu(\prod_{v\neq v_0} B_v \times C_{v_0})$. It is easy to verify, that $\tilde{\mu}_{v_0}$ is a Haar-measure, so $\mu_{v_0} = \alpha\tilde{\mu}_{v_0}$ for some $\alpha \in \mathbb{R}_{>0}$. From $\tilde{\mu}_{v_0}(B_{v_0}) = \alpha^{-1}\mu_{v_0}(B_{v_0}) = \mu(\boldsymbol{B}) = \prod_{v\notin S_\infty} \mu_v(B_v)$ follows

$$\mu(\boldsymbol{C}) = \tilde{\mu}_{v_0}(C_{v_0}) = \alpha^{-1}\mu_{v_0}(C_{v_0}) = c\prod_{v\neq v_0} \mu_v(B_v).\mu_{v_0}(C_{v_0}),$$

whence, $\mu(\boldsymbol{C}) = \mu(\prod_{v\notin S_\infty} C_v) = c\prod_{v\notin S_\infty} \mu_v(C_v)$ for any $\boldsymbol{C}$ differing in at most one place from $\boldsymbol{B}$; the claim follows. □

Using this lemma, and by assuming for the moment the convergence of the infinite product $\prod_{v\notin S_\infty} \mu_v(\mathrm{O}(\mathcal{E}_v))$ (cf. section 4.2.1), we specialize the formula (4.1.3). Take $\mathcal{F} = \{0\}$ the zero bundle on X (with trivial quadratic form on it), then $\mathcal{G}$ equals $\mathcal{E}$ and therefore $\mathsf{r}_j(\mathcal{E}', 0) = \mathsf{r}_0(\mathcal{E}', 0) = 1$, for any $\mathcal{E}'$ in the genus of $\mathcal{E}$ (definite), which gives

$$\mu(\mathrm{O}(\mathcal{E})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{E})) = c\prod_v \mu_v(\mathrm{O}(\mathcal{E}_v)) \sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}. \tag{4.1.4}$$

Taking the quotient of (4.1.3) by (4.1.4) (and using again Lemma 4.1.4, modulo the assumption on the convergence of the product) we get

$$\frac{\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G}))}{\mu(\mathrm{O}(\mathcal{E})\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{E}))} = \frac{c'\prod_v \mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{E}_v)) \sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{r}_j(\mathcal{E}_l,\mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|}}{c\prod_v \mu_v(\mathrm{O}(\mathcal{E}_v)) \sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}},$$

where c, c' are the constants from Lemma 4.1.4 for the family of measures μ_v on $\mathcal{B}(\mathcal{E})$ and $\mathcal{B}(\mathcal{G})$ respectively. (Note that we do not distinguish in the notation between the local Haar measures on different groups.)

Following Siegel, we define the **v-adic densities with respect to j** (recall $\mathcal{G}_v$ depends on $j(\mathcal{F})_v$)

$$\mathsf{d}_{v,j}(\mathcal{E}, \mathcal{F}) := \frac{\mu_v(\mathrm{O}(\mathcal{E}_v))}{\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{E}_v))},$$

and replace it above, to obtain

$$\frac{1}{\sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}} \sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{r}_j(\mathcal{E}_l, \mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|} = \frac{c\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G}))}{c'\mu(\mathrm{O}(\mathcal{E})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{E}))} \prod_{v\notin S_\infty} \mathsf{d}_{v,j}(\mathcal{E}, \mathcal{F}).$$

Writing $j = j_1, j_2, \ldots, j_g$ for a set of representatives of the genera of primitive representations of $\mathcal{F}$ by $\mathcal{E}$, define $\mathsf{R}(\mathcal{E}_l, \mathcal{F}) := \sum_{l=1}^{g} \mathsf{r}_{j_l}(\mathcal{E}_l, \mathcal{F})$ and the **v-adic density of representations of $\mathcal{F}$ by $\mathcal{E}$** as $\mathsf{d}_v(\mathcal{E}, \mathcal{F}) := \sum_{l=1}^{g} \mathsf{d}_{v,j_l}(\mathcal{E}, \mathcal{F})$. Summing up the last equation for the different representatives of the genus, and using the elementary properties of the Haar-measure, we have the following

Theorem 4.1.5. — *In the definite case, for $n \leq m \leq 4$, we have*

$$\frac{1}{\sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}} \sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{R}(\mathcal{E}_l, \mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|} = \boldsymbol{c}\,\frac{\mu_{\mathfrak{F}}(\mathrm{O}(\mathcal{G}))}{\mu_{\mathfrak{F}}(\mathrm{O}(\mathcal{E}))} \prod_{v\notin |S_\infty|} \mathsf{d}_v(\mathcal{E}, \mathcal{F}). \tag{4.1.5}$$

(Later we show more; in particular $\boldsymbol{c} = 1$.) Siegel writes his celebrated *"Main Theorem"* (see [**Sie35**] for details) as

$$\delta(\mathcal{E}, \mathcal{F}) = \lim_{\mathfrak{q} \to \infty} \delta_{\mathfrak{q}}(\mathcal{E}, \mathcal{F}),$$

where the left hand side is the **global representation density**, defined as

$$\delta(\mathcal{E}, \mathcal{F}) := \frac{\sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{R}(\mathcal{E}_l, \mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|} / \sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}}{\mu_{\mathfrak{F}}(m-n)/\mu_{\mathfrak{F}}(n)};$$

whereas on the right hand side we have the limit of the **representation densities modulo $\mathfrak{q}$**:

$$\delta_{\mathfrak{q}}(\mathcal{E}, \mathcal{F}) := \frac{\mathsf{r}(\mathcal{E}, \mathcal{F} \bmod \mathfrak{q})}{[R : \mathfrak{q}R]^{mn - \frac{n(n+1)}{2}}}.$$

The limit $\mathfrak{q} \to \infty$ means that eventually, any *(rational) effective divisor with support on* $U = \mathrm{Spec}(R)$ will divide $\mathfrak{q}$; this means, the limit should be taken over a (any) sequence of effective divisors $\mathfrak{q}_n$ with $n \in \mathbb{N}$, such that for any effective rational divisor D, there exists $N = N(D) \in \mathbb{N}$ for which $D \mid \mathfrak{q}_n$, $\forall n \geq N$. This limit coincides precisely with the product of the v-adic representation densities $\prod_v \mathsf{d}_v(\mathcal{E}, \mathcal{F})$, since for a point $\mathfrak{p} := \mathfrak{p}_v \in U \subset X$ with corresponding valuation $v \in |U|$ (cf. [**Sie35**])

$$\mathsf{d}_v(\mathcal{E}, \mathcal{F}) = \lim_{n \to \infty} \delta_{\mathfrak{p}^n}(\mathcal{E}, \mathcal{F}),$$

and for any two different effective divisors on U, $\mathfrak{q}, \mathfrak{q}'$, with disjoint support,

$$\delta_{\mathfrak{q}\mathfrak{q}'}(\mathcal{E}, \mathcal{F}) = \delta_{\mathfrak{q}}(\mathcal{E}, \mathcal{F}) \delta_{\mathfrak{q}'}(\mathcal{E}, \mathcal{F}).$$

2. Proof of the formula (first part)

In this section, we will prove the formula (4.1.5); for which we understand:

(1) *regularize* the local Haar-measures, such that the product

$$\prod_{v \notin S_\infty} \mu_v(\mathrm{O}(\mathcal{E}_v))$$

converges;

(2) prove that the Haar-measures of the fundamental domains, $\mu_{\mathfrak{F}}(\mathrm{O}(\mathcal{G}))$ only depend on the dimension of the positive definite quadratic bundle;

(3) from the regularization of the local Haar-measures and an asymptotic computation of the representation numbers $\mathsf{R}(\mathcal{E}_l, \mathcal{F})$, we should obtain the only unknown left: $\boldsymbol{c}$.

2.1. Regularization of local Haar-measures. — For a valuation $v \notin S_\infty$, we have $\mathrm{O}(\mathcal{G}_v, \pi_v R_v) \subset \mathrm{O}(\mathcal{G}_v)$, which leads to

$$\mu_v(\mathrm{O}(\mathcal{G}_v)) = [\mathrm{O}(\mathcal{G}_v) : \mathrm{O}(\mathcal{G}_v, \pi_v R_v)]\, \mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v R_v)).$$

If the quadratic bundle is regular at v, then by Kneser's Hensel Theorem §1.2.2.1.5

$$[\mathrm{O}(\mathcal{G}_v) : \mathrm{O}(\mathcal{G}_v, \pi_v R_v)] = |\mathrm{O}(\overline{\mathcal{G}_v})|.$$

Whence $\mu_v(\mathrm{O}(\mathcal{G}_v)) = |\mathrm{O}(\overline{\mathcal{G}_v})|\,\mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v R_v))$. Recall $r = \mathrm{rk}(\mathcal{G}) = m - n$. If we denote by q_v $(= \boldsymbol{N}(\pi_v))$ the cardinality of the residue field of v, we have

$$|\mathrm{O}(\overline{\mathcal{G}_v})| = 2q_v^{\frac{r(r-1)}{2}} \prod_{o<2k<r} (1 - q_v^{-2k}) \begin{cases} 1, & \overline{\mathcal{G}_v} \text{ of odd rank;} \\ 1 - q_v^{-\lfloor \frac{r}{2} \rfloor}, & \overline{\mathcal{G}_v} \text{ hyperbolic of even rank;} \\ 1 + q_v^{-\lfloor \frac{r}{2} \rfloor}, & \overline{\mathcal{G}_v} \text{ non-hyperbolic of even rank.} \end{cases}$$

$$\mu_v(\mathrm{O}(\mathcal{G}_v)) = 2q_v^{-\frac{r(r-1)}{2}} \cdot \mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v R_v)) \cdot \tag{4.2.1}$$
$$\cdot \begin{cases} 1, & r \text{ odd;} \\ \prod_{0<2k<r}(1 - q_v^{-2k})(1 - \left(\frac{\mathrm{discr}(\mathcal{G})}{p}\right) q_v^{-\lfloor \frac{r}{2} \rfloor}) & r \text{ even.} \end{cases}$$

Hence, for the *regular primes* (cf. §3.1.1) we *regularize* the local measures as

$$\mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v R_v)) := (2q_v^{-\frac{r(r-1)}{2}})^{-1}, \tag{4.2.2}$$

and we obtain

$$\prod_{v \in |X_{\mathrm{reg}}|} \mu_v(\mathrm{O}(\mathcal{G}_v)) = \begin{cases} \prod_{0<2k<r} \zeta_{R,S_{\mathrm{reg}}}(2k)^{-1}, & r \text{ odd;} \\ \frac{\prod_{v \in S_{\mathrm{reg}}}(1+q_v^{-\lfloor \frac{r}{2} \rfloor})}{L_R(\lfloor \frac{r}{2} \rfloor, \chi_{\mathrm{discr}(\mathcal{G})}) \prod_{0<2k<r} \zeta_{K,S_{\mathrm{reg}}}(2k)}, & r \text{ even,} \end{cases} \tag{4.2.3}$$

where $L_R(s, \chi) =: L_\chi(s) := \prod_{v \notin S_\infty}(1 - \chi(\mathfrak{p}_v)\,\boldsymbol{N}(\mathfrak{p}_v)^{-1})^{-1}$.
This gives item (1). For the irregular (=not regular) primes $v \in S_{\mathrm{reg}}$, it does not matter what we choose as normalized Haar-measures, what the convergence concerns; but for the whole formula, it does. We will give a procedure for normalizing the local Haar-measures, which does not depend on the regularity or irregularity of the place; which is the general way for constructing a Haar-measure on a reductive (non-semi-simple) group.
Since we started with a definite quadratic bundle $\mathcal{E}$, the bundle $\mathcal{G}$ will be also definite, and in particular $\mathcal{G}_{v,(0)}$ will be regular. Moreover, almost everywhere, when one localizes with respect to the maximal ideal of the complete local ring $\mathcal{O}_v$, the orthogonal group has good reduction, but at some *non-regular* places (see §3.1.1) the dimension of the orthogonal group over the residue field jumps up; hence the regularization of the Haar measures over these primes is *slightly different* from the ones done above. We proceed a follows - a canonical way to fix a Haar measure over reductive, non-semi-simple algebraic groups on the adeles -.
For any place v there exists a natural number $f := f(v) \in \mathbb{N}$, such that

$$1 \longrightarrow \mathrm{O}(\mathcal{G}_v, \pi_v^f R_v) \longrightarrow \mathrm{O}(\mathcal{G}_v) \longrightarrow \mathrm{O}(\mathcal{G}_v \bmod \pi_v^f) \longrightarrow 1$$

is a short exact sequence, and also $\pi_v^f \mathfrak{q}(\mathcal{G}_v^{\#}) \subset R_v$. Call

$$c(v) := \mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v^f R_v)) \Big[\mathcal{G}_v : \pi_v^f \mathcal{G}_v^{\#}\Big]^{\frac{r-1}{2}},$$

where r is the rank of $\mathcal{G}$. Then,

$$\mu_v(\mathrm{O}(\mathcal{G}_v)) = \Big[\mathrm{O}(\mathcal{G}_v) : \mathrm{O}(\mathcal{G}_v, \pi_v^f R_v)\Big]\, \mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v^f)) = \tag{4.2.4}$$

$$= \Big[\mathrm{O}(\mathcal{G}_v) : \mathrm{O}(\mathcal{G}_v, \pi_v^f R_v)\Big] \Big[\mathcal{G}_v : \pi_v^f \mathcal{G}_v^{\#}\Big]^{-\frac{r-1}{2}} c(v). \tag{4.2.5}$$

In the case $\mathcal{G}$ is regular over v, we can choose $f = 1$, as was done at the beginning of this section. This justifies, our notation for $f = f(v)$, which can be chosen big enough, so as to satisfy all necessary

conditions for any place of K. For v regular, $c(v) = 2^{-1}$ (cf. (4.2.2)). Therefore, in accordance with the regular case, we normalize the local Haar-measures at irregular points by

$$\mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v^f R_v)) := 2^{-1}\Big[\mathcal{G}_v : \pi_v^f \mathcal{G}_v^{\#}\Big]^{\frac{r-1}{2}}.$$

We still have to justify the arbitrariness of f (for every v), by

Theorem 4.2.1. — *The quantity $c(v)$ defined above is constant for $f \gg 0$ (in particular it is independent of $\mathcal{G}_v$).*

This theorem settles the regularization of the local Haar-measures and the Minkowski-Siegel formula (4.1.5). It remains now to show that the fundamental volumes depend only on the rank of the bundles, and to give an explicit formula to compute them. The strategy to compute them is rather ingenious (for the left hand side, loc. cit.). We must compute both sides of (4.1.5). In the next section we prove Theorem 4.2.1 and compute the v-adic representation densities $\mathtt{d}_v(\mathcal{E}, \mathcal{F})$. For the left hand side, we will compute the representation numbers for several $\mathcal{F}$'s, which will save us from computing the order of the orthogonal groups involved, since in the average, the representation numbers will be independent of the class in the genus and therefore the sums on the reciprocals of the order of orthogonal groups will cancel each other! This is the task of §4.4.

3. Quadratic lattices over discrete valuation rings

For further details on this section, see [**Bou03**].
Using Theorem 1.2.10, a computation shows

Lemma 4.3.1. — *Let M_v be a lattice in a quadratic space over the local field K_v, and $f \in \mathbb{N}$ such that $\pi_v^f M_v^{\#} \subset M_v$. Then*

$$\Big[M_v^{\#} : M_v\Big] = \boldsymbol{N}(\mathrm{discr}(M_v)), \text{ and}$$
$$\Big[M_v : \pi_v^f M_v^{\#}\Big] = q_v^{f\,\mathrm{rk}(M_v)}\Big[M_v^{\#} : M_v\Big]^{-1}.$$

Proof. — Let $\{e_1, \dots, e_r\}$ be an orthogonal basis for the quadratic lattice M_v (recall $\mathrm{char}(K_v) \neq 2$). Then

$$M_v^{\#} = \{\sum_{k=1}^{r} \alpha_k e_k \mid \alpha_k \in K_v,\ \mathfrak{b}(\sum_{k=1}^{r} \alpha_k e_k, e_j) \in R_v \forall j = 1, \dots, r\}.$$

Denote $b_j := \mathfrak{q}(e_j, e_j)$, for $j = 1, \dots, r$. Then it is clear, that $\{e_j^{\#} := b_j^{-1} e_j\}_{j=1}^r$ forms a basis of $M_v^{\#}$. Hence,

$$\Big[M_v^{\#} : M_v\Big] = \prod_{j=1}^{r} [R_v : b_j R_v] = \prod_{j=1}^{r} \boldsymbol{N}(b_j) = \boldsymbol{N}(\mathrm{discr}(M_v)).$$

The second equation follows directly from the multiplicativity of the norm. □

Lemma 4.3.2. — *Let $\mathcal{G}_v' \subset \mathcal{G}_v$ be a submodule, such that for some $f \in \mathbb{N}$ $\pi_v^f \mathcal{G}_v^{\#} \subset \mathcal{G}_v$, $\pi_v^f \mathcal{G}_v'^{\#} \subset \mathcal{G}_v'$ and $[\mathcal{G}_v : \mathcal{G}_v'] = \boldsymbol{N}(\pi_v)$. Then*

$$\Big[\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v'/\pi_v^f \mathcal{G}_v'^{\#}) :\Big] = q_v^{\mathrm{rk}(\mathcal{G}_v)-1}.$$

For $\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^f \mathcal{G}_v^{\#})$, we understand the subgroup of $\mathrm{O}(\mathcal{G}_v)$ formed by those (local) orthogonal transformations which are the identity when projected to $\mathcal{G}_v/\pi_v^f \mathcal{G}_v^{\#}$ (similarly for the other group, which makes sense after the assumptions above).

Proof. — The lengthy, but straightforward proof is the same as the classical case, for which we refer to [**Kne92**, §32.5]. □

Proposition 4.3.3. — *With the assumptions of Lemma 4.3.2,*

$$\frac{\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^f \mathcal{G}_v^\#))}{\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^{f+1} \mathcal{G}_v^\#))} = q_v^{\frac{r(r-1)}{2}}.$$

Proof. — From Lemma 1.2.11

$$\frac{\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^f \mathcal{G}_v^\#))}{\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^{f+1} \mathcal{G}_v^\#))} = \Big[\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^f \mathcal{G}_v^\#) : \mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^{f+1} \mathcal{G}_v^\#)\Big] = q_v^{\frac{r(r-1)}{2}}.$$

□

Proof of Theorem 4.2.1. — For f large enough, all hypothesis of the proposition (and two lemata) above are satisfied, and therefore $c(v)$ becomes $\boldsymbol{N}(\pi_v)^{\frac{r(r-1)}{2}} \boldsymbol{N}(\pi_v)^{-r}$, which is independent of f. For the independence of $\mathcal{G}_v$, it suffices to see that for any sub-lattice $\mathcal{G}'_v$ of index $\boldsymbol{N}(\pi_v)$, the quantity is preserved, which follows directly from Lemma 4.3.2. □

We claim that the orthogonal groups $\mathrm{O}(\mathcal{G}_v, \mathcal{E}_v/\pi_v^f \mathcal{E}^\#)$ and $\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^f \mathcal{G}_v^\#)$ are the same. One inclusion ($\subset$) is trivial from the sequence

$$\pi_v^f \mathcal{E}_v^\# \cap \mathcal{G}_{v,(0)} \subset \pi_v^f \mathcal{G}_v \subset \mathcal{G}_v \subset \mathcal{E}_v;$$

where in fact, the first inclusion is an equality. The other inclusion, follows without difficulty, since $\mathcal{G}_v \oplus \mathcal{F}_{v,(0)} \supset \mathcal{E}_v$; hence every orthogonal transformation $u_v \in \mathrm{O}(\mathcal{G}_v)$ which is the identity modulo $\mathcal{G}_v/\pi_v^f \mathcal{G}_v$ is also the identity modulo the larger quotient $\mathcal{E}_v/\pi_v^f \mathcal{E}_v$ (cf. §3.3).
This enables us to replace $\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{E}_v/\pi_v^f \mathcal{E}_v^\#))$ by $\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{G}_v/\pi_v^f \mathcal{G}_v^\#))$, which we know how to compute.

We are now ready to evaluate the limits of the local representation densities.

Proposition 4.3.4. —

$$\mathsf{d}_{v,j_l}(\mathcal{E}, \mathcal{F}) = \epsilon\, q_v^{-\frac{fn(m+r-1)}{2}} \boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{n}{2}} \boldsymbol{N}(\mathrm{discr}(\mathcal{F}_v))^{\frac{r-1}{2}} \cdot \\ \cdot \mathsf{r}_{j_l}(\mathcal{E}_v, \mathcal{F}_v \bmod \pi_v^f \mathcal{E}_v^\#).$$

Proof. —

$$\mathsf{d}_{v,j}(\mathcal{E}, \mathcal{F}) = \frac{\mu_v(\mathrm{O}(\mathcal{E}_v))}{\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{E}_v))} = \frac{\Big[\mathrm{O}(\mathcal{E}_v) : \mathrm{O}(\mathcal{G}_v, \mathcal{E}_v/\pi_v^f \mathcal{E}_v^\#)\Big]}{\Big[\mathrm{O}(\mathcal{G}_v, \mathcal{E}_v) : \mathrm{O}(\mathcal{G}_v, \mathcal{E}_v/\pi_v^f \mathcal{E}_v^\#)\Big]} \cdot \\ \cdot \frac{\mu_v(\mathrm{O}(\mathcal{E}_v, \mathcal{E}_v/\pi_v^f \mathcal{E}_v^\#))}{\mu_v(\mathrm{O}(\mathcal{G}_v, \mathcal{E}_v/\pi_v^f \mathcal{E}_v^\#))}.$$

The last factor is (see remark before the theorem and previous results)

$$\frac{\mu_v(\mathrm{O}(\mathcal{E}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#))}{\mu_v(\mathrm{O}(\mathcal{G}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#))}=\frac{\mu_v(\mathrm{O}(\mathcal{E}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#))}{\mu_v(\mathrm{O}(\mathcal{G}_v,\mathcal{G}_v/\pi_v^f\mathcal{G}_v^\#))}=$$
$$=\frac{\left[\mathcal{G}_v:\pi_v^f\mathcal{G}_v^\#\right]^{\frac{r-1}{2}}c_v(m)}{\left[\mathcal{E}_v:\pi_v^f\mathcal{E}_v^\#\right]^{\frac{m-1}{2}}c_v(r)}=\frac{c_v(m)}{c_v(r)}\left[\mathcal{E}_v:\pi_v^f\mathcal{E}_v\right]^{-\frac{n}{2}}\left[\mathcal{F}_v:\pi_v^f\mathcal{F}_v^\#\right]^{-\frac{r-1}{2}}=$$
$$=\frac{c_v(m)}{c_v(r)}q_v^{-\frac{n}{2}(fm)}\boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{n}{2}}\boldsymbol{N}(\pi_v)^{-\frac{r-1}{2}(fn)}\boldsymbol{N}(\mathrm{discr}(\mathcal{F}_v))^{\frac{r-1}{2}}=$$
$$=\frac{c_v(m)}{c_v(r)}\boldsymbol{N}(\pi_v)^{-\frac{fn}{2}(m+r-1)}\boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{n}{2}}\boldsymbol{N}(\mathrm{discr}(\mathcal{F}_v))^{\frac{r-1}{2}}.$$

The second factor can be computed easily from one of the fundamental isomorphisms of group theory ($H/H\cap N\cong HN/N$) as follows

$$\frac{\left[\mathrm{O}(\mathcal{E}_v):\mathrm{O}(\mathcal{E}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#)\right]}{\left[\mathrm{O}(\mathcal{G}_v):\mathrm{O}(\mathcal{G}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#)\right]}=\frac{\left[\mathrm{O}(\mathcal{E}_v):\mathrm{O}(\mathcal{E}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#)\right]}{\left[\mathrm{O}(\mathcal{G}_v,\mathcal{E}_v)\,\mathrm{O}(\mathcal{G}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#):\mathrm{O}(\mathcal{G}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#)\right]}$$
$$=\left[\mathrm{O}(\mathcal{E}_v):\mathrm{O}(\mathcal{G}_v,\mathcal{E}_v)\,\mathrm{O}(\mathcal{G}_v,\mathcal{E}_v/\pi_v^f\mathcal{E}_v^\#)\right]=\mathsf{r}_j(\mathcal{E}_v,\mathcal{F}_v \bmod \pi_v^f\mathcal{E}_v^\#).$$

□

The v-adic representation densities can therefore be written as

$$\mathsf{d}_v(\mathcal{E},\mathcal{F})=\lim_{e\to\infty}\delta_{\mathfrak{p}_v^e}(\mathcal{E},\mathcal{F})=\sum_{l=1}^{g}\mathsf{d}_{v,j_l}(\mathcal{E},\mathcal{F})= \tag{4.3.1}$$
$$=\epsilon\,q_v^{-\frac{fn(m+r-1)}{2}}\boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{n}{2}}\boldsymbol{N}(\mathrm{discr}(\mathcal{F}_v))^{\frac{r-1}{2}}\mathsf{r}_v(\mathcal{E}_v,\mathcal{F}_v \bmod \pi_v^f\mathcal{E}_v^\#), \tag{4.3.2}$$

where $\epsilon=\begin{cases}1/2 & \text{when } r=0 \text{ and } m>0;\\ 1 & \text{else.}\end{cases}$

4. Proof of the formula (cont'd.): Volume Computation

The goal of this § is to prove that $\mu(\mathrm{O}(\mathcal{G})(K)\backslash\mathrm{O}_{\mathbb{A}}(\mathcal{G}))$ depends only on r, the rank of $\mathcal{G}$, for any definite quadratic bundle $\mathcal{G}$. Siegel's idea (taken from Dirichlet and Minkowski, as he says) is to sum left and right hand side of (4.1.5), over various one dimensional quadratic bundles $\mathcal{F}$[(1)] ($n=1$). By convention, we set $\mu_{\mathfrak{F}}(0):=\mu(\mathrm{O}(\mathcal{G})(K)\backslash\mathrm{O}_{\mathbb{A}}(\mathcal{G})):=1$ for $r=0$; which after a simple computation gives $\mu_{\mathfrak{F}}(1):=\mu(\mathrm{O}(\mathcal{E})(K)\backslash\mathrm{O}_{\mathbb{A}}(\mathcal{E}))):=1/2$, for $\mathrm{rk}(\mathcal{E})=1$. We refer to the Appendix 4.5.3 and the main reference therein, for basic analytical definitions to be used here throughout.

Let us state first the result to be proved

Theorem 4.4.1. — *Let $X/\mathrm{Spec}(\mathbb{F}_q)$ be a smooth, projective, geometrically irreducible curve, S_∞ a finite set of places ($U:=X\setminus S_\infty$, and $R:=\Gamma(U,\mathcal{O}_X)$ with class number h_R). For a the representation*

(1) Please note the difference between $\mathcal{F}$ and $\mathfrak{F}$.

numbers of a definite (with respect to S_∞) quadratic bundle $\mathcal{F}$ of rank n through the genus of a definite quadratic form $\mathcal{E}$ of rank m, $4 \geq m \geq n$, holds the following Minkowski-Siegel formula

$$\frac{1}{\sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}} \sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{R}(\mathcal{E}_l, \mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|} = \frac{\mu_{\mathfrak{F}}(m-n)}{\mu_{\mathfrak{F}}(m)} \prod_{v \notin |S_\infty|} \mathsf{d}_v(\mathcal{E}, \mathcal{F}). \tag{4.4.1}$$

Here, $\mu_{\mathfrak{F}}(0) = 1$, and the other measures for fundamental volumes are given by:

$$\begin{aligned}
\mu_{\mathfrak{F}}(1) &= \frac{1}{2}, \\
\mu_{\mathfrak{F}}(2) &= \frac{\mathrm{h}_R q^{(g-1)}}{(q-1)} \cdot \zeta_R(2)^{-1}, \\
\mu_{\mathfrak{F}}(3) &= \frac{\mathrm{h}_R^2 q^{3(g-1)}}{3(q-1)^2} \cdot \zeta_R(2)^{-1} \zeta_R(3)^{-1}, \\
\mu_{\mathfrak{F}}(4) &= \frac{\mathrm{h}_R^3 q^{6(g-1)}}{36(q-1)^3} \cdot \zeta_R(2)^{-1} \zeta_R(3)^{-1} \zeta_R(4)^{-1}.
\end{aligned}$$

To compute the volumes of the fundamental domains in the formula, as we mentioned above, we sum the whole formula over $\mathcal{F}$, where $\mathcal{F}$ runs over one dimensional quadratic bundles with underlying module belonging to a fixed class $\mathfrak{a}_0$ modulo an appropriately chosen modulus c. This is the *classical strategy*, by which one obtains a recursive formula, starting from $\mu_{\mathfrak{F}}(0) = 1$.

4.1. The left hand side. — For two one dimensional quadratic bundles $\mathfrak{a}$ and $\mathfrak{a}_0$ and c an R-ideal, we write $\mathfrak{a} \equiv \mathfrak{a}_0 \pmod{c}$ if one can find associated matrices M and M_0 to the quadratic forms $\mathfrak{a}$ and $\mathfrak{a}_0$ respectively, such that $M - M_0$ has entries in the ideal c.

Remark 4.4.2. — If the class number of R is one, there is only one class of ideals, and therefore the quadratic forms over R are simply given by elements of R (by abuse of notation denoted by the same symbol), and so $\mathfrak{a} \equiv \mathfrak{a}_0 \pmod{c}$ means the element $\mathfrak{a} - \mathfrak{a}_0$ belongs to c.

We start the computation. Concretely, on the left hand side (LHS), we take

$$\sum_{\substack{\mathfrak{a} \equiv \mathfrak{a}_0 \pmod{c} \\ \boldsymbol{N}(\mathfrak{a}) < B}} \frac{1}{\sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}} \sum_{l=1}^{h(\mathcal{E})} \frac{\mathsf{R}(\mathcal{E}_l, \mathfrak{a})}{|\mathrm{O}(\mathcal{E}_l)(U)|} = \frac{1}{\sum_{l=1}^{h(\mathcal{E})} |\mathrm{O}(\mathcal{E}_l)(U)|^{-1}} \sum_{l=1}^{h(\mathcal{E})} \frac{1}{|\mathrm{O}(\mathcal{E}_l)(U)|} \sum_{\substack{\mathfrak{a} \equiv \mathfrak{a}_0 \pmod{c} \\ \boldsymbol{N}(\mathfrak{a}) < B}} \mathsf{R}(\mathcal{E}_l, \mathfrak{a}); \tag{4.4.2}$$

and the modulus will be so chosen, that the last sum will not depend on l. Throughout, we will be putting (compatible) conditions to the modulus c. We start with a c, such that for any two one dimensional sublattices

$$\mathfrak{b} \equiv \mathfrak{b}_0 \pmod{c\mathcal{E}^{\#}} \text{ implies } \mathfrak{a} \equiv \mathfrak{a}_0 \pmod{c}, \tag{4.4.3}$$

where $\mathfrak{a}_{(0)}$ is the quadratic space induced on $\mathfrak{b}$ ($\mathfrak{b}_0$) by $\mathcal{E}$. This can be achieved by simply choosing a c such that $c\mathcal{E}^{\#}$ is contained in $\mathcal{E}$ (so in particular the support of c contains the support of the discriminant of $\mathcal{E}$). This c can also be chosen to be principal (just take a power of it). Moreover, choose a quadratic subspace $\mathfrak{a}_0$ of $\mathcal{E}$, such that its associated matrix (so any) is not zero modulo c. This can be also achieved, since the lattice can be supposed to be of norm R. Namely, if the rank of $\mathcal{E}$ is greater than 1 this is clear. For a rank 1 quadratic form, we have two possibilities. Either it is defined over a module of trivial discriminant, in which case by simply scaling the form one gets a unimodular one. If not, suppose the form is defined over a module of rank one generated by

$\langle e_1, e_1' \rangle$, such that $\alpha_1 e_1 = \alpha_1' e_1'$. But even in this case, we can restrict the quadratic form to the finite index sub-lattice $\langle e_1' \rangle$, for which, as we explain in §4.4.1.1, the fundamental volume does not change. Therefore, without loss of generality, we can use this lattice for the volume computations in Theorem 4.4.1, which again can be scaled as before, to obtain a norm R quadratic form.

Now, we will need to compute

$$\begin{aligned}
\sum_{\substack{\mathfrak{a}\equiv\mathfrak{a}_0 \pmod c \\ \boldsymbol{N}(\mathfrak{a})<B}} \mathsf{R}(\mathcal{E},\mathfrak{a}) &= \sum_{\substack{\mathfrak{b}'\hookrightarrow\mathcal{E} \\ \mathfrak{a}'\equiv\mathfrak{a}_0 \pmod c \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{a}'))<B}} 1 = \\
&= \sum_{\overline{v}_0\subset\mathcal{E}/c\mathcal{E}^{\#}} \sum_{\substack{\mathfrak{b}\subset\mathcal{E} \\ \mathfrak{a}\equiv\mathfrak{a}_0 \pmod c \\ \mathfrak{b}\equiv v_0 \pmod{c\mathcal{E}^{\#}} \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{a}))<B}} 1 = \\
&= \sum_{\substack{\overline{v}_0\subset\mathcal{E}/c\mathcal{E}^{\#} \\ \mathfrak{n}(v_0)\equiv\mathfrak{a}_0 \pmod c}} \sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#} \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}} 1 = \\
&= \left(\sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#} \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}} 1 \right) \left(\sum_{\substack{\overline{v}_0\subset\mathcal{E}/c\mathcal{E}^{\#} \\ (v_0)\equiv\mathfrak{a}_0 \pmod c}} 1 \right),
\end{aligned}$$

where $\mathfrak{a}^{(\prime)}$ is the quadratic form induced from $\mathcal{E}$ on $\mathfrak{b}^{(\prime)}$. In the third equality, we used the property (4.4.3), c was chosen to have. So, we concentrate on the first factor above, since the last sum will in the end cancel with a factor on the right hand side (RHS).

In order to compute

$$\sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#} \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}} 1, \tag{4.4.4}$$

we show first, that we can suppose $\mathcal{E}$ to be a diagonalized quadratic bundle.

[1.1] We now justify, why it suffices to do the computations for diagonalized quadratic bundles (in this section we mean always over U) $(\mathfrak{q}, \mathcal{E}, \mathcal{L})$.

The first reduction, is to suppose $\det(\mathcal{E}) \cong R$. Then we can assume $\mathcal{E}$ to be trivial over $U = \mathrm{Spec}(R)$. Now we need to diagonalize the quadratic form on it. It is clearly not possible in general (for $\mathrm{rk}(\mathcal{E}) > 1$). It is easy to show that one can diagonalize the form on a finite index sub-bundle $\mathcal{E}'$ of $\mathcal{E}$.
Claim:

$$\mu_{\mathfrak{F}}(\mathrm{O}(\mathcal{E})) = \mu_{\mathfrak{F}}(\mathrm{O}(\mathcal{E}')). \tag{4.4.5}$$

Then the general formula for $\mathcal{E}$ follows from the formula for $\mathcal{E}'$.
We prove this by induction on the rank of the torsion module $\mathcal{E}/\mathcal{E}'$. We can also suppose, $\mathrm{rk}(\mathcal{E}) \geq 2$. If the rank of the torsion module is zero, the bundle is diagonalizable. If the rank is greater than 0, then we make a filtration

$$\mathcal{E}' \subset \mathcal{E}_d \subset \ldots \subset \mathcal{E}_0 = \mathcal{E};$$

where the successive quotients at each step have rank 1. Therefore, it is enough to show the statement for $\mathcal{E}'$ and $\mathcal{E}$, differing at only one prime, say v. Now the two fundamental volumes $\mathfrak{F}$ and $\mathfrak{F}'$ differ only at v. Denote by $\mu_v(\mathrm{O}(\mathcal{G}_v, \pi_v^{f^{(\prime)}}))$ the measure of $\mathfrak{F}$ ($\mathfrak{F}'$) at v. From (4.2.4) we obtain that these two volumes are the same, if we show that $\min\{f, f'\}$ is large enough. From **??**[Zusatz 15.4] (cf. Lemma 4.3.2) (and provided f is large) the index $\left[\mathrm{O}(\mathcal{G}_v) : \mathrm{O}(\mathcal{G}_v, \pi_v^f R_v)\right]$ depends only on the rank, $\left[\mathcal{G}_v : \pi_v^f \mathcal{G}_v^{\#}\right]$ also, and from Theorem 4.2.1 the remaining factor does not depend on $\mathcal{G}_v$ either. So, it remains to get $\min\{f, f'\}$ large, which can be certainly achieved by rewriting the fundamental domains with respect to principal congruence subgroups which at v have large f. This proves the claim.

Remark 4.4.3. — The claim above is, in the end, a direct consequence of Theorem 4.2.1.

Lemma 4.4.4. — *For an embedding $\iota : \mathfrak{b} \hookrightarrow \mathcal{F} \cong R \perp \mathfrak{a}$, with $\mathcal{F}$ a quadratic bundle. We set $a_1 := \mathfrak{q}(e_1)$, where e_1 generates the first summand of $\mathcal{F}$. Then*

$$\boldsymbol{N}(\mathfrak{n}(\iota(\mathfrak{b}))) = \begin{cases} \boldsymbol{N}(\mathfrak{b})^2\, \boldsymbol{N}(f_1)^2\, \boldsymbol{N}(a_1), & \boldsymbol{N}(f_1)^2\, \boldsymbol{N}(a_1) \geq \boldsymbol{N}(f_2)^2\, \boldsymbol{N}(\det(\mathfrak{a})); \\ \boldsymbol{N}(\mathfrak{b})^2\, \boldsymbol{N}(f_2)^2\, \boldsymbol{N}(\det(\mathfrak{a})), & \boldsymbol{N}(f_1)^2\, \boldsymbol{N}(a_1) < \boldsymbol{N}(f_2)^2\, \boldsymbol{N}(\det(\mathfrak{a})). \end{cases}$$

Proof. — It follows by a simple computation, since

$$\mathfrak{n}(\iota(\mathfrak{b})) = \gcd(\{b_1^2 f_1^2 a_1 + b_2^2 f_2^2 \mathfrak{q}(v) \mid b_1, b_2 \in \mathfrak{b} \text{ and } v \in \mathfrak{a}\}) = \\ = \mathfrak{b}^2 \gcd(\{\langle f_1^2 a_1 + f_2^2 \mathfrak{q}(v)\rangle\}) = \mathfrak{b}^2 \left(f_1^2 a_1 + f_2 \det(\mathfrak{a})\right).$$

Taking norms yields the result. □

Remark 4.4.5. — We will also use later the corresponding version of this lemma for higher ranks (i.e. embeddings into lattices up to 4). This statement is similar, but with the obvious additional cases (see below).

We will make abuse of notation, and write $\boldsymbol{N}(a_{\mathrm{rk}(\mathcal{E})})$ instead of $\boldsymbol{N}(\det(\mathfrak{a}))$ (see below).
By $\alpha \approx_N \beta$ we mean $\lim_{N\to\infty} \alpha/\beta = 1$, where we may omit N.

[1.2] *Rank 4-case.* — Using Lemma 4.4.4 for the case $\mathrm{rk}(\mathcal{E}) = 4$, we obtain

$$\sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#} \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}} 1 = \sum_{\mathfrak{b}\subset R} \sum_{\substack{f_1\in\langle \frac{c}{a_1}\rangle \\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}} \sum_{\substack{f_2\in\langle \frac{c}{a_2}\rangle \\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}} \sum_{\substack{f_3\in\langle \frac{c}{a_3}\rangle \\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}} \left(\star\right);$$

where $\star$ consists of 4 summands, which correspond to the four cases in the computation of the norm of $\mathfrak{n}(\iota(\mathfrak{b}))$. One can easily see, by the inclusion-exclusion principle, that $\star$ can be written as a single sum, times a factor, 6 (correspondingly, it is 2 or 1 for the cases $\mathrm{rk}(\mathcal{E}) = 3, 2$, respectively).
In the rank 4-case, the six sums correspond to the 6 4×4 *ordering boxes*. Namely, if we write $i > j$ $(i, j = 1, 2, 3, 4)$ for the inequality

$$\boldsymbol{N}(f_i)^2\, \boldsymbol{N}(a_i) > \boldsymbol{N}(f_j)^2\, \boldsymbol{N}(a_j),$$

where $\boldsymbol{N}(a_4) := \boldsymbol{N}(\det(\mathfrak{n}(\mathfrak{a})))$ (respectively for $\geq$); then the a **ordering box** is, for example, a box of the form

$$\begin{array}{ccccccc} 3 & > & 2 & > & 1 & \geq & 4 \\ 3 & > & 2 & \geq & 4 & > & 1 \\ 3 & \geq & 4 & > & 2 & > & 1 \\ 4 & > & 3 & > & 2 & > & 1, \end{array}$$

which is said to correspond to the ordering (of length 3) $3 > 2 > 1$. In a similar way, for the case $\mathrm{rk}(\mathcal{E}) = 3$, an ordering box, is a 3×3 box, which corresponds to a previously fixed ordering of *length* 2. It is easy to see, that each box contributes with a single sum (because of *telescopic* cancellation of the sums), and that the number of *ordering boxes* for the different ranks, are $6, 2, 1$, as remarked above.

We start with the case ($\mathrm{rk}(\mathcal{E}) =:) m = 4$ (which *contains* all sums to be computed in the other cases also).

$$(4.4.6) \qquad \sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#} \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}} 1 = \sum_{\mathfrak{b}\subset R} \sum_{\substack{f_1\in\langle \frac{c}{a_1}\rangle \\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}} \sum_{\substack{f_2\in\langle \frac{c}{a_2}\rangle \\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}} \sum_{\substack{f_3\in\langle \frac{c}{a_3}\rangle \\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}} \left(6 \sum_{\substack{f_4\in\langle \frac{c}{a_4}\rangle \\ \boldsymbol{N}(f_4)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_4)^{1/2}}}} 1 \right).$$

Therefore, we need to compute (also for the cases of smaller rank $m = 2, 3$) the sum

$$\sum_{\substack{f\in\mathfrak{r} \\ \boldsymbol{N}(f)<\tilde{B}}} 1.$$

Lemma 4.4.6. — *Let $\psi \in \mathrm{Dir}(\mathcal{J}_R)$ be a multiplicative function and $\mathfrak{r} = \mathfrak{p}^e$ an R-ideal, with $\mathfrak{p}$ prime and e a natural number. Then*

$$\sum_{\substack{\mathfrak{a}\in\mathcal{J}_R \\ \mathfrak{r}|\mathfrak{a} \\ \boldsymbol{N}(\mathfrak{a})\leq\tilde{B}}} \psi(\mathfrak{a}) = \sum_{n=0}^{\infty} \psi(\mathfrak{p}^{e+n}) \cdot \frac{\varphi_1(\mathfrak{p})}{\boldsymbol{N}(\mathfrak{p})} \cdot \sum_{\substack{\mathfrak{b}\in\mathcal{J}_R \\ \boldsymbol{N}(\mathfrak{b})\leq\frac{\tilde{B}}{\boldsymbol{N}(\mathfrak{p}^{e+n})}}} \psi(\mathfrak{b}).$$

Proof. —

$$\sum_{\substack{\mathfrak{a}\in\mathcal{J}_R \\ \mathfrak{r}|\mathfrak{a} \\ \boldsymbol{N}(\mathfrak{a})\leq\tilde{B}}} \psi(\mathfrak{a}) = \sum_{\substack{\boldsymbol{N}(\mathfrak{r}\mathfrak{b})\leq\tilde{B} \\ \mathfrak{b}\in\mathcal{J}_R}} \psi(\mathfrak{r}\mathfrak{b}) =$$

$$= \sum_{\substack{\mathfrak{b}\in\mathcal{J}_R\langle\mathfrak{r}\rangle \\ \boldsymbol{N}(\mathfrak{b})\leq\tilde{B}/\,\boldsymbol{N}(\mathfrak{r})}} \psi(\mathfrak{r})\psi(\mathfrak{b}) + \sum_{n=1}^{\infty} \sum_{\substack{\mathfrak{p}^n||\mathfrak{b} \\ \mathfrak{b}\in\mathcal{J}_R \\ \boldsymbol{N}(\mathfrak{b})\leq\tilde{B}/\,\boldsymbol{N}(\mathfrak{r})^{n+1}}} \psi(\mathfrak{r}\mathfrak{p}^n)\psi(\mathfrak{b}/\mathfrak{p}^n) =$$

$$= \sum_{\substack{\mathfrak{b}\in\mathcal{J}_R\langle\mathfrak{r}\rangle \\ \boldsymbol{N}(\mathfrak{b})\leq\tilde{B}/\,\boldsymbol{N}(\mathfrak{r})}} \psi(\mathfrak{r})\psi(\mathfrak{b}) + \sum_{n=1}^{\infty} \sum_{\substack{\mathfrak{b}'\in\mathcal{J}_R\langle\mathfrak{r}\rangle \\ \boldsymbol{N}(\mathfrak{b}')\leq\frac{\tilde{B}}{\boldsymbol{N}(\mathfrak{r})\,\boldsymbol{N}(\mathfrak{p})^n}}} \psi(\mathfrak{r}\mathfrak{p}^n)\psi(\mathfrak{b}') =$$

$$= \sum_{n=0}^{\infty} \psi(\mathfrak{r}\mathfrak{p}^n) \cdot \sum_{\substack{\mathfrak{b}\in\mathcal{J}_R\langle\mathfrak{r}\rangle \\ \boldsymbol{N}(\mathfrak{b})\leq \frac{\tilde{B}}{\boldsymbol{N}(\mathfrak{r})\,\boldsymbol{N}(\mathfrak{p})^n}}} \psi(\mathfrak{b}) = \sum_{n=0}^{\infty} \psi(\mathfrak{r}\mathfrak{p}^n) \cdot \frac{\varphi_1(\mathfrak{p})}{\boldsymbol{N}(\mathfrak{p})} \cdot \sum_{\substack{\mathfrak{b}\in\mathcal{J}_R \\ \boldsymbol{N}(\mathfrak{b})\leq \frac{\tilde{B}}{\boldsymbol{N}(\mathfrak{r})\,\boldsymbol{N}(\mathfrak{p})^n}}} \psi(\mathfrak{b}).$$

□

Lemma 4.4.7. — *In the previous lemma, for $\psi = 1$, we have*

$$\sum_{\substack{\mathfrak{r}|\mathfrak{a} \\ \boldsymbol{N}(\mathfrak{a})\leq\tilde{B}}} 1 \approx \frac{1}{\boldsymbol{N}(\mathfrak{r})} \cdot \sum_{\boldsymbol{N}(\mathfrak{a})\leq\tilde{B}} 1.$$

Proof. —

$$\sum_{\substack{\mathfrak{r}|\mathfrak{a} \\ \boldsymbol{N}(\mathfrak{a})\leq\tilde{B}}} 1 \approx \sum_{n=0}^{\infty} \frac{\varphi_1(\mathfrak{p})}{\boldsymbol{N}(\mathfrak{p})} \cdot \sum_{\substack{\mathfrak{b}\in\mathcal{J}_R \\ \boldsymbol{N}(\mathfrak{b})\leq \frac{\tilde{B}}{\boldsymbol{N}(\mathfrak{p}^{e+n})}}} 1 \approx$$

$$\approx \sum_{n=0}^{\infty} \frac{\varphi_1(\mathfrak{p})}{\boldsymbol{N}(\mathfrak{p})} \cdot \{\frac{\mathrm{h}_R q^{-(g-1)}}{(q-1)} \cdot \frac{\tilde{B}}{\boldsymbol{N}(\mathfrak{p})^{e+n)}}\} = \frac{\varphi_1(\mathfrak{p})\mathrm{h}_R q^{-(g-1)} B}{\boldsymbol{N}(\mathfrak{p})^{e+1}(q-1)} \cdot \sum_{n=0}^{\infty} \boldsymbol{N}(\mathfrak{p})^{-n} =$$

$$= \frac{(1-\boldsymbol{N}(\mathfrak{p}^{-1})\mathrm{h}_R q^{-(g-1)} B}{\boldsymbol{N}(\mathfrak{p})^e(q-1)} \cdot (1-\boldsymbol{N}(\mathfrak{p})^{-1})^{-1} = \frac{\mathrm{h}_R q^{-(g-1)} B}{\boldsymbol{N}(\mathfrak{p})(q-1)}.$$

□

Applying these lemata to (4.4.6) we obtain

$$\sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#} \\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}} 1 = \sum_{\mathfrak{b}\subset R} \sum_{\substack{f_1\in\langle\frac{c}{a_1}\rangle \\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}} \sum_{\substack{f_2\in\langle\frac{c}{a_2}\rangle \\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}} \sum_{\substack{f_3\in\langle\frac{c}{a_3}\rangle \\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}} \left(6 \sum_{\substack{f_4\in\langle\frac{c}{a_4}\rangle \\ \boldsymbol{N}(f_4)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_4)^{1/2}}}} 1\right) \approx$$

$$\approx 6\sum_{\mathfrak{b}\subset R} \sum_{\substack{f_1\in\langle\frac{c}{a_1}\rangle \\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}} \sum_{\substack{f_2\in\langle\frac{c}{a_2}\rangle \\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}} \sum_{\substack{f_3\in\langle\frac{c}{a_3}\rangle \\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}} \left(\frac{(q-1)}{\mathrm{h}_R} \cdot \sum_{\substack{\langle\frac{c}{a_4}\rangle|\mathfrak{a} \\ \boldsymbol{N}(\mathfrak{a})<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_4)^{1/2}}}} 1\right) \approx$$

$$\approx 6\frac{(q-1)}{\mathrm{h}_R}\cdot\frac{\boldsymbol{N}(a_4)}{\boldsymbol{N}(c)}\cdot\sum_{\mathfrak{b}\subset R} \sum_{\substack{f_1\in\langle\frac{c}{a_1}\rangle \\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}} \sum_{\substack{f_2\in\langle\frac{c}{a_2}\rangle \\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}} \sum_{\substack{f_3\in\langle\frac{c}{a_3}\rangle \\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}} \left(\sum_{\boldsymbol{N}(\mathfrak{a})<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_4)^{1/2}}} 1\right) \approx$$

$$\approx 6\frac{(q-1)}{\mathrm{h}_R}\cdot\frac{\boldsymbol{N}(a_4)}{\boldsymbol{N}(c)}\cdot\sum_{\mathfrak{b}\subset R} \sum_{\substack{f_1\in\langle\frac{c}{a_1}\rangle \\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}} \sum_{\substack{f_2\in\langle\frac{c}{a_2}\rangle \\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}} \sum_{\substack{f_3\in\langle\frac{c}{a_3}\rangle \\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}} \left(\frac{\mathrm{h}_R q^{-(g-1)}}{(q-1)}\cdot\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_4)^{1/2}}\right) \approx$$

$$\approx 6\frac{(q-1)}{\mathrm{h}_R}\cdot\frac{\boldsymbol{N}(a_4)}{\boldsymbol{N}(c)}\cdot\frac{\mathrm{h}_R q^{-(g-1)}}{(q-1)}\cdot\frac{B^{1/2}}{\boldsymbol{N}(a_4)^{1/2}}\sum_{\mathfrak{b}\subset R}\frac{1}{\boldsymbol{N}(\mathfrak{b})} \sum_{\substack{f_1\in\langle\frac{c}{a_1}\rangle \\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}} \sum_{\substack{f_2\in\langle\frac{c}{a_2}\rangle \\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}} \sum_{\substack{f_3\in\langle\frac{c}{a_3}\rangle \\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}} 1 \approx$$

$$\approx 6\cdot B^{\frac{1}{2}}\cdot\frac{\boldsymbol{N}(a_4)^{\frac{1}{2}}q^{-(g-1)}}{\boldsymbol{N}(c)}\sum_{\mathfrak{b}\subset R}\frac{1}{\boldsymbol{N}(\mathfrak{b})}\sum_{\substack{f_1\in\langle\frac{c}{a_1}\rangle\\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}}\ \sum_{\substack{f_2\in\langle\frac{c}{a_2}\rangle\\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}}\ \sum_{\substack{f_3\in\langle\frac{c}{a_3}\rangle\\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}}1$$

and repeating the same calculation for the other sums

$$\sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#}\\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}}1\approx\frac{6q^{-4(g-1)}\,\boldsymbol{N}(a_1)^{\frac{1}{2}}\,\boldsymbol{N}(a_2)^{\frac{1}{2}}\,\boldsymbol{N}(a_3)^{\frac{1}{2}}\,\boldsymbol{N}(a_4)^{\frac{1}{2}}\zeta_R(4)}{\boldsymbol{N}(c)^4}\cdot B^2.$$

Putting all together:

$$\mathrm{LHS}_{(4)}\approx 6\cdot q^{-4(g-1)}\cdot\zeta_R(4)\cdot\frac{\boldsymbol{N}(\mathrm{discr}(\mathcal{E}))^{1/2}}{\boldsymbol{N}(c)^4}\cdot B^2\cdot\left(\sum_{\substack{\overline{v}_0\subset\mathcal{E}/c\mathcal{E}^{\#}\\ \mathfrak{n}(v_0)\equiv\mathfrak{a}_0\pmod c}}1\right).\tag{4.4.7}$$

[1.3] *Rank* 3 *and* 2. — For the rank 3-case, we have (recall the beginning of §4.4.1.2)

$$\sum_{\substack{\mathfrak{b}\subset c\mathcal{E}^{\#}\\ \boldsymbol{N}(\mathfrak{n}(\mathfrak{b}))<B}}1=\sum_{\mathfrak{b}\subset R}\sum_{\substack{f_1\in\langle\frac{c}{a_1}\rangle\\ \boldsymbol{N}(f_1)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_1)^{1/2}}}}\ \sum_{\substack{f_2\in\langle\frac{c}{a_2}\rangle\\ \boldsymbol{N}(f_2)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_2)^{1/2}}}}\left(2\sum_{\substack{f_3\in\langle\frac{c}{a_3}\rangle\\ \boldsymbol{N}(f_3)<\frac{B^{1/2}}{\boldsymbol{N}(\mathfrak{b})\,\boldsymbol{N}(a_3)^{1/2}}}}1\right)=$$

$$=\frac{2q^{-3(g-1)}\,\boldsymbol{N}(a_1)^{\frac{1}{2}}\,\boldsymbol{N}(a_2)^{\frac{1}{2}}\,\boldsymbol{N}(a_3)^{\frac{1}{2}}\,\boldsymbol{N}(a_4)^{\frac{1}{2}}\zeta_R(3)}{\boldsymbol{N}(c)^3}\cdot B^{\frac{3}{2}}.$$

Therefore,

$$\mathrm{LHS}_{(3)}\approx 2\cdot q^{-3(g-1)}\cdot\zeta_R(3)\cdot\frac{\boldsymbol{N}(\mathrm{discr}(\mathcal{E}))^{1/2}B^{3/2}}{\boldsymbol{N}(c)^3}\sum_{\substack{\overline{v}_0\subset\mathcal{E}/c\mathcal{E}^{\#}\\ \mathfrak{n}(v_0)\equiv\mathfrak{a}_0\pmod c}}1;\tag{4.4.8}$$

and similarly, we obtain

$$\mathrm{LHS}_{(2)}\approx q^{-2(g-1)}\cdot\zeta_R(2)\cdot\frac{\boldsymbol{N}(\mathrm{discr}(\mathcal{E})^{1/2}B}{\boldsymbol{N}(c)^2}\sum_{\substack{\overline{v}_0\subset\mathcal{E}/c\mathcal{E}^{\#}\\ \mathfrak{n}(v_0)\equiv\mathfrak{a}_0\pmod c}}1.\tag{4.4.9}$$

for rank 2.

4.2. The right hand side. — For the computation of the RHS of (4.4.2), we recall first the local representation densities (4.3.1)

$$\mathtt{d}_v(\mathcal{E},\mathfrak{a})=q_v^{-\frac{fn(m+r-1)}{2}}\,\boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{n}{2}}\,\boldsymbol{N}(\mathrm{discr}(\mathfrak{a}_v))^{\frac{r-1}{2}}\mathtt{r}_v(\mathcal{E}_v,\mathfrak{a}_v\bmod\pi_v^f\mathcal{E}_v^{\#}).$$

For v not dividing our modulus c, the orthogonal group has good reduction (in particular, the quadratic form is regular over v). Therefore, we divide in two the product over the finite primes: the product over the primes not dividing c, and the product over the others. This last product will cancel

with the sum on the LHS left without calculation (cf. §4.4.1). So, we concentrate ourselves on the infinite product

$$\prod_{v\nmid c}\mathsf{d}_v(\mathcal{E},\mathfrak{a}).$$

Since the representation numbers $\mathsf{r}_v(\mathcal{E}_v,\mathfrak{a}_v\text{mod }\pi_v^f\mathcal{E}_v^{\#})$ essentially depend on the parity of the rank of $\mathcal{E}$, we need to make case distinction between $2,4$ and 3; this last case causing also and additional inconvenience.

Before going into the cases, we write more precisely the local representation densities for those primes v not dividing c. In this case, $\mathrm{discr}(\mathcal{E}_v)\in R_v^{\times}$, so it defines an element of $\mathbb{F}_{q_v}^{\times}$. If we denote by $\left(\frac{\star}{q_v}\right):\mathbb{F}_{q_v}^{\times}\to\{\pm1\}$ the quadratic character, from [**Kne92**, §13] we have

$$\mathsf{r}_v(\mathcal{E}_v,\mathfrak{a}_v \bmod \pi_v^f\mathcal{E}_v^{\#})=\begin{cases} q_v^{m-1}+\left(\frac{\delta_v}{q_v}\right)q_v^{\frac{m}{2}}-\left(\frac{\delta_v}{q_v}\right)q_v^{\frac{m}{2}-1}-1 & \text{for } m\equiv 0 \pmod 2,\ v\mid\mathfrak{a};\\ q_v^{m-1}-\left(\frac{\delta_v}{q_v}\right)q_v^{\frac{m}{2}-1} & \text{for } m\equiv 0 \pmod 2,\ v\nmid\mathfrak{a};\\ q_v^{m-1}+\left(\frac{\mathfrak{a}_v\delta_v}{q_v}\right)q_v^{\frac{m-1}{2}} & \text{for } m\equiv 1 \pmod 2,\ v\nmid\mathfrak{a};\\ q_v^{m-1}-1 & \text{for } m\equiv 1 \pmod 2,\ v\mid\mathfrak{a}.\end{cases} \tag{4.4.10}$$

[2.1] *Rank* $4,2$ *case.* — Summing up $\mathsf{d}_v(\mathcal{E}_v,\mathfrak{a}_v/\mathfrak{t}_v)$ for all (local) ideal divisors $\mathfrak{t}$ of $\mathfrak{a}_v$ we get

$$\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a})=\boldsymbol{N}(\mathfrak{a}_v)^{\frac{m}{2}-1}\cdot\Big(1-\Big(\frac{\delta_v}{q_v}\Big)q_v^{-\frac{m}{2}}\Big)\cdot\sum_{\pi_v^k\mid\mathfrak{a}_v}\Big(\frac{\delta_v}{q_v}\Big)^k q_v^{-k(\frac{m}{2}-1)}.$$

Now,

$$\begin{aligned}\sum_{\substack{\mathfrak{a}\equiv\mathfrak{a}_0 \pmod c\\ \boldsymbol{N}(\mathfrak{a})<B}}\prod_{v\notin S_\infty}\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a})=\prod_{v\mid c}\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a}_0 \bmod \pi_v\mathcal{E}^{\#})\cdot\prod_{v\nmid c}\Big(1-\Big(\frac{\delta_v}{q_v}\Big)q_v^{-\frac{m}{2}}\Big)\cdot\\ \cdot\sum_{\substack{\mathfrak{a}\equiv\mathfrak{a}_0 \pmod c\\ \boldsymbol{N}(\mathfrak{a})<B}}\boldsymbol{N}(\mathfrak{a}_v)^{\frac{m}{2}-1}\sum_{\mathfrak{b}\mid\mathfrak{a}}\Big(\frac{\delta_v}{\mathfrak{b}}\Big)\,\boldsymbol{N}(\mathfrak{b})^{-(\frac{m}{2}-1)}.\end{aligned} \tag{4.4.11}$$

For $m=4$ these last sums are asymptotically

$$\approx\frac{\mathrm{h}_R q^{-(g-1)}B^2}{2\,\boldsymbol{N}(c)}\cdot\sum_{\substack{\gcd(\mathfrak{b},c)=1\\ \boldsymbol{N}(\mathfrak{b})<B}}\Big(\frac{\delta_v}{\mathfrak{b}}\Big)\frac{1}{\boldsymbol{N}(\mathfrak{b})^2},$$

therefore

$$\begin{aligned}\sum_{\substack{\mathfrak{a}\equiv\mathfrak{a}_0 \pmod c\\ \boldsymbol{N}(\mathfrak{a})<B}}\prod_{v\notin S_\infty}\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a})=\frac{\mathrm{h}_R q^{-(g-1)}B^2}{2\,\boldsymbol{N}(c)}\prod_{v\mid c}\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a}_0 \bmod \pi_v\mathcal{E}^{\#})\cdot\\ \cdot\Bigg(\prod_{v\nmid c}\Big(1-\Big(\frac{\delta_v}{q_v}\Big)q_v^{-2}\Big)\sum_{\substack{\gcd(\mathfrak{b},c)=1\\ \boldsymbol{N}(\mathfrak{b})<B}}\Big(\frac{\delta_v}{\mathfrak{b}}\Big)\frac{1}{\boldsymbol{N}(\mathfrak{b})^2}\Bigg).\end{aligned}$$

Using the fact that

$$\prod_{v\nmid c}\Big(1-\Big(\frac{\delta_v}{q_v}\Big)q_v^{-s}\Big)\sum_{\gcd(\mathfrak{b},c)=1}\Big(\frac{\delta_v}{\mathfrak{b}}\Big)\frac{1}{\boldsymbol{N}(\mathfrak{b})^s}=1 \tag{4.4.12}$$

for $s > \delta = 1$ (valid also for $s = \delta$ when the character $\left(\frac{\delta_v}{\star}\right)$ is non-trivial), we see

$$\mathrm{RHS}_{(4)} \approx \frac{\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G}))}{\mu(\mathrm{O}(\mathcal{E})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{E}))}\frac{\boldsymbol{N}(\mathrm{discr}(\mathcal{E}))^{1/2}B^2}{\boldsymbol{N}(c)^4}\cdot\prod_{v|c}\mathsf{r}(\mathcal{E}_v \mod c_v\mathcal{E}_v^{\#},\mathfrak{a}_v)\frac{\mathrm{h}_R q^{-(g-1)}}{2(q-1)}.$$

For the rank 2-case, we need to compute, cf. (4.4.11), the asymptotic for

$$\sum_{\substack{\mathfrak{b}\mathfrak{c}\equiv\mathfrak{a}_0 \pmod c\\ \boldsymbol{N}(\mathfrak{b}\mathfrak{c})<B}}\left(\frac{\delta_v}{\mathfrak{b}}\right).$$

Again, we use here a trick due to Dirichlet (cf. [**Sie35**, page 566] or [**Kne92**, page 151 and ff.]). As explained in last loc.cit., this trick consists in bounding the asymptotic for the sum over three different regions defined below the hyperbola (consider this for the definitions of the regions below) $\boldsymbol{N}(\mathfrak{b}\mathfrak{c}) = B$:

$$\begin{aligned}
\mathcal{R}_1 &:= \{(\mathfrak{b},\mathfrak{c}) \mid \mathfrak{b}\mathfrak{c} \equiv \mathfrak{a}_0 \pmod c \text{ and } \boldsymbol{N}(\mathfrak{b}),\boldsymbol{N}(\mathfrak{c}) < B^{\frac{1}{2}}\};\\
\mathcal{R}_2 &:= \{(\mathfrak{b},\mathfrak{c}) \mid \mathfrak{b}\mathfrak{c} \equiv \mathfrak{a}_0 \pmod c \text{ and } \boldsymbol{N}(\mathfrak{b}) \geq B^{\frac{1}{2}},\ \boldsymbol{N}(\mathfrak{c}) < B^{\frac{1}{2}}\};\\
\mathcal{R}_3 &:= \{(\mathfrak{b},\mathfrak{c}) \mid \mathfrak{b}\mathfrak{c} \equiv \mathfrak{a}_0 \pmod c \text{ and } \boldsymbol{N}(\mathfrak{c}) \geq B^{\frac{1}{2}},\ \boldsymbol{N}(\mathfrak{b}) < B^{\frac{1}{2}}\}.
\end{aligned}$$

Computing the asymptotic for these three regions gives

$$\sum_{\substack{\mathfrak{a}\equiv\mathfrak{a}_0 \pmod c\\ \boldsymbol{N}(\mathfrak{a})<B}}\sum_{\mathfrak{b}|\mathfrak{a}}\left(\frac{\delta_v}{\mathfrak{b}}\right) \approx \frac{2\mathrm{h}_R q^{-(g-1)}}{(q-1)}\cdot\frac{B}{\boldsymbol{N}(c)}\cdot\sum_{\substack{\gcd(\mathfrak{b},c)=1\\ \boldsymbol{N}(\mathfrak{b})<B^{\frac{1}{2}}}}\left(\frac{\delta_v}{\mathfrak{b}}\right)\frac{1}{\boldsymbol{N}(\mathfrak{b})}. \tag{4.4.13}$$

Since the character $\left(\frac{\delta}{\star}\right)$ is non-trivial, (4.4.12) holds, and therefore we have

$$\mathrm{RHS}_{(2)} \approx \frac{\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G}))}{\mu(\mathrm{O}(\mathcal{E})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{E}))}\frac{\boldsymbol{N}(\mathrm{discr}(\mathcal{E}))^{1/2}B}{\boldsymbol{N}(c)^2}\cdot\prod_{v|c}\mathsf{r}(\mathcal{E}_v \mod c_v\mathcal{E}_v^{\#},\mathfrak{a}_v)\frac{2\mathrm{h}_R q^{-(g-1)}}{(q-1)}. \tag{4.4.14}$$

[2.2] *Rank* 3 *case.* — This last case is classically a *special* one, since (besides one) three is the only odd number smaller than five. The reason, why being greater or equal to five is important, is because in the computations we have seen above, some L-series coming into play must be evaluated at $(m/2)-1$; and hence we have absolute convergence only for $m \geq 5$. The case $m = 4$ is not so difficult, since there is conditional convergence (due to the non-triviality of the character, cf. §4.4.2.1), and the cases 2 and 3 are the most difficult (cf. [**Sie35**, Einleitung]).

For our last remaining computation, we can not use any of the *classical tricks* (loc.cit., [**Sie37**], [**Kne92**, Kapitel X]). They are based on standard classical computations, either on the representation number of an integer by the diagonal ternary quadratic form $\mathrm{diag}(1,1,1)$ (a result due to Gauß), or on the analytic theory of modular forms and on explicit reduction theory of quadratic forms over totally real number fields, as in [**Sie37**]. We can make the computation directly.

Recalling the local densities described at the beginning of §4.4.2 for $m = 3$, we have

$$\sum_{\mathfrak{t}_v^2|\mathfrak{a}}\mathsf{d}_v(\mathcal{E},\mathfrak{a}/\mathfrak{t}^2) = \mathsf{d}_v(\mathcal{E},\mathfrak{a}) + \mathsf{d}_v(\mathcal{E},\mathfrak{a}/\pi_v^2) + \ldots =$$

$$= \boldsymbol{N}(\mathfrak{a}_v)^{\frac{1}{2}} \cdot \Big[(1-q_v^{-2}) + \ldots + (1-q_v^{-2})q_v^{-r} + \ldots + (1-q_v^{-2})q_v^{-(e_v-1)} + \\ + \left(1 + \Big(\frac{\mathfrak{a}_v/\pi_v^{2e_v}\delta_v}{q_v}\Big)\cdot q_v^{-1} + (1 - \Big(\frac{\mathfrak{a}_v/\pi_v^{2e_v}\delta_v}{q_v}\Big)^2)q_v^{-2}\right)\Big].$$

Setting $e_v := \lfloor v(\mathfrak{a})/2 \rfloor$ and $\chi(\mathfrak{b}) := \left(\frac{\mathfrak{a}\delta}{\mathfrak{b}}\right)$, the last sum becomes

$$\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a}) = \boldsymbol{N}(\mathfrak{a}_v)^{\frac{1}{2}} \cdot \sum_{k=0}^{e_v} q_v^{-k}\left[1 + \chi(\mathfrak{a}_v/\pi_v^{2k})\cdot q_v^{-1} - (1-\chi(\mathfrak{a}_v/\pi_v^{2k})^2)q_v^{-2}\right] =$$

$$= \boldsymbol{N}(\mathfrak{a}_v)^{\frac{1}{2}} \cdot \left[\sum_{k=0}^{e_v} q_v^{-k} + \sum_{k=0}^{e_v}\chi(\mathfrak{a}_v/\pi_v^{2k})q_v^{-(k+1)} - \sum_{k=0}^{e_v}(1-\chi(\mathfrak{a}_v/\pi_v^{2k})^2)q_v^{-(k+2)}\right] =$$

$$= \boldsymbol{N}(\mathfrak{a}_v)^{\frac{1}{2}} \cdot \left[\sum_{k=0}^{e_v} q_v^{-k} + \chi(\mathfrak{a}_v/\pi_v^{2e_v})\cdot q_v^{-(e_v+1)} + (1-\chi(\mathfrak{a}_v/\pi_v^{2e_v})^2)\cdot q_v^{-(e_v+2)}\right]$$

Hence,

$$\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a}) = \boldsymbol{N}(\mathfrak{a}_v)^{\frac{1}{2}} \cdot \sum_{k=0}^{e_v} q_v^{-k} \cdot \left[1 + \frac{\chi(\mathfrak{a}_v/\pi_v^{2e_v})}{\sum_{k=0}^{e_v} q_v^k}\cdot q_v^{-1} + \frac{(1-\chi(\mathfrak{a}_v/\pi_v^{2e_v})^2)}{\sum_{k=0}^{e_v} q_v^k}\cdot q_v^{-2}\right].$$

We take now the product of the $\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a})$'s over the primes not dividing c, and obtain that the asymptotic of this product:

$$\sum_{\substack{\mathfrak{a}\equiv\mathfrak{a}_0 \pmod{c} \\ \boldsymbol{N}(\mathfrak{a})<B}} \prod_{v\nmid c} \bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a})$$

is

$$\sum_{\substack{\mathfrak{a}\equiv\mathfrak{a}_0 \pmod{c} \\ \boldsymbol{N}(\mathfrak{a})<B}} \boldsymbol{N}(\mathfrak{a})^{\frac{1}{2}} \approx \frac{1}{\boldsymbol{N}(c)} \sum_{\boldsymbol{N}(\mathfrak{a})<B} \boldsymbol{N}(\mathfrak{a})^{\frac{1}{2}} \approx \frac{1}{\boldsymbol{N}(c)}\{\frac{2\mathrm{h}_R q^{-(g-1)}\cdot B^{\frac{3}{2}}}{3(q-1)}\}.$$

Namely, over the primes dividing $\mathfrak{a}$ it is clear that the asymptotic is given by $\boldsymbol{N}(\mathfrak{a})^{\frac{1}{2}}$, since the remaining factor can be uniformly bounded by a sum $\sum_{\mathfrak{b}^2|\mathfrak{a}} \boldsymbol{N}(\mathfrak{b})$; whereas the product over the primes not dividing $\mathfrak{a}$ is precisely the special value of $L_\chi(1)$. In our case, this L-function is indeed a polynomial in q^{-s} and the independent coefficient is 1 (cf. [**Wei95**, Chapter VII, §7] or [**Ros02**, Chapter 14]). Therefore, again the main contribution of these factors is $\boldsymbol{N}(\mathfrak{a})^{\frac{1}{2}}$.

Replacing this in the formula above,

$$\mathrm{RHS}_{(3)} \approx \frac{\mu(\mathrm{O}(\mathcal{G})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{G}))}{\mu(\mathrm{O}(\mathcal{E})(K)\backslash \mathrm{O}_{\mathbb{A}}(\mathcal{E}))}\frac{\boldsymbol{N}(\mathrm{discr}(\mathcal{E}))^{1/2}B^{3/2}}{\boldsymbol{N}(c)^3}\cdot\prod_{v|c}\mathsf{r}(\mathcal{E}_v \mod c_v\mathcal{E}_v^{\#},\mathfrak{a}_v)\cdot\frac{2\mathrm{h}_R q^{-(g-1)}}{3(q-1)}.$$

Combining the computations for the left and for the right hand sides, we finished the proof of Theorem 4.4.1. □

5. Applications and Consequences

5.1. Genus-versal integral quadratic bundles. — Let $\mathfrak{q} := (\mathfrak{q},\mathcal{E})$ be a quadratic bundle over a curve X (with respect to $S \subset X$). Recall the definition of a representation: the quadratic bundle $\mathfrak{q}$

represents the quadratic bundle $\mathfrak{q}' := (\mathfrak{q}', \mathcal{E})$ if there is an isometry ϕ from $\mathfrak{q}'$ to $\mathfrak{q}$.

Definition 4.5.1. — An integral quadratic bundle $(\mathfrak{q}, \mathcal{E})$ as above is d-**genus-versal**[(2)], for $d \in \{1, 2, \ldots, m = \mathrm{rk}(\mathcal{E})\}$, if and only if every quadratic bundle $\mathfrak{q}'$ of dimension d which is represented by some quadratic bundle in the genus of $\mathfrak{q}$, is represented by $\mathfrak{q}$ itself (i.e. all isomorphism classes in the genus represent the same forms of dimension d). A 1-genus-versal quadratic bundle is simply called **genus-versal**.

One may call a genus of a quadratic bundle d-**genus-versal** if some, and hence any, form in the genus is d-genus-versal.

In this section, we will show, as an application of Theorem 4.4.1 the following

Theorem 4.5.2. — *Let R be a global ring with quotient field K, a function field. Fix a positive number $B \in \mathbb{R}_{>0}$. There are finitely many isomorphy classes of genus-versal, definite (integral) quadratic forms over R with norm not greater than B.*

Remark 4.5.3. — We will give a bound for the discriminants of genus-versal definite quadratic forms, so the restriction on the integrality of the form is not essential (cf. Proposition 2.1.9 and Remark 2.1.10).

Remark 4.5.4. — The bound B in the theorem above, is simply to avoid the following trivial fact. Let $\mathcal{E}$ be a genus-versal quadratic bundle (over $\mathrm{Spec}(R)$), then any (integral) multiple of it is again genus-versal. This means that the cardinality of the set of genus-versal quadratic forms is either 0 or infinity. But how many *essentially different* genus-versal quadratic forms do exist? In a more mathematical language, in the case of principal ideal domains (and for example also in the classical case $(\mathbb{Z}, \mathbb{Q})$), this translates into:

how many *primitive*, integral, genus-versal quadratic forms do exist?

The restriction to *primitive* forms is a particular case of the restriction on the norm written in Theorem 4.5.2; namely quadratic forms of norm smaller or equal to 1.
So, all in all, Theorem 4.5.2 generalizes what is known in the classical case, a result first proved by G.L. Watson in his Ph. D. [**Wat53**] (see also [**Wat76**])

Theorem 4.5.5. — *For each dimension $d \in \mathbb{N}$, there exist finitely many* primitive*, positive definite, integral quadratic forms over $\mathbb{Z}$.*

Note that in the function field case there are only definite forms in rank up to 4 (whereas in the classical case one has definite forms in all dimensions). The only previously known result in the function field case, is for the very special case of rational function fields $(\mathbb{F}_q[T], \mathbb{F}_q(T))$ (i.e. Theorem 4.5.2 holds for $R := \mathbb{F}_q[T]$), recently proved in [**CD05**]. In that paper, the main ingredient is the explicit reduction theory for definite quadratic forms, only available in $\mathbb{F}_q[T]$ (due to Gerstein's [**Ger03**]). So, the use

(2) In the literature, these quadratic forms are known as *regular*, after Dickson's studies in the theory of *ternary quadratic forms* over $\mathbb{Z}$. Nevertheless, this term is very inappropriate, since regular forms are indeed quadratic forms whose adjoint is bijective. For this reason, in order to avoid confusion, and recalling the definition of a *universal* quadratic form: it represents every element of the ring; we use here the term *genus-versal*. *Universal* means the quadratic form represents everything in the universe (=ring), whereas *genus-versal* means it represents everything represented by the genus (i.e. universal in the restricted universe given by the genus: elements of the ring represented by some form in the genus).

of the Minkowski-Siegel formula is a powerful ingredient to get rid of this obstruction, for proving the statement in full generality for any global ring.

For a general account, see the overview paper in the subject of *"regular"* (here genus-versal) quadratic forms: [**CEO04**].

Proof of Theorem 4.5.2. — We will show that for large $\boldsymbol{N}(\mathcal{E})$, the LHS of (4.4.1),

$$\frac{1}{\sum_{l=1}^{h(\mathcal{E})}|\mathrm{O}(\mathcal{E}_l)(U)|^{-1}}\sum_{l=1}^{h(\mathcal{E})}\frac{\mathsf{R}(\mathcal{E}_l,\mathcal{F})}{|\mathrm{O}(\mathcal{E}_l)(U)|} \tag{4.5.1}$$

becomes smaller than 1, so in particular the genus of $\mathcal{E}$ cannot be genus-versal (as one directly concludes from the inequality). It is clear from Proposition 2.1.9, that it suffices to bound the discriminant (or equivalently the reduced determinant and the norm, which is already bounded). To do so, we show that

(1) for a particularly chosen quadratic form (bundle over $\mathrm{Spec}(R)$), $\mathfrak{a}$, the local representation densities $\bar{\mathsf{d}}_v(\mathcal{E},\mathfrak{a})$ are smaller than one, at all the places where the discriminant is supported (and also the greater the valuation of the discriminant at such a place is, the smaller the local representation density is);

(2) for the places not dividing the discriminant, we obtain a universal bound depending only on the ring R; which would finish the proof.

Let $\mathfrak{q} := (\mathfrak{q},\mathcal{E})$ be a definite quadratic form of dimension m over R. Choose a quadratic form of dimension 1, $\mathfrak{a}$, represented by the genus of $\mathcal{E}$ and of minimal discriminant (the counting norm is discrete). Using Hasse Principle, we obtain that the support of the discriminant of $\mathfrak{a}$ is contained in the support of the discriminant of $\mathcal{E}$ (and also the valuations at those places of the discriminant of $\mathfrak{a}$ are at most the valuations of $\mathrm{discr}(\mathcal{E})$): $v(\mathrm{discr}(\mathfrak{a}))\leq v(\mathrm{discr}(\mathcal{E}))$.
From the computations in §4.4.2 at the places outside the support of the discriminant of $\mathcal{E}$, we see clearly for ranks 4 and 2, that the product

$$\prod_{\substack{v\notin|S_\infty|\\ v\notin\mathrm{supp}(\mathrm{discr}(\mathcal{E}))}}\mathsf{d}_v(\mathcal{E},\mathcal{F})$$

is uniformly bounded, so

$$\frac{\mu_{\mathfrak{F}}(m-1)}{\mu_{\mathfrak{F}}(m)}\prod_{\substack{v\notin|S_\infty|\\ v\notin\mathrm{supp}(\mathrm{discr}(\mathcal{E}))}}\mathsf{d}_v(\mathcal{E},\mathcal{F}) \tag{4.5.2}$$

can be bounded depending only on R (cf. Theorem 4.4.1). For the rank 3 case, we obtain this bound from the fact that the L-series appearing in §4.4.2.2 can be uniformly bounded depending only on R, since it is a polynomial in q^{-s}, with coefficients again bounded from R (actually coming from properties of the class group of R). (See [**Wei95**, Chapter VII, §7] or Rosen op.cit..)
Now, we need to show that the local representation densities contribute with numbers smaller than 1. For $m=1$ there is nothing to show.

(1) Let $m=2$, then for $v\in\mathrm{supp}(\mathrm{discr}(\mathcal{E}))$ we have $\mathcal{E}_v\cong\langle\pi_v^a,\pi_v^b\rangle$, for $0\leq a\leq b$ (clearly not both 0). Then we have

$$\pi^{f_v}\mathcal{E}_v^{\#}\subset\langle\pi_v^a,\pi_v^b\rangle\subset\langle\pi_v^{-a},\pi_v^{-b}\rangle,$$

where $f_v = 2b \geq 2$. From the choice of $\mathfrak{a}$, we have only primitive representations: $\bar{\mathsf{d}}_v(\mathcal{E}, \mathfrak{a}) = \mathsf{d}_v(\mathcal{E}, \mathfrak{a})$. But this last local density is (recall (4.3.1))

$$q_v^{-f_v}\, \boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{1}{2}} \mathsf{r}_v(\mathcal{E}_v, \mathfrak{a}_v \mod \pi_v^{f_v}\mathcal{E}_v^{\#}).$$

Now $\boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{1}{2}} = q_v^{\frac{a+b}{2}}$. The last factor is 1 in the case $a = b$ (clear, since the index $\left[\mathcal{E}_v : \pi_v^{f_v}\mathcal{E}_v^{\#}\right]$ is 1, so it can be 1 or 0 depending on the existence or not of a single representation) and we get $\mathsf{d}_v(\mathcal{E}_v, \mathfrak{a}_v) \leq q_v^{-b} < 1$ (keep in mind the dependence on b: the greatest exponent appearing in the diagonalized form of $\mathcal{E}_v$).

If $0 \leq a < b$, then $\mathsf{r}_v(\mathcal{E}_v, \mathfrak{a} \mod \pi_v^{f_v}\mathcal{E}^{\#})$ is at most $q_v^{\frac{2(b-a)}{2}}$, where $q_v^{2(b-a)}$ is the index of $\pi_v^{f_v}\mathcal{E}_v^{\#}$ in $\mathcal{E}_v$. So, we get in this case $\mathsf{d}_v(\mathcal{E}_v, \mathfrak{a}_v \mod \pi_v^{f_v}\mathcal{E}_v^{\#}) \leq q_v^{\frac{-4b+(a+b)+2(b-a)}{2}} = q_v^{\frac{-(b+a)}{2}} < 1$ and again recall that the density bound depends on the valuation of the discriminant of $\mathcal{E}$.

(2) Let $m = 3$. In this case we have (after the same observation as above about the primitivity of the representations of $\mathfrak{a}$), that

$$\bar{\mathsf{d}}_v(\mathcal{E}_v, \mathfrak{a}_v) = q_v^{-2f_v}\, \boldsymbol{N}(\mathrm{discr}(\mathcal{E}_v))^{\frac{1}{2}}\, \boldsymbol{N}(\mathrm{discr}(\mathfrak{a}_v))^{\frac{1}{2}} \mathsf{r}_v(\mathcal{E}_v, \mathfrak{a}_v \mod \pi_v^{f_v}\mathcal{E}_v^{\#}).$$

Denote $\mathcal{E}_v$ by $\langle \pi_v^a, \pi_v^b, \pi_v^c \rangle$, with $c \geq 1$ and $0 \leq a \leq b \leq c$. So, $f_v = 2c$, $\boldsymbol{N}(\mathcal{E}_v) = q_v^{a+b+c}$ and $\boldsymbol{N}(\mathfrak{a}_v) = q_v^a$. It remains to study $\mathsf{r}_v(\mathcal{E}_v, \mathfrak{a}_v \mod \pi_v^{f_v}\mathcal{E}_v^{\#})$. The index of $\pi_v^{f_v}\mathcal{E}_v^{\#}$ inside $\mathcal{E}_v$ is $q_v^{2(c-a)+2(c-b)}$, and the local representations we have to compute are the same as the representations of an element by a binary form over a ring with $q_v^{2(c-a)}$ elements (actually this gives an upper bound, since we may have enlarged the ring by q_v^{b-a}). But this number can be bounded from above. The expected number of such representations is the number of elements of the ring to the power $(2-1) - (1 \cdot (1+1)/2)$ (a simple combinatorial argument). The actual number of representations may differ from it in a power series of $q_v^{\frac{2(c-a)}{2}}$ (i.e. half the number of elements in the ring) with coefficients ± 1 (cf. Siegel [**Sie35**] or Kneser [**Kne92**, Kapitel IV] for the case the ring is a field). Hence, $\mathsf{r}_v(\mathcal{E}_v, \mathfrak{a}_v \mod \pi_v^{f_v}\mathcal{E}_v^{\#})$ can be bounded by

$$q_v^{2(c-a)+\frac{(c-a)}{2}}.$$

Putting altogether, we obtain

$$\mathsf{d}_v(\mathcal{E}_v, \mathfrak{a}_v) = q_v^{\frac{-8c+a+b+c+a}{2}} \mathsf{r}_v(\mathcal{E}_v, \mathfrak{a}_v \mod \pi_v^{f_v}\mathcal{E}_v^{\#}) \leq q_v^{\frac{-7c+2a+b}{2}} \cdot \left(q_v^{\frac{4(c-a)+(c-a)}{2}} \right) \leq$$
$$\leq q_v^{\frac{-c-3a}{2}} \leq q_v^{-\frac{c}{2}} < 1;$$

where again, the quantity is smaller than 1, and depends on the valuation of the discriminant of $\mathcal{E}$ at v (dependence again on the highest exponent c).

The remaining $m = 4$ case follows with exactly the same arguments.

Therefore, if the norm of the discriminant is big enough (for example $\boldsymbol{N}(\mathrm{discr}(\mathcal{E}))^{\frac{-1}{8}}$ bigger than the bound for (4.5.2)), then (4.5.1) is smaller than 1. □

Remark 4.5.6. — Fixing a particular global ring R, one can explicitly compute the bounds given in the proof, and so one can effectively compute, say for example for $R := \mathbb{F}_q[T]$, all genus-versal forms. Moreover, by doing this, one could also answer the still open question (cf. [**CD05**]), whether there exist or not genus-versal quadratic forms of class number strictly bigger than one. This means also, this approach seems to be more effective than the reduction theory used in op.cit..

The answer to this question above in the classical case is negative, and the counter example was constructed by Kitaoka in dimension 3 (one can see this also from the theory of (supersingular)

elliptic curves over $\mathbb{F}_{11}$, cf. [**Cer**]). Finding an example for a genus-versal, definite quadratic form using the *Brandt's correspondence* (cf. loc. cit.) in the global ring case seems to me impossible. We would rather support the conjecture, that in $\mathbb{F}_q[T]$ all genus-versal definite (integral) quadratic forms have class number one. This problem will be addressed soon jointly with J. Bureau (Louisiana, USA).

5.2. Deuring-Gekeler Maßformel. — In [**Gek83**] and in [**Gek92**] Gekeler computed the sum of the reciprocals of the cardinality of the automorphisms of supersingular Drinfeld modules of rank 2 up to isomorphisms (i.e. the **Maßformel** for Drinfeld modules), which is the analogon to the famous formula of Deuring (cf. [**Deu41**])

$$\sum_{\substack{E \text{ supersingular elliptic curve} \\ \text{over } \overline{\mathbb{F}_p}/\cong}} |\mathrm{Aut}(E)|^{-1} = \frac{(p-1)}{24}.$$

We are not going to develop the theory of supersingular Drinfeld modules of rank 2 and their relation with ternary quadratics forms; which in the classical case was studied in [**Cer**]. Instead, we would like to announce, that using the so called Brandt correspondence, we can derive the Maßformel of Gekeler cited above from our Theorem 4.4.1, by simply computing the local densities for definite ternary quadratic forms of prime discriminant. This can be easily done using some well known results (which go back to Dickson), on the order of orthogonal groups over finite fields. All this will be the subject of a forthcoming work.

5.3. Lefschetz trace formula over stacks and Minkowski-Siegel formula. — Along the lines of [**BD05**], we would like to derive the Minkowski-Siegel formula from the Lefschetz trace formula for the stack of principal orthogonal bundles on curves with a given additional *level structure*. In loc.cit., using the Lefschetz trace formula, Behrend and Dhillon obtain a formula for the *Maß* of the genus.

ARITHMETICAL SEMI-GROUPS

(We follow [**Kno75**]. Any result without proof in this section, can be found in loc. cit.) Let $\mathfrak{G}$ be a commutative semi-group with unit, $\mathcal{P} \subset \mathfrak{G}$ a countable subset, such that for any $\mathfrak{g} \in \mathfrak{G}$ there exist unique:

$$r \in \mathbb{N};\ e_1, \ldots, e_r \in \mathbb{N} \text{ and } \mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P},$$

such that $\mathfrak{g} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$. The subset $\mathcal{P}$ will be called the set of **primes of** $\mathfrak{G}$.
Moreover, let $|\cdot| : \mathfrak{G} \to \mathbb{R}_+$ be a map with the following conditions:

ASG1) $|1_{\mathfrak{G}}| = 1$;
ASG2) $|\mathfrak{p}| > 1 \, \forall \mathfrak{p} \in \mathcal{P}$;
ASG3) $|\mathfrak{g}_1\mathfrak{g}_2| = |\mathfrak{g}_1||\mathfrak{g}_2| \, \forall \mathfrak{g}_1, \mathfrak{g}_2 \in \mathfrak{G}$;
ASG4) $\#\{\mathfrak{p} \in \mathcal{P} \mid |\mathfrak{g}| \leq B\} < \infty$, $\forall B \in \mathbb{R}_{>0}$.

We call the data $(\mathfrak{G}, |\cdot|, \mathcal{P})$ an **arithmetical semi-group**.

***Example 5.0.7* (Prototype).** — $\mathfrak{G} = (\mathbb{Z}, \cdot)/\mathbb{Z}^\times$ which can be identified with $\{1, 2, 3, \ldots\}$, for $|\cdot|$ we take the ordinary absolute value, and for $\mathcal{P}$ the set of (rational) prime numbers. This is the standard example of classical analytical number theory.

Remark 5.0.8. — In other words, the triple in the example consists of the semi-group of $\mathbb{Z}$-ideals, the subset $\mathcal{P}$ consisting of the prime $\mathbb{Z}$-ideals, and the ordinary absolute value. More generally, we can take any Dedekind domain R inside a global field K, $\mathcal{J}_R$ the semi-group of the R-ideals, and $\mathcal{P}$ the set of prime ideals in R; plus an absolute value on $\mathcal{J}_R$, which can be obtained as explained above. In chapter 4, we will focus our attention to the case K being the function field of a curve X over a finite field, and R the sub-ring of regular functions on an affine Zariski open subset U of X, and $|\cdot|$ will be the norm function $\boldsymbol{N}(\cdot)$.

All arithmetical semi-groups we are going to deal with satisfy *Axiom A* ([**Kno75**, page 75]):
There exist positive constants A, δ and η, with $\delta > \eta \geq 0$, such that

$$\boldsymbol{\mathcal{A}}_{\mathfrak{G}}(B) = AB^{\delta} + O(B^{\eta}), \quad \textit{for } B \to \infty;$$

where $\boldsymbol{\mathcal{A}}_{\mathfrak{G}}(B)$ is the number of elements in $\mathfrak{G}$ of norm at most B.

Remark 5.0.9. — Resumig remark 5.0.8, one has for function fields (cf. §1.1.4) that $\delta = 1$ (as in the classical case), $A = \frac{\mathrm{h}_R q^{-(g-1)}}{(q-1)}$.

1. Arithmetical functions. Some properties

1.1 We define now, (*classical, abstract*) arithmetical functions associated with an arithmetical group $(\mathfrak{G}, |\cdot|, \mathcal{P})$ and give some properties, which will be used later on.

Denote $\boldsymbol{\mathcal{A}}_{\mathfrak{G}}(B) := \sum_{\substack{g\in\mathfrak{G}\\ |\mathfrak{g}|\leq B}} 1$, for any $B \in \mathbb{R}_+$. The Möbius function is defined by:

$$\mu(\mathfrak{g}) := \begin{cases} 1 & , \text{ if } \mathfrak{g} = 1; \\ (-1)^r & , \text{ if } \mathfrak{g} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}, \text{ and } e_i > 0; \\ 0 & , \text{ else.} \end{cases}$$

The Euler-φ function is given by

$$\varphi(\mathfrak{g}) := \sum_{\substack{g'\in\mathfrak{G}\\ |\mathfrak{g}'|\leq|\mathfrak{g}|\\ \gcd(\mathfrak{g}',\mathfrak{g})=1}} 1;$$

where the greatest common divisor can be defined, as usual, from the properties ASG1-ASG4.
We have the classical result (with the same proof)

$$\varphi(\mathfrak{g}) = \sum_{\delta|\mathfrak{g}} \mu(\delta)\, \boldsymbol{\mathcal{A}}_{\mathfrak{G}}(|\mathfrak{g}/\delta|).$$

There are also similar useful Euler-functions for a given real number r:

$$\varphi_r(\mathfrak{g}) := \sum_{\mathfrak{d}|\mathfrak{a}} \mu(\mathfrak{d})|\mathfrak{a}/\mathfrak{d}|^r.$$

They are useful, for example, for determining the asymptotic of the arithmetical semi-group obtained from a given one $\mathfrak{G}$, in the following way. Take $\mathfrak{r} \in \mathfrak{G}$ and define $\mathfrak{G}\langle\mathfrak{r}\rangle$ as the semi-group of all elements of $\mathfrak{G}$ which are coprime to $\mathfrak{r}$ (henceforth we easily obtain an arithmetical semi-group in the sense above). We are interested in the asymptotic of this newly defined semi-group.

Proposition 5.1.1. — *In the notation above, the semi-group $\mathfrak{G}\langle\mathfrak{r}\rangle$ satisfies axiom A, and has asymptotic*

$$\boldsymbol{\mathcal{A}}_{\mathfrak{G}\langle\mathfrak{r}\rangle}(B) = A\varphi_\delta(\mathfrak{r})|\mathfrak{r}|^{-\delta}B^\delta + O(B^\eta).$$

1.2 As for classical arithmetical functions, we have a more general version of the Möbuis inversion formula (proposition 5.1.2). To state it, we define first the algebra of arithmetical functions, where the general statements will hold.
The complex valued functions on $\mathfrak{G}$ form the set of **arithmetical functions**, $\mathrm{Dir}(\mathfrak{G})$. It is clearly a complex vector space, to which we add a multiplicative law:

$$(\phi \star \psi)(\mathfrak{g}) := \sum_{\delta\mathfrak{h}=\mathfrak{g}} \phi(\delta)\psi(\mathfrak{h}), \quad \text{for any } \phi, \psi \in \mathrm{Dir}(\mathfrak{G}) \text{ and } \mathfrak{g} \in \mathfrak{G},$$

called the **convolution of ϕ with ψ**.
This unital, associative algebra is the **Dirichlet algebra** of $\mathfrak{G}$.
A function $f \in \mathfrak{G}$ is called **completely multiplicative** (**multiplicative**) if $f(\mathfrak{ab}) = f(\mathfrak{a})f(\mathfrak{b})$ for any $\mathfrak{a}, \mathfrak{b} \in \mathfrak{G}$ (with $\gcd(\mathfrak{a}, \mathfrak{b}) = 1$).

Proposition 5.1.2 **(Möbius inversion formula)**. — *For any $\phi, \psi \in \mathrm{Dir}(\mathfrak{G})$ holds*

$$\psi(\mathfrak{g}) = \sum_{\delta|\mathfrak{g}} \phi(\delta) \Leftrightarrow \phi(\mathfrak{g}) = \sum_{\delta|\mathfrak{g}} \mu(\delta)\psi(\mathfrak{g}/\delta).$$

The zeta-function if an arithmetical semi-group $\mathfrak{G}$ is defined as

$$\zeta_{\mathfrak{G}}(z) := \sum_{\mathfrak{g}\in\mathfrak{G}} |\mathfrak{g}|^{-z}.$$

It is the multiplicative inverse of the Möbius function in the Dirichlet algebra.

We close this section, with a simple and useful lemma. Define for any $\phi \in \mathrm{Dir}(\mathfrak{G})$ and $B \in \mathbb{R}_+$, $\boldsymbol{\mathcal{A}}(\phi, B) := \sum_{\substack{g\in\mathfrak{G}\\ \boldsymbol{\mathcal{A}}(\mathfrak{g})\leq B}} \phi(\mathfrak{g})$.

Lemma 5.1.3. — *Let $\phi, \psi \in \mathrm{Dir}(\mathfrak{G})$. Then*

$$\boldsymbol{\mathcal{A}}(\phi \star \psi, B) = \sum_{|\mathfrak{g}|\leq B} \psi(\mathfrak{g})\, \boldsymbol{\mathcal{A}}(\psi, B/|\mathfrak{g}|) = \sum_{|\mathfrak{g}|\leq B} \psi(\mathfrak{g})\, \boldsymbol{\mathcal{A}}(\phi, B/|\mathfrak{g}|).$$

Proof. —

$$\boldsymbol{\mathcal{A}}(\phi \star \psi, B) = \sum_{|\mathfrak{g}|\leq B} \sum_{\delta\mathfrak{h}=\mathfrak{g}} \phi(\delta)\psi(\mathfrak{h}) = \sum_{|\delta\mathfrak{h}|\leq B} \phi(\delta)\psi(\mathfrak{h}) =$$

$$= \sum_{|\delta|\leq B} \phi(\delta) \sum_{|\mathfrak{h}|\leq B/|\delta|} \psi(\mathfrak{h}) = \sum_{|\mathfrak{h}|\leq B} \psi(\mathfrak{h}) \sum_{|\delta|\leq B/|\mathfrak{h}|} \phi(\delta).$$

□

2. L-functions and asymptotical properties

Here we simply recall [**Kno75**, Chapter IV, §2, Prop. 2.8] which is also of use in chapter 4.

Proposition 5.2.1. — *Let $\mathfrak{G}$ be an arithmetical semi-group satisfying axiom A. Then:*

(1)

$$\sum_{\boldsymbol{N}(\mathfrak{a})\leq B} \boldsymbol{N}(\mathfrak{a})^{-\delta} \approx_{B\to\infty} \delta A \log(B).$$

(2) *For $\Re(z) = \eta$,*

$$\sum_{\boldsymbol{N}(\mathfrak{a})\leq B} \boldsymbol{N}(\mathfrak{a})^{-z} \approx \frac{\delta A}{\delta - z} B^{\delta - z} + O(\log(B)).$$

(3) *If $\Re(z) \leq \delta$, $\Re(z) = \delta \neq \eta$ and $z \neq \delta$, then*

$$\sum_{\boldsymbol{N}(\mathfrak{a})\leq B} \boldsymbol{N}(\mathfrak{a})^{-z} \approx \frac{\delta A}{\delta - z} B^{\delta - z}.$$

With methods similar os the ones used in the proof of the above proposition (cf. op.cit), it is proved that the L-series

$$L_\chi(s) := \sum_{g\in\mathfrak{G}} \chi(g)|g|^{-s},$$

for χ a non-trivial character, defines an analytical function for $\Re(s) > \eta$ (see [**Kno75**, Chapter 9, §5]).

BIBLIOGRAPHY

[Bas74] H. Bass – "Clifford algebras and spinor norms over a commutative ring", *Amer. J. Math.* **96** (1974), p. 156–206.

[BD05] K. Behrend & A. Dhillon – "The geometry of Tamagawa numbers of Chevalley groups", (2005), p. 25, `arxiv.org/pdf/math.NT/0503383`.

[BK94] W. Bichsel & M.-A. Knus – "Quadratic forms with values in line bundles", in *Recent advances in real algebraic geometry and quadratic forms (Berkeley, CA, 1990/1991; San Francisco, CA, 1991)*, Contemporary Mathematics, vol. 155, American Mathematical Society, 1994, p. 293–306.

[Bor91] A. Borel – *Linear algebraic groups*, Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991, Second edition.

[Bou59] N. Bourbaki – *Algèbre. Chapitre 9: Formes sesquilinéares et formes quadratiques*, Actualités Scientifiques et Industrielles, vol. 1272, Hermann, Paris, 1959.

[Bou98] ———, *Commutative algebra. Chapters 1–7*, Elements of Mathematics, Springer-Verlag, Berlin, 1998.

[Bou03] ———, *Algebra II. Chapters 4–7*, Elements of Mathematics, Springer-Verlag, Berlin, 2003.

[BT87] F. Bruhat & J. Tits – "Schémas en groupes et immeubles des groupes classiques sur un corps local: II. Groupes unitaires.", *Bull. Soc. Math. France* **115** (1987), no. 2, p. 141–195.

[CD05] W. K. Chan & J. Daniels – "Definite regular quadratic forms over $\mathbb{F}_q[T]$", *Proc. Amer. Math. Soc.* **133** (2005), no. 11, p. 3121–3131.

[CEO04] W. K. Chan, A. G. Earnest & B.-K. Oh – "Regularity properties of positive definite integral quadratic forms", in *Algebraic and arithmetic theory of quadratic forms*, Contemp. Math., vol. 344, American Mathematical Society, 2004, p. 59–71.

[Cer] J. M. Cerviño – "Supersingular elliptic curves and maximal quaternionic orders", `http://arxiv.org/pdf/math.NT/0404538`, p. 10.

[Deu41] M. Deuring – "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper", *Abh. Math. Sem. Hansischen Univ.* **14** (1941), p. 197–272.

[EGAI] A. Grothendieck – "Éléments de géométrie algébrique. I. Le langage des schémas", *Inst. Hautes Études Sci. Publ. Math.* (1960), no. 4, p. 228.

[EGAII] ———, "Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes", *Inst. Hautes Études Sci. Publ. Math.* (1961), no. 8, p. 222.

[Eic73] M. Eichler – *Quadratische Formen und orthogonale Gruppen*, Grundlehren der math. Wiss., vol. 63, Springer-Verlag, Berlin, 1973.

[Eis47] G. Eisenstein – "Neue Theoreme der höheren Arithmetik", *J. reine angew. Math.* **35** (1847), p. 117–136.

[Gek83] E.-U. Gekeler – "Zur Arithmetik von Drinfeld-Moduln", *Math. Ann.* **262** (1983), no. 2, p. 167–182.

[Gek92] ———, "On the arithmetic of some division algebras", *Comment. Math. Helv.* **67** (1992), no. 2, p. 316–333.

[Ger79] L. J. Gerstein – "Unimodular quadratic forms over global function fields", *J. Number Theory* **11** (1979), no. 4, p. 529–541.

[Ger03] ———, "Definite quadratic forms over $\mathbb{F}_q[x]$", *J. Algebra* **268** (2003), no. 1, p. 252–263.

[GI63] O. Goldman & N. Iwahori – "The space of $\mathfrak{p}$-adic norms", *Acta Math.* **109** (1963), p. 137–177.

[God64] R. Godement – "Domaines fondamentaux des groupes arithmétiques", *Séminaire Bourbaki 1962/1963* **257** (1964), no. 3, p. 1–25.

[Har69] G. Harder – "Minkowskische Reduktionstheorie über Funktionenkörpern", *Invent. Math.* (1969), no. 7, p. 33–54.

[Har74] S. J. Haris – "A Siegel formula for orthogonal groups over a function field", *Trans. Amer. Math. Soc.* **190** (1974), p. 223–231.

[Har97] R. Hartshorne – *Algebraic geometry*, Graduate Text in Mathematics, vol. 52, Springer-Verlag, Berlin, 1997, corrected eight printing.

[Has02] H. Hasse – *Number theory*, Classics in Mathematics, Springer-Verlag, Berlin, 2002, translated form the third (1969) German edition, reprint of the (1980) English edition.

[KF75] A. N. Kolmogorov & S. V. Fomin – *Reelle Funktionen und Funktionalanalysis*, Hochschulbücher für Mathematik, vol. 78, Deutscher Verlag der Wissenschaften, Berlin, 1975.

[Kne67] M. Kneser – "Semi-simple algebraic groups", in *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Academic Press, 1967, p. 250–265.

[Kne69] M. Knebusch – "Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen", *S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl.* **1969/70** (1969), no. 3, p. 93–157.

[Kne92] M. Kneser – *Quadratische Formen*, Mathematisches Institut der Universität Göttingen, Göttingen, 1992.

[Kno75] J. Knopfmacher – *Abstract analytic number theory*, North-Holland Publishing Co., Amsterdam-Oxford, 1975.

[Knu91] M.-A. Knus – *Quadratic and hermitian forms over rings*, Grundlehren der mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin, 1991.

[O'M00] O. T. O'Meara – *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000.

[Ron89] M. Ronan – *Lectures on buildings*, Perspectives in Mathematics, vol. 7, Academic Press, 1989.

[Ros02] M. Rosen – *Number theory in function fields*, Graduate Text in Mathematics, no. 210, Springer-Verlag, 2002.

[Sch97] A. Schiemann – "Ternary positive definite quadratic forms are determined by their Theta series", *Math. Ann.* **308** (1997), no. 3, p. 507–517.

[Ser68] J.-P. Serre – *Corps locaux*, quatrième édition, corrigée ed., Hermann, Paris, 1968.

[Ser97] ———, *Galois cohomology*, corrected second printing 2002 ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1997, translated from the French by Patrick Ion.

[SGAD] M. Demazure & A. Grothendieck – "Schémas en groupes", Séminaire de Géométrie Algébrique de l'Institut des Hautes Ètudes Scientifiques, 1963/64, dirigé par Michel Demazure et Alexander Grothendieck.

[Sie35] C. L. Siegel – "Über die analytische Theorie der quadratischen Formen I", *Ann. of Math. (2)* **36** (1935), no. 3, p. 527–606.

[Sie37] ———, "Über die analytische Theorie der quadratischen Formen III", *Ann. of Math. (2)* **38** (1937), no. 1, p. 212–291.

[SP79] R. Schulze-Pillot – "Darstellung durch definite ternäre quadratische Formen und das Bruhat-Tits Gebäude der Spingruppe", Ph.D. Thesis, Universität Göttingen, 1979, p. 65.

[Thu96] J. L. Thunder – "An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma", *J. reine angew. Math.* **475** (1996), p. 167–185.

[Tit68] J. Tits – "Formes quadratiques, groupes orthogonaux et algèbres de Clifford", *Invent. Math.* **5** (1968), p. 19–41.

[Wat53] G. L. Watson – "Some problems in the theory of numbers", Ph.D. Thesis, University College, London, 1953.

[Wat76] ———, "Regular positive ternary quadratic forms", *J. London Math. Soc.* **13** (1976), no. 1, p. 97–102.

[Wat04] T. Watanabe – "A survey and a complement of fundamental Hermite constants", in *Algebraic and arithmetic theory of quadratic forms (International Conference held at the Universidad de Talca, Talca and Pucón, December 11–18, 2002)*, Contemporary Mathematics, vol. 344, American Mathematical Society, 2004, p. 339–350.

[Wei65] A. Weil – "Sur la formule de Siegel dans la théorie des groupes classiques", *Acta Math.* **113** (1965), p. 1–87.

[Wei82] ———, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser, Boston, Massachusetts, 1982, with appendices by M. Demazure and Takashi Ono.

[Wei95] ———, *Basic number theory*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, reprint of the second (1973) edition.