Lecture Notes on Quadratic Forms and their Arithmetic

Rainer Schulze-Pillot

Email address: `schulze-pillot@math.uni-sb.de`

2010 *Mathematics Subject Classification.* Primary 11E

Key words and phrases. Quadratic Forms

Contents

Introduction

Although there is no need for yet another book on the arithmetic of quadratic forms, after my retirement I couldn't resist the temptation to make these notes available to people who are interested in the subject. They were compiled over the years from the notes for my courses on this topic and are influenced very much by the lecture notes "Quadratische Formen" from 1974 of my teacher Martin Kneser (revised and edited as the book [**19**] in 2002 by him and Rudolf Scharlau). Other major influences come from the books of Eichler [**11**], O'Meara [**28**], Cassels [**6**] (in chronological order). I thank Gabriele Nebe and Rudolf Scharlau for sharing their respective unpublished lecture notes with me.

Perhaps I will extend these notes by a few additional sections or chapters, e.g. by a section about representations by spinor genera or a chapter about automorphic forms on orthogonal groups and theta liftings. If you would like to see such an addition don't hesitate to tell me, this would increase my motivation to go ahead with it.

Native speakers of English will undoubtedly find many linguistic errors. I will be grateful for any suggestions for corrections of such errors.

I didn't add a glossary or an index. If you would like to find a particular word in the text your pdf-reader will be a more reliable search tool than an index could be.

CHAPTER 1

Basics

1.1. Quadratic Spaces and Modules

Throughout these lecture notes R will denote a commutative ring with $1 \neq 0$ and S an R-module (usually contained in some R-algebra S'). Most often one is interested in the case that $R = S$ is an integral domain or even a field F; these assumptions make some things simpler and we will mention such possibilities for simplifications. The R-torsion elements of S (i.e, the $s \in S$ such that one has $rs = 0$ for some $0 \neq r \in R$) will also be called zero divisors, we say that 2 is not a zero divisor in S if S has no 2-torsion, i.e., if $2s = 0$ implies $s = 0$ for $s \in S$. We will also mention simplifications arising if one excludes the case that $2 = 0$ or more generally requires 2 to be a unit in R or at least not a zero divisor in S.

1.1.1. Quadratic Spaces. For the reader's convenience we treat the case that $R = F$ is a field of characteristic not 2 separately before discussing the general situation. The reader annoyed by this redundancy may safely omit this subsection.

DEFINITION 1.1. Let V be a vector space over the field F. A map $Q : V \to F$ is called an F-valued *quadratic form* on V if one has

a) $Q(ax) = a^2 Q(x)$ for all $a \in F, x \in V$.
b) $b(x, y) := Q(x+y)-Q(x)-Q(y)$ defines a symmetric bilinear form on V.

The symmetric bilinear form in b) is called the *bilinear form associated to* Q. The pair (V, Q) is called a *quadratic space* over F.

REMARK 1.2. We have $b(x, x) = 2Q(x)$ for all $x \in V$. If F is not of characteristic 2 it is more usual to put $B := b/2$ and work with the bilinear form B instead of b. One obtains then $Q(x) = B(x, x)$, which looks more convenient. In particular, one sees that Q and B determine each other uniquely. The notation chosen above is more adequate in the general situation, i.e. for quadratic forms over fields of characteristic 2 or more general over rings in which 2 is not invertible. In particular, this applies when one is dealing with integral quadratic forms and their reductions modulo the prime 2 (or a prime ideal dividing 2 in the number field case).

DEFINITION 1.3. Let V be a finite dimensional vector space over the field F with basis $\mathcal{B} = \{v_1, \dots, v_m\}$ and quadratic form Q on V with associated bilinear forms $b, B = \frac{1}{2}b$.

a) The (homogeneous) *quadratic polynomial* associated to $V, Q, \mathcal{B}$ is the homogeneous polynomial $P_{Q,\mathcal{B}} \in F[X_1, \dots, X_m]$ of degree 2 given by

$$P_{Q,\mathcal{B}}[X_1, \dots, X_m] = Q(\sum_{i=1}^m X_i v_i) = \sum_{i=1}^m Q(v_i)X_1^2 + \sum_{1 \le i < j \le m} b(v_i, v_j)X_iX_j.$$

Such a polynomial is also called a quadratic form in m variables.

b) The *Gram matrix* associated to $M, b, \mathcal{B}$ is the symmetric matrix $M_{\mathcal{B}}(b) = (m_{ij}) \in M_m^{\mathrm{sym}}(F)$ with $m_{ij} = b(v_i, v_j)$ and analogously for B.

REMARK 1.4. a) If $\mathrm{char}(F) \neq 2$, one has

$$Q(\sum_{i=1}^m x_i v_i) = P_{Q,\mathcal{B}}(x_1, \dots, x_m) = {}^t\mathbf{x}M_{\mathcal{B},B}\mathbf{x} = \frac{1}{2}{}^t\mathbf{x}M_{\mathcal{B},b}\mathbf{x}$$

for $\mathbf{x} = (x_1, \dots, x_m) \in F^m$. The theory of finite dimensional quadratic forms and spaces over such a field F (and with careful formulation also over subrings of such a field) is therefore the same as the theory of symmetric matrices over F resp. over such a subring, a point of view which is taken in part of the literature on the subject, in particular in the groundbreaking work of Carl Ludwig Siegel. The language of quadratic spaces has been introduced in 1937 by Ernst Witt and has become the usual description since then.

b) If E is an extension field of F, the quadratic form Q along with its associated bilinear form b extends in a unique way to the E-vector space $V \otimes_F E$ (extension of scalars); with respect to a basis of type $\{v_i \otimes 1\}$ the extended form has the same Gram matrix and the same associated homogeneous polynomial as the original one with respect to the $v_i \in V$ and will also be denoted by Q.

DEFINITION AND LEMMA 1.5. *Let (V, Q) be a quadratic space over the field F with* $\mathrm{char}(F) \neq 2$*, with associated symmetric bilinear forms b and $B = \frac{1}{2}b$, let $\mathcal{B} = \{v_1, \dots, v_m\}, \mathcal{B}' = \{w_1, \dots, w_m\}$ be bases of V with $w_j = \sum_{i=1}^m t_{ij}v_i$, let $T = (t_{ij}) \in GL_m(F)$ be the matrix describing this change of basis. Then*

$$M_{\mathcal{B}'}(b) = {}^tTM_{\mathcal{B}}(b)T, \quad M_{\mathcal{B}'}(B) = {}^tTM_{\mathcal{B}}(B)T.$$

Symmetric matrices A, A' related in this way are called congruent *over F or* F-equivalent. *Similarly, the homogeneous quadratic polynomials $P_{\mathcal{B},Q}, P_{\mathcal{B}',Q}$ are called equivalent over F.*
The square class $\det(M_{\mathcal{B}}(b))(F^\times)^2 \subseteq F$ *in F of the determinant of a Gram matrix of (V, Q) with respect to some basis $\mathcal{B}$ of V is called the* determinant $\det_Q(V) = \det_b(V)$ *of the quadratic space (V, Q) (or the bilinear space (V, b)); one often writes* $\det(V)$ *if Q is understood. It is independent of the choice of basis. We write* $\det_B(V)$ *for the square class of the determinant of a Gram matrix of $B = \frac{1}{2}b$. Sometimes the determinant is also called the (unsigned) discriminant of the space.*

DEFINITION AND LEMMA 1.6. *Let (V, Q) be a quadratic space over the field F with* $\mathrm{char}(F) \neq 2$*, with associated symmetric bilinear forms b and $B = \frac{1}{2}b$. The* radical *of (V, Q) is*

$$\mathrm{rad}(V) = \mathrm{rad}_b(V) = \mathrm{rad}_B(V) = V^{\perp} = \{x \in V \mid b(x, v) = 0 \text{ for all } v \in V\}.$$

$\mathrm{rad}(V)$ *is a subspace of V with $Q(\mathrm{rad}(V)) = \{0\}$, and on the quotient space $V_0 := V/\mathrm{rad}(V)$ one can define a quadratic form Q_0 by $Q_0(x+\mathrm{rad}(V)) := Q(x)$, its associated symmetric bilinear form b_0 is non degenerate and satisfies $b_0(x + \mathrm{rad}(V), y + \mathrm{rad}(V)) = b(x, y)$ for all $x, y \in V$.*
If $U \subseteq V$ is a subspace complementary to $\mathrm{rad}(V)$*, i.e., with $V = U \oplus \mathrm{rad}(V)$, the restriction of b to U is non-degenerate too.*

PROOF. Exercise. □

1.1.2. Quadratic Modules. We return now to the general situation.

DEFINITION 1.7. Let M be an R-module. A map $Q : M \to S$ is called an S-valued *quadratic form* on M if one has

a) $Q(ax) = a^2 Q(x)$ for all $a \in R, x \in M$.
b) $b(x, y) := Q(x + y) - Q(x) - Q(y)$ defines a symmetric bilinear map $b : M \times M \to S$, which we will also call a bilinear form on M with values in S.

If $R = S$ the phrase "R-valued" is omitted.
The symmetric bilinear form in b) is called the *bilinear form associated to Q*. The pair (M, Q) is called a *quadratic module* over R (with values in S), a *quadratic space* in the case that R is a field.

REMARK 1.8.
a) If S has no 2-torsion and $b(M, M) \subseteq 2S$ holds one can write $b(x, y) := 2B(x, y)$ with a unique symmetric bilinear form B; one has then $Q(x) = B(x, x)$ for all $x \in M$. This notation is in particular usual if S is a field of characteristic not 2, it is also often used for $R = \mathbb{Z}$ with $S = \mathbb{Z}$ or $S = \frac{1}{2}\mathbb{Z}$ or similarly for rings of integers in a number field.
b) Conversely, for any symmetric bilinear form B on M (with values in S) we can define a quadratic form on M with associated symmetric bilinear form $2B$ by putting $Q(x) := B(x, x)$ for all $x \in M$, one has then $Q(x + y) = Q(x) + Q(y) + 2B(x, y)$. This convention is used in many books on quadratic forms which focus on situations in which one has $R = S$ and 2 is not a zero divisor, the form b does then usually not appear at all. If 2 is not a unit the quadratic form is then called even or even integral if it takes values in $2R$ and $B(M, M) \subseteq R$ holds. Obviously, this convention is inadequate if 2 is allowed to be a zero divisor, in particular, if one wants to treat fields without excluding the case of characteristic 2.

EXAMPLE 1.9.
a) For $M = R^n$ and $R = S$ we define for $\mathbf{x} = (x_1, \dots, x_n)$ by $Q(\mathbf{x}) = \sum_{i=1}^{n} x_i^2$ a quadratic form with associated bilinear form

$b(\mathbf{x}, \mathbf{y}) = 2\sum_{i=1}^n x_i y_i$ and $B(x, y) = \langle x, y\rangle = \sum_{i=1}^n x_i y_i$ equal to the standard bilinear form on R^n.

b) If 2 is not a zero divisor in R it is invertible in some extension ring of R. We can then set $S = \frac{1}{2}R$ and define $Q : R^n \to S$ by $Q(\mathbf{x}) = \frac{1}{2}\sum_{i=1}^n x_i^2$ to obtain a quadratic form with associated symmetric bilinear form given by $b(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i y_i$.

c) For $R = S = \mathbb{F}_2, M = R^2$ and $Q(\mathbf{x}) = x_1 x_2$ we have $b(\mathbf{x}, \mathbf{y}) = x_1 y_2 + x_2 y_1$. The form B can then not be defined. In fact, there exists no symmetric bilinear form B' on M with $B'(\mathbf{x}, \mathbf{x}) = Q(\mathbf{x})$ for all $\mathbf{x} \in M$: for a symmetric bilinear form B' with $B'((1, 0), (1, 0)) = a, B'((0, 1), (0, 1)) = c$ we obtain $B'(\mathbf{x}, \mathbf{x}) = ax_1^2 + cx_2^2$, so $a = c = 0$ implies that $B'(\mathbf{x}, \mathbf{x})$ is identically zero. More generally, if 2 is a zero divisor we can not write all quadratic forms as $Q(x) = B(x, x)$ with a symmetric bilinear form B, and not all symmetric bilinear forms are attached to some quadratic form.

A generalization of the last example merits a separate definition, as it gives a fundamental building block of the theory:

DEFINITION 1.10. Let M be an R-module with dual module $M^* = \mathrm{Hom}(M, R)$, put $H(M) = M \oplus M^*$ (external direct sum). On $H(M)$ we define a quadratic form Q by $Q(v + v^*) = v^*(v)$ for $v \in M, v^* \in M^*$, with associated symmetric bilinear form $b(v + v^*, w + w^*) = v^*(w) + w^*(v)$.
The quadratic R-module $(H(M), Q)$ is called the hyperbolic module over M.
More generally, for an R-module S we can define an S-valued hyperbolic quadratic module $(H_S(M), Q_S)$ by setting $H(M)_S = M \oplus \mathrm{Hom}(M, S)$ and $Q(v, \varphi) = \varphi(v) \in S$ for all $v \in M, \varphi \in \mathrm{Hom}(M, S)$. This construction is mainly of use if S is a quotient module of R.

EXAMPLE 1.11. If M above is a free module with basis $(v_1, \dots, v_n)$ and $(v_1^*, \dots, v_n^*)$ is the dual basis of M^*, we have $Q(\sum_i x_i v_i + \sum_i y_i v_i^*) = \sum_i x_i y_i$, which in the case $R = \mathbb{R}$ and $n = 1$ explains the use of the word "hyperbolic".

LEMMA 1.12. *Let Q be a quadratic form on the R-module M.*

a) *Q is uniquely determined by its associated symmetric bilinear form b if 2 is not a zero divisor in S.*

b) *Let β be any (not necessarily symmetric) S-valued bilinear form on M and define $Q : M \to S$ by $Q(x) := \beta(x, x)$. Then Q is a quadratic form whose associated symmetric bilinear form is the symmetrization $b(x, y) = \beta(x, y) + \beta(y, x)$ of β.*

c) *If β_1, β_2 are bilinear forms on M inducing the same quadratic form Q on M as above, the form $\beta_1 - \beta_2$ is alternating.*

d) *If M is finitely generated projective, every quadratic form Q on M can be written as $Q(x) = \beta(x, x)$ for some not necessarily symmetric bilinear form β.*

PROOF. Exercise. For d), the case of a finitely generated free module is easy: If $(v_1, \dots, v_n)$ is a basis, one puts $\beta(v_i, v_i) := Q(v_i)$, $\beta(v_i, v_j) = b(v_i, v_j)$ for $i < j$, $\beta(v_i, v_j) = 0$ for $i > j$ and extends bilinearly. For a projective module one supplements it first by a suitable direct summand to obtain a free module, extend Q to that free module and restrict the β obtained there to the original module. □

EXAMPLE 1.13. If we consider the module $H(M) = M \oplus M^*$ as in definition 1.10 and equip it with the not symmetric bilinear form β_1 given by $\beta(v + v^*, w + w^*) = v^*(w)$, we obtain as Q and b the same forms as in that definition. The same result is obtained by using $\beta_2(v+v^*, w+w^*) = w^*(v)$. The difference $A := \beta_1 - \beta_2$ is the standard alternating form on the module $H(M)$.

DEFINITION 1.14. Let (M, Q) be a quadratic module over R with values in the commutative R-algebra S and associated symmetric bilinear form b; assume that M is a finitely generated R-Module with a generating set $\mathcal{G} = \{v_1, \dots, v_m\}$.

a) The (homogeneous) *quadratic polynomial* associated to $M, Q, \mathcal{G}$ is the homogeneous polynomial $P_{Q,\mathcal{G}} \in S[X_1, \dots, X_m]$ of degree 2 given by

$$P_{Q,\mathcal{G}}[X_1, \dots, X_m] = Q(\sum_{i=1}^{m} X_i v_i) = \sum_{i=1}^{m} Q(v_i) X_1^2 + \sum_{1 \le i < j \le m} b(v_i, v_j) X_i X_j.$$

b) The *Gram matrix* associated to $M, b, \mathcal{G}$ is the symmetric matrix $M_{\mathcal{G}}(b) = (m_{ij}) \in M_m^{\mathrm{sym}}(S)$ with $m_{ij} = b(v_i, v_j)$.

REMARK 1.15. a) Whenever $B = \frac{1}{2}b$ is defined, one has $P_{Q,\mathcal{G}}(x_1, \dots, x_m) = {}^t\mathbf{x} M_{\mathcal{G},B} \mathbf{x} = \frac{1}{2} {}^t\mathbf{x} M_{\mathcal{G},b} \mathbf{x}$ for $\mathbf{x} = (x_1, \dots, x_m) \in R^m$. Otherwise, there is no such direct connection between the polynomial $P_{Q,\mathcal{G}}$ and the Gram matrix.

b) Let $P \in S[X_1, \dots, X_m]$ be a homogeneous quadratic polynomial and M a free R-module of rank m with basis $\mathcal{B}$. Then there is a unique quadratic form Q on M such that $P = P_{\mathcal{B},Q}$.

c) If R' is any R-algebra, the quadratic form Q extends in a natural way to the R'-module $M \otimes_R R'$ (extension of scalars) with values in $R' \otimes_R S$; this extension will also be denoted by Q. With respect to a generating set of type $\{v_i \otimes 1\}$ the Gram matrix of the extended form is obtained by tensoring all entries of the original Gram matrix with 1, and the associated homogeneous polynomial is obtained in the same way from the original one with respect to the $v_i \in M$.

LEMMA 1.16. *Let (M, Q) be a quadratic module over the ring R with generating sets $\mathcal{G} = (v_1, \dots, v_m)$ and $\mathcal{G}' = (w_1, \dots w_n)$ satisfying $w_j = \sum_{i=1}^m t_{ij} v_i$ for $1 \le j \le n$, put $T = (t_{ij}) \in M_{m,n}(R)$.*

a) *One has*
$$M_{\mathcal{G}'}(b) = {}^tT M_{\mathcal{G}}(b) T.$$
b) *With* $x_i = \sum_{j=1}^n t_{ij} y_j$ *one has*
$$P_{Q,\mathcal{G}}(x_1, \dots, x_m) = P_{Q,\mathcal{G}'}(y_1, \dots, y_n).$$
c) *If* M *is a free module over* R *with a finite basis* $\mathcal{B} = (v_1, \dots, v_m)$ *and* S *is contained in an* R*-algebra* S'*, the square class* $\det(M_{\mathcal{B}}(b))(R^\times)^2$ *in* S' *is independent of the choice of basis* $\mathcal{B}$ *and is called the determinant (sometimes also the (unsigned) discriminant) of the quadratic module.*

PROOF. For c), since the rank of a finitely generated free module is well defined over any commutative ring, the transformation matrix between any two bases is an invertible square matrix and has invertible determinant. a) and b) are easy exercises: for a) we put $A = (a_{ij}) = M_{\mathcal{G}'}(b)$ and have $b(w_k, w_l) = \sum_{i,j} t_{ik} a_{ij} t_{jl}$, for b) we have $Q(\sum_i x_i v_i) = Q(\sum_{i,j} t_{ij} y_j v_i) = Q(\sum_j y_j w_j)$. □

DEFINITION 1.17. a) Let $(M, Q), (M', Q')$ be quadratic R-modules. An injective R- linear map $\phi : M \to M'$ is called *isometric* or an *isometry* or a *representation of* (M, Q) *by* (M', Q') if $Q'(\phi(x)) = Q(x)$ holds for all $x \in M$. If such an isometric linear map exists one says that (M, Q) is *represented* by (M', Q'). The quadratic modules (M, Q) and (M', Q') are called *isometric* if there exists an isometric linear isomorphism $\phi : M \to M'$.

b) An isometric linear automorphism of (M, Q) is called an *orthogonal map* of the quadratic module. The set of all orthogonal maps of (M, Q) is the *orthogonal group* $O(M, Q) = O_Q(M) = O_{(M,Q)}(R) = O_M(R)$ of the quadratic module. (We will use these variants of notation in the sequel. The last version is the one from algebraic group theory, it will be preferred when we deal with extensions of the ground ring or field.)

c) Let $P_1 \in S[X_1, \dots, X_m], P_2 \in S[X_1, \dots, X_n]$ be homogenous quadratic polynomials. One says that P_2 is represented by P_1 over R, if there exists a matrix $T = (t_{ij}) \in M_{m,n}(R)$ such that one has $P_1(y_1, \dots, y_m) = P_2(x_1, \dots, x_n)$ for all $\mathbf{x} = (x_1, \dots, x_n) \in R^n$, where we put $y_i = \sum_{j=1}^m t_{ij} x_j$ for $1 \leq i \leq n$. If each of P_1, P_2 is represented over R by the other one we say that they are R*-equivalent* or equivalent over R.

d) A symmetric $n \times n$ matrix B over S is said to be *represented over* R by the $m \times m$-matrix A, if one has $B = {}^tTAT$ for some $T \in M_{m,n}(R)$. The matrices A, B above are called R*-congruent* or R*-equivalent* if each of them is represented over R by the other one.

REMARK 1.18. a) The condition of injectivity is sometimes omitted in the definition of isometry or of representation.

b) An isometry is also compatible with the bilinear forms b, b' associated to Q, Q'. If 2 is not a zero divisor in S the reverse direction is also true.
c) It is easily seen that R equivalent matrices must have the same size and that R-equivalent polynomials must have the same number of variables.

PROPOSITION 1.19. a) *Let $(M, Q), (M', Q')$ be quadratic modules with finite generating systems $\mathcal{G}, \mathcal{G}'$ and with associated symmetric bilinear forms b, b' such that (M', Q') is represented by (M, Q).*

Then the polynomial $P_{\mathcal{G}',Q'}$ is represented by $P_{\mathcal{G},Q}$ over R, and the Gram matrix $M_{\mathcal{G}'}(b')$ is represented by $M_{\mathcal{G}}(b)$.

b) *Let $P_1 \in S[X_1, \dots, X_m], P_2 \in S[X_1, \dots, X_n]$ be homogenous quadratic polynomials such that P_2 is represented by P_1 over R.*

Let M, M' be free R-modules M of rank m and M' of rank n with quadratic forms Q, Q' and bases $\mathcal{B}, \mathcal{B}'$ such that $P_1 = P_{\mathcal{B},Q}, P_2 = P_{\mathcal{B}',Q'}$.

Then (M', Q') is represented by (M, Q).

We recall from linear algebra that a bilinear form β (with values in R) on the R-module M induces an R-linear map $\tilde{\beta} : v \mapsto \tilde{\beta}(v) = \tilde{\beta}_v \in M^* = \mathrm{Hom}(M, R)$ from M to M^* by setting $\tilde{\beta}_v(x) := \beta(v, x)$ for all $x \in M$. If the form β is symmetric it is *non degenerate* if and only if this map is injective, it is *regular* if and only if it is an isomorphism of R-modules. These two notions coincide if R is a field and M a finite dimensional vector space over R. For example, for $R = \mathbb{Q}$ in a) of Example 1.9 the bilinear form b is regular, for $R = \mathbb{Z}$ it is non degenerate but not regular, whereas the forms b in b) and in c) of that example are regular. If the module is free of finite rank, the symmetric bilinear form b is regular if and only if the determinant of the Gram matrix with respect to a basis $\mathcal{B}$ is invertible, and the matrix of the linear map $\tilde{\beta} : M \to M^*$ with respect to the basis $\mathcal{B}$ of M and the dual basis $\mathcal{B}^*$ of M^* is the Gram matrix of b with respect to the basis $\mathcal{B}$. The bilinear form is non-degenerate if and only if the determinant of the Gram matrix with respect to a basis is not a zero divisor (to prove this latter fact, use that a linear map $R^n \to R^n$ is injective if and only if its determinant is not a zero divisor; a fact of (multi-)linear algebra not found in many places outside Bourbaki's Algèbre).
Conversely, if $\lambda : M \to M^*$ is an R-linear map it induces a bilinear form β on M by setting $\beta(v, x) = \lambda(v)(x)$; this bilinear form is symmetric if and only if λ is equal to the pullback of its transpose to M under the canonical mapping $\iota : M \to M^{**}$.
In the more general situation that Q and b take values in the R-module S, we obtain similarly a map $\tilde{b} : M \to \mathrm{Hom}(M, S)$ and call b non degenerate if this map is injective. The notion of regularity will only be used if one has $R = S$, it doesn't make much sense otherwise.

If N is a submodule of the quadratic module M we write as usual $N^{\perp} = \{m \in M \mid b(m, N) = 0\}$ (without mentioning b in the notation) for the orthogonal complement of N in M with respect to b.

EXAMPLE 1.20. The hyperbolic module $H(M)$ over some R-module M is non degenerate if and only if for every $\mathbf{0} \neq x \in M$ there exists $f \in M^*$ with $f(x) \neq 0$; such a module is also called a torsionless module (which is not the same as a torsion free module). If M is finitely generated projective, it is also reflexive and one sees that $H(M)$ is regular.
A regular quadratic module which is free is necessarily of finite rank, since otherwise a basis of the dual module has higher cardinality than a basis of the module itself.
If $R = F$ is a field and not of characteristic 2, every one dimensional quadratic space Fx with $Q(x) \neq 0$ is regular.

DEFINITION 1.21. Let M be an R-module with symmetric bilinear form b. The *radical* of (M, b) is

$$\mathrm{rad}(M) = \mathrm{rad}_b(M) = M^{\perp} = \{x \in M \mid b(x, m) = 0 \text{ for all } m \in M\}.$$

If (M, Q) is a quadratic module with associated symmetric bilinear form we call the radical of (M, b) the *bilinear radical* and define the radical of the quadratic module to be

$$\mathrm{rad}_Q(M) := \{x \in \mathrm{rad}_b(M) \mid Q(x) = 0\}.$$

REMARK 1.22. If (M, Q) is a quadratic module and 2 is a not zero divisor one has $\mathrm{rad}_Q(M) = \mathrm{rad}_b(M)$. However, if 2 is a zero divisor, the restriction of the quadratic form Q to $\mathrm{rad}_b(M)$ is not necessarily zero and $\mathrm{rad}_Q(M)$ may become a proper subset of $\mathrm{rad}_b(M)$. For example, for $M = R = S = \mathbb{F}_2$ and $Q(x) = x^2$ we have $\mathrm{rad}_b(M) = M$ and $\mathrm{rad}_Q(M) = \{0\}$. As another example, put $R = M = \mathbb{Z}$ and $S = \mathbb{Z}/6\mathbb{Z}$, with $Q(x) = x^2 + 6\mathbb{Z}$. Then $\mathrm{rad}_b(M) = 3\mathbb{Z}$ and $\mathrm{rad}_Q(M) = 6\mathbb{Z}$.

LEMMA 1.23. *Let (M, Q) be a quadratic module with associated symmetric bilinear form b.*

a) $\mathrm{rad}_b(M)$ *is a submodule of M, and on the quotient module $M_0 := M/\mathrm{rad}_b(M)$ one can define a non degenerate symmetric bilinear form b_0 by $b_0(x + \mathrm{rad}_b(M), y + \mathrm{rad}_b(M)) := b(x, y)$.*
b) *The restriction of Q to $rad_b(M)$ is $\mathbb{Z}$-linear (equivalently: additive) and* $\mathrm{rad}_Q(M)$ *is a submodule of* $\mathrm{rad}_b(M)$ *which equals* $\mathrm{rad}_b(M)$ *if 2 is not a zero divisor in S. On the quotient module $M_1 = M/\mathrm{rad}_Q(M)$ one can define a quadratic form Q_1 by $Q_1(x + \mathrm{rad}_Q(M)) := Q(x)$.*
c) *If $N_0 \subseteq M$ is a submodule with $M = N_0 \oplus \mathrm{rad}_b(M)$, the natural map $n_0 \mapsto n_0 + \mathrm{rad}_b(M)$ from N_0 to $M/\mathrm{rad}_b(M)$ is a linear isomorphism compatible with the bilinear forms $b|_{N_0}$ and b_0. In particular, the restriction of b to N_0 is non-degenerate too.*
d) *If $N_1 \subseteq M$ is a submodule with $M = N_1 \oplus \mathrm{rad}_Q(M)$, the natural map $n_1 \mapsto n_1 + \mathrm{rad}_Q(M)$ from N_1 to $M/\mathrm{rad}_Q(M)$ is an isometry.*

PROOF. Exercise. □

REMARK 1.24. If R is a field, complementary subspaces N_0, N_1 in the above sense to $\mathrm{rad}_b(M), \mathrm{rad}_Q(M)$ always exist, for an arbitrary ring R this is not necessarily the case.

1.2. Orthogonal splittings and orthogonal groups

DEFINITION 1.25. Let M be an R-module with (S-valued) symmetric bilinear form b.

a) If $M = N_1 \oplus N_2$ is a direct sum decomposition with $b(N_1, N_2) = \{0\}$, one writes $M = N_1 \perp_b N_2 = N_1 \perp N_2$and says that M is the *orthogonal sum* (with respect to b) of N_1 and N_2.
b) For a submodule N of M the *orthogonal complement* (with respect to b) is $N^{\perp_b} = N^\perp := \{x \in M \mid b(x, N) = \{0\}\}$.
c) If $N \subseteq M$ is a submodule with $M = N \perp N^\perp$ one says that N *splits off* in M or splits M orthogonally.
d) Analogously one writes
$$M = N_1 \perp \cdots \perp N_r = \perp_{i=1}^r N_i$$
if one has $M = \bigoplus_{i=1}^r N_i$ with $b(N_i, N_j) = \{0\}$for $i \neq j$.
e) A basis $(v_1, \dots, v_m)$ of M with $b(v_i, v_j) = 0$ for $i \neq j$ is called on orthogonal basis of V (with respect to b). Its Gram matrix with respect to this basis is then a diagonal matrix with entries $2Q(v_i)$, and we write $(M, Q) \cong [Q(v_1), \dots, Q(v_m)]$ as a short notation for the isometry class of the quadratic module.

REMARK 1.26. If $(M_1, b_1), (M_2, b_2)$ are modules with (S-valued) symmetric bilinear forms one can in an obvious way form the external orthogonal sum of M_1, M_2. We will usually not distinguish between external and internal orthogonal sums.

LEMMA 1.27. *Let (M, Q) be a quadratic module and assume that $M = N_1 \perp N_2$ for submodules N_1, N_2 of M. Then $O(N_1, Q|_{N_1}) \times O(N_2, Q|_{N_2})$ can be naturally embedded into $O(M, Q)$ by mapping $(\varphi_1, \varphi_2)$to the map $\psi = \varphi_1 \perp \varphi_2$ given by $\psi(v_1 + v_2 = \varphi_1(v_1) + \varphi_2(v_2)$ for all $v - 1 \in N_1, v_2 \in N_2$. In particular, $O(N_1, Q|_{N_1})$ is embedded into $O(M, Q)$ by mapping $\varphi \in O(N_1, Q|_{N_1})$ to $\varphi \perp \mathrm{Id}_{N_2}$. The image of this embedding is contained in $O(M, N_2, Q) := \{\psi \in O(M, Q) \mid \psi|_{N_2} = \mathrm{Id}_{N_2}\}$ and equal to it if $(N_2, Q|_{N_2})$ is non degenerate; one writes just $O(M, N_2)$ if Q is understood.*

PROOF. Only the characterization of the image of the embedding of $O(N_1, Q|_{N_1})$ into $O(M, Q)$ is not obvious. For this assume (N_2, Q) to be non degenerate, let $\psi \in O(M, N_2, Q)$ and write $\psi(v) = w_1 + w_2$ for $v \in N_1$. Then $0 = b(v, w) = b(\psi(v), \psi(w)) = b(w_1 + w_2, w) = b(w_2, w)$ for all $w \in N_2$, hence $w_2 \in N_2^\perp \cap N_2 = \{\mathbf{0}\}$ by assumption, so we have

$\psi(N_1) \subseteq N_1$ and $\psi = \varphi \perp \mathrm{Id}_{N_2}$ with $\varphi = \psi|_{N_1} \in O(N_1, Q)$. The other inclusion is obvious. □

LEMMA 1.28. *Let (M, b) be an R-module with symmetric bilinear form and assume that $M = N_1 \perp N_2$ for submodules N_1, N_2 of M.*
Then (M, b) is non degenerate resp. regular if and only if both $(N_1, b|_{N_1})$, $(N_2, b|_{N_2})$ have the respective property.

PROOF. Exercise. □

THEOREM 1.29. *Let (M, b) be a module with S-valued symmetric bilinear form b, let $N \subseteq M$ be a submodule. For $v \in M$ let $\tilde{b}^{(N)}(v) = \tilde{b}^{(N)}_v \in$ $\mathrm{Hom}(M, S)$ be the linear map given by $\tilde{b}^{(N)}(v)(x) = b(v, x)$ for $x \in N$.*

a) *$M/N^\perp \cong \tilde{b}^{(N)}(M) \subseteq N^*$.*
b) *If (N, b) is non degenerate with $\tilde{b}^{(N)}(M) = \tilde{b}^{(N)}(N)$ one has $M = N \perp N^\perp$.*
c) *If $R = S$ and (N, b) is regular one has $M = N \perp N^\perp$.*
d) *If $R = S = F$ is a field and $(M, b) = (V, b)$ is finite dimensional and non degenerate one has $\dim(N) + \dim(N^\perp) = \dim(M)$ and $(N^\perp)^\perp = N$.*

PROOF.
a) This follows from the homomorphy theorem of linear algebra.
b) By assumption, for all $v \in M$ the the linear functional $\tilde{b}^{(N)}(v)$ on N can also be obtained as $\tilde{b}^{(N)}(w_1)$ for some $w_1 \in N$, i.e., there is $w_1 \in N$ with $b(w_1, x) = b(v, x)$ for all $x \in N$, and one has $w_2 := v - w_1 \in N^\perp$. Since we also have $N \cap N^\perp = \{0\}$ by assumption, $M = N \perp N^\perp$ holds as asserted.
c) This is a special case of b).
d) In this case non degeneracy implies regularity, and the linear map $\tilde{b}^{(N)} : M \to N^*$ surjective with kernel $N^\perp$, which shows the asserted equation for the dimensions. Since $(N^\perp)^\perp \supseteq N$ is obvious, this implies $(N^\perp)^\perp = N$.

□

EXAMPLE 1.30. Let $M = R^2$ with the quadratic form $Q(x_1, x_2) = x_1 x_2$, this quadratic module is called the *hyperbolic plane* (over R), it is obviously regular. If 2 is invertible in R, the submodule $N = R\binom{1}{1}$ is regular and can be split off with orthogonal complement $N^\perp = R\binom{1}{-1}$. The submodule $N' = R\binom{1}{0}$ is not regular, in fact, it is its own orthogonal complement, so one sees that the dimension formula and $((N')^\perp)^\perp = N'$ are indeed satisfied.

DEFINITION AND LEMMA 1.31. *Let (M, Q) be a quadratic module with values in S. Let $z \in M$ with $b(z, M) \subseteq Q(z) \cdot R$ and such that $Q(z)$ is not a zero divisor in S. The* symmetry *or* reflection *with respect to z is the linear map M to$M$ given by*

$$\tau_z(x) = x - \frac{b(x, z)}{Q(z)} z \textit{ for all } x \in M.$$

One has

a) $\tau_z^2 = \mathrm{Id}_M$.
b) $\tau_z \in O(M, Q)$.
c) $\tau_z(z) = -z$ *and* $\tau_z|_{(Rz)^\perp} = \mathrm{Id}_{(Rz)^\perp}$.
d) *If* $x \in M$ *satisfies* $Q(x) = Q(z)$ *and* $Q(x-z) \neq 0$, *one has* $\tau_{x-z}(x) = z, \tau_{x-z}(z) = x$.

PROOF. We have

$$\begin{aligned}\tau_z(\tau_z(x)) &= \tau_z(x) - \frac{b(\tau_z(x), z)}{Q(z)} z \\ &= x - \frac{b(x,z)}{Q(z)} z - \frac{b(x,z) - \frac{b(x,z)b(z,z)}{Q(z)}}{Q(z)} z \\ &= x - \frac{b(x,z)}{Q(z)} z - (-\frac{b(x,z)}{Q(z)} z) \\ &= x.\end{aligned}$$

The rest is similarly shown by direct computation. □

THEOREM 1.32 (Witt's generation Theorem). *Let* $R = S = F$ *be a field,* $\mathrm{char}(F) \neq 2$*, let* (V, Q) *be a non degenerate finite dimensional quadratic space over* F.
Then the orthogonal group $O(V) = O(V, Q)$ *is generated by symmetries.*
More precisely: Each $\sigma \in O(V)$ *can be written as a product of at most* $\dim(V)$ *symmetries.*

PROOF. We prove only the first part, using induction on $n = \dim(V)$, for the assertion about the number of symmetries see e.g. Dieudonne.
The case $n = 1$ is trivial. Let $\dim(V) = n > 1$, assume the assertion to be proven for all non degenerate (W, Q') with $\dim(W) < n$ and let $\sigma \in O(V)$. Since V is non degenerate there exists $x \in V$ with $Q(x) \neq 0$. We have $Q(x - \sigma(x)) = 2Q(x) - b(x, \sigma(x)), Q(x + \sigma(x)) = 2Q(x) + b(x, \sigma(x))$ and hence $Q(x + \sigma(x)) \neq 0$ or $Q(x - \sigma(x)) \neq 0$. In the latter case, we put $y = x - \sigma(x)$ and have $\tau_y(\sigma(x)) = x$ and therefore $\tau_y \circ \sigma((Fx)^\perp) = (Fx)^\perp =: U$ with $\dim(U) = n - 1$. By the inductive assumption we can write $\tau_y \circ \sigma|_U = \tau_{z_1} \circ \ldots \circ \tau_{z_r}$ wit $r \in \mathbb{N}$ and vectors $z_i \in U$ with $Q(z_i) \neq 0$. Since the τ_{z_i} satisfy $\tau_{z_i}(x) = x$, we have $\tau_y \circ \sigma(x) = (\tau_{z_1} \circ \ldots \circ \tau_{z_r})(x)$ as well and hence $\tau_y \circ \sigma = \tau_{z_1} \circ \ldots \circ \tau_{z_r}$, which gives $\sigma = \tau_y \circ \tau_{z_1} \circ \ldots \circ \tau_{z_r}$.
In the other case we put $y = x + \sigma(x)$ and obtain in the same way as above $\tau_y \circ \sigma|_U = (\tau_{z_1} \circ \ldots \circ \tau_{z_r})|_U$ and $\tau_y \circ \sigma(x) = -x$. From this we get $\sigma = \tau_x \circ \tau_y \circ \tau_{z_1} \circ \ldots \circ \tau_{z_r}$. □

1.3. Hyperbolic Modules, Primitivity and Regular Embeddings

DEFINITION 1.33. Let M be an R-module.

a) A submodule $N \subseteq M$ is called a *primitive* submodule if N is a direct summand in M, i.e., $M = N \oplus N'$ for some submodule N' of M.

b) Let b be an R-valued symmetric bilinear form on M. Then a submodule $N \subseteq M$ is called *sharply primitive* or *b-primitive* or *regularly embedded* with respect to b if one has $\tilde{b}^{(N)}(M) = N^*$, i.e., if for every $\varphi \in N^*$ there exists $v \in M$ with $b(v, w) = \varphi(w)$ for all $w \in N$.

REMARK 1.34. Obviously, a monogenic submodule $N = Rw$ is regularly embedded if and only if one has $b(w, M) = R$.
Moreover, any regular submodule N is regularly embedded. If M is regular, every primitive submodule N of M is regularly embedded since any linear form on N can be extended to all of M and is hence in $\tilde{b}^{(N)}(M)$. In particular, if $R = F = S$ is a field and (V, Q) is a regular quadratic space over F, every subspace is regularly embedded. If the space (V, Q) is not regular, a subspace U is regularly embedded if and only if the restriction to U of the projection π to the regular space $\bar{V} = V/\operatorname{rad}_b(V)$ is injective, i.e., $U \cap \operatorname{rad}_b(V) = \{\mathbf{0}\}$. We can then view it as a subspace of "the regular part" of V in the sense that for each subspace W of V which is complementary to $\operatorname{rad}_b(V)$ (and hence regular) we obtain a natural embedding of U into W. This explains the terminology "regularly embedded".
To see this, assume first that there is $\mathbf{0} \neq u \in U \cap \operatorname{rad}(V)$. Then all linear forms in the image of $\tilde{b}^{(U)}$ are zero on u, so $\tilde{b}^{(U)}(V) = U^*$ can not hold. Conversely, assume $\pi|_U$ to be injective. Then its transpose $\bar{V}^* \to U^*$ is surjective, and since $\bar{V}$ is regular we see that for every $f \in U^*$ there exists $y \in V$ with $b(y, x) = g(\pi(x)) = f(x)$ for all $x \in U$, where we denote by g a preimage under the transpose of $\pi|_U$ of f. The subspace U is therefore regularly embedded in V.
Conversely, if $N \subseteq M$ is finitely generated projective and regularly embedded, it is a primitive submodule of M. This is trivial in the case of vector spaces and follows for modules from the fact that $\tilde{b}^{(N)}(M) = N^*$ implies that every linear functional on N can be extended to M, i.e., the map $M^* \to N^*$ given by restriction to N is surjective. For finitely generated projective modules this latter property is well known to be equivalent to N being a direct summand in M. To see this if N is finitely generated free with basis $(v_1, \dots, v_n)$ consider the dual basis $(v_1^*, \dots, v_n^*)$ of N^* and pick $\phi_1, \dots, \phi_n \in M^*$ with $\phi_1|_N = v_i^*$. We can then write $v \in M$ as $(\sum_{i=1}^n \phi_i(v)v_i) + (v - (\sum_{i=1}^n \phi_i(v)v_i)$ and denote by P the set of all the $(v - (\sum_{i=1}^n \phi_i(v)v_i$ for $v \in M$, this give as $M = N \oplus P$. To prove it for general finitely generated projective N, you can e.g. consider the (by projectivity split) exact sequence $0 \to N^{\perp} = (M/N)^* \to M^* \to N^* \to 0$, dualize it and use reflexivity.

LEMMA 1.35. *Let N_1 be a finitely generated projective submodule of the bilinear R-module (M, b) which is regularly embedded.*
Then there exists a finitely generated projective submodule N_2 of M such that $\tilde{b}^{(N_1)}|_{N_2} N_2 \to N_1^*$ is an isomorphism.

Moreover, N_2 is regularly embedded into M and $\tilde{b}^{(N_2)}|_{N_1} : N_1 \to N_2^*$ is an isomorphism.

PROOF. Since N_1 is projective, the exact sequence $0 \to N_1^\perp \to M \to N_1^* \to 0$ splits, i.e., there exists a module homomorphism $h : N_1^* \to M$ with $b^{(N_1)} \circ h = \mathrm{Id}_{N_1^*}$, and we can take N_2 as the image of the splitting homomorphism $N_1^* \to M$. If N_1 is finitely generated free, we can mor directly take N_2 to be the linear span of any set of preimages of a set of basis vectors of N_1^* under the map $b^{(N_1)}$.
N_1, being finitely generated projective, is a reflexive module (i.e., $(N_1^*)^*$ is naturally isomorphic to N_1), and we can view the transpose (or dual map) of $\tilde{b}^{(N_1)}|_{N_2} N_2 \to N_1^*$ as an isomorphism $N_1 \to N_2^*$; it is easily checked that this transpose is nothing but $\tilde{b}^{(N_2)}|_{N_1}$. □

DEFINITION 1.36. Let (M, Q) be a quadratic module.

a) $\mathbf{0} \neq x \in M$ is called *isotropic* if $Q(x) = 0$, *anisotropic* otherwise.
b) (M, Q) is called isotropic if it contains an isotropic vector, anisotropic otherwise.
c) A nonzero submodule $N \subseteq M$ with $Q(N) = \{0\}$ is called *totally isotropic* or *singular*.

EXAMPLE 1.37. In the hyperbolic R-module $H(M) = M \oplus M^*$ over some R-module M both M and M^* are totally isotropic submodules (if nonzero).

THEOREM 1.38. *Let (M, Q) be a quadratic module, $N \subseteq M$ a finitely generated projective submodule which is totally isotropic and regularly embedded. Then there is a submodule N' of M such that $N \oplus N'$ with the restriction of Q as quadratic form is isometric to the hyperbolic module over N.*
In particular, every totally isotropic subspace of a regular quadratic space (V, Q) over a field F can be supplemented to a hyperbolic space in which it is a maximal totally isotropic subspace.

PROOF. We find first a finitely generated projective submodule P of M such that $\tilde{b}^{(N)}|_P : P \to N^*$ and $\tilde{b}^{(P)}|_N : N \to P^*$ are isomorphisms. There is a (not necessarily symmetric) bilinear form β on P satisfying $Q(x) = \beta(x, x)$ for all $x \in P$, and using the isomorphism $\tilde{b}^{(P)}|_N : N \to P^*$ we can define a map $f : P \to N$ by requiring $b(y, f(x)) = \beta(y, x)$ for all $x, y \in P$. Obviously, f is linear and one has $Q(x - f(x)) = 0$ for all $x \in P$. The submodule $N' = \{x - f(x) \mid x \in P\}$ is then as desired. □

REMARK 1.39. If N is free with basis $(v_1, \dots, v_n)$, it is easy to construct N' explicitly: Since N is regularly embedded one finds first $w_1, \dots, w_n \in M$ with $b(v_i, w_j) = \delta_{ij}$ and denotes by P the linear span of the w_j (which are obviously linearly independent). The map f above is then given by linear continuation of $w_j \mapsto Q(w_j)v_j + \sum_{i=1}^{j-1} b(w_i, w_j)v_i \in N$. The linearly independent vectors $v_j' = w_j - f(w_j)$ span then the free and totally isotropic submodule N' and satisfy $b(v_i, v'_j) = \delta_{ij}$ so that $N \oplus N'$ is isometric to the hyperbolic module $H(N)$.

COROLLARY 1.40. *Let $R = F = S$ be a field of characteristic different from 2 and (V, Q) a two dimensional regular quadratic space over F. Then the following are equivalent:*

a) *(V, Q) is a hyperbolic plane.*
b) *(V, Q) is isotropic.*
c) *$\det(V, Q) = -1 \cdot (F^\times)^2$.*

PROOF. The equivalence of a) and b) follows from the previous theorem. For the equivalence of b) and c) let (v, w) be a basis of V. The quadratic equation $0 = Q(x + cy) = Q(x) + cb(c, y) + c^2Q(y)$ is then solvable with $c \in F$ if and only if the discriminant $-4Q(v)Q(w)+b(v, w)^2$ is a square. $\square$

1.4. Witt's Theorems and the Witt Group

The following basic theorems of Witt can be generalized to quadratic (or rather bilinear) modules over an arbitrary local ring, as has been observed by Kneser. For the reader's convenience we give here first the statements for quadratic spaces over a field with proofs that assume the ground field to be of characteristic different from 2. We will return to the general case at the end of this section.

THEOREM 1.41 (Witt's extension theorem over fields). *Let $R = F = S$ be a field and (V, Q) a finite dimensional quadratic space over F.*
Let $U_1, U_2 \subseteq V$ be isometric subspaces with an isometric isomorphism $\rho : U_1 \to U_2$ and assume that V is regular or the subspaces U_1, U_2 are regular. Then ρ can be extended to all of V, i.e., there is $\sigma \in O(V, Q)$ with $\sigma|_{U_1} = \rho$.

PROOF. Let (for now) $\mathrm{char}(F) \neq 2$. We assume first that U_1, U_2 are regular and use induction on $r = \dim(U_1) = \dim(U_2)$.
For $r = 1$ we have $U_i = Fx_i (i = 1, 2)$ with $Q(x_i) \neq 0$ and $\rho(x_1) = x_2$. We can then put $\sigma = \tau_{x_1-x_2}$ or $\sigma = \tau_{x_2} \circ \tau_{x_1+x_2}$ as in the proof of Theorem 1.32..
Let $r > 1$ and assume the theorem to be proven for subspaces of dimension $< r$. There is $x_1 \in U_1$ with $Q(x_1) \neq 0$, we put $x_2 = \rho(x_1) \in U_2$ and set $W_1 := (Fx_1)^\perp \subseteq U_1, W_2 = \rho(W_1) = (Fx_2)^\perp$, so that $U_1 = Fx_1 \perp W_1, U_2 = Fx_2 \perp W_2$ holds.
By the inductive assumption there exists $\sigma_1 \in O(V)$ with $\sigma|_{W_1} = \rho|_{W_1}$, so that we have $\sigma_1^{-1} \circ \rho|_{W_1} = \mathrm{Id}_{W_1}$. The vector $y_1 := (\sigma_1^{-1} \circ \rho)(x_1)$ is in $W_1^\perp$ since it satisfies $b(y_1, w_1) = b(\rho(x_1), \rho(w_1)) = 0$ for all $w_1 \in W_1$, and we can find as in the case of $r = 1$ above a map $\sigma_2 \in O(V)$ with $\sigma_2(x_1) = y_1$, and since σ_2 is a product of symmetries with respect to vectors in $W_1^\perp$ it satisfies $\sigma_2|_{W_1} = \mathrm{Id}_{W_1}$.
Setting $\sigma = \sigma \circ \sigma_2$ we see that we have $\sigma|_{W_1} = \rho|_{W_1}$ as well as $\sigma(x_1) = \rho(x_1)$, so that σ is as desired. This finishes the proof in the case that U_1, U_2 are regular and $\mathrm{char}(F) \neq 2$ holds.

Assume now, still with $\mathrm{char}(F) \neq 2$, that V is regular and U_1, U_2 are arbitrary isometric subspaces. For $i = 1, 2$ we write $U_i = U_i^{(0)} + \mathrm{rad}(U_i)$ with regular subspaces $U_i^{(0)}$.
By applying Theorem 1.38 to the (regular) orthogonal complement $V_1 \subseteq V$ of the $U_1^{(0)}$ in V we obtain a hyperbolic subspace $W_1 \subseteq V$ which is orthogonal to $U_1^{(0)}$ and contains $\mathrm{rad}(U_1)$ as a maximal totally isotropic subspace. In the same way find a hyperbolic space W_2 orthogonal to $U_2^{(0)}$ in which $\mathrm{rad}(U_2)$ is a maximal totally isotropic subspace.
In particular, W_1, W_2 are hyperbolic spaces of the same dimension and hence isometric, with an isometry that sends $\mathrm{rad}(U_1)$ to $\mathrm{rad}(U_2)$, which implies that there is an isometry from the regular quadratic space $\tilde{U}_1 := U_1^{(0)} \perp W_1$ to $U_2^{(0)} \perp W_2$ mapping U_1 onto U_2. By Theorem 1.41 this isometry can be extended to all of V. □

COROLLARY 1.42 (Witt's cancellation theorem). *Let F be a field and (V, Q) a quadratic space over F with orthogonal splittings*

$$V = U_1 \perp W_1 = U_2 \perp W_2,$$

where U_1, U_2 are regular isometric subspaces of V.
Then W_1 is isometric to W_2.

PROOF. By the previous theorem (whose validity in the case $\mathrm{char}(F) = 2$ we will prove below along with Theorem 1.43) there is $\sigma \in O(V)$ with $\sigma(U_1) = U_2$. Since by regularity of U_1, U_2 we have $U_i^{\perp} = W_i$ for $i = 1, 2$, one sees that $\sigma(W_1) = \sigma(U_1^{\perp}) = U_2^{\perp} = W_2$ must hold so that W_1, W_2 are isometric. □

We turn now to the version of Theorem 1.41 for modules over a local ring, also covering the result for fields of characteristic 2.

THEOREM 1.43 (Witt's extension theorem over a local ring). *Let R be a local ring and (M, Q) be a quadratic module over R (with values in R). Let N_1, N_2 be regularly embedded isometric submodules which are free of finite rank with an isometry $\sigma : N_1 \to N_2$.*
Then σ can be extended to an element of the orthogonal group $O(M, Q)$.
Moreover, if X is a submodule of M with $\tilde{b}^{(N_i)}(X) = N_i^*$ for $i = 1, 2$ and such that $\sigma(v) \equiv v \bmod X$ for all $v \in N_1$ holds, the extension $\tilde{\sigma}$ can be chosen such that it is trivial on $X^{\perp}$ and satisfies $\tilde{\sigma}(v) \equiv v \bmod X$ for all $v \in M$.
In particular, Theorem 1.41 is valid over any field.

PROOF. We follow the proof from [**19**].
Let P denote the maximal ideal of R and let $k = R/P$ be the residue field. By $\bar{Y} = Y/PY$ we denote the reduction of a module Y modulo P, by $\bar{Q}, \bar{b}$ the reductions of the quadratic and the bilinear form.
Following [**19**] we adapt the idea of the proof of Theorem 1.41 suitably to the present more general situation. It will turn out that this is easier if we

assume that in the case $k \ncong \mathbb{F}_2$ one has $\bar{Q}(\bar{X}) \neq \{0\}$ whereas for $k \cong \mathbb{F}_2$ one has $\bar{Q}(\bar{X}^\perp) \neq \{0\}$ (with the orthogonal complement taken inside $\bar{X}$); we will dispose of the two exceptional cases in the end.
We proceed by induction, starting with $N_i = Rw_i$ being of rank 1, $\sigma(w_1) = w_2 = w_1 + x$ with $x \in X$.
If $Q(x) \in R^\times$ holds we have $\tau_x(w_1) = w_2$ for the reflection τ_x, and we are done with $\tilde{\sigma} := \tau_x$.
Otherwise we have $Q(x) \in P$ and $\tau_x(w_1) = w_2$ implies

$$Q(x) = -b(w_1, x) = b(w_2, x) \in P,$$

hence

$$\bar{Q}(\bar{x}) = 0 = \bar{b}(\bar{w}_1, \bar{x}) = \bar{b}(\bar{w}_2, \bar{x}) = 0.$$

We write $\bar{X}_i = \{\bar{x} \in \bar{X} \mid \bar{b}(\bar{w}_i, \bar{x}) = 0\}$ and proceed to show that $\bar{Q}(\bar{X} \setminus \bar{X}_1 \cup \bar{X}_2) = \{0\}$ would contradict our assumptions. Indeed, if that was the case we had

$$\bar{t}^2\bar{Q}(\bar{y}) + \bar{t}\bar{b}(\bar{y}, \bar{z}) = \bar{Q}(\bar{t}\bar{y} + \bar{z}) = 0$$

for all $\bar{t} \in k, \bar{y} \in \bar{X}_1 \cap \bar{X}_2, \bar{z} \in \bar{X} \setminus (\bar{X}_1 \cup \bar{X}_2)$. If we have $k \ncong \mathbb{F}_2$ with $\bar{Q}(\bar{X}) \neq \{0$ this implies $\bar{Q}(\bar{y}) = 0 = \bar{b}(\bar{y}, \bar{z})$. Since we have $\bar{x} \in \bar{X}_1 \cap \bar{X}_2$ we see in particular $\bar{b}(\bar{x}, \bar{X} \setminus (\bar{X}_1 \cup \bar{X}_2) = \{0\}$. Moreover, an easy exercise in linear algebra shows that $\bar{X} \setminus \bar{X}_1 \cup \bar{X}_2$ generates $\bar{X}$ in this case, and we see $\bar{b}(\bar{x}, \bar{X}) = \{0\}$, and $\bar{w}_2 = \bar{w}_1 + x$ implies $\bar{X}_1 = \bar{X}_2$. But then $\bar{X}_1 \cap \bar{X}_2 = \bar{X}_1 \cup \bar{X}_2 = \bar{X}_1$ and we obtain $\bar{Q}(\bar{X}) = \{0\}$, which contradicts our assumptions. If, on the other hand, we have $\bar{Q}(\bar{X}^\perp) \neq \{0\}$, we notice first that we have

$$\bar{Q}(\bar{y}) = \bar{Q}(\bar{y} + \bar{z}) = 0$$

for all

$$\bar{y} \in \bar{X}^\perp \cap \bar{X}_1 \cap \bar{X}_2, \bar{z} \in \bar{X}^\perp \cap (\bar{X} \setminus (\bar{X}_1 \cup \bar{X}_2)).$$

Obviously, we have $\bar{X}^\perp \cap \bar{X}_1 = \bar{X}^\perp \cap \bar{X}_2$, which implies that $\bar{X}^\perp$ is the union of $\bar{X}^\perp \cap \bar{X}_1 \cap \bar{X}_2$ and $\bar{X} \setminus (\bar{X}_1 \cup \bar{X}_2)$, and we get $\bar{Q}(\bar{X}^\perp) = \{0\}$ contrary to our assumptions.
Summing up this discussion, we have established that $\bar{Q}(\bar{X} \setminus (\bar{X}_1 \cup \bar{X}_2)) \neq \{0\}$ holds. We may therefore choose $y \in X$ with $Q(y) \in R^\times, b(w_1, y) \in R^\times, b(w_2, y) \in R^\times$. Writing $w_2 = \tau_y(w_1) + z$ we have

$$\begin{aligned} z &= b(w_1, y)Q(y)^{-1}y + x \\ Q(z) &= b(w_1, y)b(w_2, y)Q(y)^{-1} + Q(x), \end{aligned}$$

hence $Q(z) \in R^\times$ and $\tau_z\tau_y(w_1) = w_2$, so that $\tilde{\sigma} := \tau_z\tau_y$ is as desired and the assertion for N_i of rank 1 is proven.
Let now $r > 1$. By the assumptions of the theorem we can choose a basis $(w_1, \dots, w_r)$ of N_1 and vectors $x_1, \dots, x_r \in X$ with $b(w_i, x_j) = \delta_{ij}$ and have $X = \sum_{i=1}^r Rx_i \oplus (X \cap N_1^\perp)$. With the inductive step and our additional assumptions on X in mind we make this choice as follows: We take a vector $x \in X$ with $Q(x) \notin P$ and $\bar{x} \in \bar{X}^\perp$ in the case $k = \mathbb{F}_2$ and choose $x_r \in X \setminus (N_1^\perp \cap X)$ in such a way that one has $\bar{x} \in k\bar{x}_r + \overline{N_1^\perp \cap X}$. The vector

$\bar{x}_r$ can be extended to a basis $\bar{x}_1, \dots, \bar{x}_r$ of $\bar{X}$ modulo $N_1^\perp \cap X$. We choose representatives $x_i \in X$ of the $\bar{x}_r$ and let $(w_1, \dots, w_r)$ be the basis dual to $(x_1, \dots, x_r)$ of N_1.
By the inductive assumption we find a product ρ of reflections in vectors of $x \in X$ with $Q(x) \in R^\times$ that satisfies $\rho| \sum_{i=1}^{r-1} w_i = \sigma| \sum_{i=1}^{r-1} w_i$. Replacing σ by $\rho^{-1} sigma$ we may assume that one has $\sigma(w_i) = w_i$ for $1 \le i \le r-1$, which implies $b(\sigma(x) - x, w_i) = 0$ for $1 \le 1 \le r-1$. and $\sigma(x) - x \in Rx_r \oplus \oplus (X \cap N_1^\perp) =: \tilde{X}$. We consider now $Rf_r := \tilde{F}$ instead of F and and $\tilde{X}$ instead of X. It is clear that the conditions of the theorem are satisfied in this situation, and by our choice of the x_i, w_i the additional conditions $Q(\tilde{X}) \not\subseteq P$ in the case $k \not\cong \mathbb{F}_2$ and $\bar{Q}(\overline{\tilde{X}}) \neq \{0\}$ in the case $k = \mathbb{F}_2$ are satisfied too.
We may therefore apply the case of rank 1 to this situation and obtain a reflection $\tau_y \in O(M, Q)$ satisfying $\tau_y|N_1 = \sigma$ which is congruent to the identity modulo X and is trivial on $X^\perp$ and finish the induction.
To complete our proof we have to consider the situations where our additional assumptions are violated. We take then a hyperbolic plane $H = Re + Rf$ (so $Q(e) = Q(f) = 0, b(e, f) = 1$) and set $M' := M \perp H, N_1' = N_1 \perp Re, N_2' = N_2 + Re, X' = X \perp R(e+f), \sigma' = \sigma \perp \mathrm{Id}_{Re}$. We have $Q(e+f) = 1$ and in addition $e + f \in X'^\perp$ in the case $k = \mathbb{F}_2$, so our additional assumptions are satisfied in this situation and we obtain an extension ρ of σ' which fixes e and the vector $e - f \in X'^\perp$, hence also $e + f$. We can therefor write $\rho = \tilde{\sigma} \perp \mathrm{Id}_{R(e+f)}$ and obtain the desired extension $\tilde{\sigma}$ of σ.
If $R = F$ is a field, recall from Remark 1.34 that the subspaces $U_1 = N_1, U_2 = N_2$ of $M = V$ are regularly embedded if V is regular or U_1, U_2 are regular.

□

REMARK 1.44. If one of the two additional conditions stated in the beginning of the proof is satisfied, the proof above shows that the extension of σ can be chosen to be a product of reflections τ_y in vectors $y \in X$ with $Q(y) \in R^\times$.

COROLLARY 1.45. *Let (V, Q) be a finite dimensional quadratic space over the field F. Then all maximal totally isotropic regularly embedded subspaces of V have the same dimension. This dimension is also equal to the maximal number of hyperbolic planes that can be split off orthogonally in V, and one can write V as $V = \perp_{i=1}^r H \perp \mathrm{rad}_b(V) \perp U$, where r is the Witt index, H denotes a hyperbolic plane, and U is a regular anisotropic quadratic space.*

PROOF. By remark 1.34 we have to treat only the case that (V, Q) is regular. If U_1, U_2 are maximal totally isotropic spaces with $\dim(U_1) \le \dim(U_2)$, we let W_1 be a subspace of U_2 of dimension $\dim(U_1)$. This space is obviously isometric to U_1, one can therefore find $\sigma \in O(V)$ with $\sigma(U_1) = W_1$. But then $\sigma^{-1}(U_2) \supseteq U_1$ is a totally isotropic subspace containing U_1, so by maximality equal to U_1 and we see $\dim(U_1) = \dim(U_2)$. The rest of the assertion follows immediately. $\square$

DEFINITION 1.46 (Witt index). Let (V,Q) be a finite dimensional quadratic space over the field F. Then the dimension of a maximal totally isotropic regularly embedded subspace is called the *Witt index* of (V,Q).

THEOREM 1.47 (Witt decomposition). *Let F be a field and (V,Q) a finite dimensional quadratic space over F of Witt index r.*
Then V has an orthogonal decomposition

$$V = V_{\mathrm{an}} \perp H_r \perp \mathrm{rad}_b(V),$$

where V_{an} is anisotropic regular and H_r is a hyperbolic space of dimension $2r$.
The isometry class of the space V_{an} is uniquely determined.
If $\mathrm{char}(F) \neq 2$, the restriction of Q to $\mathrm{rad}_b(V)$ is identically zero.

PROOF. Replacing V by a (regular) subspace compIementary to $\mathrm{rad}_b(V)$ and using that this space is isometric to the quotient space $V/\mathrm{rad}_b(V)$ we see that it suffices to assume that (V,Q) is regular. In that case we split off orthogonally a maximal $2r$-dimensional hyperbolic subspace whose orthogonal complement V_{an} is necessarily anisotropic. If we have another such splitting $V = V'_{\mathrm{an}} \perp H'_r$, the hyperbolic spaces H_r, H'_r of dimension $2r$ are isometric, and by the Witt cancellation theorem the anisotropic spaces $V_{\mathrm{an}}, V'_{\mathrm{an}}$ are isometric as well. $\square$

DEFINITION 1.48. The up to isometry unique subspace V_{an} with Q restricted to it in the decomposition of the theorem (as well as its isometry class) is called the anisotropic kernel of (V,Q).

LEMMA 1.49. *Let (M,Q) be a finitely generated projective regular quadratic module. Then the (external) orthogonal sum $(M,Q) \perp (M,-Q)$ is isometric to the hyperbolic module $H(M)$ over M.*

PROOF. We denote by β a bilinear form on M with $\beta(x,x) = Q(x)$ for all $x \in M$ and define maps $\phi : (M,Q) \perp (M,-Q) \to H(M), \psi : H(M) \to (M,Q) \perp (M,-Q)$ by

$$\begin{aligned} \phi((x,y)) &= (x+y, \tilde{\beta}(x) + \tilde{\beta}(y) - \tilde{b}(y)) \\ \psi((z,z^*) &= ((x,y)) \text{ where } \tilde{b}(y) = \tilde{\beta}(z) - z^*, \quad x = z - y; \end{aligned}$$

notice that the regularity of (M,Q) implies that the vector y in the definition of ψ exists and is uniquely determined.
A direct calculation shows that ϕ, ψ are mutually inverse isometries. $\square$

DEFINITION AND THEOREM 1.50. *Let R be a ring, denote by $\tilde{W}(R)$ the set of isometry classes of finitely generated projective regular quadratic modules (M,Q) over R.*

Denote by $\sim$ the relation on $\tilde{W}(R)$ given by $(M_1, Q_1) \sim (M_2, Q_2)$ (where we do not distinguish in the notation between the quadratic module and its isometry class) if and only if there exist finitely generated projective hyperbolic modules H_1, H_2 such that $(M_1, Q_1) \perp H_1$ is isometric to $(M_2, Q_2) \perp H_2$. Then the relation $\sim$ is an equivalence relation which is compatible with forming orthogonal sums, and the set $W(R)$ of equivalence classes with addition defined by taking orthogonal sums of representatives is an abelian group, the Witt group *of R. The neutral element of the group is the class of hyperbolic spaces, the inverse to the class of (M, Q) is the class of $(M, -Q)$. If $R = F$ is a field, each class in the Witt group is represented by the isometry class of a uniquely determined regular anisotropic quadratic space.*

PROOF. It is obvious that $\sim$ is an equivalence relation and that it is compatible with forming orthogonal sums, so that one obtains an addition on the set $W(R)$ of equivalence classes induced by taking orthogonal sums of quadratic modules. It is also obvious that this addition is associative and commutative and that the class of hyperbolic modules is a neutral element for this addition. Finally, Lemma 1.49 shows that each class has an additive inverse in $W(R)$.
If $R = F$ is a field, the Witt decomposition theorem shows that each class in $W(R)$ has a representative which is anisotropic, and the Witt cancellation theorem gives the uniqueness of the isometry class of an anisotropic representative. □

1.5. Orthogonal Bases

In this section we let F be a field.

THEOREM 1.51. *Let (V, Q) be a finite dimensional regular quadratic space over F.*

a) *If* $\mathrm{char}(F) \neq 2$*, the space V has an orthogonal basis.*
b) *If* $\mathrm{char}(F) = 2$*, the space F has a decomposition into an orthogonal sum of (regular) 2-dimensional subspaces. In particular,* $\dim(V)$ *is even.*

PROOF. The regular space V contains a vector x with $Q(x) \neq 0$. If $\mathrm{char}(F) \neq 2$, the one dimensional space Fx is regular and can be split off orthogonally, so the assertion follows by induction. If $\mathrm{char}(F) = 2$, by regularity there is a vector $y \in V$ with $b(x, y) = 1$, and $b(x, x) = 2Q(x) = 0$ implies that x, y are linearly independent. The Gram matrix of the two dimensional subspace $W = Fx + Fy \subseteq V$ with respect to the basis (x, y) has then determinant $-(F^\times)^2$, so this space is regular and can be split off orthogonally, and the assertion follows again by induction on the dimension of V. □

REMARK 1.52. a) If $\mathrm{char}(F) \neq 2$, an arbitrary basis of the space V can be transformed into an orthogonal basis by the well known Gram-Schmidt algorithm of linear algebra, with slight modifications to admit isotropic vectors in the original basis.

b) If $\mathrm{char}(F) = 2$, an odd dimensional quadratic space $V = U \perp Fx$ is called *half regular* if U is regular and $Q(x) \neq 0$ holds. Such a space has one dimensional bilinear radical $\mathrm{rad}_b(V)$ and trivial Q-radical $\mathrm{rad}_Q(V)$. It follows that all isotropic vectors are regularly embedded. These spaces can also (see Kneser's book [**19**]) be characterized by the non vanishing of the so called half determinant: Consider for odd n the symmetric matrix $A_X = (a_{ij})$ over the ring $\mathbb{Z}[\{X_{ij} \mid 1 \leq i \leq j \leq n\}]$ with even diagonal elements $a_{ii} = 2X_{ii}$ and $a_{ij} = a_{ji} = X_{ij}$ for $i < j$. Then it is an exercise in linear algebra to prove that $\det(A_X)$ as a polynomial over $\mathbb{Z}$ in the variables X_{ii} for $1 \leq i \leq n$ and X_{ij} for $1 \leq i < j \leq n$ has even coefficients, so that $\frac{1}{2}\det(A_X)$ is still an integral polynomial. The half determinant of a finitely generated free quadratic module of odd dimension over the ring R with basis $(v_1, \dots, v_n)$ is then the square class of the value of the polynomial $\frac{1}{2}\det(A_X)$ upon insertion of the $Q(v_i)$ for X_{ii} and the $b(v_i, v_j)$ for X_{ij} for $i < j$. The half regular spaces over the field F of characteristic 2 are then the spaces whose half determinant (with respect to any basis) does not vanish.

1.6. Lattices and their duals

DEFINITION 1.53. Let R be an integral domain with field of fractions F, let V be a vector space over F of finite dimension n.
An R-submodule Λ of V is called an R-lattice in V if there is a basis $(v_1, \dots, v_n)$ of V with $\Lambda \subseteq \bigoplus_{j=1}^n Rv_j$. It is called a R-lattice on V if the subspace of V generated by Λ over F is equal to V, it is called a lattice of rank $r \leq n$ in V, if that subspace has dimension r over F.

REMARK 1.54. Lattices are usually considered over a ground ring R which is noetherian, which implies that they are finitely generated R-modules. Over a general integral domain this condition is sometimes added to the definition.

LEMMA 1.55. *Let R, F, V be as above, let Λ be an R-lattice on V.*
An R-submodule M of V is an R-lattice in V if and only if there exists $0 \neq a \in R$ with $aM \subseteq \Lambda$.
In particular, for two R-lattices Λ_1, Λ_2 on V there exist nonzero $a, b \in F$ with $a\Lambda_2 \subseteq \Lambda_1 \subseteq b\Lambda_2$.

PROOF. If M is a lattice, let $(v_1, \dots v_n)$ be a basis of V with $M \subseteq \bigoplus_{j=1}^n Rv_j$, let $w_1, \dots, w_n$ be n linearly independent vectors in Λ and write $v_j = \sum_{i=1}^n c_{ij} w_i$ with $c_{ij} \in F$. If we let a be the product of the denominators of the c_{ij} when these are written as fractions of elements in R, we have $av_j \in \Lambda$ for all j and hence $aM \subseteq \Lambda$.

If conversely M is an R-submodule of V and $0 \neq a \in R$ with $aM \subseteq \Lambda$, let $\Lambda \subseteq \bigoplus_{j=1}^n Rv_j$ for a suitable basis $(v_1, \dots, v_n)$ of V. Then the $w_j = a^{-1}v_j$ form a basis of V with $M \subseteq \bigoplus_{j=1}^n Rw_j$. □

LEMMA 1.56. a) *R-submodules of R-lattices in V are R-lattices in V.*
b) *If U is a subspace of V, an R-submodule of U is a lattice in U if and only if it is a lattice in V.*

PROOF. Obvious. □

DEFINITION 1.57. Let R, F be as above and let (V, Q) be a finite dimensional non degenerate quadratic space over F with associated symmetric bilinear form b, let Λ be an R-lattice on V.
The dual of Λ is

$$\Lambda^\# := \{v \in V \mid b(v, \Lambda) \subseteq R\}.$$

REMARK 1.58. The dual $\Lambda^\#$ of Λ is the image of $\Lambda^* = \mathrm{Hom}_R(\Lambda, R) \subseteq V^*$ under the isomorphism $\tilde{b}^{-1} : V^* \to V$.

LEMMA 1.59. *Let the notations be as above.*
a) *$\Lambda^\#$ is a lattice on V.*
b) *$\Lambda \subseteq \Lambda^\#$ if and only if $b(\Lambda, \Lambda) \subseteq R$.*
c) *If $b(\Lambda, \Lambda) \subseteq R$ holds, the factor module $\Lambda^\#/\Lambda$ is a torsion module.*
d) *If M is another R-lattice on V, one has $(M \cap \Lambda)^\# = M^\# + \Lambda^\#$ and $(M + \Lambda)^\# = M^\# \cap \Lambda^\#$.*

PROOF. For a), let $(w_1, \dots, w_n)$ be a basis of V contained in Λ, let $(w_1^\#, \dots, w_n^\#)$ be the dual basis of V with respect to b, i.e, $b(w_i, w_j^\#) = \delta_{ij}$. Then one has $\Lambda^\# \subseteq \bigoplus_{j=1}^n Rw_j^\#$, so $\Lambda^\#$ is a lattice in V. If $(v_1, \dots, v_n)$ is a basis of V with $\Lambda \subseteq \bigoplus_{j=1}^n Rv_j$ and dual basis $(v_1^\#, \dots, v_n^\#)$ of V with respect to b, the $v_j^\#$ are in $\Lambda^\#$ and generate V over F, so Λ is a lattice on V.
Assertions b) and d) are obvious. If we have $\Lambda \subseteq \Lambda^\#$, we let $(w_1, \dots, w_n)$ and $(w_1^\#, \dots, w_n^\#)$ be as in the proof of a). Let c be such that $cA \in M_n(R)$, where A is the matrix obtained by expressing the $w_j^\#$ as linear combinations of the basis vectors w_i. Then we have $c\Lambda^\# \subseteq \Lambda$ and obtain c).
For e), we have $\Lambda = \bigoplus_{j=1}^n Rv_j$ for a basis of V and hence $\Lambda^\# = \bigoplus_{j=1}^n Rv_j^\#$, where again the $v_j^\#$ form the dual basis of V with respect to b. From this we see that $(\Lambda^\#)^\# = \Lambda$ holds. □

DEFINITION 1.60. Let Λ_1, Λ_2 be two free R-lattices on the finite dimensional vector space V of dimension n over F.
The *R-index* $\mathrm{ind}_R(\Lambda_1/\Lambda_2) = (\Lambda_1 : \Lambda_2)_R$ is the class $\det(T)R^\times$, where $T = (t_{ij}) \in M_n(F)$ is any matrix expressing an R- basis $(w_1, \dots, w_n)$ of Λ_2 by the vectors $(v_1, \dots, v_n)$ of a basis of Λ_1, i.e, with $w_j = \sum_{i=1}^n t_{ij}v_i$ for $1 \le j \le n$.
We will also denote any such $\det(T)$ by $\mathrm{ind}_R(\Lambda_1/\Lambda_2)$ or $(\Lambda_1 : \Lambda_2)_R$.

REMARK 1.61. If $\Lambda_2 \subseteq \Lambda_1$ is a sublattice of Λ_1, the group index $(\Lambda_1 : \Lambda_2)$ is equal to the order of the factor ring $R/\mathrm{ind}_R(\Lambda_1/\Lambda_2)R$. In particular for $R = \mathbb{Z}$ it is equal to the absolute value of $\mathrm{ind}_R(\Lambda_1/\Lambda_2)$.

LEMMA 1.62. *Let Λ_1, Λ_2, V be as in the definition above and let b be a non degenerate symmetric bilinear form on V.*
Then

$$\det_b(\Lambda_2) = ((\Lambda_1 : \Lambda_2)_R)^2 \det_b(\Lambda_2).$$

In particular, if one has $\Lambda_1 \subseteq \Lambda_2$, the lattices have equal determinant if and only if they are equal.

PROOF. Obvious. □

LEMMA 1.63. *Let $\Lambda, \Lambda_1, \Lambda_2$ be reflective R- lattices on the regular finite dimensional quadratic space (V, Q) over F with associated symmetric bilinear form b.*

a) $(\Lambda^\#)^\# = \Lambda$.
b) *One has $\Lambda_1 \subseteq \Lambda_2$ if and only if one has $\Lambda_2^\# \subseteq \Lambda_1^\#$.*
c) *If Λ is free of finite rank, one has*

$$\det(\Lambda)R^\times = (\Lambda^\# : \Lambda)_R, \quad \det(\Lambda^\#) = (\det(\Lambda))^{-1}$$

PROOF. a) is easily seen to follow from the reflectivity of Λ and the fact that $\tilde{b} : \Lambda \to \Lambda^*$ is an isomorphism of modules.
In b) the direction from left to right is obvious, the reverse direction then follows from a).
For the computation of the determinants in c) we may assume, multiplying Λ by a suitable $a \in R$, that $\Lambda \subseteq \Lambda^\#$ holds. Furthermore, we see that $b(v_i, v_k) = b(\sum_{j=1}^m b(v_i, v_j)v_j^\#, v_k)$ holds for all i, j, k, which implies $v_i = \sum_{j=1}^m b(v_i, v_j)v_j^\#$ for all i. In other words, the Gram matrix of b with respect to the basis of Λ consisting of the v_i is the matrix obtained upon expressing the v_i as linear combinations of the $v_j^\#$. By the definition of $(\Lambda^\# : \Lambda)_R$ we see that $\det(\Lambda) = (\Lambda^\# : \Lambda)_R(R^\times)^2$ is true. For the determinant of $\Lambda^\#$ exchange the roles of $\Lambda, \Lambda^\#$ in the above argument.
□

1.7. Lattices and orthogonal decompositions

LEMMA 1.64. *Let (V, Q) be a finite dimensional regular quadratic space over F with an orthogonal decomposition $V = U_1 \perp U_2$, let Λ be a lattice of full rank on V with $b(\Lambda, \Lambda) \subseteq R$ (equivalently, $\Lambda \subseteq \Lambda^\#$). Let $L_i = \Lambda \cap U_i (i = 1, 2)$ and denote by π_i the orthogonal projection $\pi_i : V \to U_i$. Then one has*

a) $U_i \cap \Lambda^\# = (\pi_i(\Lambda))^\#$ *for $i = 1, 2$ (where the dual on the right hand side is taken inside U_i).*
b) $\pi_1(\Lambda)/L_1 \cong \pi_2(\Lambda)/L_2$ *as R-modules.*

PROOF. a) Let $u \in U_1$ be given, write $x \in \Lambda$ as $x = \pi_1(x) + \pi_2(x)$. Then $u \in \Lambda^\#$ is equivalent to $b(u, \pi_1(x)) = b(u, x) \in R$ for all $x \in \Lambda$, hence to $b(u, \pi_1(\Lambda)) \subseteq R$, hence to $u \in (\pi_1(\Lambda))^\#$.

b) For $u_1 = \pi_1(x) \in \pi_1(\Lambda)$ there exists $u_2 \in \pi_2(\Lambda) \subseteq U_2$ with $u_1 + u_2 \in \Lambda$ (e.g. $\pi_2(x)$), and the coset $u_2 + L_2$ is independent of the choice of u_2 since $u_1 + u_2' \in \Lambda$ implies $u_2 - u_2' \in U_2 \cap \Lambda = L_2$. The R-linear map from $\pi_1(\Lambda)$ to $\pi_2(\Lambda)/L_2$ given by $u_1 \to u_2$ as above has kernel $\{\pi_1(x) \mid x \in \Lambda, \pi_2(x) \in \Lambda\} = L_1$ and is obviously surjective.

□

DEFINITION 1.65. a) Let the notations be as above. The lattice Λ is called unimodular if $\Lambda = \Lambda^\#$, it is called even unimodular if in addition $Q(\Lambda) \subseteq R$ (equivalently, $b(x,x) \in 2R$ for all $x \in \Lambda$) holds.

b) The lattice R is called I-modular for an ideal $I \subseteq R$ if one has $\Lambda = I\Lambda^\#$, it is called even I-modular if in addition $Q(\Lambda) \subseteq I$ holds. It is called (even) modular if it is (even) I-modular for some ideal $I \subseteq R$.

REMARK 1.66. The lattice Λ is even unimodular if and only if (Λ, Q) is a regular quadratic R-module

LEMMA 1.67. *Let Λ be an I-modular R-lattice on V which is a free R-module.*

a) $\tilde{b}^{(\Lambda)}(\Lambda) = \mathrm{Hom}_R(\Lambda, I)$.

b) $\Lambda = \{v \in V \mid b(v, \Lambda) \subseteq I\}$.

PROOF. a) is obvious. For b) let v be in the set on the right hand side. Then $\tilde{b}^{(\Lambda)}(v) \in \mathrm{Hom}_R(\Lambda, I)$, so by a) and since $\tilde{b}$ is injective we have $v \in \Lambda$. The other inclusion is trivial. □

LEMMA 1.68. *Let R be an integral domain with field of fractions F, let (V, Q) be a regular quadratic space over F, let Λ be an R-lattice on V and let $K \subseteq \Lambda$ be an I-modular sublattice of Λ for some ideal $I \subseteq R$, i.e., K generates over F a regular subspace U of V and is an I-modular lattice on U.*
Then K splits off orthogonally in Λ if and only if one has $b(K, \Lambda) \subseteq I$.

PROOF. Since K is I-modular, we have $\tilde{b}^{(K)}(K) = \mathrm{Hom}_R(K, I)$, the assumption $b(K, \Lambda) \subseteq I$ gives $\tilde{b}^{(K)}(\Lambda) \subseteq \mathrm{Hom}_R(K, I)$, hence $\tilde{b}^{(K)}(\Lambda) = \tilde{b}^{(K)}(K)$, and Theorem 1.29 implies that K splits off orthogonally.
The other direction is trivial. □

REMARK 1.69. The results of this section remain valid if we omit the condition that R is an integral domain and replace F with the total ring of fractions of R and the vector space V by a free module over F. The quadratic module (V, Q) is then required to be regular.

CHAPTER 2

Special Ground Rings

Obviously the theory of quadratic modules over a fixed ground ring depends very much on the ring. Our main concern being the arithmetic of quadratic forms we are particularly interested in the case where the ground ring is a number field or a number ring, i.e., the ring of integers in such a field. For these, important information is contained in the study of the real and complex embeddings of the field and of the reduction modulo prime ideals of the ring of integers, hence in the study of finite fields. Since many interesting properties of forms over the rational integers or over number rings can be studied in the more general context of principal ideal domains respectively of Dedekind domains, we will also study the basic properties of forms over these in this chapter.

2.1. Real and Complex Numbers

THEOREM 2.1.

$$W(\mathbb{C}) \cong \mathbb{Z}/2\mathbb{Z}.$$

PROOF. Since all elements of $\mathbb{C}$ are squares, every 2-dimensional regular quadratic space is hyperbolic. $\square$

REMARK 2.2. Obviously, the same results holds for all *quadratically closed* fields F, i.e., fields admitting no quadratic extension.

THEOREM 2.3 (Sylvester).

$$W(\mathbb{R}) \cong \mathbb{Z}.$$

PROOF. A regular quadratic space (V, Q) has an orthogonal basis consisting of r_+ vectors x_j with $Q(x_j) = 1$ and r_- vectors y_j with $Q(y_j) = -1$; it is hyperbolic if and only if $s = r_+ - r_-$ is zero. $\square$

2.2. Finite Fields

Let $F = \mathbb{F}_q$ be the finite field of characteristic p with $q = p^s$ elements.

THEOREM 2.4 (Chevalley-Warning). *Let $f \in F[X_1, \dots, X_n]$ be a homogeneous polynomial of degree $d > n$.*
Then f has a nontrivial zero in F.

PROOF. With $g := 1 - f^{q-1}$ one has (since $a^{q-1} = 1$ for all $a \neq 0$ in F)

$$\sum_{\mathbf{x} \in F^n} g(\mathbf{x}) = \sum_{\{\mathbf{x} \in F^n \mid f(\mathbf{x})=0\}} 1_F = N_f \cdot 1_F,$$

where N_f is the number of zeroes of f in F^n.
On the other hand, let $m = X_1^{e_1} \dots X_n^{e_n}$ be a monomial occurring in g. Since the degree of f is less than n, all monomials occurring in g have degree less than $n(q-1)$, so at least one of the e_i satisfies $e_i < q-1$, w.l.o.g we assume $e_1 < q-1$. The contribution of m to $\sum_{\mathbf{x}\in F^n} g(\mathbf{x})$ is then

$$\sum_{\mathbf{x}\in F^n} m(\mathbf{x}) = \sum_{x_1\in F} x_1^{e_1} \sum_{(x_2,\dots,x_n)} x_2^{e_2} \dots x_n^{e_n}$$

with $\sum_{x_1\in F} x_1^{e_1} = q \cdot 1_F = 0$ if $e_1 = 0$ and

$$\sum_{x_1\in F} x_1^{e_1} = \sum_{j=0}^{q-2} (\alpha^j)^{e_1} = \frac{(\alpha^{e_1})^{q-1} - 1}{\alpha^{e_1} - 1} = 0$$

for $0 < e_1 < q-1$, where α is a generator of the (cyclic) multiplicative group $F^\times$ of F and where $\alpha^{e_1} \neq 1$ because of $0 < e_1 < q-1$.
So all monomials contribute 0 to $\sum_{\mathbf{x}\in F^n} g(\mathbf{x})$, and we must have $p \mid N_f$. Since f, being homogeneous, has at least the trivial zero $\mathbf{0}$, there must be at least $p-1$ nontrivial zeroes. $\square$

COROLLARY 2.5. *Every quadratic space (V, Q) of dimension $m \geq 3$ over the finite field F is isotropic.*

PROOF. This is an obvious consequence of the Chevalley-Warning theorem since the number of variables in the associated homogeneous quadratic polynomial (with respect to any basis) over F is at least 3. $\square$

DEFINITION 2.6. A quadratic module (M, Q) over R with values in R is called universal if $Q(M) = R$ is true.

EXAMPLE 2.7. The hyperbolic module $H(M)$ over a non zero finitely generated free module M is universal since for any $z^* \in M^*$ with $1 \in z^*(M)$ the values $z^*(z)$ for the $z \in M$ run through all of R.

COROLLARY 2.8. *Every 2-dimensional regular quadratic space over a finite field F is universal.*

PROOF. If (V, Q) is isotropic, it is hyperbolic and hence universal. Otherwise let $0 \neq a \in F$ and consider the space $W := V \perp Fy$ (external orthogonal sum), where Fy is a 1-dimensional quadratic space with $Q(y) = -a$. Then W is isotropic, since it has dimension 3, and an isotropic vector $z \in W$ must be of the form $z = x + cy$ with $c \neq 0$ since we assumed (V, Q) to be anisotropic. We have therefore $Q(x) = c^2 a$, hence $Q(\frac{x}{c}) = a$ as desired. $\square$

LEMMA 2.9. *Let q be odd.*
Then two regular quadratic spaces over F are isometric if and only if they have the same dimension and the same determinant.
In particular, in each dimension there are precisely two isometry classes of regular quadratic spaces over $F = \mathbb{F}_q$.

PROOF. The assertion is trivial in dimension 1. In dimension 2 let a regular space (V, Q) be given and put $W := V \perp Fy$ with a 1-dimensional space Fy with $Q(y) = -1$. Then W is isotropic and splits as $W = H \perp Fz$ with a hyperbolic plane H, and we have $-2\det(V) = \det(W) = -2Q(z)(F^\times)^2$. Moreover, since $\mathrm{char}(F) \neq 2$ we can split H as $H = Fx_1 \perp Fx_2$ with $Q(x_1) = -1, Q(x_2) = 1$. By the Witt cancellation theorem we obtain $V \cong Fx_2 \perp Fz$ with $Q(x_2) = 1, Q(z) \in \det(V)$, the isometry class of which depends only on $\det(V)$. The assertion for arbitrary dimension follows by induction since all regular spaces of dimension ≥ 3 are isotropic and split off a hyperbolic plane. □

THEOREM 2.10. *The Witt group of F for* $\mathrm{char}(F) = 2$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$.
For $\mathrm{char}(F) \neq 2$ *we have*

$$W(F) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & q \equiv -1 \bmod 4 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & q \equiv 1 \bmod 4. \end{cases}$$

PROOF. Let q be odd. Since all anisotropic spaces are of dimension 1 or 2 we see that $W(F)$ has order 4. If $q \equiv -1 \bmod 4$, the Witt classes of the 1-dimensional regular spaces have order 4 since $-a^2$ is not a square for $a \neq 0$, otherwise they have order 2, and they generate the group.
Assume now $\mathrm{char}(F) = 2$, let (V, Q) be an anisotropic regular quadratic space of dimension 2. Since (V, Q) is universal and regular we have a basis (v, w) of V with $Q(v) = 1 = b(v, w), Q(w) = a \neq 0$. Moreover, since (V, Q) is anisotropic we have $0 \neq Q(xv + w) = x^2 + x + a$ for all $x \in F$, hence a is not in the additive subgroup $S := \{x^2 + x \mid x \in F\}$ of F of index 2. Another binary anisotropic space (V', Q') is then of the same type with basis (v', w') and an $a' \notin S$. But then there exists $x \in F$ with $a = x^2 + x + a'$, and the linear map sending v to v' and w to $xv' + w'$ is an isometry from (V, Q) onto (V', Q'). Since every class in the Witt group of F is represented by some 2-dimensional space, the assertion is proven in this case too. □

2.3. Dedekind domains

A Dedekind domain R is a noetherian integrally closed integral domain in which every non zero prime ideal is maximal. In particular, all principal ideal domains are Dedekind domains, and the ring $\mathfrak{o}_F$ of all over $\mathbb{Z}$ integral elements of an algebraic number field F is a Dedekind domain. In this section R is a Dedekind domain with field of quotients F.
The theory of lattices over Dedekind domains is very similar to the theory over a principal ideal domain since all localizations are principal ideal domains. We therefore treat both cases together in this section.
We summarize first some basic facts from [**7, 8, 4**].

A finitely generated module M over the Dedekind domain R is projective if and only if it is torsion free, if R is a principal ideal domain, it is free. In particular, all R - submodules of a finite dimensional vector space V

over F are projective, free in the PID-case. A submodule N of the finitely generated projective module M is a direct summand if and only if M/N is torsion free. The localizations M_P of the finitely generated projective module M with respect to the maximal ideals P of R are free R_P-modules of rank r independent of P, the number r (possibly ∞) is called the rank of M. If M is a finitely generated projective module over R there are linearly independent vectors $x_1, \dots, x_r \in M$ and a fractional ideal $\mathfrak{a}$ of R such that $M = Rx_1 \oplus \dots Rx_{r-1} \oplus \mathfrak{a}x_r$, where r is the rank of M. The class of $\mathfrak{a}$ modulo principal fractional ideals is uniquely determined and is called the Steinitz class of M. If one has $M = \mathfrak{a}_1 y_1 \oplus \cdots \oplus \mathfrak{a}_r y_r$ with linearly independent vectors $y_i \in M$ and fractional ideals $\mathfrak{a}_i$ of R the Steinitz class of M is equal to the class modulo principal fractional ideals of $\prod_{i=1}^r \mathfrak{a}_i$. Two finitely generated projective modules over R are isomorphic as R-modules if and only if they have the same rank and the same Steinitz class. If V is a finite dimensional vector space over F the R-lattices in V are precisely the finitely generated projective R-modules contained in V, such a module is a lattice on V if and only if its rank equals the dimension of V.
Let Λ_1, Λ_2 be lattices on the finite dimensional vector space V over F. Then there exist a basis $(v_1, \dots, v_n)$ of V and fractional ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n, \mathfrak{b}_1, \dots, \mathfrak{b}_n$ with $\mathfrak{b}_1 \supseteq \mathfrak{b}_2 \supseteq \cdots \supseteq \mathfrak{b}_n$ and

$$\Lambda_1 = \bigoplus_{i=1}^n \mathfrak{a}_i v_i, \quad \Lambda_2 = \bigoplus_{i=1}^n \mathfrak{b}_i \mathfrak{a}_i v_i.$$

The $\mathfrak{b}_i$ are unique, they are called the invariant factors of Λ_2 in Λ_1. We will denote by $\mathfrak{ind}_R(\Lambda_1/\Lambda_2)$ the product of these invariant factors and call it the *R-index ideal* in analogy to the case of free modules; if both lattices are free it is the ideal generated by $\mathrm{ind}_R(\Lambda_1/\Lambda_2) = (\Lambda_1 : \Lambda_2)_R$.

LEMMA 2.11. *Let Λ_1, Λ_2 be lattices on the finite dimensional vector space V over F.*
For a prime ideal $\mathfrak{p}$ of R let $R_\mathfrak{p} := \{\frac{a}{b} \in F \mid a, b \in R, b \notin \mathfrak{p}\} \subseteq F$ denote the localization of R at the prime ideal $\mathfrak{p} \subseteq R$ and denote by $(\Lambda_i)_\mathfrak{p}$ the $R_\mathfrak{p}$ module generated by Λ_i in V (called the localization of Λ_i at $\mathfrak{p}$).

a) *One has $(\Lambda_1)_\mathfrak{p} = (\Lambda_2)_\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ of R and $\Lambda_1 = \Lambda_2$ if and only if $(\Lambda_1)_\mathfrak{p} = (\Lambda_2)_\mathfrak{p}$ holds for all prime ideals $\mathfrak{p}$ of R.*
b) *If conversely Λ is an R-lattice on V and one is given finitely many prime ideals $\mathfrak{p}_i \subseteq R$ $(1 \le i \le n)$ and $R_{\mathfrak{p}_i}$-lattices L_i on V for these $\mathfrak{p}_i$, there is a unique R-lattice Λ' on V such that $\Lambda'_{\mathfrak{p}_i} = L_i$ for $1 \le i \le n$ and $\Lambda'_\mathfrak{p} = \Lambda_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ different from the $(\mathfrak{p}_i)$.*

PROOF. a) By the general theory of lattices there are $a, b \in R \setminus \{0\}$ such that one has $a\Lambda_2 \subseteq \Lambda_1 \subseteq b\Lambda_2$. For all maximal ideals $\mathfrak{p}$ of R with $ab \notin \mathfrak{p}$ (and hence for almost all $\mathfrak{p}$) one has then $(\Lambda_1)_\mathfrak{p} = (\Lambda_2)_\mathfrak{p}$. The second part of the assertion is clear.
b) Let the $\mathfrak{p}_i, L_i$ be given, let $(v_1, \dots, v_m)$ be a basis of Λ. Dividing Λ by a suitable element of R (divisible by high enough powers of the

$\mathfrak{p}_i$) if necessary we can assume without loss of generality $L_i \subseteq \Lambda_{\mathfrak{p}_i}$ for $1 \leq i \leq n$. For $1 \leq i \leq n$ one has $c_{jk}^{(i)} \in R_{\mathfrak{p}_i}$ such that the $w_k^{(i)} := \sum_{j=1}^m c_{jk}^{(i)} v_j$ for $1 \leq k \leq m$ form a basis of the $R_{\mathfrak{p}_i}$-module L_i, and the $c_{jk}^{(i)}$ can even be chosen to be in R since their denominators are units in $R_{\mathfrak{p}_i}$.

By the chinese remainder theorem we can then find $c_{jk} \in R$ which are congruent to the $c_{jk}^{(i)}$ modulo $\mathfrak{p}_i^r$ for all i and for an integer r which is large enough to imply $w_k^{(i)} - w_k \in \mathfrak{p}_i L_i$ for $1 \leq i \leq n$, where we set $w_k := \sum_{j=1}^m c_{jk} v_j$ for $1 \leq k \leq m$. The matrix over $R_{\mathfrak{p}_i}$ expressing the w_k as linear combinations of the $w_l^{(i)}$ has therefore determinant in $R_{\mathfrak{p}_i}^\times$, i.e., the w_k form a basis of the $R_{\mathfrak{p}_i}$-module L_i for $1 \leq i \leq r$. Let $M \subseteq \Lambda$ be the R-lattice generated by the w_k. We can find an ideal $\mathfrak{c} \subseteq R$ which is a product of powers of the $\mathfrak{p}_i$ such that $\mathfrak{c}\Lambda_{\mathfrak{p}_i} \subseteq L_i = M_{\mathfrak{p}_i}$ for $1 \leq i \leq n$ and have $\Lambda_{\mathfrak{p}} = \mathfrak{c}\Lambda_{\mathfrak{p}}$ for all $\mathfrak{p}$ different from all the $\mathfrak{p}_i$. The Lattice $\Lambda' := \mathfrak{c}\Lambda + M$ is then as desired.

□

REMARK 2.12. Instead of the localizations $R_{\mathfrak{p}}, \Lambda_{\mathfrak{p}}$ we could also use the v-adic completions R_v, Λ_v for the non archimedean valuations $v = v_{\mathfrak{p}}$ associated to the maximal ideals $\mathfrak{p}$ of R, the chinese remainder theorem is then replaced by the strong approximation theorem in the proof.

DEFINITION 2.13. Let V be a finite dimensional vector space over F with non degenerate symmetric bilinear form b, let Λ be an R-lattice on V. The fractional R-ideal generated by the determinants of Gram matrices with respect to b of free sublattices of Λ of full rank is called the volume ideal $\mathfrak{v}_b\Lambda = \mathfrak{v}\Lambda$ of Λ.

REMARK 2.14. For any maximal ideal $\mathfrak{p}$ of R the $\mathfrak{p}$-part of the volume ideal $\mathfrak{v}\Lambda$ is given as the power of $\mathfrak{p}$ in the determinant of the free local lattice $\Lambda_{\mathfrak{p}}$.

LEMMA 2.15. *Let Λ be an R- lattice on the finite dimensional vector space V over F. A submodule M of Λ which generates over F the subspace $W = FM$ of V is a primitive submodule of Λ if and only if one has $M = W \cap \Lambda$. In particular, a vector $x \in \Lambda$ can be extended to an R-basis of Λ if and only if it is a primitive vector in the sense that $cx \in \Lambda$ for some $c \in F$ implies $c \in R$.*

PROOF. The condition of the lemma is equivalent to Λ/M being torsion free.

□

THEOREM 2.16. *Let (V, Q) be a finite dimensional regular quadratic space over F with an orthogonal decomposition $V = U_1 \perp U_2$, let Λ be a lattice of full rank on V with $b(\Lambda, \Lambda) \subseteq R$ (equivalently, $\Lambda \subseteq \Lambda^\#$). Let $L_i = \Lambda \cap U_i (i =$*

$1,2)$ *and denote by* π_i *the orthogonal projection* $\pi_i : V \to U_i$. *Then one has*

a)
$$\Lambda^\#/(L_1 \perp U_2 \cap \Lambda^\#) \cong L_1^\#/L_1.$$

b) $\mathfrak{d}(\pi_2(\Lambda)) \cdot \mathfrak{d}(L_1) = \mathfrak{d}(\Lambda)$,
$\mathfrak{d}(L_1) = \mathfrak{d}(\Lambda) \cdot \mathfrak{d}(U_2 \cap \Lambda^\#)$,
$\mathfrak{d}(L_1)\mathfrak{d}(L_2) = \mathfrak{d}(\Lambda)(\pi_2(\Lambda) : L_2)_R^2 = \mathfrak{d}(\Lambda)(\pi_1(\Lambda) : L_1)_R^2$.

c) $\mathfrak{d}(\Lambda)\mathfrak{d}(L_1) = \mathfrak{d}(L_2)(L_1^\# : \pi_1(\Lambda))_R^2$.
In particular, if $U_1 = Fx$ *has dimension* 1 *with* $L_1 = Rx$, *one has with* $b(x, \Lambda) =: aR$

$$\begin{aligned} \mathfrak{d}(\Lambda) &= b(x,x)\mathfrak{d}(\pi_2(\Lambda)) \\ b(x,x)\mathfrak{d}(\Lambda) &= a^2\mathfrak{d}(L_2). \end{aligned}$$

d) *If* Λ *is unimodular, one has*

$$\begin{aligned} L_i^\# &= \pi_i(\Lambda) \quad (i = 1,2) \\ L_1^\#/L_1 &\cong L_2^\#/L_2 \text{ as } R\text{-modules} \\ \mathfrak{d}(L_1) &= \mathfrak{d}(L_2). \end{aligned}$$

PROOF. Since all parts of the assertion are true if and only if they are true for all localisations it is sufficient to prove them for principal ideal domains, replacing $\mathfrak{d}$ by det.

a) By assertion a) of Lemma 1.64 we have $U_i \cap \Lambda^\# = (\pi_i(\Lambda))^\#$, and from $(\Lambda^\#)^\# = \Lambda$ one sees that $L_i = U_i \cap \Lambda = (\pi_i(\Lambda^\#))^\#$ holds. Dualizing both sides of this equality we obtain $L_i^\# = \pi_i(\Lambda^\#)$ for $i = 1,2$. We obtain from this a surjective R-linear map $\Lambda^\# \to L_1^\#/L_1$, whose kernel is $\{x \in \Lambda^\# \mid \pi_1(x) \in L_1\}$. The latter set is nothing but $L_1 \perp (U_2 \cap \Lambda^\#)$ as asserted.

b) Let $(v_1, \dots, v_n)$ be a basis of Λ for which $(v_1, \dots, v_r)$ is a basis of L_1. The linear map $\phi : V \to V$ with $\phi(v_i) = v_i$ for $1 \le i \le r$ and $\phi(v_i) = \pi_2(v_i)$ for $i > r$ has determinant 1 and image $L_1 \perp \pi_2(\Lambda)$, which implies the first part of the assertion. The second part follows from the first part and $\pi_2(\Lambda) = (U_2 \cap \Lambda)^\#$, the third part from $\det(L_2) = \det(\pi_2(\Lambda))(\pi_2(\Lambda) : L_2)_R^2$ and the first part.

c) From b) we obtain

$$\begin{aligned} \det(\Lambda)\det(L_1) &= \det(L_1)^2\det(L_2)(\pi_1(\Lambda) : L_1)_R^{-2} \\ &= \det(L_2)(d_{L_1^\#/L_1})^2(\pi_1(\Lambda) : L_1)_R^{-2} \\ &= \det(L_2)(L_1^\# : \pi_1(\Lambda))_R^2. \end{aligned}$$

For $\dim(U_1) = 1$ we have $(\pi_1(\Lambda) : L_1)_R = b(x,x)a^{-1}R^\times$ (with $b(x,\Lambda) = aR$) and obtain the second formula. The first formula for this case follows from the first formula in b).

d) The assertions are a), b) of Lemma 1.64 and c) with $\Lambda^\# = \Lambda$ inserted.

□

DEFINITION 2.17. Let (V,Q) be a finite dimensional regular quadratic space over F.
An R-lattice Λ of full rank on V is called maximal if $Q(\Lambda) \subseteq R$ holds and if Λ is maximal with respect to this property.
For a fractional R-ideal $I \subseteq F$ an I-maximal lattice is defined analogously.

LEMMA 2.18. *Let I be a fractional R-ideal in F. Every R-lattice Λ with $Q(\Lambda) \subseteq I$ on the finite dimensional regular quadratic space (V,Q) over F is contained in an I- maximal lattice.*

PROOF. If Λ is not I-maximal it has a strict overlattice Λ_1 with $Q(\Lambda_1) \subseteq I$, and proceeding in the same way as long as possible we obtain an ascending chain of lattices L_i with $Q(\Lambda_i) \subseteq I$.
From $Q(\Lambda) \subseteq I$ we see that $\Lambda \subseteq I\Lambda^\#$, and in the same way all the Λ_i above are contained in $I\Lambda^\#$. Since $I\Lambda^\#$ is noetherian any ascending chain of sublattices of it becomes stationary after finitely many steps, and we obtain the assertion. □

THEOREM 2.19. *Let (V,Q) be an m-dimensional isotropic regular quadratic space over F and Λ a maximal lattice on V. Then $\Lambda = H \perp \Lambda_1$, where H is a regular hyperbolic R-lattice of rank $2r \leq m$ and Λ_1 is a maximal lattice on an anisotropic subspace of V.*

PROOF. Let x be an isotropic vector of V, we have $\mathfrak{a}x^{-1} = Fx \cap \Lambda^\#$ for some ideal $\mathfrak{a} \subseteq R$. The lattice $L := \Lambda + \mathfrak{a}^{-1}x$ satisfies then $Q(L) \subseteq R$, by maximality of Λ we have $L = \Lambda$ so that $\mathfrak{a}^{-1}x \subseteq \Lambda$. Since we have $\mathfrak{a}^{-1}x = Fx \cap \Lambda^\#$ we see that $\mathfrak{a}^{-1}x$ is a regularly embedded totally isotropic submodule of Λ, so by Theorem 1.38 there is a regular hyperbolic sublattice of rank 2 of Λ containing $\mathfrak{a}^{-1}x$ which can be split off orthogonally in Λ. The assertion follows by induction on m. □

REMARK 2.20. An analogous result is valid for an I-maximal lattice, where I is a fractional R-ideal. The hyperbolic module H above is then replaced by a module isometric to $M \oplus IM^*$.

CHAPTER 3

Reduction Theory of Positive Definite Quadratic Forms

In this chapter and the next one we deal with geometric and computational properties of spaces of real valued quadratic forms over the rational integers. Reduction theory is concerned with the task of selecting special forms in an equivalence class or equivalently special bases of a given quadratic module. The computational aim is to obtain Gram matrices with small entries in order to facilitate computations, the geometric aim is the study of the geometric properties of the action of the group $GL_n(\mathbb{Z})$ on the space, in particular the construction of fundamental domains for this action. We deal with positive definite forms in this chapter and with indefinite forms in the next chapter. Our presentation in this chapter follows for the most part [**6, 37**]. The general study of the properties of quadratic forms over number rings will be continued after this interlude.

3.1. Minkowski reduced forms and successive minima

A lattice in $\mathbb{R}^n$ of rank r is a $\mathbb{Z}$-module $L = \mathbb{Z}f_1 + \ldots + \mathbb{Z}f_r \subseteq \mathbb{R}^n$, where the f_i are $\mathbb{R}$-linearly independent vectors in $\mathbb{R}^n$. Let Q be a positive definite quadratic form on $\mathbb{R}^n$ with associated bilinear form b, let $B = b/2$ as usual.

DEFINITION 3.1. Let $L \subseteq \mathbb{R}^n$ be a $\mathbb{Z}$-lattice of full rank n with basis $f_1, \ldots, f_n$. Put put $L_0 := \{0\}$, for $1 \le i \le n$ put $L_i := L_i(\{f_j\}) := \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_i$. The basis $\mathcal{B} = (f_1, \ldots, f_n)$ of L is called Minkowski reduced with respect to Q (or B) if one has for $1 \le i \le n$:
For all $x \in L$ for which $L'_i(x) := L_{i-1} + \mathbb{Z}x$ is primitive in L one has $Q(x) \ge Q(f_i)$.
Its Gram matrix $M_{\mathcal{B}}(B)$ is then called a Minkowski reduced matrix and the quadratic polynomial $P(X_1, \ldots, X_n) = \sum_{i,j} m_{ij} X_i X_j$ with $M_{\mathcal{B}}(B) = (m_{ij})$ a Minkowski reduced quadratic form.

REMARK 3.2.
a) An equivalent formulation is: A basis $f_1, \ldots, f_n$ of L is Minkowski reduced if $Q(f_i)$ is minimal among the $Q(x)$ for which $x + L_{i-1}$ is primitive in L/L_{i-1} for all i.
b) The positive definite matrix $A \in M_n^{\mathrm{sym}}(\mathbb{R})$ is Minkowski reduced if and only if the standard basis $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ of $\mathbb{Z}^n$ is a reduced basis of the lattice $\mathbb{Z}^n$ with the quadratic form Q_A given by $Q_A(\mathbf{x}) = {}^t\mathbf{x}A\mathbf{x}$.

LEMMA 3.3.
a) *The positive definite matrix* $A \in M_n^{\mathrm{sym}}(\mathbb{R})$ *is Minkowski reduced if and only for* $1 \le i \le n$ *one has* $a_{ii} \le {}^t\mathbf{x}A\mathbf{x}$ *for all* $\mathbf{x} \in \mathbb{Z}^n$ *with* $\gcd(x_i, \ldots, x_n) = 1$.

b) *A Minkowski reduced matrix* $A = (a_{ij})$ *satisfies*

$$0 < a_{11} \leq a_{22} \leq \cdots \leq a_{nn},$$
$$|2a_{ij}| \leq a_{ii} \quad \textit{for all } 1 \leq i < j \leq n.$$

PROOF. The first assertion follows from the fact that $\mathbb{Z}\mathbf{e}_1 + \cdots + \mathbb{Z}\mathbf{e}_{i-1} + \mathbb{Z}\mathbf{x}$ is a primitive sublattice of $\mathbb{Z}^n$ if and only if one has $\gcd(x_i, \ldots, x_n) = 1$. The second assertion follows from taking $\mathbf{x} = \mathbf{e}_j$ respectively $\mathbf{x} = \mathbf{e}_i + \mathbf{e}_j$ for $i < j$. □

For the rest of this chapter we consider the standard scalar product $\langle \quad , \quad \rangle =: b(\quad , \quad)$ on the space $\mathbb{R}^n$. As usual we put $Q(\mathbf{x}) = b(x, x)/2 = B(x, x)$. Instead of $\det_b(L)$ as in earlier chapters we will usually consider $\det_B(L) = 2^{-n}\det_b(L)$.
Restricting attention to Q instead of an arbitrary positive definite quadratic form on $\mathbb{R}^n$ doesn't lose generality since all positive definite quadratic forms on $\mathbb{R}^n$ are equivalent over $\mathbb{R}$ to Q. The lattice L is called integral if all the $b(f_i, f_j) = \langle f_i, f_j \rangle$ are in $\mathbb{Z}$. If one has in addition $Q(L) \subseteq \mathbb{Z}$ the lattice is called even integral.
Since in this case the classes modulo squares of units in $\mathbb{Z}$ consist of one element only we may treat $\det_B(L)$ as a real number instead of a square class when this is convenient.

THEOREM 3.4. *Every lattice has a Minkowski reduced basis. Equivalently, for every Minkowski reduced positive definite symmetric matrix A there exists an integrally equivalent Minkowski reduced matrix.*

PROOF. Obvious. □

REMARK 3.5. We will see in Section 3.3 that for fixed dimension n already a finite set of the reduction conditions $a_{ii} \leq {}^t\mathbf{x}A\mathbf{x}$ suffices to characterize Minkowski reduced matrices. Such finite sets of reduction conditions are explicitly known for $n \leq 7$ (see [**36**] for the case $n = 7$). Nevertheless, for $\mathrm{rk}(L) = n > 4$ it is in general computationally difficult to determine a Minkowski reduced basis of a given lattice effectively.

For the cases $n \leq 4$ Minkowski has shown in [**29**] that already the vectors $\mathbf{x}$ with components $x_i \in \{0, \pm 1\}$ suffice, see also Lemma 12.1.2 of [**6**], whose proof we follow:

EXAMPLE 3.6. For $2 \leq n \leq 4$ a matrix $Y \in \mathcal{P}_n$ is Minkowski reduced if and only if

a) $0 \leq y_{11} \leq y_{22} \leq \cdots \leq y_{nn}$
b) $P_Y(\mathbf{x}) := {}^t\mathbf{x}Y\mathbf{x}$ satisfies $P_Y(\mathbf{x}) \geq y_{jj}$ for all $\mathbf{x} \in \mathbb{Z}^n$ with $x_i \in \{0, \pm 1\}$, $x_j = 1$, $x_i = 0$ for $i > j$.

PROOF. It is obvious that a reduced matrix satisfies the conditions a), b). Assume conversely that Y satisfies a) and b). We have to show that any $\mathbf{x} \in \mathbb{Z}^n$ with $\gcd(x_r, \ldots, x_n) = 1$ for some $1 \leq r \leq n$ satisfies $P_Y(\mathbf{x}) \geq y_{rr}$, in fact we claim that (under our assumption $n \leq 4$) this even holds for all

$\mathbf{x}$ with $x_r \neq 0$. Since deleting the j-th row and column from Y and the jth coordinate x_j from $\mathbf{x}$ for all j with $x_j = 0$ and multiplying the j-th row and column of Y and the entry x_j of $\mathbf{x}$ by -1 for all j with $x_j < 0$ doesn't change the validity of our claim we may assume that $x_i > 0$ for $1 \leq i \leq n$ and have to show $P_Y(\mathbf{x}) \geq y_{nn}$. We proceed by induction on $S := \sum_{i=1}^n x_i$, the case $S = 1$ being a trivial consequence of b) and $n = 1$ being trivial as well. Let now $S > 1$ and set $c := \min(x_i) > 0$, let k be maximal with $x_k = c$. We set $z_i = x_i - c$ for $i\ nek$ and $z_k = x_k$ and let $\mathbf{z} = (z_1, \dots, z_n)$. We have $z_n > 0$ and $\sum_{i=1}^n z_i < \sum_{i=1}^n x_i$, so by the inductive assumption we have $P_Y(\mathbf{z}) \geq y_{nn}$. We are done if we can show $P_Y(\mathbf{x}) \geq P_Y(\mathbf{z})$. Indeed we have, using $y_{ij} = y_{ji}$ for all i, j, $x_i - z_i = c$ for $i \neq k$, and $x_k - z_k = 0$:

$$
\begin{aligned}
P_Y(\mathbf{x}) - P_Y(\mathbf{z}) &= \sum_j y_{kj}(cx_j - cz_j) + \sum_{i\neq k} y_{ik}(x_i c - z_i c) \\
&\quad + \sum_{i\neq k}\sum_{j\neq k} y_{ij}(x_i x_j - z_i z_j) \\
&= 2\sum_{j\neq k} c^2 y_{kj} + \sum_{i\neq k}\sum_{j\neq k} y_{ij}(c^2 + cz_i + cz_j) \\
&= c^2(P_Y(1,\dots,1) - y_{kk}) + 2c\sum_{i\neq k} z_i \sum_{j\neq k} y_{ij} \\
&\geq 2c\sum_{i\neq k} z_i\big((2-\frac{n}{2})y_{ii} + \frac{1}{2}\sum_{j\neq k, j\neq i}(y_{ii} + 2y_{ij})\big) \\
&\geq 0.
\end{aligned}
$$

□

DEFINITION 3.7. With notations as before

$$\mu_1 := \mu_1(L) := \min\{Q(x) \mid x \in L \setminus \{0\}\}$$

is called the minimum of the lattice L and a vector X satisfying $Q(x) = \mu_1$ is called a minimum vector.
For $2 \leq j \leq n$ the j-th successive minimum μ_j of L is the smallest $a \in \mathbb{R}$ for which there are linearly independent vectors $x_1, \dots, x_j \in L$ satisfying $Q(x_1) \leq \cdots \leq Q(x_j) \leq a$.
for $1 \leq j \leq n$ linearly independent vectors $x_1, \dots, x_j \in L$ satisfying $Q(x_i) = \mu_i$ for $1 \leq i \leq j$ are called successive minimum vectors.

REMARK 3.8.
a) For each $C > 0$ the set $\{x \in \mathbb{R}^n \mid Q(x) \leq C\}$ is compact and can hence contain only finitely many points of the discrete set L. The minimum μ_1 and the successive minima can therefore indeed be defined as minima instead of infima.
b) Let $x_1, \dots, x_j$ be successive minimum vectors of L and let $y_1, \dots, y_{j+1}$ be linearly independent vectors with $Q(y_i) \leq \mu_{j+1}$ for $1 \leq i \leq j+1$. Then at least one of the y_i is not in the linear span of the x_i, hence

$$\min\{Q(x) \mid \{x_1, \dots, x_j, x\} \text{ is linearly independent}\} \leq \mu_{j+1}$$

holds. Since the reverse inequality is obvious, we can also define the successive minima recursively, defining μ_{j+1} by fixing already given successive minimum vectors $x_1, \dots, x_j$ and requiring the equation above to hold for all x which are linearly independent from the given vectors.

c) The successive minima too are in general difficult to determine effectively.

THEOREM 3.9. *There exists a constant (called* Hermite's constant*) γ_n depending only on n so that each positive definite $\mathbb{Z}$-lattice Λ of rank n with associated symmetric bilinear forms b, $B = b/2$ satisfies*

$$\mu_1 \cdots \mu_r \leq \gamma_n^r (\det_B(\Lambda)^{\frac{r}{n}}$$

for $1 \leq r \leq n$. In particular one has

$$\mu_1 \leq \gamma_n (\det_B(\Lambda))^{1/n}.$$

PROOF. We show first by induction on n that one can find a constant γ_n such that $\mu_1(\Lambda) \leq \gamma_n(\det_B(\Lambda)^{1/n}$ is true for all positive definite lattices Λ of rank n, the case $n = 1$ being trivial with $\gamma_1 = 1$.

Let then $n > 1$, let $e_1 \in \Lambda$ with $Q(e_1) = \mu_1$, let L' be the orthogonal projection of Λ onto $e_1^\perp$. By b) of Theorem 2.16 we have $\det_B(L') = \frac{\det_B(\Lambda)}{\mu_1}$, notice that this part of the proof of that theorem does not need the bilinear form to take values in $\mathbb{Q}$.

By the inductive assumption we find $x' \in L'$ satisfying

$$Q(x') \leq \gamma_{n-1}(\frac{\det_B \Lambda}{\mu_1})^{\frac{1}{n-1}}.$$

We can then find $\alpha \in \mathbb{R}$ with $0 \leq |\alpha| \leq \frac{1}{2}$ and $x := \alpha e_1 + x' \in \Lambda$, hence

$$\mu_1 \leq Q(x) \leq \frac{\mu_1}{4} + \gamma_{n-1}(\frac{\det_B(\Lambda)}{\mu_1})^{\frac{1}{n-1}}.$$

From this we obtain

$$\begin{array}{rcl} \frac{3\mu_1}{4} & \leq & \gamma_{n-1}(\frac{\det_B \Lambda}{\mu_1})^{\frac{1}{n-1}} \\ (\frac{3}{4})^{n-1}\mu_1^n & \leq & \gamma_{n-1}^{n-1}\det_B(\Lambda) \\ \mu_1^n & \leq & (\frac{4}{3}\gamma_{n-1})^{n-1}\det_B(\Lambda) \end{array}$$

From $\gamma_1 = 1$ we obtain recursively that

$$\gamma_n := (\frac{4}{3})^{\frac{n-1}{2}}$$

is as desired: Inserting $\gamma_{n-1} = (\frac{4}{3})^{\frac{n-2}{2}}$ in the equation above we get

$$\begin{aligned} \mu_1^n &\leq (\tfrac{4}{3})^{n-1}(\tfrac{4}{3})^{\frac{(n-2)(n-1)}{2}}\det{}_B(\Lambda) \\ &= (\tfrac{4}{3})^{(n-1)(1+\frac{n-2}{2})}\det{}_B(\Lambda) \\ &= (\tfrac{4}{3})^{\frac{(n-1)}{2}n}\det{}_B(\Lambda) \end{aligned}$$

and hence

$$\mu_1 \leq (\frac{4}{3})^{\frac{n-1}{2}}(\det{}_B\Lambda)^{\frac{1}{n}}.$$

To show the first inequality of the theorem for any γ_n satisfying the inequality for μ_1 we let $f_1, \dots, f_n \in \Lambda$ be successive minimum vectors and denote by $\{f_i'\}$ the orthogonal basis of $V = \mathbb{R}^n$ obtained from the f_i by the Gram-Schmidt orthogonalization procedure, i. e.,

$$\begin{aligned} f_1' &= f_1 \\ f_2' &= f_2 - \frac{B(f_1, f_2)}{B(f_1, f_1)}f_1 \end{aligned}$$

und recursively

$$f_j' = f_j - \sum_{i=1}^{j-1} \frac{B(f_j, f_i')}{B(f_i', f_i')}f_i'.$$

In particular one has

$$\mathbb{R}f_1' + \cdots + \mathbb{R}f_i' = \mathbb{R}f_1 + \cdots + \mathbb{R}f_i,$$

and the Gram matrix of B with respect to $f_1', \dots, f_n'$ has the same determinant as that taken with respect to $f_1, \dots f_n$.

We define then a quadratic form Q' on V with associated symmetric bilinear forms $b', B' = b'/2$ by requiring the f_i' to be pairwise orthogonal with respect to B' and setting

$$Q'(f_i') = \frac{Q(f_i')}{\mu_i}.$$

The determinants of $\bigoplus_{i=1}^n \mathbb{Z}f_i$ with respect to B and to B' differ by the same factor as $\det_B(\Lambda)$ and $\det_{B'}(\Lambda)$, and we see

$$\det{}_{B'}(\Lambda) = \frac{\det_B(\Lambda)}{\mu_1 \cdots \mu_n}.$$

Let now $y \in \Lambda$, $y \neq 0$ and j minimal, such that $y = \sum_{i=1}^j y_i f_i' \in \mathbb{R}f_1' + \cdots + \mathbb{R}f_j'$ is true. Then

$$\begin{aligned} Q'(y) &= \textstyle\sum_{i=1}^j y_i^2 \frac{Q(f_i')}{\mu_i} \\ &\geq \mu_j^{-1} \textstyle\sum_{i=1}^j y_i^2 Q(f_i') \\ &= \mu_j^{-1} Q(y) \geq 1, \end{aligned}$$

since y is linearly independent of the $f_1, \dots, f_{j-1}$.

This implies

$$1 \le \min_{Q'}(\Lambda) \le \gamma_n \left(\frac{\det_B(\Lambda)}{\mu_1 \cdots \mu_n} \right)^{\frac{1}{n}},$$

and hence $\mu_1 \cdots \mu_n \le \gamma_n^n \det_B(\Lambda)$. Finally, for $1 \le r \le n$ we have

$$(\mu_1 \cdots \mu_r)^n \le (\mu_1 \cdots \mu_n)^r \le \gamma_n^{rn} \det_B((\Lambda))^r.$$

□

COROLLARY 3.10. *The minimal determinant $m_r(\Lambda)$ of a sublattice of rank r of Λ satisfies for $1 \le r \le n$*

$$m_r(\Lambda) \le \gamma_n^r (\det_B(\Lambda))^{\frac{r}{n}}.$$

PROOF. Let $f_1, \dots, f_n$ be successive minimum vectors of Λ. By Hadamard's inequality the lattice $L_r(\Lambda) := \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_r$ satisfies $\det_B(L_r(\Lambda)) \le \mu_1(\Lambda) \cdots \mu_r(\Lambda)$, and the assertion follows from the theorem. □

LEMMA 3.11. *Let $(v_1, \dots, v_n)$ be a basis of the $\mathbb{Z}$-lattice $\Lambda \subseteq \mathbb{R}^n$ with Gram-Schmidt orthogonalization $(v_1', \dots, v_n')$, let $1 \le j \le n$ and $L_j = \bigoplus_{i=1}^j \mathbb{Z}v_i$, let $z \in \mathbb{R}L_j$.*
Then there is $y \in L_j$ such that one has $z - y = \sum_{i=1}^j \alpha_i v_i'$ with $|\alpha_i| \le \frac{1}{2}$ (for $1 \le i \le j$).

PROOF. Write $z = \sum_{i=1}^j \beta_i v_i'$ and choose $\alpha_j' \in \mathbb{Z}$ with $|\beta_j - \alpha_j'| \le \frac{1}{2}$. We have then $z - \alpha_j v_j = (\beta_j - \alpha_j)v_j' + z'$ with $z' \in \mathbb{R}L_{j-1}$.
We can then find $y' \in L_{j-1}$ with $z' - y' = \sum_{i=1}^{j-1} \alpha_i v_i'$, $|\alpha_i| \le \frac{1}{2}$. Setting $y = y' + \alpha_j v_j$ one sees $z - y = (\beta_j - \alpha_j')v_j' + z' - y'$, and with $\alpha_j := \beta_j - \alpha_j'$ the vector $z - y$ is as desired. □

THEOREM 3.12. *Let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a Minkowski reduced basis of Λ, let $\{v_1', \dots, v_n'\}$ denote the Gram-Schmidt orthogonalization of $\mathcal{B}$ and μ_i the successive minima of Λ. Then one has*

a) $Q(v_j') \le Q(v_j)$
b) $\mu_j \le Q(v_j)$
c) *There exist constants $c_1(j)$ independent of Λ and Q such that $Q(v_j) \le c_1(j)\mu_j$ for $1 \le j \le n$.*
d) *There exist constants $c_2(n)$ independent of Λ und Q with $\mu_j \le c_2(n)Q(v_j')$ for $1 \le j \le n$.*

PROOF. a) $v_j' = v_j - p_{j-1}(v_j)$, where p_i is the orthogonal projection onto the space spanned by $v_1', \dots, v_i'$i. e.,

$$\begin{aligned} Q(v_j) &= Q(v_j') + Q(p_{j-1}(v_j)) \\ &\ge Q(v_j') \end{aligned}.$$

b) Obvious.

c) We use induction on j, the start $j = 1$ being trivial. Let linearly independent vectors $w_1, \dots, w_n$ with $\mu_i = Q(w_i)$ be given. Let $1 \leq k \leq j$ be such that $\{v_1, \dots, v_{j-1}, w_k\}$ are linearly independent and choose $v_j^* \in \Lambda$ such that $v_1, \dots, v_{j-1}, v_j^*$ form a basis of $(\mathbb{R}L_{j-1} + \mathbb{R}w_k) \cap \Lambda = (L_{j-1} + \mathbb{R}w_k) \cap \Lambda$. That is possible since L_{j-1} is a primitive sublattice of this lattice.

In particular, $L_{j-1} + \mathbb{Z}v_j^*$ is then a primitive sublattice of Λ, and we have $Q(v_j) \leq Q(v_j^*)$.
We change v_j^* by a vector of L_{j-1} or multiply it by -1 if necessary to achieve

$$w_k = \sum_{i=1}^{j-1} t_i v_i + s v_j^*, \ 0 < s \in \mathbb{Z},\ t_i \in \mathbb{Z}$$

with $|t_i| \leq \frac{s}{2}$.
Using $\sqrt{Q(x+y)} \leq \sqrt{Q(x)} + \sqrt{Q(y)}$ we see then

$$\sqrt{Q(v_j)} \leq \sqrt{Q(v_j^*)} \leq \frac{1}{s}\sqrt{\mu_k} + \frac{1}{2}\sum_{i=1}^{j-1}\sqrt{Q(v_i)} \leq \sqrt{\mu_j} + \frac{1}{2}\sum_{i=1}^{j-1}\sqrt{c_1(i)}\sqrt{\mu_j},$$

and notice that $\sqrt{Q(v_i)} \leq \sqrt{c_1(i)}\sqrt{\mu_i} \leq \sqrt{c_1(i)}\sqrt{\mu_j})$ holds by the inductive assumption.
$c_1(j)^{\frac{1}{2}} = 1 + \frac{1}{2}\sum_{i=1}^{j-1} c_1(i)^{\frac{1}{2}}$ is then as desired.

d) We have $\prod_{i=1}^n Q(v_i') = \det_B(\Lambda)$ and $\prod_{i=1}^n \mu_i \leq \gamma_n^n \det_B(\Lambda)$. This implies

$$\begin{aligned}
\gamma_n^n &\geq \prod_{i=1}^n \frac{\mu_i}{Q(v_i')} \\
&\geq \frac{\mu_j}{Q(v_j')}\prod_{i\neq j}\mu_i\frac{c_1(i)^{-1}}{\mu_i} \\
&= \frac{\mu_j}{Q(v_j')}\prod_{i\neq j} c_1(i)^{-1},
\end{aligned}$$

and we have

$$\mu_j \leq Q(v_j') \underbrace{\gamma_n^n \max_j\{\prod_{i\neq j} c_1(i)\}}_{=c_2(n)}.$$

□

COROLLARY 3.13. *Let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a Minkowski reduced basis of the lattice Λ, denote by μ_j the successive minima of Λ.*
Then for $1 \leq j \leq 4$ one has $Q(v_j) = \mu_j$, for $j \geq 5$ one has $Q(v_j) \leq \left(\frac{5}{4}\right)^{j-4}\mu_j$.
For $1 \leq j \leq 3$ any choice of first j minimum vectors can be extended to a Minkowski reduced basis.

PROOF. Proceeding as in the proof of the theorem we want to show that one can choose $c_1(j) = 1$ for $1 \le j \le 4$ and $c_1(j) = \left(\frac{5}{4}\right)^{j-4}$ for $j > 4$.
We obtain first $w_k = \sum_{i=1}^{j-1} t_i v_i + s v_j^*$, $0 < s \in \mathbb{Z}$, $t_i \in \mathbb{Z}$.
If one has here $s = 1$, the lattice $L_{j-1} + \mathbb{Z}w_k$ is primitive in Λ and we have $Q(v_j) \le Q(w_k) = \mu_k \le \mu_j$.
Otherwise we decompose $v_j^* = z_1 + z_2$ with $z_1 \in \mathbb{R}L_{j-1}$, $z_2 \perp L_{j-1}$ and have

$$w_k = \left(\sum_{i=1}^{j-1} t_i v_i + s z_1\right) + s z_2.$$

One has then

$$Q(w_k) \ge s^2 Q(z_2),$$

hence

$$Q(z_2) \le \frac{1}{4}\mu_k \le \frac{1}{4}\mu_j.$$

By the previous lemma we can change v_j^* modulo L_{j-1} in such a way that $z_1 = \sum_{i=1}^{j-1} \alpha_i v_i'$ with $|\alpha_i| \le \frac{1}{2}$ holds and see $Q(z_1) \le \frac{1}{4}\sum_{i=1}^{j-1} Q(v_i')$.

Putting things together we get

$$\begin{aligned} Q(v_j) \le Q(v_j^*) &\le \tfrac{1}{4}\mu_j + \tfrac{1}{4}\textstyle\sum_{i=1}^{j-1} Q(v_i') \\ &\le \tfrac{1}{4}\mu_j + \tfrac{1}{4}\textstyle\sum_{i=1}^{j-1} Q(v_i) \\ &\le \tfrac{1}{4}\mu_j + \tfrac{1}{4}\textstyle\sum_{i=1}^{j-1} c_1(i)\mu_i \\ &\le \tfrac{1}{4}\mu_j(1 + \textstyle\sum_{i=1}^{j-1} c_1(i)) \end{aligned}$$

and hence

$$Q(v_j) \le \mu_j \cdot \max\{1, \frac{1}{4} + \frac{1}{4}\sum_{i=1}^{j-1} c_1(i)\}.$$

With $c_1(1) = 1$ we see in particular that one can choose

$$c_1(2) = c_1(3) = c_1(4) = 1.$$

Using induction on j we see finally $c_1(j) = (\frac{5}{4})^{j-4}$ for $j \ge 4$.
For $1 \le j \le 3$ the argument above shows that $s > 1$ would imply $Q(v_j) < \mu_j$, a contradiction which shows the second part of the assertion. □

EXAMPLE 3.14. a) Let $\Lambda \subseteq \mathbb{R}^5$ be the lattice with basis
$v_1 = (1,0,0,0,0)$, $v_2 = (0,1,0,0,0)$, $v_3 = (0,0,1,0,0)$,
$v_4 = (0,0,0,1,0)$, $v_5 = (\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$.
Then it is easily seen that this basis is Minkowski reduced and that all five successive minima are equal to 1, so we have $Q(v_5) = \frac{5}{4} > 1 = \mu_5$.

b) Let $\Lambda \subseteq \mathbb{R}^4$ be the lattice with basis $(1,-1,0,0),(0,1,-1,0),$ $(0,0,1,-1),(0,0,1,1)$ (the D_4-lattice in the root lattice terminology). The vectors $(1,-1,0,0),(1,1,0,0),(0,0,1,-1),(0,0,1,1)$ are successive minimum vectors but do not generate the lattice.

3.2. Siegel domains

We recall from linear algebra:

LEMMA 3.15. *Let $\mathcal{B} = \{v_1,\dots,v_n\}$ be a basis of the vector space V and $\{v'_1,\dots,v'_n\}$ the Gram-Schmidt orthogonalization. Then the matrix $C = (c_{ij})$ given by $v_j = \sum_{i=1}^n c_{ij} v'_j$ is upper triangular with diagonal entries* 1 *and for the Gram matrix $M_{\mathcal{B}}$ of the symmetric bilinear form B with respect to $\mathcal{B}$ one has*

$$M_{\mathcal{B}} = C^t \begin{pmatrix} h_1 & & & & \\ & \cdot & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & h_n \end{pmatrix} C$$

with $h_i = Q(v'_i)$ and

$$Q(\sum_{i=1}^n x_i v_i) = \frac{1}{2}\sum_{i=1}^n h_i \xi_i^2, \quad \xi_i = \sum_{j=1}^n c_{ij} x_j.$$

The matrix C and the h_i with these properties are uniquely determined.

DEFINITION 3.16. Let $\delta > 1$, $\epsilon > 0$ be given. The Siegel domain $\mathcal{S}_n(\delta,\epsilon) = \mathcal{S}(\delta,\epsilon)$ is the set of all positive definite symmetric $(n \times n)$-matrices M for which the decomposition

$$M = C^t \begin{pmatrix} h_1 & & & & \\ & \cdot & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & h_n \end{pmatrix} C$$

satisfies

$$\begin{array}{rcl} 0 < h_j & \leq & \delta h_{j+1}, \\ |c_{ij}| & \leq & \epsilon \quad \forall i,j. \end{array}$$

THEOREM 3.17. *There exist $\delta = \delta(n)$, $\epsilon = \epsilon(n)$, such that all Minkowski reduced bases $\mathcal{B} = \{v_1,\dots,v_n\}$ satisfy*

$$M = M_{\mathcal{B}} \in \mathcal{S}(\delta(n),\epsilon(n)).$$

PROOF. With $Q(v_j) = m_{jj}$ and $Q(v'_J) = h_j$ we have

$$h_j \leq m_{jj} \leq m_{j+1,j+1} \leq c_1(j+1)c_2(n)h_{j+1}. \qquad (*)$$

For $i < j$ we see moreover

$$m_{ij} = h_i c_{ij} + \sum_{k<i} h_k c_{ki} c_{kj},$$

hence

$$|c_{ij}| \leq \frac{|m_{ij}|}{h_i} + \sum_{k<i} \frac{h_k}{h_i} |c_{ki} c_{kj}|$$

for $i < j$.

We have $|m_{ij}| \leq \frac{1}{2} m_{ii} \leq \frac{1}{2} c_1(i) c_2(n) h_i$ and $\frac{h_k}{h_i} \leq c_3(n)^{i-k}$ for $k < i$ with $c_3(n) = c_2(n) \max_{j \leq n} c_1(j)$. With $H_k = \max_{\ell > k} |c_{k\ell}|$ it follows that

$$|c_{ij}| \leq \frac{1}{2} c_3(n) + \sum_{k<i} c_3(n)^{i-k} H_k^2$$

holds. Since the matrix $M_{\mathcal{B}}$ is reduced, $|c_{1j}| = |\frac{m_{1j}}{m_{11}}| \leq \frac{1}{2}$, hence $H_1 \leq \frac{1}{2}$. By induction the H_i are bounded by a constant depending only on n, which proves the assertion. □

LEMMA 3.18. *There exists a constant $C_1 = C_1(n, \delta, \epsilon)$ depending only on n, δ, ϵ such that all $M \in S(\delta, \epsilon)$ satisfy: For $1 \leq j \leq n$ all ratios of the h_j, m_{jj}, μ_j are bounded by C_1, where the μ_j are the successive minima of $\mathbb{Z}^n$ with the quadratic form $Q = Q_M$ given by $2Q(\mathbf{x}) = {}^t\mathbf{x} M \mathbf{x}$.*

PROOF. $m_{jj} = h_j + \sum_{i<j} h_i c_{ij}^2$ implies $m_{jj} \leq c_4 h_j$ with a constant $c_4 = c_4(n, \delta, \epsilon)$, in the opposite direction $m_{jj} \geq h_j$ is trivial. We see moreover

$$\begin{aligned} \mu_j \leq \max_{i \leq j} m_{ii} &\leq c_4 \max_{i \leq j} h_i \\ &\leq c_5 h_j \ \text{(with a constant } c_5 = c_5(\delta, \epsilon, n)). \end{aligned}$$

Let finally $v_1, \ldots, v_n$ be the standard basis vectors of $\Lambda = \mathbb{Z}^n$ and $v'_1, \ldots, v'_n$ their Gram-Schmidt orthogonalization with respect to Q. If $v \in \Lambda$ is linearly independent of $v_1, \ldots, v_{j-1}$ we write $v = \sum_{i=1}^n x_i v_i = \sum_{i=1}^n \xi_i v'_i$ with $x_i \in \mathbb{Z}$, $x_i \neq 0$ for at least one $i \geq j$. If i_0 is maximal with $x_{i_0} \neq 0$ one has $\xi_{i_0} = x_{i_0} \in \mathbb{Z}$, hence $Q(v) \geq Q(v'_{i_0}) = h_{i_0}$ with $i_0 \geq j$. This estimate also holds for the j-th minimum vector, and we see $\mu_j \geq \min(h_j, \ldots, h_n) \geq c_7 h_j$ with a constant $c_7 = c_7(\delta, n)$. □

THEOREM 3.19. *Let $n \in \mathbb{N}$ and $\delta, \eta > 0$ be given. There exists a constant $C(n, \delta, \eta)$ such that one has*

$$|t_{ij}| \leq C(n, \delta, \eta)$$

for all $M_1, M_2 = T^t M_1 T$ in $S_n(\delta, \eta)$ with $T \in GL_n(\mathbb{Z})$.

In particular, let M_1 und $M_2 = T^t M_1 T$ be equivalent Minkowski reduced matrices with $T = (t_{ij}) \in GL_n(\mathbb{Z})$ and let δ and ϵ be as in Theorem $|t_{ij}| \leq C(n, \delta, \epsilon)$.

For the proof of the Theorem we need an auxiliary lemma:

LEMMA 3.20. *Let n, δ, ϵ be given. There exists $C' = C'(n, \delta, \epsilon)$ with the following property:*

If $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a basis of V with Gram matrix $M = M_{\mathcal{B}} \in S(\delta, \epsilon)$ and if $w_i = \sum_{j=1}^n \alpha_{ji} v_j$ are successive minimum vectors of $\mathbb{Z}^n$ with respect to $Q = Q_M$, one has $|\alpha_{ji}| \leq C'(n, \delta, \epsilon)$ for all i, j.

PROOF. We denote by $\{v'_1, \dots, v'_n\}$ the Gram-Schmidt orthogonalization of $\mathcal{B}$, put $w_i = \sum \beta_{ji} v'_j$ and fix i, j.
If we have $Q(v_k) < \mu_i$ for all $k \le j$, we must have $j < i$ and $v_1, \dots, v_j, w_i$ must be linearly independent. Putting

$$w_i^* = w_i + \sum_{\ell=1}^{j} t_\ell v_\ell \in w_i + L_j$$

with arbitrary $t_\ell \in \mathbb{Z}$, one must have $Q(w_i^*) \ge \mu_i = Q(w_i)$ since otherwise w_i were a linear combination of the linearly independent vectors $v_1, \dots, v_j, w_i^*$ which have length strictly smaller than μ_i, which contradicts the defining property of successive minimum vectors.
By Lemma 3.11 we can choose such a vector w_i^* satisfying

$$w_i^* = \sum_\ell \beta^*_{\ell i} v'_\ell \quad \text{with } |\beta^*_{\ell i}| \le \frac{1}{2} \text{ for } 1 \le \ell \le j.$$

One has then $\beta_{\ell i} = \beta^*_{\ell i}$ for $\ell > j$ since $w_i - w_i^* \in L_j$ holds and have therefore the same projection onto $L_j^\perp$.
From this we get

$$\begin{aligned} \textstyle\sum_{\ell \le j} h_\ell \beta_{\ell i}^2 &= Q(w_i) - \textstyle\sum_{\ell > j} h_\ell \beta_{\ell i}^2 \\ &\le Q(w_i^*) - \textstyle\sum_{\ell > j} h_\ell \beta_{\ell i}^2 \\ &= \textstyle\sum_{\ell \le j} h_\ell \beta_{\ell i}^{*2} \\ &\le \tfrac{1}{4} \textstyle\sum_{\ell \le j} h_\ell \le \tfrac{1}{4}(\delta^{j-1} + \dots + 1) h_j, \end{aligned}$$

and hence $\beta_{ji}^2 \le \frac{1}{4}(\delta^{j-1} + \dots + 1)$.

If on the other hand there exists $1 \le k \le j$ satisfying $\mu_i \le Q(v_k)$, one has

$$\begin{array}{rcl} \mu_i \le Q(v_k) & \le & c_8 Q(v'_k) \le \delta^{j-k} c_8 h_j \\ & & \quad \| \\ & & \quad h_k \\ & \le & \delta^{n-1} c_8 h_j, \end{array}$$

and hence $\mu_i = \sum \beta_{\ell i}^2 h_\ell \le \delta^{n-1} c_8 h_j$. From this we see $\beta_{ji}^2 h_j \le \delta^{n-1} c_8 h_j$, $\beta_{ji}^2 \le \delta^{n-1} c_8$ so that the β_{ji} are bounded. Since we can express the coordinates with respect to the v_i by those with respect to the v'_i with coefficients bounded by the constants of the Siegel domain considered, the assertion follows. □

We can now prove the theorem:

PROOF OF THEOREM 3.19. Let $\mathcal{B} = (v_1, \dots, v_n), \tilde{\mathcal{B}} = (\tilde{v}_1, \dots, \tilde{v}_n)$ be two bases of the lattice $\Lambda = \mathbb{Z}^n$ with Gram matrices M_1, M_2 in $\mathcal{S}(\delta, \epsilon)$ and let $w_i = \sum_{j=1}^n \alpha_{ji} v_j = \sum_{j=1}^n \widetilde{\alpha_{ji}} \tilde{v}_j$ be successive minimum vectors of Λ.
By the lemma the $\widetilde{\alpha_{ji}}$ and the α_{ji} are bounded.

Then the coefficients of the $\tilde{v}_j$ with respect to the w_i and therefore also the coefficients of the $\tilde{v}_j$ with respect to the v_i are bounded, and the assertion is proved. □

COROLLARY 3.21. *There exists a constant $C(n)$ such that each equivalence class of positive definite symmetric matrices contains at most $C(n)$ Minkowski reduced matrices.*

PROOF. Obvious. □

3.3. The geometry of the space of positive definite matrices

We will now study the geometry of the space of positive definite real symmetric matrices.

LEMMA 3.22. *Let $\mathcal{P}_n = \{Y \in M_n^{\mathrm{sym}}(\mathbb{R}) \mid Y > 0\}$. Then $\mathrm{GL}_n(\mathbb{R})$ acts on $\mathcal{P}_n$ by*

$$g.Y := {}^t g^{-1} Y g^{-1} =: Y[g^-1].$$

The stabilizer of 1_n is $O_n(\mathbb{R})$, and elements of $\mathcal{P}_n$ belong to the same $\mathrm{GL}_n(\mathbb{Z})$-orbit if and only if they are integrally equivalent.

REMARK 3.23. For $Y = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \in \mathcal{P}_2$ let z be the unique zero of $az^2 + 2bz + c = 0$ in the upper half plane H, we have then $\mathrm{Re}(z) = \frac{-b}{a}$ and $|z| = c/a$. For $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ one has

$$\begin{aligned}
(\gamma z + \delta)^2 & \left(a \left(\frac{\alpha z + \beta}{\gamma z + \delta} \right)^2 + 2b \left(\frac{\alpha z + \beta}{\gamma z + \delta} \right) + c \right) \\
&= a(\alpha z + \beta)^2 + 2b(\alpha z + \beta)(\gamma z + \delta) + c(\gamma z + \delta)^2 \\
&= z^2(a\alpha^2 + 2b\alpha\gamma + c\gamma^2) + z(2a\alpha\beta + 2b(\alpha\delta + \gamma\beta) + 2c\gamma\delta) \\
&\qquad + a\beta^2 + 2b\beta\delta + c\delta^2.
\end{aligned}$$

Hence, if $\frac{\alpha z+\beta}{\gamma z+\delta}$ is the point in H corresponding to $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$, we see that z is the point corresponding to

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

That is, if we let $\mathrm{SL}_2(\mathbb{R})$ act on H via $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right).z = \frac{\alpha z+\beta}{\gamma z+\delta}$ by fractional linear transformations, the map $\Phi : \mathcal{P} \longrightarrow H$ with $Y \longmapsto z$ as above is compatible with the $\mathrm{SL}_2(\mathbb{R})$-actions: $\Phi(g.Y) = g.\Phi(Y)$.

THEOREM 3.24. *$\mathcal{P}_n$ is a convex open set in $M_n^{\mathrm{sym}}(\mathbb{R}) = \mathbb{R}^{n(\frac{n+1}{2})}$. The closure $\overline{\mathcal{P}}_n$ of $\mathcal{P}_n$ in $M_n^{\mathrm{sym}}(\mathbb{R})$ is the set of positive semidefinite matrices in $M_n^{\mathrm{sym}}(\mathbb{R})$.*

PROOF. Obviously, $\mathcal{P}_n$ is convex and open and the closure of $\mathcal{P}_n$ in $M_n^{\mathrm{sym}}(\mathbb{R})$ is contained in the set of positive semidefinite matrices. On the other hand, if Y is positive definite and Y_1 is positive semidefinite, $\lambda Y + (1 - \lambda)Y_1$is positive definite for all $0 < \lambda \leq 1$, so that Y_1 is in the closure of $\mathcal{P}_n$. □

DEFINITION 3.25. A Minkowski reduced basis $\mathcal{B}$ and the Gram matrix $M_{\mathcal{B}} \in \mathcal{P}_n$ associated to it are called strictly reduced if the inequalities $Q(x) \geq Q(v_i)$ in Definition 3.1 are satisfied with strict inequality for all admissible $x \neq \pm v_i$.

THEOREM 3.26. *Let* $1 \leq j \leq n$,

$$\mathcal{W}_j := \{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n \setminus \{\pm \mathbf{e}_j\} \mid \gcd(x_j, \dots, x_n) = 1\}$$

be the set of reduction conditions. Let the set of satisfiable reduction conditions be defined as the set $\mathcal{W}_j^*$ *of all* $\mathbf{x} \in \mathcal{W}_j$ *for which there exists a Minkowski reduced matrix* Y *satisfying* ${}^t\mathbf{x}Y\mathbf{x} = y_{jj}$. *Then*

a) *The set* $\mathcal{R}_n^0$ *of strictly reduced matrices in* $\mathcal{P}_n$ *is equal to*

$$\{Y \in M_n^{\mathrm{sym}}(\mathbb{R}) \mid y_{11} > 0, y_{jj} < {}^t\mathbf{x}Y\mathbf{x} \quad \textit{for all } 1 \leq j \leq n, \mathbf{x} \in \mathcal{W}_j^*\}.$$

b) *For the set* $\mathcal{R}_n$ *of Minkowski reduced matrices in* $\mathcal{P}_n$ *one has*

$$\mathcal{R}_n = \{Y \in M_n^{\mathrm{sym}}(\mathbb{R}) \mid y_{11} > 0, y_{jj} \leq {}^t\mathbf{x}Y\mathbf{x} \quad \textit{for all } 1 \leq j \leq n, \mathbf{x} \in \mathcal{W}_j^*\}.$$

c) $\mathcal{W}_j^*$ *is finite.*

PROOF. For a vector $\mathbf{x}$ in $\mathcal{W}_j^*$ there exists a Minkowski reduced matrix Y and a $T \in \mathrm{GL}_n(\mathbb{Z})$ having $\mathbf{x}$ as its j-th column such that ${}^tTYT =: Y'$ is again Minkowski reduced. By Theorem 3.19 T and hence $\mathbf{x}$ has then bounded entries, which shows c).
For a), we want to show for a matrix $Y_0 \in M_n^{\mathrm{sym}}(\mathbb{R}), Y_0 \notin \mathcal{R}_n^0$ that at least one of the satisfiable reduction conditions does not hold with strict inequality for Y, i. e., that for some j there exists $\mathbf{x} \in \mathcal{W}_j^*$ with ${}^t\mathbf{x}Y\mathbf{x} \leq y_{jj}$.
For $Y_1 \in \mathcal{R}_n^0$ and $0 \leq \lambda \leq 1$ put

$$(y_{ij}^{(\lambda)}) = Y_\lambda = (1-\lambda)Y_0 + \lambda Y_1 \text{ and } w_\lambda(\mathbf{x}) = {}^t\mathbf{x}Y_\lambda\mathbf{x} \text{ for } \mathbf{x} \in \mathbb{Z}^n.$$

Let $\mu = \sup\{\lambda \in [0,1] \mid Y_\lambda \notin \mathcal{R}_n^0\}$. Then $Y_\mu \in \overline{\mathcal{R}_n^0}$ and $Y_\mu \notin \mathcal{R}_n^0$ since the set of strictly reduced matrices is open.
Since Y_μ is in the closure of $\mathcal{R}_n^0$ it satisfies all reduction conditions. If Y_μ is positive definite, it is hence reduced but not strictly reduced, hence there exist j and $\mathbf{x} \in \mathcal{W}_j^*$ with ${}^t\mathbf{x}Y_\mu\mathbf{x} = y_{jj}^{(\mu)}$. One has ${}^t\mathbf{x}Y_1\mathbf{x} > y_{jj}^{(1)}$ since $Y_1 \in \mathcal{R}_n^0$, and we see that ${}^t\mathbf{x}Y_0\mathbf{x} \leq y_{jj}^{(0)}$ must hold. Thus, Y_0 is not in the set described in a).
If Y_μ is semidefinite but not definite, one has $y_{11}^{(\mu)} = 0$ since the radical of the quadratic form has to intersect $\mathbb{Z}^n$. We see then as above $y_{11}^{(0)} \leq 0$, so that Y_0 is not in the set described in a) in this case too.
On the other hand, $\mathcal{R}_n^0$ is obviously contained in this set.

For b), $\mathcal{R}_n$ is obviously contained in the set R' on the right hand side and the closure of $\mathcal{R}_n^0$ contains R'. Since $R' \subseteq \mathcal{P}_n$ by definition and $\overline{\mathcal{R}_n^0} \cap \mathcal{P}_n \subseteq \mathcal{R}_n$ holds, we see that $\mathcal{R}_n = R'$ as asserted. □

COROLLARY 3.27. *$\mathcal{R}_n^0$ is a convex open subset of $\mathcal{P}_n$. More precisely, $\mathcal{R}_n^0$ is a convex open cone bounded by finitely many hyperplanes.*

PROOF. This follows from the theorem. □

THEOREM 3.28. *The set $\mathcal{P}_n$ has a decomposition $\mathcal{P}_n = \bigcup_{T\in \mathrm{GL}_n(\mathbb{Z})} T(\mathcal{R}_n)$ (where we put $T(\mathcal{R}_n) := \{T.Y = Y[T^{-1}] \mid Y \in \mathcal{R}_n\}$), and one has*

a) *If $T_1, T_2 \in GL_n(\mathbb{Z})$ satisfy $T_1(\mathcal{R}_n^0) \cap T_2(\mathcal{R}_n) \neq \emptyset$, the matrix $T_2^{-1}T_1$ is diagonal with entries ± 1.*
b) *If $T(\mathcal{R}_n) = \mathcal{R}_n$ holds for some $T \in GL_n(\mathbb{Z})$ the matrix T is diagonal with entries ± 1.*

PROOF. a) Let Y be strictly reduced and $T\langle Y\rangle = Y_1$ reduced, let $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ be the standard basis of $\mathbb{R}^n$.
then $\mathbf{e}_1$ is a minimum vector for Y_1, hence $T^{-1}\mathbf{e}_1$ a minimum vector for Y, and since Y is strictly reduced we must have $T^{-1}\mathbf{e}_1 = \pm\mathbf{e}_1$. In the same way we see $T^{-1}\mathbf{e}_j = \pm\mathbf{e}_j$ for $1 \leq j \leq n$.
b) follows from a).
□

THEOREM 3.29. $\Sigma = \{T \in \mathrm{GL}_n(\mathbb{Z}) \mid T(\mathcal{R}_n) \cap \mathcal{R}_n \neq \emptyset\}$ *is a finite set.*

PROOF. This follows from Theorem 3.17. □

REMARK 3.30. We have shown that the set $\mathcal{R}_n$ of Minkowski reduced matrices is a fundamental domain for the action of $GL_n(\mathbb{Z})$ on $\mathcal{P}_n$ in the sense that the translaes $T(\mathcal{R}_n)$ cover $\mathcal{P}_n$ and meet only in boundary points.

THEOREM 3.31. *The translates $T(\mathcal{R}_n)$ of the set $\mathcal{R}_n$ of Minkowski reduced matrices form a locally finite covering of $\mathcal{P}_n$, i. e., for any compact set $K \subseteq \mathcal{P}_n$ there are only finitely many translates $T(\mathcal{R}_n)$ with $T(\mathcal{R}_n) \cap K \neq \emptyset$.*

PROOF. We choose $\delta, \epsilon > 0$ with $\mathcal{R}_n \subseteq \mathcal{S}_n(\delta, \epsilon)$. For $\delta' > \delta$, $\epsilon' > \epsilon$ the set $\mathcal{R}_n$ lies then in the interior $\mathcal{S}_0$ of $\mathcal{S}_n(\delta', \epsilon')$. The covering of K by the open sets $T\mathcal{S}_0$ for $T \in \mathrm{GL}_n(\mathbb{Z}))$ has then a finite subcover by certain $T_j\mathcal{S}_0, 1 \leq j \leq r$. Each of these $T_j\mathcal{S}_0$ meets only finitely many $T\mathcal{S}_0$ by Theorem 3.17, which implies the assertion. □

THEOREM 3.32. *Let Σ_1 denote the set of all $T \in \mathrm{GL}_n(\mathbb{Z})$, for which $T\mathcal{R}_n \cap \mathcal{R}_n$ has codimension 1 in $\mathcal{R}_n$, hence dimension $\frac{n(n+1)}{2} - 1$.*
Then Σ_1 generates $\mathrm{GL}_n(\mathbb{Z})$.

PROOF. Let $T \in \mathrm{GL}_n(\mathbb{Z})$, let $Y_0 \in \mathcal{R}_n^0$ be a strictly reduced matrix. Let $K \subset T\mathcal{R}_n$ be a closed ball, let $L := \{(1-\lambda)Y_0 + \lambda Y_1 \mid 0 \leq \lambda \leq 1, Y_1 \in K\}$. Since L is compact the previous theorem implies that there are only finitely many $U \in \mathrm{GL}_n(\mathbb{Z})$ with $U\mathcal{R}_n \cap L \neq \emptyset$.
Let D be the union of all $U_1\mathcal{R}_n \cap U_2\mathcal{R}_n$ with $U_1, U_2 \in \mathrm{GL}_n(\mathbb{Z})$, $U_1\mathcal{R}_n \cap L \neq \emptyset \neq U_2\mathcal{R}_n \cap L$ for which $U_1\mathcal{R}_n \cap U_2\mathcal{R}_n$ has codimension ≥ 2 in $\mathcal{P}_n$.
Then D too has codimension ≥ 2 in $\mathcal{P}_n$, there is $Y_1 \in K$such that $L_1 := \{(1-\lambda)Y_0 + \lambda Y_1 \mid 0 \leq \lambda \leq 1\} \cap D = \emptyset$.

The line L_1 meets only finitely many $T_j\mathcal{R}_n$ ($T_j \in \mathrm{GL}_n(\mathbb{Z})$), each of these intersections is an interval, since the $T_j(\mathcal{R}_n)$ are convex sets. We write $L_1 = (T_1(\mathcal{R}_n) \cap L_1) \cup \cdots \cup (T_r(\mathcal{R}_n) \cap L_1)$ and number the T_j in such a way that the intervals $T_j(\mathcal{R}_n)$ and $T_{j+1}(\mathcal{R}_n)$ intersect and $T_1 = \mathrm{Id}, T_r = T$.
We have then $T_j^{-1}T_{j+1} \in \Sigma_1$, hence $T_{j+1} = T_jU_j$ with $U_j \in \Sigma_1$. Putting things together we obtain $T = U_1 \cdots U_r$ with $U_i \in \Sigma_1$ as asserted. □

3.4. Extreme forms and sphere packings

DEFINITION 3.33. A matrix $Y \in \mathcal{R}_n$ with $y_{11} = 1$ is called *extreme* if the determinant has a local minimum in Y as function on the hypersurface $\{Y' \in \mathcal{R}_n \mid y'_{11} = 1\}$ hat. It is called *absolutely extreme* if it is extreme and the minimum is an absolute minimum.

REMARK 3.34. a) If Y is an extreme matrix, the quadratic form Q_Y given by $Q_Y(\mathbf{x}) = \frac{1}{2}{}^t\mathbf{x}Y\mathbf{x}$ is called an extreme form and a lattice with this quadratic form is called an extreme lattice. The same term is often used for all matrices or forms proportional to Y resp. Q_Y.

b) Let $L := \bigoplus_{i=1}^n \mathbb{Z}v_i$ be a lattice on $\mathbb{R}^n$ with Gram matrix Y with respect to the basis $v_1, \dots, v_n$ and the standard scalar product and put spheres of radius $\frac{1}{2}$around the lattice points. The spheres form then a (non overlapping) lattice sphere packing in $\mathbb{R}^n$. A fundamental parallelotope of L has then volume $\det(Y)$, and the part of it that is covered by the spheres has volume $(\frac{1}{2})^n\frac{V_n}{\sqrt{\det Y}}$,where V_n is the volume of the n-dimensional unit sphere. A lattice whose Gram matrix is absolutely extreme gives therefore the densest possible lattice sphere packing in $\mathbb{R}^n$.

THEOREM 3.35. *There exists an absolutely extreme $Y \in \mathcal{R}_n$.*

PROOF. We fix a matrix $Y_0 \in \mathcal{R}_n$ with $D_0 = \det(Y_0), y_{11}^{(0)} = 1$ and put $\mathcal{R}_n^{(1)} = \{Y \in \mathcal{R}_n \mid y_{11} = 1\}$.
The set $M = \{Y \in \mathcal{R}_n^{(1)} \mid \det Y \le D_0\}$ is compact: For $Y \in M$ we have $y_{11} \cdots y_{nn} \le C \cdot D_0$ with a constant C, and therefore

$$y_{nn} \le \frac{C \cdot D_0}{y_{22} \cdots y_{n-1,n-1}} \le C \cdot D_0.$$

All y_{ij} are then bounded by $C \cdot D_0$.
Since det is a continuous function it has to assume a minimum in M. □

LEMMA 3.36 (Concavity of the determinant). *Let $Y_1 \neq Y_2 \in \mathcal{P}_n$ with* $\det Y_1 = \det Y_2 = 1$, *let* $0 < \lambda < 1$.
Then $\det((1-\lambda)Y_1 + \lambda Y_2) > 1$.

PROOF. Y_1 and Y_2 can be simultaneously diagonalized by $Y_j \longmapsto {}^tTY_jT$ for some $T \in \mathrm{GL}_n(\mathbb{R})$, i.e., we may assume Y_1, Y_2 to be diagonal matrices with entries a_i resp. b_i.

If we put

$$D(\lambda) := \det((1-\lambda)Y_1 + \lambda Y_2) = \prod_{i=1}^{n}(a_i + \lambda(b_i - a_i)),$$

we have $D(0) = D(1) = 1$ and

$$\frac{d^2}{d\lambda^2}\log D(\lambda) = -\sum_{i=1}^{n}\left(\frac{b_i - a}{a_i + \lambda(b_i - a_i)}\right)^2 < 0$$

for $\lambda \in (0,1)$.
This implies $\log D(\lambda) > 0$ in $(0,1)$, hence $D(\lambda) > 1$ in $(0,1)$. □

COROLLARY 3.37 (Arithmetic geometric mean inequality). *For* $1 \leq j \leq n$ *let* $\alpha_j, \beta_j, \gamma_j > 0$*,* $(\alpha_1, \dots, \alpha_n)$ *and* $(\beta_1, \dots, \beta_n)$ *not proportional, the* γ_j *not all equal. We have then*

a) $\prod_{i=1}^{n}(\alpha_i + \beta_i)^{\frac{1}{n}} > \prod_{i=1}^{n}(\alpha_i)^{\frac{1}{n}} + \prod_{i=1}^{n}(\beta_i)^{\frac{1}{n}}$
b) $\frac{1}{n}\sum_{i=1}^{n}\gamma_i > (\prod_{i=1}^{n}\gamma_i)^{\frac{1}{n}}$
c) *The hypersurface* $\det Y = 1$ *lies strictly above the tangent hyperplane at any point* Y_0.

PROOF. for a) let $A = (\prod_{i=1}^{n}\alpha_i)^{\frac{1}{n}}$, $B = (\prod_{i=1}^{n}\beta_i)^{\frac{1}{n}}$ and let $t \in [0,1]$ be such that $\frac{B}{A} = \frac{t}{1-t}$. There is $c > 0$ with $B = ct, A = c(1-t)$, we put $a_i = \frac{\alpha_i}{c(1-t)}$ and $b_i = \frac{\beta_i}{ct}$.
Then $\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} b_i = 1$, $(a_1, \dots, a_n) \neq (b_1, \dots, b_n)$, and by the previous lemma we have

$$\begin{aligned}\left(\prod_{i=1}^{n}(\alpha_i + \beta_i)\right)^{\frac{1}{n}} &= c \cdot \prod_{i=1}^{n}((1-t)a_i + tb_i)^{\frac{1}{n}} \\ &= c = A + B \\ &= \left(\prod_{i=1}^{n}\alpha_i\right)^{\frac{1}{n}} + \prod_{i=1}^{n}(\beta_i)^{\frac{1}{n}}.\end{aligned}$$

For b) we consider a) with $(\beta_1, \dots, \beta_n) = (1, \dots, 1)$, $\alpha_i = t\gamma_i$. We have then for all t

$$\prod_{i=1}^{n}(1 + t\gamma_i) > \left(1 + t\prod_{i=1}^{n}(\gamma_i)^{\frac{1}{n}}\right)^n.$$

We view this as polynomial in t and see for $t \to 0$ by comparing the terms at t that

$$\gamma_1 + \dots + \gamma_n > n\prod_{i=1}^{n}(\gamma_i)^{\frac{1}{n}}.$$

For c) we consider Y_0, Y_1 with $\det Y_0 = \det Y_1 = 1$, $Y_0 \neq Y_1$. As above we may assume that Y_0, Y_1 are diagonal matrices with entries a_i, b_i respectively.

The gradient of det in Y_0 is the diagonal matrix with entries $\frac{1}{a_i}$ which has scalar product n with Y_0, so that the tangent hyperplane at Y_0 is given as $\{X = (x_{ij}) \mid \sum_{i=1}^{n} \frac{x_{ii}}{a_i} = n\}$.
By b) we have

$$\frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{a_i} > \left(\prod_{i=1}^{n}\frac{b_i}{a_i}\right)^{\frac{1}{n}} = 1,$$

hence

$$\sum_{i=1}^{n}\frac{b_i}{a_i} > n,$$

so that Y_1 lies above the tangent hyperplane. □

THEOREM 3.38. *An extreme matrix $Y \in \mathcal{R}_n^1$ is a corner of $\mathcal{R}_n^1$.*

PROOF. If Y were not a corner one could find $Y_1 \neq Y_2$ in $\mathcal{R}_n^1$ such that $Y = (1-\lambda)Y_1 + \lambda Y_2$ holds for some $0 < \lambda < 1$, and we can choose Y_1, Y_2 as close to Y as we want.
We may again assume Y_1, Y_2 to be diagonal matrices with entries $(a_1, \dots, a_n)$ resp. $(b_1, \dots, b_n)$ and have

$$\begin{aligned}
(\det Y)^{\frac{1}{n}} &= \prod_{i=1}^{n}((1-\lambda)a_i + \lambda b_i)^{\frac{1}{n}} \\
&> (1-\lambda)\prod_{i=1}^{n} a_i^{\frac{1}{n}} + \lambda \prod_{i=1}^{n} b_i^{\frac{1}{n}} \\
&= (1-\lambda)(\det Y_1)^{\frac{1}{n}} + \lambda(\det Y_2)^{\frac{1}{n}}.
\end{aligned}$$

One sees that one of $\det(Y_1), \det(Y_2)$ must be smaller than $\det Y$, in contradiction to the assumption that Y is extreme. □

COROLLARY 3.39. *An extreme matrix (which is known to exist by Theorem 3.35) has rational coefficients.*

PROOF. Being a corner of $\mathcal{R}_n^1$ means to lie in a one-dimensional intersection of the finitely many hyperplanes bounding the set $\mathcal{R}_n$ of reduced matrices. Since all these hyperplanes are given by homogeneous linear equations with coefficients in $\mathbb{Z}$ we see that an extreme matrix Y is a multiple of a rational matrix. Since $y_{11} = 1$, the matrix Y itself has to be rational. □

COROLLARY 3.40. *Let $Y \in \mathcal{R}_n^1$ be extreme, let $\{\mathbf{x}_1, \dots, \mathbf{x}_N \mid {}^t\mathbf{x}_j Y \mathbf{x}_j = 1\} \subseteq \mathbb{Z}^n$ be the set of all minimum vectors.*
Then Y is the only solution in $M_n^{\mathrm{sym}}(\mathbb{R}^n)$ of the system of equations ${}^t\mathbf{x}_j Y \mathbf{x}_j = 1$ for $1 \leq j \leq n$. In particular, the minimum vectors $\mathbf{x}_1, \dots, \mathbf{x}_N$ span the space $\mathbb{Q}^n$.

PROOF. It the set of solutions of this system of linear equations was at least one dimensional, we could again find positive definite reduced matrices

Y_1 und Y_2 such that Y is on the line connecting them and such that both of them satisfy all N equations ${}^t\mathbf{x}_j Y_i \mathbf{x}_j = 1$.
If Y_1 and Y_2 are sufficiently close to Y the forms Q_{Y_i} given by $2Q_{Y_i}(\mathbf{x}) = {}^t\mathbf{x}Y_i\mathbf{x}$ assume their minimum on one of the $\mathbf{x}_j$ for Y, in particular they have minimum 1 and are in $\mathcal{R}_n^1$, which contradicts the fact that Y is a corner of $\mathcal{R}_n^1$.
If finally the $\mathbf{x}_j$ spanned a genuine subspace of $\mathbb{Q}^n$, the system ${}^t\mathbf{x}_j Y \mathbf{x}_j = 1$ for $1 \leq j \leq N$ had rank smaller than $\frac{n(n+1)}{2}$. □

3.5. The LLL algorithm

DEFINITION 3.41. Let $\mathcal{B} = (v_1, \ldots, v_n)$ be a basis of the $\mathbb{Z}$-lattice L and let $L_i := \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_i$ for $1 \leq i \leq n$, $L_0 := \{\mathbf{0}\}$.
For $x \in V$ denote by $\tilde{p}_i(x)$ the orthogonal projection of x onto $(\mathbb{R}L_i)^\perp$ (with $\tilde{p}_0 = \mathrm{Id}$) and by $\{\tilde{p}_{j-1}v_j =: v_j'\}$ the Gram-Schmidt orthogonalization of $\mathcal{B}$, write $v_j' = v_j - \sum_{i=1}^{j-1} c_{ij} v_i'$.
The basis $\mathcal{B}$ is called Hermite-Korkine-Zolotarev reduced (HKZ-reduced), if the following conditions are satisfied:

a) $|c_{ij}| \leq \frac{1}{2}$ for all i, j.
b) $Q(\tilde{p}_{j-1}v_j)$ is minimal in $Q(\tilde{p}_{j-1}(L)) \setminus \{0\}$ for $1 \leq j \leq n$.

A symmetric matrix A is called HKZ-reduced if it is the Gram matrix of an HKZ-reduced basis of a lattice.

To see that HKZ-reduced bases exist we need the following lemma:

LEMMA 3.42. *Let R be an integral domain with field of quotients F, let Λ be a lattice of full rank on the n-dimensional vector space V over F. Let $V = U_1 \oplus \cdots \oplus U_r$ be a direct sum decomposition and put $W_j' = U_1 \oplus \cdots \oplus U_j$, $W_j = U_{j+1} \oplus \cdots \oplus U_r$ for $0 \leq j < r$, denote by p_j the projection of V onto W_j with respect to the decomposition $V = W_j' \oplus W_j$.*
For $1 \leq j \leq r$ let L_j be a lattice on U_j such that $p_j(L_{j+1}) \subseteq W_j$ is a primitive sublattice of $p_j(\Lambda) \subseteq W_j$ for $0 \leq j < r$, in particular, L_1 is a primitive sublattice of U_1.
Then $\Lambda = L_1 \oplus \cdots \oplus L_r$ holds.
In particular, if $r = n$ and $L_j = Rv_j$ is free of rank 1, the vectors $v_1, \ldots, v_n$ form a basis of Λ.

PROOF. We prove this by induction on r, beginning with $r = 2$. Let $v \in \Lambda, v = u + p_1(v)$ with $u_1 \in U_1, p_1(v) \in U_2 \cap p_1(\Lambda) = p_1(L_2)$, hence $p_1(v) = p_1(v')$ with $v' \in L_2$. We have then $v - v' \in \ker(p_1) \cap \Lambda = U_1 \cap \Lambda = L_1$, hence $v \in L_1 \oplus L_2$.
Let now $r > 2$ and assume that the assertion is true for decompositions into $r' < r$ subspaces.
Applying this inductive assumption to the lattice $p_1(\Lambda)$ and the sublattices $p_1(L_j)$ for $2 \leq j \leq r$ we see that one has $p_1(\Lambda) = p_1(L_2) \oplus \cdots \oplus p_1(L_r) = p_1(L_2 \oplus \cdots \oplus L_r)$.

But then the case $r = 2$ with the decomposition $V = U_1 \oplus (U_2 \oplus \cdots \oplus U_r)$ shows that indeed $\Lambda = L_1 \oplus (L_2 \oplus \cdots \oplus L_r) = L_1 \oplus \cdots \oplus L_r$ is true. □

THEOREM 3.43. *Let Λ be a positive definite $\mathbb{Z}$-lattice. Then Λ has an HKZ-reduced basis.*

PROOF. With notations as in Definition 3.41 we let $v_1, \dots, v_n$ be vectors in Λ for which $Q(\tilde{p}_{j-1}(v_j))$ is minimal in $Q(\tilde{p}_{j-1}(\Lambda)) \setminus \{0\}$ and hence primitive. By the Lemma the v_j form a basis of Λ. Subtracting a vector $y \in L_{j-1} = \oplus_{i=1}^{j-1} \mathbb{Z} v_i$ from v_j doesn't change $v'_j = \tilde{p}_{j-1}(v_j)$, and by Lemma 3.11 we can choose the vector y in such a way that the modified v_j satisfy $v'_j = v_j - \sum_{i=1}^{j-1} c_{ij} v'_i$ with $|c_{ij}| \leq \frac{1}{2}$ for $1 \leq i \leq j-1$. □

THEOREM 3.44. *The Gram matrix of a Hermite-Korkine-Zolotarev reduced basis is in $\mathcal{S}_n(\frac{4}{3}, \frac{1}{2})$.*

PROOF. By $\tilde{p}_j(v_{j+1}) = v_{j+1} - c_{j,j+1} v'_j - \sum_{i=1}^{j-1} c_{i,j+1} v'_i$ we have $\tilde{p}_j(v_{j+1}) + c_{j,j+1} \tilde{p}_{j-1} v_j = v_{j+1} - y$ with $y \in L_{j-1}$.
Thus

$$\begin{aligned} Q(\tilde{p}_{j-1} v_j) &\leq Q(\tilde{p}_{j-1} v_{j+1}) \\ &= Q(\tilde{p}_j v_{j+1} + c_{j,j+1} \tilde{p}_{j-1} v_j) \\ &\leq Q(\tilde{p}_j v_{j+1}) + \frac{1}{4} Q(\tilde{p}_{j-1} v_j), \end{aligned}$$

which gives $\frac{3}{4} Q(\tilde{p}_{j-1} v_j) \leq Q(\tilde{p}_j v_{j+1})$ or $h_j \leq \frac{4}{3} h_{j+1}$. The bound on the c_{ij} is part of the definition of HKZ-reduced. □

A slight weakening of the conditions for being HKZ-reduced has the advantage of being algorithmically easier to use, it gives the conditions of Lenstra, Lenstra and Lovasz for their concept of reduction [**27**].

DEFINITION 3.45. Let $\frac{1}{4} < \alpha \leq 1$ be given. The basis $\mathcal{B} = (v_1, \dots, v_n)$ of the lattice Λ is called α-LLL reduced if

a) $|c_{ij}| \leq \frac{1}{2}$ for all i, j.
b)
$$\alpha Q(\tilde{p}_{j-1} v_j) \leq Q(\tilde{p}_{j-1} v_{j+1}) \quad \text{for } 1 \leq j \leq n-1.$$

A symmetric matrix A is called α-LLL reduced if it is the Gram matrix of an α-LLL reduced basis of a lattice.

THEOREM 3.46. *The Gram matrix of an α-LLL reduced basis is in the Siegel domain $\mathcal{S}_n(\frac{1}{\alpha - \frac{1}{4}}, \frac{1}{2})$. Moreover, an α-LLL reduced basis satisfies*

a) $Q(v_1) \leq (\alpha - \frac{1}{4})^{1-n} \mu_1$.
b) $Q(v_1) \cdots Q(v_n) \leq (\alpha - \frac{1}{4})^{-n(n-1)/2} \det_B(\Lambda)$.
c) $Q(v_1) \leq (\alpha - \frac{1}{4})^{\frac{1-n}{2}} (\det_B(\Lambda))^{\frac{1}{n}}$.

PROOF. From

$$\begin{aligned} Q(\tilde{p}_{j-1}v_j) &\leq \alpha^{-1}Q(\tilde{p}_{j-1}v_{j+1}) \\ &= \alpha^{-1}Q(\tilde{p}_j v_{j+1} + c_{j,j+1}\tilde{p}_{j-1}v_j) \\ &\leq \alpha^{-1}(Q(\tilde{p}_j v_{j+1}) + \frac{1}{4}Q(\tilde{p}_{j-1}v_j)) \end{aligned}$$

we obtain

$$\begin{aligned} Q(\tilde{p}_{j-1}v_j)(1 - \frac{\alpha^{-1}}{4}) &\leq \alpha^{-1}Q(\tilde{p}_j v_{j+1}), \\ Q(\tilde{p}_{j-1}v_j) &\leq \frac{1}{\alpha - \frac{1}{4}}Q(\tilde{p}_j v_{j+1}), \end{aligned}$$

which says that the Gram matrix is indeed in $\mathcal{S}_n((\alpha - \frac{1}{4})^{-1}, \frac{1}{2})$. We see further

$$Q(\tilde{p}_{j-1}v_j) \geq (\frac{1}{\alpha - \frac{1}{4}})^{-j+1}Q(v_1),$$

hence

$$\min_j Q(v'_j) \geq (\alpha - \frac{1}{4})^{n-1}Q(v_1)$$

or $Q(v_1) \leq (\alpha - \frac{1}{4})^{1-n} \min_j Q(v'_j)$.
Let now $\mathbf{0} \neq x \in L$ be any non zero vector. Let j be such that $x = \sum_{i=1}^{j} a_i v_i = a_j v_j + y_1$ holds with $a_j \neq 0, y_1 \in L_{j-1}$. We have then $x = a_j v'_j + y_2$ with $y_2 \in \mathbb{R}L_{j-1}$, hence $Q(x) = a_j^2 Q(v'_j) + Q(y_2) \geq Q(v'_j)$. This implies $\min_j Q(v'_j) \leq \mu_1$, and the assertion in a) is proven.
For b) and c) notice that

$$Q(v_1) \leq (\alpha - \frac{1}{4})^{1-j}Q(\tilde{p}_{j-1}v_j)$$

implies

$$\begin{aligned} Q(v_1)^n &\leq (\alpha - \frac{1}{4})^{-\sum_{i=0}^{n-1} i}\prod_{j=1}^{n} Q(v'_j) \\ &= (\alpha - \frac{1}{4})^{-\frac{n(n-1)}{2}}\det{}_B(\Lambda). \end{aligned}$$

We have therefore

$$Q(v_1) \leq (\alpha - \frac{1}{4})^{-\frac{n-1}{2}}\det{}_B(\Lambda)^{\frac{1}{n}}.$$

Moreover,

$$\begin{aligned} Q(v_j) &\leq Q(\tilde{p}_{j-1}v_j) + \frac{1}{4}\sum_{i=1}^{j-1} Q(\tilde{p}_{i-1}v_i) \\ &\leq Q(\tilde{p}_{j-1}v_j)(1 + \frac{1}{4}\sum_{i=1}^{j-1}(\alpha - \frac{1}{4})^{-j+i}), \end{aligned}$$

which implies

$$\begin{aligned}
Q(v_j) &\leq Q(v_j')(1+\frac{1}{4}\frac{(\alpha-\frac{1}{4})^{1-j}-1}{1-(\alpha-\frac{1}{4})}) \\
&= Q(v_j')(1+\frac{(\alpha-\frac{1}{4})^{1-j}-1}{5-4\alpha}) \\
&\leq Q(v_j')(\alpha-\frac{1}{4})^{1-j}.
\end{aligned}$$

From this we get

$$\prod_{i=1}^{n} Q(v_i) \leq \det(M_{\mathcal{B}}) \cdot (\alpha-\frac{1}{4})^{\frac{-n(n-1)}{2}}$$

as asserted. $\square$

REMARK 3.47. If one just says LLL-reduced without specifying an α, one usually means the case $\alpha = \frac{3}{4}$. In that case the estimate for the length of the first basis vector becomes $Q(v_1) \leq 2^{n-1}\mu_1$.

PROPOSITION 3.48. *Let $v_1, \dots, v_n$ be a basis of the lattice Λ with integral Gram matrix. Then for $\frac{1}{4} < \alpha < 1$ the following algorithm produces an α-LLL reduced basis $w_1, \dots, w_n$ in a number of steps which is polynomial in n and in* $\max_{1\leq i\leq n} \log Q(v_i)$.

I) $w_i = v_i$ *for* $i = 1, \dots, n$

II) *For* $i = 1, \dots, n$ *write*

$$w_i - \tilde{p}_{i-1}w_i = \sum_{j=1}^{i-1} \alpha_{ji}w_j,$$

where $\tilde{p}_j$ denotes the orthogonal projection onto $(\mathbb{R}w_1+\cdots+\mathbb{R}w_j)^{\perp}$.

Let $\tilde{\alpha}_{ji}$ be the closest integer to α_{ji}, replace w_i by $w_i - \sum_{j=1}^{i-1}\tilde{\alpha}_{ji}w_j$.

(After this step $w_i - \tilde{p}_{i-1}w_i = \sum_{j=1}^{i-1}\alpha_{ji}w_j$ with $|\alpha_{ji}| \leq \frac{1}{2}$ for all i, j.)

III) *If $Q(\tilde{p}_{j-1}w_j) \leq \alpha^{-1}Q(\tilde{p}_{j-1}w_{j+1})$ holds for all j, terminate, output the w_i as an α-LLL reduced basis.*

Otherwise, let k be the first index with $Q(\tilde{p}_{k-1}w_{k+1}) < \alpha Q(\tilde{p}_{k-1}w_k)$. Interchange w_k and w_{k+1} and return to the beginning of step II).

(We have then for $i \leq k$ $|\alpha_{ji}| \leq \frac{1}{2}$ for $j \leq i-1$, and for $i = k+1$ one has $|\alpha_{j,k+1}| \leq \frac{1}{2}$ for all $j < k$. If one performs the transformation $w_{k+1} \longmapsto w_{k+1} - \sum_{j=1}^{k}\tilde{\alpha}_{j,k+1}w_j$ the vector $\tilde{p}_{k-1}w_{k+1}$ changes and it is possible that the comparison of $Q(\tilde{p}_{j-1}w_j)$ with $\alpha^{-1}Q(\tilde{p}_{j-1}w_{j+1})$ in step III) may stop at $j = k$ again.)

PROOF. We put

$$\begin{aligned} D(w_1, \dots, w_n) &= \textstyle\prod_{i=1}^n Q(\tilde{p}_{i-1} w_i)^{n-i+1} \\ &= \textstyle\prod_{k=1}^n \det((B(w_i, w_j))_{i,j=1}^k) = \prod_{k=1}^n D_k \end{aligned}$$

Step II of the algorithm doesn't change D.
From $D_j = \prod_{i=1}^j Q(\tilde{p}_{i-1} w_i)$ and $Q(\tilde{p}_{j-1} w_j) > \alpha^{-1} Q(\tilde{p}_{j-1} w_{j+1})$ we see that step III replaces D_j by $D'_j < \alpha D_j$.
Each application of step II therefore reduces $D(w_1, \dots, w_n)$ at least by the factor $\alpha < 1$. Since $D(w_1, \dots, w_n) \geq 1$ holds, step III can be applied at most $\log_\alpha D$ times, where we put $D := D(v_1, \dots, v_n)$.
On the other hand, we have

$$\begin{aligned} D_j(v_1, \dots, v_n) &= \prod_{i=1}^n Q(v'_j) \\ &\leq \prod_{i=1}^j Q(v_j), \end{aligned}$$

which implies

$$D(v_1, \dots, v_n) \leq ((\max_i Q(v_i))^{\frac{n(n+1)}{2}}.$$

Step III is therefore applied at most

$$C \cdot \frac{n(n+1)}{2} \log(\max_i 2Q(v_i))$$

times. Since Step II consists of $\sim n^2$ operations, we see that the total number of operations is indeed polynomial in n and in the $Q(v_i)$. The running time of each of these operations depends on the size of the $Q(v'_j), Q(w_j)$ occurring. A computation of the orthogonal projections occurring shows that all the coefficients α_{ji} and hence all the $Q(v'_j), Q(w_j)$ can be bounded in the same way. □

We consider the following application:

THEOREM 3.49. *Let $\alpha_1, \dots, \alpha_n \in \mathbb{Q}$ and $0 < \epsilon < 1$ be given. Then one can find $p_1, \dots, p_n$, $q \in \mathbb{Z}$ satisfying*

$$|p_i - q\alpha_i| \leq \epsilon \quad \textit{and} \quad 0 < q \leq 2^{\frac{n(n+1)}{4}} \epsilon^{-n}$$

in a number of steps which is polynomial in $\frac{1}{\epsilon}$ and the logarithms of the $|\alpha_i|$.

PROOF. consider the matrix

$$Y = \begin{pmatrix} 1 & 0 & \cdots & 0 & \alpha_1 \\ & \ddots & & & \vdots \\ 0 & & & 1 & \alpha_n \\ & & & & \epsilon/Q \end{pmatrix}$$

for some $Q > 0$ and let Λ be the lattice spanned by the columns $v_1, \dots, v_{n+1}$ of Y.

For a vector $w = \sum_{i=1}^{n+1} p_i v_i$ with $\sqrt{Q(w)} \leq \epsilon$ one has $\sqrt{Q(w)} \geq |p_i - q\alpha_i|$ $(i = 1, \ldots, n)$ with $q = -p_{n+1}$ and $\epsilon \geq \sqrt{Q(w)} \geq \epsilon q/Q$, hence $q \leq Q$. Using $Q = 2^{\frac{n(n+1)}{4}}\epsilon^{-n}$ we know by the proposition that we can find $w \in \Lambda$ satisfying

$$\begin{aligned} Q(w) &\leq 2^{\frac{(n-\alpha)}{2}} \det Y^{\frac{2}{n}} \\ &\leq 2^{\frac{n}{2}}(\frac{\epsilon}{Q})^{\frac{2}{n+1}} \end{aligned}$$

in polynomial time. We have then $\sqrt{Q(w)} \leq \epsilon$, hence $q \leq 2^{\frac{n(n+1)}{4}}\epsilon^{-n}$, and the inequalities $|p_i - q\alpha_i| \leq \epsilon$ are satisfied. $\square$

CHAPTER 4

Reduction Theory of Indefinite Quadratic Forms

The reduction theory of indefinite quadratic forms is more complicated than that of definite forms because the finiteness arguments used in the latter case are not valid here. Hermite's idea was to play the problem back to the study of associated definite quadratic forms. We formulate most of the theory in terms of matrices. As usual we write $A[T] :=^t TAT$ for $A \in M_n^{\mathrm{sym}}(\mathbb{R}), T \in M(n \times r, \mathbb{R})$, in particular for $T = \mathbf{x} \in \mathbb{R}^n = M(n \times 1, \mathbb{R})$. We also write $Q_A(\mathbf{x}) = \frac{1}{2}A[\mathbf{x}]$.

4.1. The space of majorants

DEFINITION 4.1. Let $A \in M_n^{\mathrm{sym}}(\mathbb{R})$ be a non singular symmetric matrix. A positive definite matrix $P \in M_n^{\mathrm{sym}}(\mathbb{R})$ is called a *(Hermite) majorant* of A if

$$A[\mathbf{x}] = |^t\mathbf{x}A\mathbf{x}| \leq^t \mathbf{x}P\mathbf{x} = P[\mathbf{x}] \text{ for all } \mathbf{x} \in \mathbb{R}^n.$$

Let the positive definite matrices in $M_n^{\mathrm{sym}}(\mathbb{R})$ be partially ordered by

$$P_1 \leq P_2 \text{ if and only if } P_1[\mathbf{x}] \leq P_2[\mathbf{x}] \text{ for all } \mathbf{x} \in \mathbb{R}^n.$$

Then a majorant P of A is called a *minimal majorant* if and only if it is minimal with respect to this ordering among the majorants of A.
The set of minimal majorants of $A \in M_n^{\mathrm{sym}}(\mathbb{R})$ is denoted by $\mathfrak{H}(A)$ and is called the *space of (minimal) majorants* of A.

LEMMA 4.2. *With notations as above the following statements are equivalent:*

a) $P \in \mathfrak{H}(A)$.
b) *There is a decomposition* $\mathbb{R}^n = V_1 \oplus V_2$ *of* $\mathbb{R}^n$ *into subspaces* V_1, V_2 *such that* V_1, V_2 *are orthogonal to each other with respect to both* Q_A, Q_P *(respectively their associated symmetric bilinear forms* b_A, b_P*) and such that*

$$\begin{aligned} Q_A|_{V_1} &= Q_P|_{V_1} \\ Q_A|_{V_2} &= -Q_P|_{V_2}. \end{aligned}$$

c) *There exists* $T \in GL_n(\mathbb{R})$ *satisfying*

$$A[T] = E_{a,b}, P[T] = E_n,$$

where (a, b) *is the signature of A and* $E_{a,b}$ *denotes the diagonal matrix with a entries* $+1$ *and b entries* -1.
d) $(AP^{-1})^2 = E_n$.

PROOF. By linear algebra we can diagonalize A and P simultaneously by a suitable change of basis $A \mapsto A[T], P \mapsto P[T]$, we may therefore assume

$$\begin{aligned} Q_M(\mathbf{x}) &= \sum_{i=1} 1^a x_i^2 - \sum_{j=1}^{b} x_{i+a}^2 \\ Q_P(\mathbf{x}) &= \sum_{i=1}^{n} c_i x_i^2 \end{aligned}$$

with $c_i \in \mathbb{R}, c_i > 0$. It is then clear that P is a minimal majorant of A if and only if all c_i are 1, it is equally clear that this condition is equivalent to the validity of both b) and c).
If c) is satisfied with $T \in GL_n(\mathbb{R})$ we have

$$\begin{aligned} AP^{-1}AP^{-1} &= ({}^tT^{-1}E_{a,b}T^{-1})(T^tT)({}^tT^{-1}E_{a,b}T^{-1})(T^tT) \\ &= {}^tT^{-1}E_n^tT \\ &= E_n, \end{aligned}$$

hence d). If conversely d) holds it is also true for $A[T], P[T]$ in place of A, T, and we can again assume without loss of generality that A and P are diagonal as above. But then the condition d) implies that all the c_i^2 and hence the c_i are 1, so that c) is satisfied. □

COROLLARY 4.3. a) *There is a natural bijection between $\mathfrak{H}(A)$ and the set of subspaces V_1 of $\mathbb{R}^n$ which are maximal positive definite with respect to Q_A. It is given by associating to $P \in \mathfrak{H}(A)$ the radical of the quadratic form $Q_A - Q_P$ and to V_1 the matrix P associated to the quadratic form $Q_P(\mathbf{x}) = Q_A(p_1\mathbf{x}) - Q_A(p_2\mathbf{x})$, where p_1, p_2 are the orthogonal projections onto V_1 and onto the orthogonal complement V_2 of V_1 with respect to Q_A respectively.*

b) *The orthogonal group $O_{Q_A}(\mathbb{R})$ acts transitively on $\mathfrak{H}(A)$, the stabilizer of $P \in \mathfrak{H}(A)$ is conjugate to $O_a(\mathbb{R}) \times O_b(\mathbb{R})$, where $O_m(\mathbb{R})$ denotes the orthogonal group of the standard scalar product on $\mathbb{R}^m$.*

PROOF. The first assertion follows directly from the lemma and its proof. For the second assertion we use Witt's extension theorem (Theorem 1.41) to find for given totally positive spaces V_1, V_1' a $\phi \in O_{Q_A}(\mathbb{R})$ with $\phi(V_1) = V_1'$. Considering the splitting $\mathbb{R}^n = V_1 \oplus V_2$ associated to $P \in \mathfrak{H}(A)$ we may choose bases of V_1, V_2 with respect to which Q_M has matrix E_a resp. $-E_b$, in the basis of V obtained from these the stabilizer of P has the required shape. □

REMARK 4.4. The stabilizer in the corollary is obviously a compact subgroup of the orthogonal group $O_{Q_A}(\mathbb{R})$ of the real quadratic form of signature (a, b). In fact it is maximal compact, and every compact subgroup K is contained in a conjugate of it. To see this, denote by $\langle , \rangle$ a scalar product on $V = \mathbb{R}^n$ which is invariant under the action of K, such a scalar product can be obtained from the standard scalar product by integration over K. Since the symmetric bilinear form b_A associated to Q_A is non degenerate, there exists a unique isomorphism $f : V \to V$ satisfying $\langle f(v), w\rangle = b_A(v, w)$ for all $v, w \in V$. In view of

$$\langle f(v), w\rangle = b_A(v, w) = b_A(w, v) = \langle f(w), v\rangle$$

the map f is self adjoint with respect to $\langle , \rangle$ so that V is the orthogonal (with respect to $\langle , \rangle$) sum of the eigenspaces V_λ of f. Moreover, we have for $k \in K$ and $v, w \in V$

$$\langle kf(v), w\rangle = \langle f(v), k^{-1}w\rangle = b_A(v, k^{-1}w) = b_A(kv, w),$$

so that $kf(v) = f(kv)$ for all $k \in K, v \in V$. In particular, k leaves the eigenspaces V_λ invariant.
On V_λ we have $2Q_A(v) = b_A(v, v) = \langle f(v), v\rangle = \lambda\langle v, v\rangle$, which implies that Q is positive definite on the sum V_+ of the V_λ for $\lambda > 0$, negative definite on the sum V_- of the V_λ with $\lambda < 0$. It follows that K is contained in the group $O_{V_+}(\mathbb{R}) \times O_{V_-}(\mathbb{R})$ as asserted.
The space $mfH(A)$ of minimal majorants of A can therefore be viewed as a homogeneous space $K\backslash O_{Q_A}(\mathbb{R})$ with a maximal compact subgroup K.

4.2. Hermite reduction of indefinite forms

DEFINITION 4.5. With notations as before the matrix A is called Hermite reduced if the space $\mathfrak{H}(A)$ of its minimal majorants contains a Minkowski reduced matrix.

LEMMA 4.6. *Every non degenerate real symmetric matrix A is integrally equivalent to a Hermite reduced matrix.*

PROOF. Let P be a minimal majorant of A and choose $T \in GL_n(\mathbb{Z})$ so that $P[T]$ is Minkowski reduced. Then $A[T]$ is Hermite reduced. □

We want to prove a finiteness result for integral Hermite reduced matrices. For this we need first an auxiliary lemma.

LEMMA 4.7. *Let $\delta > 0, \epsilon > 0, n \in \mathbb{N}$ be given. Then there exists ϵ_1 depending on n, ϵ such that for any positive definite symmetric matrix P in the Siegel domain $\mathcal{S}_n(\delta, \epsilon)$ one has $JP^{-1}J \in \mathcal{S}_n(\delta, \epsilon_1)$, where* $J = \begin{pmatrix} 0 & \dots & 0 & 1 \\ & & \iddots & \\ & \iddots & & \\ 1 & 0 & \dots & 0 \end{pmatrix}$.

PROOF. We write $P = H[C]$ where the entries h_j of the diagonal matrix H satisfy $h_j \le \delta h_{j+1}$ and the entries c_{ij} of the upper triangular matrix T are bounded in absolute value by ϵ. with $C_1 :=^t C^{-1}[J], H_1 = H^{-1}[J]$ we have $P^{-1}[J] = H_1[C_1]$. The coefficients of the upper triangular matrix C_1 are then bounded in absolute value by a suitable $\epsilon_1 > 0$, and the diagonal entries $h'_1 = h_n^{-1}, \dots, h'_n = h_1^{-1}$ of H_1 satisfy $h'_i \le \delta h'_{i+1}$. □

THEOREM 4.8. *For fixed $n \in \mathbb{N}, 0 \neq d \in \mathbb{Z}$ there exist only finitely many integral Hermite reduced matrices $A \in M_n^{\mathrm{sym}}(\mathbb{Z})$ with $\det(A) = d$. Moreover, for $n \in \mathbb{N}$ fixed there exists a constant $c(n) \in \mathbb{R}$ such that for any integral Hermite reduced $A = (a_{ij}) \in M_n^{\mathrm{sym}}(\mathbb{Z})$ of determinant d with anisotropic Q_A one has $|a_{ij}| \leq c(n)d$.*

PROOF. We set $d = \det(A)$ and consider first the case that Q_A is anisotropic. We have then $|Q_A(\mathbf{x})| \geq 1$ for all $\mathbf{x} \in \mathbb{Z}^n \setminus \{0\}$ and hence $Q_P(\mathbf{x}) \geq 1$ for all $\mathbf{x} \in \mathbb{Z}^n \setminus \{0\}$ for any minimal majorant P of A. The successive minima $\mu_j(P)$ of such a P satisfy then

$$\mu_1(P) \dots \mu_n(P) \leq \gamma_n^n \det(P) = \gamma_n^n d,$$

by Theorem3.9, where γ_n is Hermite's constant. Since we have $\mu_j(P) \geq 1$ for all j this implies $\mu_j(P) \leq \gamma_n^n d$ for all j. If P is Minkowski reduced the coefficients p_{ij} of P are bounded in absolute value by $c'(n)d$ for a suitable constant $c'(n)$ by Theorem 3.12. From this we get

$$\begin{aligned} |a_{ij}| &= |Q_A(\mathbf{e}_i + \mathbf{e}_j) - Q_A(\mathbf{e}_i) - Q_A(\mathbf{e}_j)| \\ &\leq Q_P(\mathbf{e}_i + \mathbf{e}_j) + Q_P(\mathbf{e}_i) + Q_P(\mathbf{e}_j) \\ \leq c(n)d \end{aligned}$$

with a suitable constant $c(n)$.
In the case that Q_A is isotropic we consider again a Minkowski reduced minimal majorant P of the integral Hermite reduced matrix A. Let $\mathbf{f}^{(1)}, \dots, \mathbf{f}^{(n)} \in \mathbb{Z}^n$ be successive minimum vectors of Q_P with components $f_j^{(i)}$, let $\delta, \epsilon > 0$ be such that $P \in \mathcal{S}_n(\delta, \epsilon)$, where δ, ϵ depend only on n by Theorem 3.17. By Lemma 3.20 there exists then a constant $c'(n)$ with $|f_j^{(i)}| \leq c'(n)$ for all i, j. By the lemma there exists $\epsilon_1 = \epsilon_1(n) > 0$ depending only on n with $P^{-1}[J] \in \mathcal{S}_n(\delta, \epsilon_1)$, and we have $P = AP^{-1}A = (P^{-1}[J])[T]$, where $T = JA \in M_n^{\mathrm{sym}}(\mathbb{Z})$ with $|\det(T)| = |d|$. The vectors $T\mathbf{f}^{(i)}$ are therefore successive minimum vectors of the lattice $T\mathbb{Z}^n$ with respect to $P^{-1}[J]$, with the lattice $T\mathbb{Z}^n$ having index $|d|$ in $\mathbb{Z}^n$. By Lemma 3.20 the coefficients of the $T\mathbf{f}^{(i)}$ in terms of the basis of $T\mathbb{Z}^n$ consisting of the $T\mathbf{e}_i$ are then bounded in absolute value by a constant depending only on n, and since $T\mathbb{Z}^n$ has index $|d|$ in $\mathbb{Z}^n$ the coefficients of the matrix $F' = TF$ with columns $T\mathbf{f}^{(i)}$ are bounded in absolute value by some $c'(n, d)$. But then the coefficients of $T = F'F^{-1}$ and hence the coefficients of $A = JT$ are bounded in absolute value by a suitable $c(n, d)$ too. □

4.3. Compactness results for anisotropic forms

For anisotropic A we can also prove two further boundedness results.

THEOREM 4.9. *Let $A \in M_n^{\mathrm{sym}}(\mathbb{Z})$ with anisotropic Q_A. There exists a constant $c(A)$ such that for all $S \in =_{Q_A}(\mathbb{R})$ there exists $T \in O_{Q_A}(\mathbb{R}; \mathbb{Z}^n) := GL_n(\mathbb{Z}) \cap O_{Q_A}(\mathbb{R})$ such that all coefficients of ST are bounded in absolute value by $c(A)$.*

In other words, there exists a compact fundamental domain for the action of $O_{Q_A}(\mathbb{R};\mathbb{Z}^n)$ *on* $O_{Q_A}(\mathbb{R})$ *by translations.*

PROOF. By the previous theorem there are only finitely many Hermite reduced integral matrices $A = A_1[U_1], A_2 = A[U_2], \dots, A_r = M[U_r]$ (with $U_i \in GL_n(\mathbb{Z})$) which are integrally equivalent to A. for each of these we choose Minkowski reduced minimal majorants $P_i \in \mathfrak{H}(A_i)$ and have $P_i[U_i^{-1}] \in \mathfrak{H}(A)$. Since $O_{Q_A}(\mathbb{R})$ acts transitively on $\mathfrak{H}(A)$ we obtain $S_i \in O_{Q_A}(\mathbb{R})$ with $P_i[U_i^{-1}] = P[S_i]$ which implies $P_i = P[S_iU_i]$ for $1 \leq i \leq r$.
Let now $S \in O_{Q_A}(\mathbb{R})$ be given and choose $U \in GL_n(\mathbb{Z})$ such that $P[SU] = P[S][U]$ is a Minkowski reduced majorant of $A[S][U] = A[U]$. Then $A[U]$ is Hermite reduced and integrally equivalent to A, hence equal to $A_j = A[U_j]$ for some j, which gives $UU_j^{-1} =: T \in O_{Q_A}(\mathbb{R};\mathbb{Z}^n)$. Moreover, as in the proof of the anisotropic case in the previous theorem we can bound the coefficients of $P[S][U]$ by $c_1(n)d$ for a suitable constant $c_1(n)$ depending only on n.
With $V := (S_jU_j)^{-1}SU$ we have $P[SU] = P_j[V]$. Since the coefficients of $P[SU]$ are bounded and P_j is positive definite, the coefficients of V are bounded by some constant $c'(n,d)$. Since there are only finitely many possibilities (not depending on S) for the S_j, U_j, this implies that the coefficients of $ST = S_jU_jVU_j^{-1}$ are bounded by some constant depending on A but not on S, which proves the assertion. □

REMARK 4.10. In the isotropic case Siegel proved that there is a fundamental domain of finite volume with respect to the Haar measure on the orthogonal group $O_{Q_A}(\mathbb{R})$. A compact fundamental domain does not exist in that case.

THEOREM 4.11. *Let* $A \in M_n^{\mathrm{sym}}(\mathbb{Z})$ *with* Q_A *anisotropic.*
There exists a constant $c_1(A)$ *such that for any* $\mathbf{0} \neq \mathbf{x} \in \mathbb{R}^n$ *there exists* $T \in O_{Q_A}(\mathbb{R};\mathbb{Z}^n)$ *with* $\|T\mathbf{x}\|^2 \leq c_1(A)Q_A(\mathbf{x})$.
In other words, each nonzero $O_{Q_A}(\mathbb{R};\mathbb{Z}^n)$*-orbit in* $\mathbb{R}^n$ *contains vectors of bounded length.*

PROOF. We choose a vector $\mathbf{y} \in \mathbb{R}^n$ with $Q_A(\mathbf{x}) = Q_A(\mathbf{y})$ and such that the coefficients of $\mathbf{y}$ are bounded by a constant multiple of $|Q_A(\mathbf{x})|^{1/2}$ (e.g., by multiplying a fixed vector of Q_A-value in $\{\pm 1\}$ by $|Q_A(\mathbf{x})|^{1/2}$).
By Witt's extension theorem (Theorem 1.41) there exists $S \in O_{Q_A}(\mathbb{R})$ with $S\mathbf{x} = \mathbf{y}$, and by the previous theorem we find a constant $c(A)$ and $T \in O_{Q_A}(\mathbb{R};\mathbb{Z}^n)$ such that the coefficients of TS^{-1} are bounded in absolute value by $c(A)$. Then $T\mathbf{x} = TS^{-1}\mathbf{y}$ is as asserted. □

CHAPTER 5

Quadratic Lattices over Discrete Valuation Rings

As is well known from algebraic number theory, an important tool for the study of number rings is the study of their completions with respect to prime ideals, i.e., the study of local fiels and their valuation rings. Our principal interest in this chapter therefore is the theory of quadratic forms or modules over local fields and their valuation rings. Since many of the results are valid in the more general context of local rings and their completions, we will work in this more general context whenever this doesn't complicate the exposition and will indicate differences in results and proofs where these occur. Since over a local ring all finitely generated projective modules are free we will restrict our attention to free modules.

5.1. Local rings, discrete valuation rings, local fields

We recall some definitions and results from commutative algebra:

DEFINITION 5.1. A discrete valuation ring R is an integral domain satisfying the following equivalent conditions:

a) R is a principal ideal domain with precisely one class of prime elements modulo units.
b) There is a surjective map v from the nonzero elements of the field of fractions F of R to $\mathbb{Z}$, called a discrete (additive) valuation, such that
    i) $v(ab) = v(a) + v(b)$ for all $a, b \in F^\times$.
    ii) $v(a + b) \geq \min(v(a), v(b))$ for all $a, b \in F^\times$ with $a + b \neq 0$.
    iii) $R = \{a \in F^\times \mid v(a) \geq 0\} \cup \{0\}$.
c) R is a local ring with a unique non zero prime ideal P.

The field $k := R/P$ is called the residue field of R, the field of fractions F is called a discretely valued field.
The discrete valuation ring and its field of fractions are called complete if they are complete metric spaces with respect to the metric derived from the absolute value given by $|a|_v = c^{-v(a)}$ for $a \neq 0$, $|0|_v = 0$, where $0 < c < 1$ is arbitrary.

DEFINITION 5.2. A valuation ring is an integral domain R with field of fractions F such that for all $0 \neq a \in F$ one has $a \in R$ or $a^{-1} \in R$.

THEOREM 5.3. *Let R be a valuation ring with field of fractions F.*

a) *Every finitely generated ideal in R is principal, every finitely generated R-submodule of F is free of rank* 1.

b) *The ideals are totally ordered by inclusion, the same is true for the R-submodules of F.*
c) *A valuation ring is a discrete valuation ring if and only if it is noetherian.*
d) *There is a totally ordered abelian group G and a surjective map v from $F^\times$ to G , called an (additive) valuation, such that*
   i) $v(ab) = v(a) + v(b)$ *for all* $a, b \in F^\times$.
   ii) $v(a + b) \geq \min(v(a), v(b))$ *for all* $a, b \in F^\times$ *with* $a + b \neq 0$.
   iii) $R = \{a \in F^\times \mid v(a) \geq 0\} \cup \{0\}$.

THEOREM 5.4. *Let R be a complete discrete valuation ring with field of quotients F and maximal ideal P and additive valuation v.*
Then the following are equivalent:

a) *F is a local field (i.e., it is locally compact with respect to the metric induced by v).*
b) *R is compact with respect to the metric induced by v.*
c) *R/P is finite.*

REMARK 5.5. Whenever convenient we will extend the valuation v to all of F by setting $v(0) = \infty$ and write $v(b) < v(0)$ for all $b \neq 0$ accordingly.

THEOREM 5.6. *Let R be a discrete valuation ring with field of quotients F and additive valuation v.*
Then there is an up to valuation preserving isomorphism unique complete discrete valuation ring $\hat{R} \supseteq R$ (the completion of R) with field of quotients $\hat{F} \supseteq F$ (the completion of F with respect to v) and valuation $\hat{v}$ extending v such that R resp. F is dense in $\hat{R}$ resp. $\hat{F}$ with respect to the metric induced by $\hat{v}$.
One has $R/P \cong \hat{R}/\hat{P}$, where $\hat{P} \supseteq P$ is the maximal ideal of $\hat{R}$, in particular, $\hat{F}$ is a local field if and only if R/P is finite.

EXAMPLE 5.7. For any prime number p the ring $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, p \nmid b\}$ is a discrete valuation ring with maximal ideal $P = p\mathbb{Z}_{(p)}$. Its completion is the ring $\mathbb{Z}_p$ of p-adic integers, with field of quotients $\mathbb{Q}_p$, the field of p-adic rationals. Similarly, for a number field K with ring of integers $\mathfrak{o}_K$, the localization of $\mathfrak{o}_K$ at a prime ideal P is a discrete valuation ring, and the completion of K with respect to the corresponding valuation is denoted by K_P.
It is well known that all non archimedean local fields (i.e, local fields different form $\mathbb{R}, \mathbb{C}$) arise in this way either from an algebraic number field or an algebraic function field, i.e., a separable extension of the field of rational functions over a finite field.

A key property of complete local rings is the validity of Hensel's lemma, i.e., the fact that zeros or factorisations of polynomials modulo sufficiently high powers of the maximal ideal can be lifted to genuine zeroes respectively factorisations:

THEOREM 5.8 (Hensel's Lemma). *Let R be a local ring with maximal ideal P and residue field $k = R/P$.*

a) *Let $f \in R[X]$ and $a \in R$ be such that $f(a) \in f'(a)^2 P$, where f' is the formal derivative of f.*
   Then for all $n \in \mathbb{N}$ there is $a_n \in R$ with $a_{n+1} - a_n \in f'(a)P$ and $f(a_{n+1}) \in f(a)P^n$.
   If R complete with respect to the P-adic topology, there is $b \in R$ with $f(b) = 0$ and $b - a \in f'(a)P$, in particular $b \in a + P$.
b) *Let $f \in R[X]$ be a monic polynomial of degree n such that the reduction $\bar{f} \in k[X]$ of f modulo P has a factorization $\bar{f} = \tilde{g}\tilde{h}$ into coprime polynomials $\tilde{g}, \tilde{h} \in k[X]$ of degrees $r, n - r$, assume R to be noetherian and complete with respect to the P-adic topology and put $k = R/P$. Then there are polynomials $g, h \in R[X]$ of degrees $r, n - r$ with $\bar{g} = \tilde{g}, \bar{h} = \tilde{h}, f = gh$.*

PROOF. The usual proof by induction on n of a) for (complete) discrete valuation rings carries over to the present more general situation: We write $f(a) = (f'(a))^2 y$ with $y \in P$ and put $a_1 := a$. Let $n \geq 1$ and assume that a_n with the asserted properties has been found, assume in addition that $f'(a_n)R = f'(a)R$ holds, in particular we have $f(a_n) \in (f'(a_n))^2 P$.
We put $a_{n+1} = a_n - f'(a_n)y \in a_n + P$ and obtain

$$\begin{aligned} f(a_{n+1}) &= f(a_n) - f'(a_n)f'(a_n)y + f(a_n)yz_1 \\ &= f(a_n)yz_1 \\ &\in f(a_n)P \end{aligned}$$

with $z_1 \in R$ by looking at the Taylor expansion of F around a_n.
Similarly, we have $f'(a_{n+1}) = f'(a_n) + f'(a_n)yz_2 \in f'(a_n)(1 + P)$ with $z_2 \in R$, so that $f'(a_{n+1})R = f'(a_n)R$ and $f(a_{n+1}) \in (f'(a_{n+1}))^2 P$ hold and a_{n+1} is as required. If R is complete, the sequence of the a_n converges to a limit b, and since $\cap_{n=1}^{\infty} P^n = \{0\}$ holds for a complete local ring (using the definition of [**1, 13**]), one has $f(b) = 0$.
In a similar way, the usual proof of b) for discrete valuation rings is easily modified for the present situation. □

REMARK 5.9. a) If R is a discrete valuation ring with valuation v, the condition in a) above becomes $v(f(a)) > 2v(f'(a))$, and the assertions for a_n resp. for b become $v(a_n - a) \geq v(f(a)) - v(f'(a))$ and $v(f(a_n)) \geq v(f(a) + (n-1)(v(f(a)) - 2v(f'(a))) \geq v(f(a)) + n - 1$ respectively $v(b - a) \geq v(f(a)) - v(f'(a))$.
b) A different proof for complete local rings can be found in [**4, 13**].

5.2. Orthogonal decomposition of lattices over valuation rings

THEOREM 5.10. *Let R be a valuation ring with field of fractions F, let (V, Q) be a regular quadratic space over F and let Λ be a free R-lattice on V with $b(\Lambda, \Lambda) =: I \subseteq R$.*

Then Λ contains an I-modular sublattice K which splits off orthogonally in Λ, the orthogonal complement $K^\perp$ is free.

PROOF. The ideal $I \subseteq R$ is finitely generated (by the $b(v_i, v_j)$ where the v_i, v_j run through a basis of Λ), hence principal, say $I = aR$ with $a \in R, a \neq 0$.
If there exists $v \in \Lambda$ with $b(v,v)R = I$, the one dimensional lattice $K = Rv$ is as desired. Otherwise, we can find linearly independent $v, w \in \Lambda$ with $b(v,w) = a$ and $b(v,v) \in aP, b(w,w) \in aP$. We put $K = Rv + Rw$ and see that $K^\# = a^{-1}K$, i.e., K is I-modular.
In both cases, Lemma 1.68 shows that K splits off orthogonally in Λ. In the special case that R is a discrete valuation ring, the freeness of $K^\perp$ follows immediately from the main theorem on modules over principal ideal domains. For a general valuation ring, since K and Λ are free, its complement $K^\perp$ is stably free, which for modules over a valuation ring (or more generally a Bezout ring) implies free. □

COROLLARY 5.11. *Any lattice Λ as in the theorem has a decomposition into an orthogonal sum of modular lattices of rank* 1 *or* 2*. If* 2 *is a unit in R it has an orthogonal basis.*

PROOF. This follows by induction from the proof of the theorem. □

DEFINITION AND COROLLARY 5.12 (Jordan decomposition). *Let Λ be as in the theorem with $b(\Lambda, \Lambda) = I \subseteq R$.*
Then there are nonzero principal ideals $J_1 = I \supsetneq J_2 \supsetneq \cdots \supsetneq J_r$ in R and a decomposition $\Lambda = K_1 \perp \cdots \perp K_r$ into an orthogonal sum of J_i-modular lattices K_i.
Such a decomposition is called a Jordan decomposition.

PROOF. Again the assertion follows from the theorem by induction. □

REMARK 5.13.
a) Our proof is practically the same as the usual proof (see e. g. [**28**]) for discrete valuation rings. It seems not to be possible to generalize it further to an arbitrary local ring, at least not easily.
b) The fact that this decomposition is possible for arbitrary valuation rings has been noticed by Zemel [**41**].
c) If 2 is not a unit in R we will call the lattice Λ totally even if it has a Jordan decomposition into even modular lattices. Equivalently, $Q(x) \in b(x, \Lambda)$ holds for all $x \in \Lambda$.
d) The name "Jordan decomposition" for an orthogonal decomposition as above has probably first beeen used by O'Meara. It is unclear whether there is a historical reason for this or whether he just used this name in analogy to the Jordan normal form of an endomorphism and the corresponding decomposition of the underlying vector space into invariant subspaces in linear algebra.

LEMMA 5.14. *Let Λ as above have a Jordan decomposition as above with ideals $J_i = c_i R$.*

Then one has $\Lambda^\# = c_1^{-1}K_1 \perp \cdots \perp c_r^{-1}K_r$ *and* $c_r\Lambda^\# \subseteq \Lambda$.

5.3. Hensel's lemma and lifting of representations

For quadratic forms and their isometries we have the following specialized version of Hensel's Lemma.

THEOREM 5.15 (Kneser's Hensel Lemma for quadratic forms). *Let R be a local integral domain with maximal ideal P and field of fractions F, let (V, Q) and (W, Q') be finite dimensional quadratic spaces over F with associated symmetric bilinear forms b, b' and let L, M be free submodules of V, W respectively. Let $I \subseteq R$ be an ideal with $IQ'(M) \subseteq P$.*
Let $f : L \to W$ be an R-linear map with $f(L) \subseteq M^\# := \{z \in W \mid b'(z, M) \subseteq R\}$ and write $\widetilde{b'}_f$ for the linear map from W to $\mathrm{Hom}_R(L, F)$ *with $\widetilde{b'}_f(z)(x) = b'(f(x), z)$ for all $x \in L$.*
Assume that one has $Q'(f(x)) \equiv Q(x) \bmod I$ for all $x \in L$ and $L^* = \widetilde{b'}_f(M) + PL^*$.
Then there is an R- linear map $f' : L \to W$ with $f'(x) \equiv f(x) \bmod IM$ and $Q'(f'(x)) \equiv Q(x) \bmod IP$ for all $x \in L$. Moreover, f' also satisfies the condition above, i.e., we have $L^* = \widetilde{b'}_{f'}(M)+PL^*$, so that we can iterate the above procedure and improve the congruence for $Q'(f'(x))$ as much as desired.
If R is complete with respect to the P-adic topology there exists an R-linear isometric map $\phi : (L, Q) \to (W, Q')$ satisfying $\phi(x) \equiv f(x) \bmod IM$ for all $x \in L$.

PROOF. The proof is an easy modification of the original proof of Kneser in [**19**]:
There exists (see Lemma 1.12) an I-valued R-bilinear form β on L such that $\beta(x, x) = Q'(f(x)) - Q(x)$ for all $x \in L$, and for fixed $y \in L$ we have the R-linear form $\lambda_y : L \to I$ given by $\lambda_y(x) = \beta(x, y)$ for $x \in L$.
By assumption we have $\mathrm{Hom}_R(L, I) = IL^* = \widetilde{b'}_f(IM) + \mathrm{Hom}_R(L, IP)$, so there exists a vector $g'(y) \in IM$ satisfying $\widetilde{b'}_f(g'(y))(x) \equiv -\beta(x, y) \bmod IP$ for all $x \in L$. We let y run through a basis $(y_1, \dots, y_r)$ of L and denote by $g : L \to IM$ the R-linear map with $g(y_j) = g'(y_j)$ for $1 \le j \le r$, it satisfies $\widetilde{b'}_f(g(y))(x) \equiv -\beta(x, y) \bmod IP$ for all $x, y \in L$.
Setting $f' = f + g$ we have $f' \equiv f \bmod IM$ and

$$\begin{aligned} Q'(f'(x)) &= Q'(f(x)) + b'(f(x), g(x)) + Q'(g(x)) \\ &= Q(x) + \beta(x, x) + \widetilde{b'}_f(g(x))(x) + Q'(g(x)) \\ &\equiv Q(x) \bmod IP, \end{aligned}$$

as asserted. Finally, for $x \in L$ and $z \in M$ we have $b'(f'(x), z) = b'(f(x), z)+ b'(g(x), z)$ with $b'(g(x), z) \in b'(IM, M) \subseteq IQ'(M) \subseteq P$, so that $\widetilde{b'}_{f'}(z) \in \widetilde{b'}_f(z) + PL^*$ holds for all $z \in M$, and we see that indeed $L^* = \widetilde{b'}_{f'}(M) + PL^*$is true.

If R is complete with respect to the P-adic topology, we can then obtain a sequence of linear maps f_k which converges to an isometric linear map ϕ. $\square$

REMARK 5.16. The proof remains valid if we omit the condition that R should be an integral domain and replace the field of fractions F by the total ring of fractions $\tilde{R}$.

COROLLARY 5.17. *With the notations as in the theorem assume that* $\mathrm{rk}(L) = \dim(V) = \dim(W)$, *that* (V,Q) *and* (W,Q') *are regular, and that* R *is complete with respect to the* P*-adic topology. Let* $J \subseteq R$ *be an ideal with* $JQ(L^\#) \subseteq R$, *let* $f : L \to K \subseteq W$ *be an* R*-linear isomorphism satisfying* $Q'(f(x)) \equiv Q(x) \bmod JP^k$ *for all* $x \in L$ *for some* $k > 0$.
Then there is an isometry $\phi : L \to K'$ *with* $\phi(x) \equiv f(x) \bmod P^kJK^\#$ *for all* $x \in L$. *In particular, if* $k > 0$ *satisfies* $JP^kK^\# \subseteq K$ *the quadratic modules* $(L,Q),(K,Q')$ *are isometric.*
In particular, two free regular quadratic modules $(L,Q),(K,Q')$ *over* R *(i.e.,* $Q(L), Q'(K) \subseteq R, L^\# = L, K^\# = K$*) are isometric if and only if they are isometric modulo* P.

PROOF. We take $M = K^\#$ in the theorem and obtain the assertion. $\square$

REMARK 5.18. An ideal J as above always exists: Let $(v_1,\dots,v_n)$ be a basis of $L^\#$. The R-module J' generated by $Q(L^\#)$ is then generated by the $Q(v_j), b(v_i,v_j)$. The ideal J generated by the product of the denominators of the $Q(v_j), b(v_i,v_j)$, when these are written as fractions of elements of R, is then as required.
If R is a discrete valuation ring, we can write $J' = P^{-\ell}$ for some integer ℓ above and have $J = P^\ell$. One calls the ideal P^ℓ the level of L.

COROLLARY 5.19. *Let* R *be a local integral domain with maximal ideal* P *and field of fractions* F, *let* (V,Q) *and* (W,Q') *be finite dimensional quadratic spaces over* F *with associated symmetric bilinear forms* b, b' *and let* L, M *be free submodules of* V, W *respectively.*

a) *Assume that* (L,Q) *is a regular quadratic module (phrased differently: An even unimodular* R*-lattice) and let* $f : L \to M$ *be an* R*-linear map satisfying* $Q'(f(x)) \equiv Q(x) \bmod P$ *for all* $x \in L$.
   Then there exists an R*-linear isometric map* $\phi : L \to M$ *with* $\phi(x) \equiv f(x) \bmod PM$ *for all* $x \in L$.
   Equivalently, an isometry modulo P *of* L *into* M *can be lifted to an isometry from* L *into* M *whose reduction modulo* PM *it is.*
b) *Assume that* (M,Q') *is a regular quadratic module over* R *(an even unimodular* R*-lattice) and let* $f : L \to M$ *be an injective* R*-linear map satisfying* $Q'(f(x)) \equiv Q(x) \bmod P$ *for all* $x \in L$ *such that* $f(L)$ *is a primitive submodule of* M.
   Then there exists an R*-linear isometric map* $\phi : L \to M$ *with* $\phi(x) \equiv f(x) \bmod PM$ *for all* $x \in L$. *Equivalently, an isometry*

modulo P of L into M with primitive image can be lifted to an isometry from L into M whose reduction modulo PM it is.

PROOF. a) Let $(v_1, \dots, v_r)$ be an R-basis of L. The Gram matrix of b' with respect to $(f(v_1), \dots, f(v_r))$ has entries congruent modulo P to the $b(v_i, v_j)$ in R and hence determinant in $R^\times$. The R-lattice $(f(L), Q')$ is hence regular, and application of the previous corollary to L and $K = f(L)$ gives the assertion.

b) We have $PQ'(M) \subseteq P$ and $f(L) \subseteq M^\# = M$ by assumption. Let $\varphi \in L^*$. Since f is injective we can write $\varphi = {}^t f(\psi)$ for some linear form ψ on $f(L) \subseteq M$, and since $f(L)$ is a direct summand of M by assumption we can extend ψ to a linear form $\tilde{\psi}$ on M. Since (M, Q') is regular there exists $z \in M$ with $b'(z, y) = \tilde{\psi}(y)$ for all $y \in M$, in particular we have $b'(f(x), z) = \varphi(x)$ for all $x \in L$. We have shown that $\widetilde{b'}_f(M) = L^*$, so that application of the theorem gives the assertion.

□

REMARK 5.20. If we denote by X the set of isometric R- embeddings of L into M in either of the above two situations and by $\bar{X}$ the set of isometric R/PR-embeddings of L/PL into M/PM, the corollary asserts that the reduction map from X to $\bar{X}$ is surjective. From a geometric point of view this is often expressed by saying that X is smooth over R.

COROLLARY 5.21. *Let R be a complete valuation ring with quotient field F, let (V, Q) be a non degenerate quadratic space over F, let L be an R-lattice on V which is totally even (see Remark 5.13).*
Then any Jordan decomposition $L = L'_0 \perp \cdots \perp L'_s$ of L has even components L'_i with $s = t$ and L'_i is isometric to L_i for all i.

PROOF. We may assume that L_0 is not zero. Of course L'_0 has to be even and nonzero if that is true for L_0. Since L_1 is even, the radical of the quadratic space L/PL over R/P with the modulo P reduced quadratic form is equal to its bilinear radical, and both L_0/PL_0, L'_0/PL'_0 are are isometric to the the quotient of L/PL modulo its (bilinear or quadratic) radical, hence are isometric to each other. By the previous corollary we have $L_0 \cong L'_0$. By the Witt Theorem for local rings (Theorem 1.43) we have that $L_1 \perp \cdots \perp L_t \cong L'_1 \perp \cdots \perp L'_s$, and the assertion follows by induction on the dimension of V. □

REMARK 5.22. It is known that the decomposition is not unique if $2 \in P$ and there are modular components which are not even.

COROLLARY 5.23. *Let R be a complete local ring with maximal ideal M and $a \in R^*$, assume that $2 \neq 0$ in R.*
Then a is a square in R if and only if a is congruent to a square modulo $4P$.

PROOF. Let F be the total ring of fractions of R and $V = Fv$ be a free module of rank 1 over F with quadratic form Q given by $Q(cv) = ac^2$, let

$L = Rv$. Let similarly $W = Fw$ with $Q'(w) = 1$ and $K = Rw$. We have $L^\# = R\frac{v}{2}$ with $4PQ(L^\#) \subseteq P$ and $4PL^\# \subseteq L$. If $a \equiv b^2 \bmod 4P$ holds, the linear map f given by $f(v) = bw$ satisfies $Q'(f(x)) \equiv Q(x) \bmod 4P$ for all $x \in L$ and can be lifted to an isometry, which implies that a is a square in R. The other direction is trivial. $\square$

REMARK 5.24. The assertion of the corollary can also be proven using the first version of Hensel's Lemma for the polynomial $X^2 - a$.

THEOREM 5.25. *Let R be a complete local ring with maximal ideal P, residue field $k = R/P$ and field of quotients F. Let (M, Q) be a free quadratic module over R with associated symmetric bilinear form b and denote by $\bar{M}$ the k-vector space M/PM with the modulo P reduced quadratic form $\bar{Q}$.*
Let $a \in R^\times$ be such that $\bar{a} = a + P \in k$ is represented by $(\bar{M}, \bar{Q})$. If $\mathrm{char}(k) = 2$ *assume in addition that there is such a representation by a vector generating a regularly embedded subspace of $\bar{M}$. Then a is represented by M.*
In particular, if (M, Q) is regular of rank ≥ 2 and k is finite, all units in R are represented by (M, Q).

PROOF. By assumption, there exist $y \in M$ with $Q(y) + P = \bar{a}$ and $z \in M$ with $b(z, y) \in R^\times$. Let $L = Rv$ be a free module of rank 1 with quadratic form Q_1 given by $Q_1(v) = a$. Then Theorem 5.15 is applicable to L, M with $I = P$, and we obtain an isometric linear map $\phi : L \to M$ which gives $x = \phi(v) \in M$ with $Q(x) = a$.
If (M, Q) is regular, the reduction $\bar{M}$ is regular too, and if k is finite it represents all of k by Corollary 2.8, and a representing one dimensional subspace is regularly embedded since $\bar{M}$ is regular. $\square$

THEOREM 5.26. *With notations as above assume that $(\bar{M}, \bar{Q})$ contains a hyperbolic plane.*
Then M contains a regular hyperbolic plane H and can be decomposed as $M = M' \perp H$.
In particular, M splits off a regular hyperbolic plane if k is finite, $\mathrm{rk}(M) \geq 3$ *and $(\bar{M}, \bar{Q})$ is regular or half regular.*

PROOF. This is again a direct consequence of Theorem 5.15. The assertion for finite k follows from Corollary 2.5 which guarantees an isotropic vector in $\bar{M}$, by the (half)-regularity assumption the space generated by it is regularly embedded into $\bar{M}$. Theorem 1.38 gives then a hyperbolic plane contained in $\bar{M}$. $\square$

5.4. Maximal lattices

THEOREM 5.27. *Let R be a complete valuation ring with field of fractions F, maximal ideal P and residue field k.*
Let (V, Q) be a regular or half regular anisotropic quadratic space over F, let I be an ideal in R.

Then $M_I := \{x \in V \mid Q(x) \in I\}$ is an R-module.
If R is a discrete valuation ring, M_I is the unique I-maximal lattice on V.

PROOF. Let $v, w \in M_I$ and assume that $a := b(v, w) \notin I$ and hence $Ra \nsubseteq I$ holds. Since R is a valuation ring, this implies that we have $I \subsetneq Ra$ and hence $Q(v) \in Pa, Q(w) \in Pa$. If v, w were linearly dependent $b(v, w) \in I$ would follow, since then one of the vectors were an R-multiple of the other one. The reduction of the free R-module $Rv + Rw$ with the quadratic form $a^{-1}Q$ modulo P is then a regular quadratic space over k with determinant -1, hence isometric to a hyperbolic plane. By Corollary 5.17, $Rv + Rw$ with $a^{-1}Q$ is a regular hyperbolic plane, in particular isotropic, which contradicts the assumption that (V, Q) is anisotropic.
So we have $b(v, w) \in I$ for all $v, w \in M_I$, and we see that M_I is an R-module.
If R is a discrete valuation ring, it is a principal ideal domain and any R-submodule of a finite dimensional F-vector space is free. That M_I has rank $\dim(V)$ is trivial. □

REMARK 5.28. a) It is not clear whether M_I is free
b) If R is a discrete valuation ring we write $M_k := M_{P^k}$ for $k \in \mathbb{N}_0$.

COROLLARY 5.29. *Let R be a complete discrete valuation ring and (V, Q) a regular or half regular quadratic space over its field of fractions F, let $I \subseteq R$ be an ideal.*
Then all I-maximal lattices on V are isometric.

PROOF. By scaling the quadratic form we can assume $I = R$. If Λ is a maximal lattice on V we have $\Lambda = H \perp \Lambda_1$, where H is regular hyperbolic of rank $2\,\mathrm{ind}(V, Q)$ and Λ_1 is maximal on the anisotropic space V_1 by Theorem 2.19. Since the isometry class of V_1 is uniquely determined by Theorem 1.47, the assertion follows from the previous theorem. □

THEOREM 5.30. *Let R be a complete discrete valuation ring with field of fractions F and finite residue field k, let π be a prime element of R.*
Then there is up to isometry precisely one anisotropic quadratic space of dimension 2 over F on which the maximal lattice is regular.

PROOF. For each such space (with M_k as above) the quadratic space $M_0/\pi M_0$ is the unique anisotropic regular quadratic space of dimension 2 over k. This determines the isometry class of (M_0, Q) and hence that of (V, Q). □

THEOREM 5.31. *Let R be a complete discrete valuation ring with field of fractions F and finite residue field k, let π be a prime element of R.*
Then every regular or half regular anisotropic quadratic space (V, Q) over F has dimension ≤ 4, and up to isometry there exists precisely one anisotropic regular quadratic space of dimension 4 over F. This space has determinant 1 and isuniversal.

PROOF. With notations as in the previous theorem the quadratic forms Q respectively $\pi^{-1}Q$ induce k-valued quadratic forms on the k vector spaces M_0/M_1 and M_1/M_2 which are anisotropic. Hence these k-vector spaces are of dimension ≤ 2 by Corollary 2.5. Since one has

$$\dim_F(V) = \dim_k(M_0/M_2) = \dim_k(M_0/M_1) + \dim_k(M_1/M_2),$$

the first part of the assertion follows.
If V has dimension 4, we see that both M_0/M_1 and M_1/M_2 have dimension 2 over k. We let $L \subseteq M_0$ be a regular preimage of rank 2 of M_0/M_1 and see that L splits M_0, so one has $M_0 = L \perp L'$ with a sublattice $L' \subseteq M_1$ of rank 2. Since L is anisotropic modulo P we have $M_1 \cap L = \pi L$, $M_1 = L' \perp \pi L$. This implies that M_1/M_2 and $L'/\pi L'$ with the quadratic forms induced by $\pi^{-1}Q$ are regular 2- dimensional and isometric over k, which determines the isometry class of $(L', \pi^{-1}Q)$ and hence that of (M_0, Q) and of (V, Q). The existence of a space as described also follows. $\square$

CHAPTER 6

Quadratic Forms over Global Fields and their Integers

We are now ready to see how the properties of quadratic forms over number fields and number rings (ore slightly more generally global fields and rings of integers in these) can be studied with the help of the local theory developed in the previous chapter, in particular we will prove the local-global principle of Minkowski and Hasse.
In this chapter F will be a global field, i.e., an algebraic number field or an algebraic function field, with $\operatorname{char}(F) \neq 2$. We write Σ_F for the set of places of F (i.e., the set of equivalence classes of non trivial valuations) and identify Σ_F with a set of representatives for these equivalence classes, using $|a|_v$ to denote the v-value of $a \in F$. For $v \in \Sigma_F$ we denote by F_v the completion of F with respect to the valuation v and use $|\cdot|_v$ for the extension of the valuation to F_v as well. The group of ideles of F is denoted by J_F, with J_F^2 denoting the subgroup of squares of ideles. $F^\times$ is identified with the set of principal ideles. The ring of adeles is $\mathbb{A}_F$ and F is identified with its image in $\mathbb{A}_F$ under the diagonal embedding.

If F is a number field we let R be its ring of integers. More generally, for some finite set T of places of F containing all archimedean places we consider the ring $R = R_T := \{a \in F^\times \mid |a|_v \leq 1 \text{ for all } v \notin T\}$ and call it a ring of integers in F or the T-integers in F. If F is a global function field we consider similarly R_T as above for any finite non empty set of places of F and call these rings again rings of integers in F. We denote then by $R_v \subseteq F_v$ the completion of R with respect to v for $v \notin T$ (equivalently: The closure of R in F_v) and set $R_v = F_v$ for $v \in T$.
The most important special case will of course be $F = \mathbb{Q}$ with $R = \mathbb{Z}$ or $R = \mathbb{Z}[\frac{1}{a}]$ for some nonzero $a \in \mathbb{Z}$.

6.1. The local-global-principle of Minkowski and Hasse

THEOREM 6.1 (Strong Minkowski-Hasse Theorem). *Let (V, Q) be a regular quadratic space of dimension n over F and assume that the completions $V_v = F_v \otimes V$ are isotropic with respect to the natural extension of Q to V_v for all non trivial valuations v of F.*
Then (V, Q) is isotropic.

PROOF. We will use without proof three results of algebraic number theory, the first two of which are special cases of theorems from global class field theory. The last one is actually valid for all fields, for $F = \mathbb{Q}$ it is an easy consequence of the chinese remainder theorem.

- Let $a \in F$ be a square in all completions F_v. Then a is a square in F.
- Let E/F be a quadratic extension of F and assume that $a \in F$ is a norm in all extensions E_w/F_v for valuations v of F with extension w to E.
  Then a is a norm of some $b \in E$.
- (Weak approximation theorem) Let T be a finite set of inequivalent non trivial valuations of F and let $a_v \in F_v$ be given for all $v \in T$. Then for any $\epsilon > 0$ there exists $a \in F$ with $|a - a_v|_v < \epsilon$ for all $v \in T$.

We can assume that V represents 1, so that for $n = 2$ there is an orthogonal basis (x_1, x_2) of V with $Q(b_1 w_1 + b_2 w_2) = b_1^2 - d b_2^2$ for some $d \in F^\times$. If (V_v, Q) is isotropic for all v we see that d is a square in all F_v, hence in F, so (V, Q) is hyperbolic and hence isotropic.
For $n = 3$ we choose again an orthogonal basis (x_1, x_2, x_3) of V with $Q(x_1) = 1, Q(x_2) = -d, Q(x_3) = -c$. If b is a square, (V, Q) is hyperbolic and we are done. Otherwise we put $U = Fx_1 + Fx_2, W = Fx_3$ Since (V_v, Q) is isotropic for all v, the equation $a_1^2 - da_2^2 = c$ is solvable in F_v for all v, so that c is a norm in all local extensions E_w/F_v with $E = F(\sqrt{d})$. Then c is a norm in E/F, so $c = a_1^2 - da_2^2$ is solvable in F, so (V, Q) is isotropic.
For $n = 4$ assume first that $\det(V, Q)$ is a square. Over F_v the space (V_v, Q) is isotropic, hence spits off a hyperbolic plane, and since the determinant is a square, the complement in this splitting is a hyperbolic plane as well. But then V_v contains a two dimensional totally isotropic subspace, so for any 3-dimensional $U \subseteq V$ all completions U_v are isotropic. Since the ternary case of the theorem is already established, we are done in this case.
Assume now that $n = 4$ and that $\det(V, Q)$ is not a square, let $E = F(\sqrt{d})$. The vector space $V_E := E \otimes V$ (with the natural extension of Q to it) over E has then also the property that all its completions are isotropic. Since its determinant is a square, it is isotropic. An isotropic vector of V_E can be written as $z + \sqrt{d}y$ with $z, y \in V$, and $Q(z + \sqrt{d}y) = 0$ implies $b(z, y) = 0, Q(z) = -dQ(y)$. If $Q(z) = Q(y) = 0$, the space (V, Q) is isotropic, otherwise we have a basis $(x_1 = z, x_2 = y, x_3, x_4)$ of V and put $U = Fz + Fy, W = Fx_3 + Fx_4$. Then we see that $d = \det(V, Q) = \det(U, Q)\det(W, Q) = -d \det(W, Q)$, so $-\det(W, Q)$ is a square and (W, Q) is a hyperbolic plane. So (V, Q) is isotropic in that case as well.
We now start induction on $n = \dim(V)$. Let $n > 4$ and assume the assertion has been proven for $\dim(V) < n$. Write $V = U \perp W$, where $U = Fx_1 + Fx_2$ has dimension 2. If W_v is isotropic for all non trivial valuations v of F, we are done by the inductive assumption. Otherwise, the set T of $v \in \Sigma_F$ for which (W_v, Q) is anisotropic is finite, since a maximal lattice on W is unimodular at almost all v and of rank ≥ 3. Since (V_v, Q) is isotropic for all v, we can find $c_v \in F_v$ with $c_v = Q(a_v u_1 + b_v u_2) \in Q(U_v), -c_v \in Q(W_v)$ for all $v \in T$. By Hensel's lemma and its corollary for squares in complete

local rings, any $c \in F$ with $|c - c_v|_v$ small enough will be a multiple of c_v by a square in F_v. By the weak approximation theorem we can find $a, b \in F$ which are arbitrarily close to a_v, b_v respectively at all $v \in T$ and make $|Q(au_1 + bu_2) - a_v|_v$ as small as we want for all $v \in T$. This gives us a vector $x \in U$ with $Q(x) = c \in c_v(F_v^\times)^2$ for all $v \in T$, so the space $Fx + W$ is isotropic at all $v \in T$ and hence at all $v \in \Sigma_F$. By the inductive assumption it is isotropic, so (V, Q) is isotropic. □

As an immediate consequence we obtain

THEOREM 6.2 (Weak Minkowski Hasse theorem). *Let (V, Q) and (W, Q') be regular quadratic spaces over F and assume that (W_v, Q'_v) is represented by (V_v, Q_v) for all $v \in \Sigma_F$, i.e., that there exist isometric embeddings $\phi_v : W_v \to V_v$ for all $v \in \Sigma_F$.*
Then (W, Q') is represented by (V, Q).
In particular, if (V_v, Q) and (W_v, Q') are isometric for all $v \in \Sigma_F$,the quadratic spaces (V, Q) and (W, Q') are isometric.

PROOF. We prove this by induction on $n = \dim(W)$. For $n = 1$ we have $W = Fx$ with $Q(x) = a$ and $a \in Q(V_v)$ for all v, so the space $V \perp Fy$ with $Q(y) = -a$ is isotropic over all F_v, hence isotropic over F by the previous theorem, and it follows that V represents a.
Let $n > 1$ and assume that the assertion is proved for all W with $\dim(W) < n$. Let $0 \neq a \in Q(W)$. Then a is represented by all (V_v, Q), hence represented by (V, Q) by our result for the case $n = 1$. We can then write $V = Fx \perp V'$ and $W = Fy \perp W'$ with $Q(x) = Q(y) = a$. If $\phi_v : W_v \to V_v$ is an isometric embedding, we can find by Witt's theorem a $\psi_v \in O(V_v, Q)$ with $\psi_v \circ \phi_v(y) = x$ and hence $\psi_v \circ \phi_v(W') \subseteq V'_v$. Thus W' is represented by all (V'_v, Q) and therefore by (V', Q) by the inductive assumption, and $W = Fy \perp W'$ is represented by $V = Fx \perp V'$. □

COROLLARY 6.3 (Theorem of Meyer). *Let (V, Q) be a quadratic space over $\mathbb{Q}$ which is indefinite (i.e., isotropic over $\mathbb{R}$). Then (V, Q) is isotropic.*

PROOF. Since every (regular) quadratic space over $\mathbb{Q}_p$ (for a prime p) is isotropic, this follows from the strong Minkowski-Hasse theorem. □

COROLLARY 6.4. *There is a well defined injective group homomorphism $L : W(F) -$ to $\prod_{v \in \Sigma_F} W(F_v)$ satisfying $L([(V, Q)] = ([(V_v, Q)])_{v \in \Sigma_F}$ for regular quadratic spaces (V, Q) over F.*

PROOF. Obviously, if (V, Q) and (W, Q') are Witt equivalent, their completions at$v \in \Sigma_v$ are Witt equivalent as well, so we can define the map as given above. It is, again obviously, a group homomorphism, and that the kernel is $\{0\}$ follows from the weak Minkowski-Hasse theorem. □

REMARK 6.5. a) One can show that a tuple $([(V_v, Q_v)])_{v \in \Sigma_F}$ of Witt classes of quadratic spaces of equal dimension on the right hand side is in the image of our map L if and only if

- There exists $d \in F^\times$ with $d(F_v^\times)^2 = \det(V_v, Q_v)$ for all $v \in \Sigma_F$
- Almost all of the Hasse invariants of the (V_v, Q_v) are 1 and their product equals 1.

The necessity of these conditions follows from the Hilbert reciprocity law, for their sufficiency see O'Meara's book [**28**].

b) A precise description of the Witt group of $\mathbb{Q}$ along with a different and more elementary proof of the weak Hasse-Minkowski theorem can be found in the books by Cassels, Kneser, Lam, W. Scharlau [**6, 19, 26, 31**].

6.2. Lattices over $\mathbb{Z}$

DEFINITION 6.6. Let Λ_1, Λ_2 be R-lattices on regular quadratic spaces (V_1, Q_1), (V_2, Q_2) over F.
One says that (Λ_2, Q_2) is in the genus of (Λ_1, Q_1) if their completions $\Lambda_i \otimes R_v$ are isometric as quadratic R_v-modules for all $v \in \Sigma_F$, one writes then $(\Lambda_2, Q_2) \in \operatorname{gen}((\Lambda_1, Q_1))$ (or vice versa).

REMARK 6.7. a) If $(\Lambda_1, Q_1), (\Lambda_2, Q_2)$ are in the same genus, their underlying quadratic spaces are isometric by the weak Hasse-Minkowski theorem. We will therefore in general assume that lattices in the same genus have the same underlying quadratic space.

b) An integral local-global principle is not true: Lattices may be in the same genus without being isometric. A simple example for this are the $\mathbb{Z}$-lattices with Gram matrix $\begin{pmatrix} 2 & 0 \\ 0 & 110 \end{pmatrix}$ respectively $\begin{pmatrix} 10 & 0 \\ 0 & 22 \end{pmatrix}$.

c) A genus of quadratic lattices consists of full isometry classes.

d) The adelic orthogonal group $O_{(V,Q)}(\mathbb{A}_F)$ of the quadratic space (V, Q) operates transitively on the set of lattices in the genus of a given lattice Λ on V: A given $\phi = (\phi_v)_{v \in \Sigma_F} \in O_{(V,Q)}(\mathbb{A}_F)$ satisfies (by definition of the adele group) $\phi_v(\Lambda_v) = \Lambda_v$ for almost all $v \in \Sigma_F$, so there exists (by Lemma 2.11) a unique lattice $\Lambda' = \phi(\Lambda)$ on V with $\Lambda'_v = \phi_v(\Lambda_v)$ for all $v \in \Sigma_F$, which is then in the genus of Λ. By definition, all lattices on V in the genus of Λ can be obtained is this way. The stabilizer of the isometry class of Λ under this action is the set $O_{(V,Q)}(F)O_{V,Q}(\mathbb{A}_F, \Lambda)$, where $O_{V,Q}(\mathbb{A}_F, \Lambda)$ denotes the set of all adeles $(\phi_v)_v$ with $\phi_v(\Lambda_v) = \Lambda_v$ for all $v \in \Sigma_F$, i.e., the stabilizer of the lattice Λ under this group action. The set of isometry classes in the genus of Λ is then in bijection with the double cosets $O_{(V,Q)}(F)\psi O_{V,Q}(\mathbb{A}_F, \Lambda)$ in $O_{(V,Q)}(\mathbb{A}_F)$.

LEMMA 6.8. *Let Λ_1, Λ_2 be lattices on the regular quadratic space (V, Q) over F in the same genus. Then $(d_1 R^\times)^2 := \det(\Lambda_1, Q) = \det(\Lambda_2, Q) =: d_2(R^\times)^2$.*

PROOF. By definition of the genus we must have $d_1(R_v^\times)^2 = d_2(R_v^\times)^2$ for all $v \in \Sigma_F$, so in particular $d_1 R_v^\times = d_2 R_v^\times$ for all $v \in \Sigma_F$, which implies $d_1 R = d_2 R$. Since d_1, d_2 differ by the square of a $c \in F^\times$, we must in fact have $d_1(R^\times)^2 = d_2/R^\times)^2$ as asserted. □

We turn now attention to the special case $R = \mathbb{Z}, F = \mathbb{Q}$. The following theorem generalizes a result which we already obtained for positive definite lattices in chapter 3.

THEOREM 6.9 (Hermite). *Let Λ be a $\mathbb{Z}$-lattice on the regular quadratic space (V, Q) over $\mathbb{Q}$ of dimension n with associated symmetric bilinear forms $b, B = \frac{1}{2}b$, let $d = \det_B(\Lambda)$, let*

$$\mu := \mu(\Lambda) := \min\{|Q(x)| \mid x \in \Lambda \setminus \{0\}.$$

Then

$$\mu(\Lambda) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} |d|^{\frac{1}{n}}.$$

PROOF. By scaling the quadratic form with a suitable integer we may assume $Q(\Lambda) \in \mathbb{Z}$ and see that the minimum μ is indeed assumed. If $\mu = 0$, we are done, otherwise we can proceed as in the proof of Theorem 3.9. □

THEOREM 6.10. *There are only finitely many isometry classes of integral quadratic $\mathbb{Z}$-lattices (Λ, Q) of rank n and fixed determinant d.*

PROOF. The assertion is trivial for $n = 1$. We let $n > 1$ and assume the assertion to be proven for lattices of rank $< n$. Let $0 \neq x \in \Lambda$ be a primitive vector with $|Q(x)| = \mu$ and $B(x, \Lambda) = a\mathbb{Z}$. If $\mu \neq 0$ we put $M = Rx$ and $N = (\mathbb{Z}x)^\perp = (Fx)^\perp \cap \Lambda$. By Theorem 2.16 b) we have $\det(N, Q)a^2 = \mu d$, in particular $\det(N, Q)$ is a divisor of μd and hence bounded in absolute value by a constant times a power of d. By the inductive assumption, there is only a finite number of possible isometry classes of (N, Q). Since we have $M \perp N \subseteq \Lambda \subseteq M^\# \perp N^\#$ and $M \perp N$ has finite index in $M^\# \perp N^\#$, there are only finitely many possibilities for the isometry class of Λ.
In the case $\mu = 0$ we look at the Gram matrix of (Λ, Q) with respect to a basis of Λ beginning with the vector x and see that we can divide both the first column and the first row by a, so that $a^2 \mid d$ must hold.
We find then $y' \in \Lambda$ with $B(x, y') = a$ with $B(x, \Lambda) = a\mathbb{Z}$. Replacing y' by a suitable $y = y' - cx$ we can achieve $|Q(y)| = |Q(y') - 2ca| \leq a$, so the rank 2-sublattice $M = \mathbb{Z}x + \mathbb{Z}y$ has a Gram matrix with entries bounded by d, so that there are only finitely many possible isometry classes for M. Again by b) of Theorem 2.16 we see that $N = (Fx + Fy)^\perp \cap \Lambda$ has determinant and hence by the inductive assumption isometry class from a finite set. We obtain as above that there are only finitely many possibilities for the isometry class of Λ. □

REMARK 6.11. By the work of Humbert [**17**] the Theorem remains valid if one replaces $\mathbb{Z}$ by the ring of integers $\mathfrak{o}$ of a number field and the determinant by the norm of the volume ideal of an $\mathfrak{o}$-lattice Humbert's proof is for classes of symmetric matrices (equivalently, for free lattices) but carries over to the more general situation.

COROLLARY 6.12. *The number of isometry classes in a fixed genus of $\mathbb{Z}$-lattices is finite.*

PROOF. If Λ_1, Λ_2 are in the same genus, we assume them to be on the same space and have $\det((\Lambda_1, Q)) = c^2 \det((\Lambda_2, Q))$ for some $c \in \mathbb{Q}$. Since the completions are isometric over all $\mathbb{Z}_p$, the number c is a unit in all $\mathbb{Z}_p$, hence must be ± 1, so that the lattices have the same determinant. By the previous theorem there can be only finitely many isometry classes of this determinant. $\square$

REMARK 6.13. By the previous remark the assertion of the Corollary remains valid if one replaces $\mathbb{Z}$ by the ring of integers $\mathfrak{o}$ of a number field.

EXAMPLE 6.14. For simplicity of notation we will write $\langle a_1, \dots, a_n\rangle$ for a lattice with diagonal Gram matrix with entries $a_1, \dots, a_n$ in the diagonal and $I_n = \langle 1, \dots, 1\rangle, -I_n = \langle -1, \dots, -1\rangle$.

a) for $2 \le n \le 5$ our bound for the minimum of Λ is < 2 for $d = 1$.

   For $\mu = 1$, the one dimensional sublattice $\mathbb{Z}x$ generated by a minimal vector splits off orthogonally, and its complement has again determinant ± 1 with respect to B, so that Λ has an orthgonal basis of vectors x_i with $Q(x_i) = \pm 1$. If both signs occurred here, the lattice was isotropic and had minimum 0, so (Λ, Q) is up to multiplication of the quadratic form by -1 isometric to the cube lattice I_n generated by the standard basis vectors of $\mathbb{R}^n$ equipped with the standard scalar product as B.

   For $\mu = 0$ we see that the lattice $M = \mathbb{Z}x + \mathbb{Z}y$ in the proof of the theorem is a regular hyperbolic plane H or has Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, which is equivalent to $\langle 1, -1\rangle$. In both cases it splits off orthogonally. For $n = 2$ this finishes the discussion, for $n = 3$ the orthogonal complement is spanned by a vector z with $Q(z) = \pm 1$. Since $H \perp \langle \pm 1\rangle$ is isometric to $\langle 1, -1, \pm 1\rangle$ we have Λ isometric to $\langle 1, 1, -1\rangle$ or to $\langle 1, -1, -1\rangle$. For $n = 4$ we can have Λ isometric to $H \perp H$ or to $I_r \perp -I_s$ with $r + s = 4$ and $0 \neq r \neq s$. For $n = 5$ we get $I_r \perp -I_s$ with $r + s = 5, 0 \neq r \neq s$. We see that H and $H \perp H$ are distinguished from the other possibilities by the 2-adic behaviour, namely by $Q(x) = B(x, x)$ having only even values, and that the remaining cases are distinguished by rank and signature at the real place. In any case we see that the 2-adic information and the signature determine the genus and that each genus consists of a single isometry class.

b) For $2 \le n \le 4$ and $d = 2$ the bound for the minimum is again 1. By similar arguments as above we obtain the possibilities $\langle \pm 1, \pm 2\rangle$ with $\langle 1, -2\rangle$ isometric to $\langle -1, 2\rangle$, $H \perp \langle \pm 2\rangle, \langle \pm 1, \pm 1, \pm 2\rangle, \langle \pm 1, \pm 1, \pm 1, \pm 2\rangle$, where the isometry class depends only on the number of $+$-signs and the number of $-$-signs but not on whether the sign occurs in front of a 1 or a 2. This shows that the genus of the lattice is determined by the signature at the real place and the 2-adic class (even values for $Q(x)$ or odd and even values) and that each genus consists of a single isometry class.

6.3. Representations

We recall that an isometric embedding $\phi : (M, Q') \to (\Lambda, Q)$ of quadratic modules over the ring R is also called a representation of (M, Q') by (Λ, Q), it is a primitive representation if the image of ϕ is a direct summand in Λ. If R is a principal ideal domain with field of quotients F and V, W are the F-vector spaces obtained from Λ, M respectively by extending scalars to F, a representation ϕ as above is primitive if and only if $\phi(M) = \Lambda \cap \phi(W)$ holds. The same is true if R is the ring of integers of the global field F, since then the R-module $\phi(M)$ is a direct summand in Λ if and only if its completion at $v \in \Sigma_F$ is a direct summand in Λ_v for all $v \in \Sigma_F$ and the intersection condition localizes as well. We say that (M, Q') is represented (primitively) by (Λ, Q) if there exists a representation $\phi : (M, Q') \to (\Lambda, Q)$.

THEOREM 6.15. *Let $(M, Q'), (\Lambda, Q)$ be R-lattices on the quadratic spaces W, V with (V, Q) or (W, Q') regular and assume that for all $v \in \Sigma_F$ there is a representation $\phi_v : M_v \to \Lambda_v$. Then there is a representation $\phi : M \to \Lambda'$, where Λ' is a lattice on the space V of Λ in the genus of Λ. If all the representations ϕ_v are primitive, the representation ϕ can also be chosen to be primitive.*

PROOF. By the Minkowski-Hasse theorem there exists an isometric embedding (a representation) $\phi : W \to V$ so that we can assume that M is a lattice in V (but in general not on V). For almost all $v \in \Sigma_F$ we have $M_v \subseteq \Lambda_v$, so the set T of places v where $M_v \not\subseteq \Lambda_v$ is finite. By assumption, for each such v there exists a lattice $N_v \subseteq \Lambda_v$ which is isometric to M_v, and by Witt's extension theorem (Theorem 1.41) an isometry can be extended to a map $\psi_v \in O_V(F_v)$ with $\psi_v(N_v) = M_v$. We let Λ' be the lattice on V with $\Lambda'_v = \Lambda_v$ for all $v \notin T$ and $\Lambda'_v = \psi_v(\Lambda)$ for all $v \in T$ and have $M_v \subseteq \Lambda'_v$ for all $v \in \Sigma_F$, hence $M \subseteq \Lambda$. Obviously, Λ' is in the genus of Λ.
If all the ϕ_v are primitive, we enlarge T to a still finite set T^* by demanding M_v to be a primitive sublattice of Λ_v for all $v \notin T$ and choose primitive sublattices N_v of Λ_v for all $v \in T^*$, leaving the rest of the proof unchanged. □

COROLLARY 6.16. *Let (Λ, Q) be an R-lattice for which the genus contains only one isometry class. Then Λ represents (primitively) all R-lattices (M, Q') which are represented (primitively) locally everywhere by Λ.*
In particular:

a) *(Theorem of Euler) The integer $a \in \mathbb{Z}$ is a sum of two coprime integral squares if and only if all its prime factors are congruent to* 1 *mod* 4 *and it is not divisible by* 4*. It is a sum of two arbitrary integral squares if and only if all primes* $\equiv 3 \bmod 4$ *divide a to an even power.*
b) *(Theorem of Gauß-Legendre) The integer $a \in \mathbb{Z}$ is a sum of three integral squares if and only if it is not of the form* $4^\nu(8k + 7)$ *with*

$v, k \in \mathbb{N}_0$. *It is a sum of three coprime integers if in addition it is not divisible by* 4.

c) *(Theorem of Lagrange) All positive integers a are sums of four integral squares. A representation by relatively prime integers exists if and only if a is not divisible by* 8.

PROOF. The first statement is a trivial consequence of the theorem. For the classical results about representation of integers as sums of squares we have to check that the conditions given are equivalent to the condition that a is represented (primitively) locally everywhere. This is reduced by Hensel's lemma to routine computations modulo 8 for representation over $\mathbb{Z}_2$ and modulo p for $\mathbb{Z}_p$ with p odd. □

REMARK 6.17. We can obtain analogous results for representation of integers in the form x^2+2y^2 or as $x^2+y^2+2z^2$. If the class number of the genus of the representing lattice is bigger than 1 it is possible to obtain results on representation of sufficiently large numbers by analytic methods.

6.4. Lattices over $\mathbb{Z}$, continued

DEFINITION 6.18. A positive definite $\mathbb{Z}$-lattice (Λ, Q) is called decomposable if it contains nontrivial sublattices M, N with $\Lambda = M \perp N$, indecomposable otherwise.

THEOREM 6.19 (Eichler, Kneser). *Any positive definite* $\mathbb{Z}$*-lattice* (Λ, Q) *has a unique (up to order) decomposition into an orthogonal sum of indecomposable sublattices.*

PROOF. The existence of such a decomposition is trivial, we have to prove the uniqueness. We call a vector $x \in \Lambda$ indecomposable if it can not be written as $x = y + z$ with $b(x, y) = 0, x, y \in \Lambda, x \neq 0 \neq y$. The lattice Λ is obviously generated by its indecomposable vectors. We call two indecomposable vectors x, y connected, if there exists a chain $x = x_1, \dots, x_r$ of indecomposable vectors of Λ with $b(x_i, x_{i+1}) \neq 0$ for $1 \leq i < r$. Being connected defines an equivalence relation among the indecomposable vectors of Λ and any two equivalence classes are mutually orthogonal.
If we have a decomposition $\Lambda = \perp_{i=1}^t L_i$, any indecomposable vector lies in some L_j and and if x, y are connected indecomposable vectors of Λ they lie in the same L_j, so for each j the set of indecomposable vectors in L_j consists of full equivalence classes of connected indecomposable vectors of Λ. If L_j contained more than one equivalence class it could not be indecomposable. This implies that in the decomposition $\Lambda = \perp_{i=1}^t L_i$, each L_j contains a unique equivalence class S_j of connected indecomposable vectors of Λ which generates it. So the L_j are the sublattices generated by the equivalence classes of connected indecomposable vectors of Λ and therefore uniquely determined. □

EXAMPLE 6.20. a) Denote by A_n the lattice $\{\mathbf{x} \in \mathbb{Z}^n \mid \sum_{i=0}^n x_i = 0\}$ with the standard scalar product of $\mathbb{Q}^{n+1}$ as symmetric bilinear form

b and $Q(\mathbf{x}) = \frac{1}{2}\sum_{i=0}^{n} x_i^2$. Since it is the orthogonal complement of $(1,\ldots,1)$ in $\mathbb{Z}^{n+1}$ it has determinant $n+1$ by Theorem 2.16. The vectors $\mathbf{e}_i - \mathbf{e}_j$ with $i \neq j$, where $(\mathbf{e}_1,\ldots,\mathbf{e}_{n+1})$ is the standard basis of $\mathbb{Q}^{n+1}$, are indecomposable and connected and generate A_n, so this lattice is indecomposable. It occurs as a root lattice in the theory of Lie algebras.

b) Denote by D_n the lattice $\{\mathbf{x} \in \mathbb{Z}^n \mid \sum_{i=0}^{n} x_i \equiv 0 \bmod 2\}$, again with quadratic form $Q(\mathbf{x}) = \frac{1}{2}\sum_{i=0}^{n} x_i^2$ so that the standard scalar product is the associate symmetric bilinear form. The lattice is of index 2 in $\mathbb{Z}^n$, so $\det_b(A_n) = 4$. It is generated by the indecomposable vectors $\pm\mathbf{e}_i \pm \mathbf{e}_j$ with $i \neq j$ which generate the lattice and are connected for $n > 2$, so for $n > 2$ it is also indecomposable. It occurs as a root lattice in the theory of Lie algebras. For $n = 3$ it is isometric to the lattice A_3 above.

c) for $n \equiv 0 \bmod 8$ denote by $D_n^+ = \Gamma_n$ the lattice $D_n + \mathbb{Z}\frac{1}{2}\sum_{i=1}^{n} \mathbf{e}_i$. One has $Q(D_n^+) \subseteq \mathbb{Z}$ and $(D_n^+ : D_n) = 2$, so D_n^+ is an even unimodular lattice in $\mathbb{Q}^n$. The indecomposable vectors $\pm\mathbf{e}_i \pm \mathbf{e}_j$ with $i \neq j$ generate a sublattice of full rank and are connected, so this lattice is indecomposable too. For $n = 8$ this lattice is usually denoted by E_8 because it occurs with this notation as a root lattice in the theory of Lie algebras. It has the indecomposable sublattices $E_7 := \{\mathbf{x} \in E_8 \mid x_7 = x_8\}$ of rank 7 and determinant 2 and $E_6 := \{\mathbf{x} \in E_8 \mid x_6 = x_7 = x_8\}$ of rank 6 and determinant 3 which occur as root lattices too and together with E_8 and the lattices D_n and A_n from above exhaust the list of indecomposable root lattices.

For $n = 16$ we see that we know two even unimodular lattices, one of them (D_{16^+}) indecomposable and one of them $(E_8 \perp E_8)$ decomposable, so in particular they are not isometric.

It can be shown that these two represent all isometry classes of even unimodular positive definite $\mathbb{Z}$-lattices of rank 16. It can also be shown that even unimodular positive definite $\mathbb{Z}$-lattices can occur only with ranks which are divisible by 8.

CHAPTER 7

Clifford Algebra, Invariants, and Classification

To a quadratic module one can construct a natural associative algebra, the Clifford algebra, which provides important insights and is a useful tool for classification.
For our purpose it will be sufficient to treat the case of quadratic spaces over fields of characteristic zero. Slightly more general, in this chapter F is a field of characteristic different from 2. Modifications that include the case of even characteristic can be found in [**19, 22, 31**]; we omit the details since we are mainly interested in the number theoretic aspects of the theory of quadratic forms. As earlier we write $(V, Q) \cong [a_1, \dots, a_m]$ for a quadratic space (V, Q) with an orthogonal basis $(v_1, \dots, v_m)$ satisfying $Q(v_i) = a_i$ for $1 \le i \le m$.

7.1. Quaternion Algebras and Brauer group

DEFINITION 7.1. A central simple algebra of dimension 4 over F is called a quaternion algebra over F.

THEOREM 7.2. a) *If A is a quaternion algebra over F there exist linearly independent elements $x, y \in A$ with $x^2 \in F^\times, y^2 \in F^\times, xy = -yx$. The elements $1, x, y, xy$ form then a basis of A as F-vector space.*
b) *Conversely, let $a, b \in F^\times$ be given. Then there exist a quaternion algebra over F and linearly independent vectors $x, y \in A$ with $x^2 = a, y^2 = b, xy = -yx$.*

PROOF. Wedderburn's theorem about central simple algebras implies that A is either a division algebra or isomorphic to $M_2(F)$. In the latter case, the matrices $x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ are as requested.
If A is a division algebra, every element x of $A \setminus F$ has an irreducible minimal polynomial of degree 2 over F, and changing x by an element of F we can assume the minimal polynomial to be of the form $X^2 - a$ with $a \neq 0$, i.e., $x^2 = a \in F^\times$.
With $A^0 := \{0\} \cup \{x \in A \setminus F \mid x^2 \in F\}$ we have then $A = F + A^0$, in particular we can find $x, y \in A^0$ such that $1, x, y$ are linearly independent. Since $1, x, y$ can not generate a (division) subalgebra of dimension 3 over F, the vectors $1, x, y, xy$ must then be an F-basis of A, and $xy + yx$ commutes with all basis vectors and must hence be in the center F of A. From this we see that we can subtract a suitable multiple of x from y in order to obtain

$0 \neq y_1 \in A^0$ with $xy_1 + y_1x = 0$, so that x and y_1 are as requested. We notice in passing that $xy + yx \in F$ implies $(x+y)^2 \in F$, i.e., $x + y \in A^0$. Conversely, if $a, b \in F^\times$ are given one can define a 4-dimensional F-algebra A generated by linearly independent vectors $1 = e_0, e_1, e_2, e_3$ by prescribing a multiplication table with $e_0e_j = e_je_0 = e_j, e_0^2 = 1, e_1^2 = a, e_3^2 = -ab, e_1e_2 = -e_1e_2 = e_3, e_2e_3 = -be_1 = -e_3e_2, e_3e_1 = -ae2 = -e_1e_3$ and extending this multiplication distributively to the whole vector space; it is then easily checked by explicit calculation that A with this law of multiplication satisfies the axioms for an F-algebra and is central simple. □

LEMMA 7.3. *Let A be a quaternion algebra over F with basis $1 = e_0, e_1, e_2, e_3 = e_1e_2$ satisfying $e_1^2, e_2^2 \in F^\times, e_2e_1 = -e_3$ as above. Then*

$$\{0\} \cup \{x \in A \setminus F \mid x^2 \in F\} = Fe_1 + Fe_2 + Fe_3 =: A^0,$$

and the map given by $a + x \mapsto \overline{a+x} := a - x$ for $a \in F, x \in A^0$ is an involution of the first kind on A satisfying $x\bar{x} =: n(x) \in F, x + \bar{x} = \mathrm{tr}(x)$ for all $x \in A$.

PROOF. This is checked by explicit calculation. The fact that A^0 is a 3-dimensional vector space over F can also be seen from the proof of the theorem above if A is a division algebra, if A is the matrix ring $M_2(F)$ it is obvious that A^0 is the space of matrices of trace 0. □

DEFINITION 7.4. With notations as in the previous lemma we call A^0 the space of pure quaternions, the map $x \mapsto \bar{x}$ the (quaternionic) conjugation on A and the maps $x \to n(x), x \mapsto \mathrm{tr}(x)$ the quaternion norm resp. trace. The quaternion algebra with generators $e_0 = 1, e_1, e_2, e_3 = e_1e_2 = -e_2e_1$ satisfying $e_1^2 = a, e_2^2 = b$ as above is denoted by $(a, b)_F = \left(\frac{a,b}{F}\right)$ and the vectors $e_0, \ldots, e_4$ are called a standard basis of $(a, b)_F$.

REMARK 7.5.
a) In the terminology of the theory of (central simple) algebras the quaternion norm and trace are the reduced norm and trace in the algebra A.
b) For the matrix algebra $M_2(F)$ the quaternion norm is the determinant, the quaternion trace the matrix trace and the conjugation the map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

c) If $A = (a, b)_F$ is a quaternion division algebra and $\delta \in A^0$ with $\delta^2 = a \in F^\times$ one can embed A into the matrix ring $M_2(F(\delta))$ over the quadratic extension $E = F(\delta) = F(\sqrt{a})$ as the subgroup generated by the matrices

$$\tilde{e_0} = 1_2, \tilde{e_1} = \begin{pmatrix} \delta & 0 \\ 0 & -\delta \end{pmatrix}, \quad \tilde{e_2} = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}.$$

The quaternion norm and trace coincide then with the determinant and the matrix trace in this representation. In particular for the Hamilton quaternions $\mathbb{H} = (-1,-1)_{\mathbb{R}}$ over R one obtains the usual identification of $\mathbb{H}^1 := \{x \in \mathbb{H} \mid n(x) = 1\}$ with the special unitary group $SU_2(\mathbb{C})$.

We recall that the Brauer group $Br(F)$ of F is by definition the set of isomorphism classes of central simple F-algebras modulo the equivalence relation $A \otimes M_r(F) \sim B \otimes M_s(F)$ (similarity of algebras), where the group multiplication is induced by the tensor product of algebras. Each such class is represented by a unique division algebra with center F.

LEMMA 7.6. *The class of a quaternion division algebra over F in the Brauer group of F has order* 2.

PROOF. Denoting by A^{op} the opposed algebra of F, i. e., A with multiplication in opposite order, it is well known that $A \otimes A^{op}$ is isomorphic to a matrix ring over F for any central simple algebra A over F. The properties of the quaternionic conjugation show that a quaternion algebra is isomorphic to its opposed algebra, which implies the assertion. □

LEMMA 7.7. *Let A be a quaternion algebra over F. The quaternion norm n defines a quadratic form on A with associated symmetric bilinear form $b(x,y) = \mathrm{tr}(x\bar{y})$, and the quadratic space (A,n) over F has square determinant. It is isotropic if and only if $A \cong M_2(F)$ holds.*

PROOF. Since the norm is multiplicative a quaternion x is invertible if and only if its norm is nonzero, so A is a division algebra if and only if (A,n) is anisotropic. The rest of the assertion is obvious. □

REMARK 7.8. Since over a finite field F every quadratic space of dimension ≥ 3 is isotropic we see that the only quaternion algebra over a finite field F is the matrix ring $M_2(F)$ (in fact, by a well known theorem of Wedderburn there exists no non trivial division algebra with center F).

LEMMA 7.9. *Let $a,b,c,d \in F^\times$. then the following are equivalent:*

a) $[1,-a,-b,ab] \cong [1,-c,-d,cd]$
b) $[-a,-b,ab] \cong [-c,-d,cd]$
c) *The quaternion algebras $(a,b)_F, (c,d)_F$ are isomorphic.*

PROOF. The equivalence of a) and b) follows from Witt's cancellation law, and c) obviously implies b). For the reverse direction denote by $e_0 = 1, e_1, e_2, e_3$ a standard basis of $(a,b)_F$. By assumption there exists a linear isometry τ from $(a,b)_F$ to $(c,d)_F$ with $\tau(1) = 1 and \tau((a,b)_F^0) = (c,d)_F^0$. With $f_1 := \tau(e_1), f_2 := \tau(e_2), f_3 = f_1f_2$ we have $\mathrm{tr}(f_1\bar{f}_2) = \mathrm{tr}(e_1\bar{e}_2) = 0$ and hence $f_1f_2 = -f_2f_1$. With $f_i^2 = -n(f_i) = n(e_i) = -e_i^2$ for $i = 1,2$ we see that $1, f_1, f_2, f_3$ is a standard basis of $(c,d)_F$ with $f_1^2 = a, f_2^2 = b$ and hence $(c,d)_F \cong (a,b)_F$. □

LEMMA 7.10. *Let $a, b, c, d \in F^\times, ab \in cd(F^\times)^2$.
Then $[a, b] \cong [c, d]$ (as quadratic spaces) is equivalent to $(a, b)_F \cong (c, d)_F$ (as algebras).*

PROOF. By assumption the isometry of quadratic spaces is equivalent to the isometry $[-a, -b, -cd] \cong [-c, -d, cd]$, which is equivalent to the algebras being isomorphic. □

LEMMA 7.11. *Let $a, b, c, \alpha, \beta, \gamma \in F^\times$ with $\alpha\beta\gamma \in abc(F^\times)^2$. Then $[a, b, c] \cong [\alpha, \beta, \gamma]$ (as quadratic spaces) is equivalent to $(-bc, -ac)_F \cong (-\beta\gamma, -\alpha\gamma)_F$ (as algebras).*

PROOF. Scaling the quadratic forms with abc resp. α, β, γ shows that the isometry of quadratic spaces is equivalent to the isometry $[bc, ac, ab] \cong [\beta\gamma, \alpha\gamma, \alpha\beta]$, which in turn is equivalent to the isomorphy of algebras is question. □

LEMMA 7.12. *Let $a, b, \alpha, \beta \in F^\times$. The map sending the pair (a, b) to the quaternion algebra $(a, b)_F$ has the following properties:*

a) $(a, b)_F \cong (a\alpha^2, b\beta^2)_F$.
b) $(a, b)_F \cong (b, a)_F$.
c) $M_2(F) \cong (1, a)_F \cong (a, -a)_F \cong (a, 1 - a)_F$ *(with the last isomorphy supposing $a \neq 1$).*
d) $(a, a)_F \cong (a, -1)_F$.

PROOF. All assertions follow from a consideration of the associated quadratic spaces. □

LEMMA 7.13. *Let $a, b, c \in F^\times$, denote by $\sim$ the equivalence relation (similarity) between central simple algebras defining the Brauer group.
Then*

$$(a, bc)_F \sim (a, b)_F \otimes (a, c)_F, \quad (ab, c)_F \sim (a, c)_F \otimes ((b, c)_F.$$

In particular, the map sending a pair $(a, b) \in F^\times \times F^\times$ to the class of the quaternion algebra $(a, b)_F$ in the $2-$ torsion subgroup of the Brauer group $Br(F)$ is a Steinberg symbol.

PROOF. We show the assertion by proving

$$(a, b)_F \otimes (a, c)_F \cong (a, bc)_F \otimes (c, -ac^2)_F.$$

We let $e_0 = 1, e_1, e_2, e_3$ resp. $f_0 = 1, f_1, f_2, f_3$ be standard bases for the quaternion algebras on the left hand side and put $A = F1 \otimes 1 + Fe_1 \otimes 1 + Fe_2 \otimes f_2 + Fe_3 \otimes f_2$ and $B = F1 \otimes 1 + F1 \otimes f_2 + F \otimes e_1 \otimes f_3 + F(e_1 \otimes f_1)$. Then A, B are isomorphic to the quaternion algebras on the right hand side and commute. From this we obtain an algebra homomorphism $A \otimes B \to (a, b)_F \otimes (a, c)_F$, which must be an isomorphism since $A \otimes B$ is simple. The definition of Steinberg symbols shows that we have indeed defined such a symbol. □

7.2. The Clifford Algebra

DEFINITION AND THEOREM 7.14. *Let (V, Q) be a quadratic space over F. Then there is a unique up to unique isomorphism F- algebra $C(V, Q) = C(V) = C_V$ with a linear map $i : V \to C(V, Q)$ such that*

a) $i(v)^2 = Q(v)1 \in C(V, Q)$ *for all* $v \in V$.
b) *If C' is any F-algebra with an F-linear map $i' : V \to C'$ satisfying $(i'(v))^2 = Q(v)1 \in C'$ for all $v \in V$, there is a unique algebra homomorphism $\phi : C(V, Q) \to C'$ with $i' = \phi \circ i$.*

The algebra $C(V, Q)$ is called the Clifford algebra of (V, Q), it is generated by the elements $i(v)$ for $v \in V$. It has a natural $\mathbb{Z}/2\mathbb{Z}$-grading $C(V, Q) = C_0(V, Q) + C_1(V, Q)$, where the even Clifford algebra $C_0(V, Q)$ is generated by products of even length of the $i(v)$ and $C_1(V, Q)$ is generated (as vector space over F) by the products of odd length and is a module over $C_0(V, Q)$.

In particular one has $C_1(V, Q)C_1(V, Q) \subseteq C_0(V, Q)$.

PROOF. Let I be the two sided ideal of the Tensor algebra $T(V) = \bigoplus_{j=0}^{\infty} V^{\otimes j}$ of V generated by the elements $x \otimes x - Q(x)1$. Then it is easily checked that $C(V, Q) := T(V)/I$ with the map $i : v \mapsto v + I$ has the desired property. From this it is clear that the $i(V)$ generate $C(V, Q)$. We let $T_0(V), T_1(V)$ respectively be the sum of the $V^{\otimes j}$ for even resp. odd j and obtain a $\mathbb{Z}/2\mathbb{Z}$-grading of $T(V)$. Then we have $I = I \cap T_0(V) \oplus I \cap T_1(V)$, so that $C_0(V, Q) = T_0(V)/I \cap T_0(V), C_1(V, Q) = T_1(V)/I \cap T_1(V)$ give the desired decomposition of $C(V, Q)$. $\square$

LEMMA 7.15. *Identifying $x \in V$ with its image $i(x) \in C(V, Q)$ we have*

a) $xy + yx = b(x, y)1 \in C(V, Q)$.
b) *$x \in V$ is invertible in $C(V, Q)$ if and only if $Q(x) \neq 0$ holds.*
c) *If $\{x_1, \dots, x_r\}$ is a generating set of the vector space V, the $x_1^{\epsilon_1} \dots x_r^{\epsilon_r}$ with $\epsilon_i \in \{0, 1\}$ generate $C(V, Q)$ as vector space over F.*

PROOF. Obvious. $\square$

LEMMA 7.16 (Functoriality of the Clifford algebra). *Let (V, Q) be a quadratic space over F.*

a) *To $\phi \in O(V)$ there is a unique algebra automorphism $C(\phi)$ of $C(V)$ with $C(\phi)(i(v)) = i(\phi(v))$ for all $v \in V$, and one has $C(\psi \circ \phi) = C(\psi) \circ C(\phi)$, for $\phi, \psi \in O(V)$, $C(\mathrm{Id}_V) = \mathrm{Id}_{C(V)}$.*

The map $C(-\mathrm{Id}_V)$ is the identity map on $C_0(V)$ and $-\mathrm{Id}$ on $C_1(V)$.
b) *On $C(V)$ one has an involution $x \mapsto \bar{x}$ with $\overline{i(v)} = -i(v)$ for all $v \in V$ and $\overline{v_1 \dots v_r} = (-1)^r v_r \dots v_1$ for $v_1, \dots, v_r \in V$ (identifying v with $i(v) \in C(V)$).*

PROOF. Existence and properties of $C(\phi)$ are direct consequences of the universal property of the Clifford algebra.

For b) the universal property gives us an algebra homomorphism $\imath : C(V) \to C(V)^{op}$ leaving the $i(v)$ fixed, it becomes an anti-automorphism of order 2 if we view it as a map from $C(V)$ to itself. Putting $\bar{x} = \imath(C(-\mathrm{Id}_V)(x))$ we obtain the desired map. □

EXAMPLE 7.17. a) Let Q be identically zero. Then the Clifford algebra $C(V, Q)$ is isomorphic to the exterior algebra $\bigwedge V$ because in this case the universal property of the Clifford algebra is the same as that used in the definition of the exterior algebra by a universal property.

b) Let $V = Fx \cong [a]$ with $a \in F$. Then $C(V, Q) \cong F[X]/(X^2 - a)$. In particular, if a is not a square in F, the Clifford algebra is isomorphic to the quadratic extension field $F(\sqrt{a})$. The involution $x \mapsto \bar{x}$ from Lemma 7.16 of the Clifford algebra maps to the non trivial F-automorphism of the quadratic extension. We will also use the notation $(a)_F$ for this algebra.

c) $V = Fx \perp Fy \cong [a, b]$ with $a, b \in F^\times$. Then $C(V, Q)$ is generated by $1, x, y, xy$ with $x^2 = a, y^2 = b, xy = -yx$ and hence $(xy)^2 = -ab$. Therefore, we have an algebra homomorphism from $(a, b)_F$ to $C(V, Q)$ sending the standard basis vectors to $1, x, y, xy$. Since the quaternion algebra $(a, b)_F$ is simple this must be an isomorphism and we have that $C(V, Q)$ is isomorphic to the quaternion algebra $(a, b)_F$ over F. The involution $x \mapsto \bar{x}$ from Lemma 7.16 of the Clifford algebra maps to the quaternionic conjugation.

d) Let $(V, Q) \cong [a, b, c]$ with $a, b, c \in F^\times$. We claim that one has then

$$\begin{aligned} C_0(V) &\cong (-ac, -bc)_F \\ C(V) &\cong C_0(V) \otimes (-abc)_F, \end{aligned}$$

where $(-abc)_F$ denotes (as above) the algebra $F[X]/(X^2 + abc)$.

To prove this, let x_1, x_2, x_3 be an orthogonal basis of (V, Q) with $Q(x_1) = a, Q(x_2) = b, Q(x_3) = c$. The even Clifford algebra $C_0(V, Q)$ is then generated as F-vector space by $1, f_1 = x_1x_3, f_2 = x_3x_2, f_3 = cx_1x_2$ with $f_1^2 = -ac, f_2^2 = -bc, f_1f_2 = f_3 = -f_2f_1$. As above this gives us an algebra homomorphism from $(-ac, -bc)_F$ onto $C_0(V, Q)$ which must be an isomorphism. The involution $x \mapsto \bar{x}$ from Lemma 7.16 of the Clifford algebra corresponds to the quaternionic conjugation under this isomorphism.

The subalgebra $F1 + Fx_1x_2x_3 \cong (-abc)_F \subseteq C(V, Q)$ commutes with $C_0(V)$ and generates $C(V, Q)$ together with $C_0(V, Q)$. The universal property of the tensor product gives us an algebra homomorphism from $(-ac, -bc)_F \otimes (-abc)_F$ onto $C(V, Q)$ which is an isomorphism since $(-ac, -bc)_F \otimes (-abc)_F$ is simple.

THEOREM 7.18. *Let A, B be finite dimensional F-algebras with $\mathbb{Z}/2\mathbb{Z}$ gradings $A = A_0 \oplus A_1, B = B_0 \oplus B_1$.*

Then the tensor product of F-vector spaces $A \otimes B$ has a unique structure as an F-algebra denoted by $A \hat{\otimes} B$ with the property

$$(a_i \otimes b_j)(a'_k \otimes b'_l) = (-1)^{jk} a_i a'_k \otimes b_j b'_l$$

for all $a_i \in A_i, a'_k \in A_k, b_j \in B_j, b'_l \in B_l, i, j, k, l \in \{0, 1\}$. The algebra $A \hat{\otimes} B$ is graded by setting

$$(A \hat{\otimes} B)_0 = (A_0 \otimes B_0) \oplus (A_1 \otimes B_1), \quad (A \hat{\otimes} B)_1 = (A_0 \otimes B_1) \oplus (A_1 \otimes B_0)$$

as vector spaces and is called the graded tensor product *of A and B. It is characterized up to unique isomorphism by the following universal property: If $f : A \to C, g : B \to C$ are graded algebra homomorphisms of A, B to the $\mathbb{Z}/2\mathbb{Z}$ graded F-algebra C satisfying*

$$f(a_i)g(b_j) = (-1)^{ij} g(b_j)f(a_i) \textit{ for } a_i \in A_i, b_j \in B_j, i, j \in \{0, 1\}$$

there is a unique graded algebra homomorphism $\phi : A \hat{\otimes} B \to C$ satisfying

$$\phi(a \otimes 1_B) = f(a), \quad \phi(1_A \otimes b) = g(b) \textit{ for all } a \in A, b \in B.$$

PROOF. This an easy consequence of the universal property of the tensor product of vector spaces, see e. g. [**26**]. □

THEOREM 7.19. *Let (V, Q) be a quadratic space over F with an orthogonal decomposition $V = U_1 \perp U_2$. Then $C(V, Q)$ is isomorphic to the graded product $C(U_1, Q|_{U_1}) \hat{\otimes} C(U_2, Q|_{U_2})$.*

PROOF. We have natural homomorphisms $\alpha_j : C(U_j, Q|_{U_j}) \to C(V, Q), j = 1, 2$. Since U_1, U_2 are orthogonal these satisfy $\alpha_1(u_1)\alpha_2(u_2) = -\alpha_2(u_2)\alpha_1(u_1)$ for $u_1 \in U_1, u_2 \in U_2$ (identifying vectors with their images in the Clifford algebra as usual), which implies $\alpha_1(x_i)\alpha_2(y_j) = (-1)^{ij}\alpha_2)(y_j)\alpha_1(x_i)$ for $x_i \in C_i(U_1, Q|_{U_1}), y_j \in C_j(U_2, Q|_{U-2})$ with $i, j \in \{0, 1\}$. By the universal property of the graded tensor product we obtain a graded algebra homomorphism $\phi : C(U_1, Q|_{U_1}) \hat{\otimes} C(U_2, Q|_{U_2}) \to C(V, Q)$ satisfying $\phi(x \otimes 1) = \alpha_1(x), \phi(1 \otimes y) = \alpha_2(y)$ for $x \in C(U_1, Q|_{U_1}), y \in C(U_2, Q|_{U_2})$.
On the other hand, we have an F-linear map $j : V \to C(U_1, Q|_{U_1}) \hat{\otimes} C(U_2, Q|_{U_2})$ given by $j(u_1 + u_2) := u_1 \otimes 1 + 1 \otimes u_2$ for $u_1 \in U_1, u_2 \in U_2$, and j satisfies $j(u_1 + u_2)^2 = (Q(u_1) + Q(u_2))1$.
The universal property of the Clifford algebra gives us an F-algebra homomorphism $\psi : C(V, Q) \to C(U_1, Q|_{U_1}) \hat{\otimes} C(U_2, Q|_{U_2})$ satisfying $\psi(u_1 + u_2) = j(u_1 + u_2) = u_1 \otimes 1 + 1 \otimes u_2$ for $u_1 \in U_1, u_2 \in U_2$, and it is easily checked that ϕ, ψ are inverses of each other. □

COROLLARY 7.20. *Let (V, Q) be a quadratic space over F of dimension n. Then $C(V, Q)$ has dimension 2^n and $C_0(V, Q)$ has dimension 2^{n-1} as vector space over F.*
In particular the generators $x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ with $\epsilon_j \in \{0, 1\}$ of $C(V, Q)$ for a basis $(x_1, \dots x_n)$ of V over F constitute a basis of $C(V, Q)$ as a vector space over F and the mapping $i : V \to C(V, Q)$ is injective.

PROOF. Since the Clifford algebra of a one dimensional space has dimension 2 over F this follows from the theorem. $\square$

REMARK 7.21. It can be shown that in the more general context of Clifford algebras of finitely generated projective quadratic modules over a commutative ring the mapping j from the module to its Clifford algebra is injective, see [**19, 22**]. In fact, it is enough to require that the quadratic form Q can be written as $Q(v) = \beta(v, v)$ for a not necessarily symmetric bilinear form β. It seems to be hard to find a counterexample if this condition is violated.

THEOREM 7.22. *Let (V, Q) be a non degenerate quadratic space over F of dimension n, put $m = \lfloor \frac{n}{2} \rfloor$ and $\delta(F^\times)^2 = (-1)^m \det_B(V)$.*

a) *If n is even, $C(V, Q)$ is central simple over F and isomorphic to a tensor product of quaternion algebras. The second Clifford algebra $C_0(V, Q)$ has center isomorphic to $F[X]/(X^2 - \delta)$ and is central simple over $F(\sqrt{\delta})$ if δ is not a square in F.*
b) *Let n be odd. Then $C_0(V, Q)$ is central simple over F and isomorphic to a tensor product of quaternion algebras. The center of $C(V, Q)$ is isomorphic to $F[X]/(X^2 - \delta) \cong (\delta)_F$ and $C(V, Q)$ is central simple over $F(\sqrt{\delta})$ if δ is not a square in F. Moreover, one has $C(V, Q) \cong C_0(V, Q)\hat{\otimes}(\delta)_F$ as graded algebras.*

PROOF. We have already proven the assertion for $n = 1, 2, 3$ and proceed by induction for general $n > 3$, assuming the assertion to be proven for smaller dimensions.
We split V into a sum $V = U \perp W$ with non degenerate $U, W, \dim(U) = 3$ and have $C(V, Q) \cong C(U, Q)\hat{\otimes}C(W, Q)$. By Example 7.17 and Theorem 7.19 we have $C(U, Q) \cong A_U \otimes (-\det_B(U))_F$, where A_U is a trivially graded quaternion algebra over F and is isomorphic to the second Clifford algebra $C_0(U, Q)$. Again by Theorem 7.19 we have $(-\det_B(U))_F\hat{\otimes}C(W, Q) \cong C(W_1, Q_1)$, where the $(n-2)$ dimensional space (W_1, Q_1) is the orthogonal sum of (W, Q) and a one dimensional space of determinant $-\det_B(U)$, so that $C(V, Q) \cong A_U \otimes C(W_1, Q)$ (where the tensor product may be taken ungraded since A_U is trivially graded). By the inductive assumption the assertion follows. $\square$

REMARK 7.23. The graded center $\hat{Z}(A)$ of a $\mathbb{Z}/2\mathbb{Z}$-graded algebra A is defined as $\hat{Z}(A) = \hat{Z}_0(A) \oplus \hat{Z}_1(A)$ where $z \in \hat{Z}_i(A) \subseteq A_i$ satisfies $za = (-1)^{ij} az$ for all $a \in A_j(A)$, see [**38, 26**]. A graded algebra is then called a central simple graded algebra if it is simple and has trivial graded center. As in the theory of central simple algebras, the tensor product of central simple graded algebras is again a central simple graded algebra, and one can define the Brauer-Wall group of central simple graded algebras, see again [**38, 26**]. In particular, one proves as above by induction that the Clifford algebra of a non degenerate quadratic space is a central simple graded algebra and one may consider its class in the Brauer-Wall group. Notice that [**38**] treats the case that F has characteristic 2 as well, with slightly different definitions.

7.3. The invariants of Clifford-Witt and Hasse

DEFINITION 7.24. Let (V, Q) be a non degenerate quadratic space over the field F.

a) The Clifford-Witt invariant $cw(V) = cw(V, Q)$ is the class of $C(V, Q)$ in the Brauer group $Br(F)$ if $n = \dim(V)$ is even and the class of $C_0(V, Q)$ in $Br(F)$ if n is odd.
b) Let $(V, Q) \cong [a_1, \dots, a_n]$. Then the Hasse invariant $s(V) = s(V, Q)$ of (V, Q) is the class of

$$\bigotimes_{1 \le i < j \le n} (a_i, a_j)_F$$

in $Br(F)$.

REMARK 7.25. a) Since both the Clifford-Witt and the Hasse invariant are a product of classes of quaternion algebras in the Brauer group, they are in fact elements of the 2-torsion subgroup $Br_2(F)$ of the Brauer group of F.
b) The definition of the Hasse invariant seems to depend on the choice of an orthogonal basis of V. We will show that this is not the case.
c) The name Clifford-Witt invariant is a combination of the name Witt invariant that has been T. Y. Lam in [**26**] and the names Clifford invariant and Witt invariant used by W. Scharlau, who defines a (more general) Witt invariant related to K-theory by its relation to the Hasse invariant and a Clifford invariant in the same way as we do and then shows that they coincide when both are defined. The invariant in this form seems to have first been used by C. T. C. Wall in his article "Graded Brauer algebras" of 1964, without giving it a name there (it is called the invariant D of the Clifford algebra). Witt used a related but somewhat different invariant.

THEOREM 7.26. *Let $(V, Q), (W, Q')$ be non degenerate quadratic spaces over F and write* $\operatorname{disc}_B(V) = (-1)^{\lfloor \dim(V)/2 \rfloor} \det_B(V)$. *Then*

$$cw(V \perp W) = cw(V)cw(W) \cdot \begin{cases} (\operatorname{disc}_B(V), \operatorname{disc}_{B'}(W))_F & \dim(W) \equiv \dim(V) \bmod 2 \\ (-\operatorname{disc}_B(V), \operatorname{disc}_{B'}(W))_F & \dim(V) \textit{ odd}, \dim(W) \textit{ even} \end{cases}.$$

PROOF. Let first $V \cong [d]$ have dimension 1. If $\dim(W)$ is odd, we have

$$\begin{aligned} C(V \perp W) &\cong (d)_F \hat{\otimes} C(W) \\ &\cong (d) \hat{\otimes} (\operatorname{disc}_{B'}(W)) \hat{\otimes} C_0(W) \\ &\cong (\operatorname{disc}_B(V), \operatorname{disc}_{B'}(W))_F \otimes C_0(W), \end{aligned}$$

which implies $cw(V \perp W) = (\operatorname{disc}_B(V), \operatorname{disc}_{B'}(W))_F cw(V)cw(W)$.

If $\dim(W) \geq 2$ is even we set $W = W_1 \perp [a]$ and have, using Example 7.17,

$$\begin{aligned} C(V \perp W) &= C(W_1 \perp [a, d]) \\ &\cong C_0(W_1)\hat{\otimes}(\mathrm{disc}_{B'}(W_1)_F\hat{\otimes}(a)_F\hat{\otimes}(d)_F \\ &\cong C_0(W_1)\hat{\otimes}(-d \cdot \mathrm{disc}_{B'}(W_1), -ad)_F\hat{\otimes}(-ad \cdot \mathrm{disc}_{B'}(W_1))_F \end{aligned}$$

and hence $C_0(W \perp [d]) \cong C_0(W_1) \otimes (-d \cdot \mathrm{disc}_{B'}(W_1), -ad)_F$.
On the right hand side of the assertion we compute

$$\begin{aligned} &cw(W)cw(V)(-d, -\mathrm{disc}_{B'}(W))_F \\ &\quad = C_0(W_1)\hat{\otimes}(\mathrm{disc}_{B'}(W_1))_F\hat{\otimes}(a)_F(-d, -\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(W_1) \cdot (\mathrm{disc}_{B'}(W_1), a)_F \cdot (-d, -a \cdot \mathrm{disc}_{B'}(W_1))_F \\ &\quad = cw(W_1)(a, \mathrm{disc}_{B'}(W_1))_F(-d, \mathrm{disc}_{B'}(W_1)_F(-d, -a)_F \\ &\quad = cw(W_1)(-ad, \mathrm{disc}_{B'}(W_1))_F(-d, -ad)_F \\ &\quad = cw(W_1)(-d\mathrm{disc}_{B'}(W_1), -ad)_F, \end{aligned}$$

and we are done with the case $\dim(V) = 1$.
We use now induction on $\dim(V) + \dim(W)$. If both dimensions have opposite parity we may assume that $\dim(V)$ is odd. We write $V = V_1 \perp [d]$ and have

$$\begin{aligned} &cw(V \perp W) \\ &\quad = cw(V_1 \perp W \perp [d]) \\ &\quad = cw(V_1 \perp W)(-d, \mathrm{disc}_B(V_1)\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V_1)cw(W)(\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F(-d, \mathrm{disc}_B(V_1)\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V)(-d, \mathrm{disc}_B(V_1))_F cw(W)(\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F(-d, (\mathrm{disc}_B(V_1)\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V)cw(W)(\mathrm{disc}_B(V_1), -d)_F(\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F(-d, \mathrm{disc}_B(V_1)\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V)cw(W)(\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F(-d, \mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V)cw(W)(-\mathrm{disc}_B(V), \mathrm{disc}_{B'}(W))_F \end{aligned}$$

as asserted.
If both dimensions have the same parity we assume first that both are even and write $V = V_1 \perp [d]$ again and obtain

$$\begin{aligned} &cw(V \perp W) \\ &\quad = cw(V_1 \perp W)(d, \mathrm{disc}_B(V)\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V_1)cw(W)(-\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F(d, \mathrm{disc}_B(V)\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V)cw(W)(d, \mathrm{disc}_B(V_1))_F)(-\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F(d, \mathrm{disc}_B(V)\mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V)cw(W)(-d\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F \\ &\quad = cw(V)cw(W)(\mathrm{disc}_B(V), \mathrm{disc}_{B'}(W))_F \end{aligned}$$

as asserted. If finally both dimensions are odd, we obtain in the second step above a factor $(\mathrm{disc}_B(V_1), -\mathrm{disc}_{B'}(W))_F$ instead of $(-\mathrm{disc}_B(V_1), \mathrm{disc}_{B'}(W))_F$ and proceed analogously. $\square$

COROLLARY 7.27. *The Clifford-Witt invariant $cw(V,Q)$ depends only on the Witt class of (V,Q). In particular, if (V,Q) is hyperbolic or the orthogonal sum of a hyperbolic space and a one dimensional space, the Clifford-Witt invariant $cw(V,Q)$ is trivial.*

PROOF. From Example 7.17 we see that a hyperbolic plane has trivial Clifford-Witt invariant. The corollary then follows from the theorem since hyperbolic spaces have discriminant 1. □

PROPOSITION 7.28. *The Clifford-Witt invariant and the Hasse invariant are related by*

$$s(V) = cw(V) \cdot \begin{cases} 1 & \dim(V) \equiv 1,2 \bmod 8 \\ (-1,-\det_B(V))_F & \dim(V) \equiv 3,4 \bmod 8 \\ (-1,-1)_F & \dim(V) \equiv 5,6 \bmod 8 \\ (-1,\det_B(V))_F & \dim(V) \equiv 0,7 \bmod 8 \end{cases}.$$

In particular, the Hasse invariant is independent of the choice of an orthogonal basis of (V,Q).

PROOF. We write $V = V_1 \perp [a]$ and use induction on $\dim(V)$; the assertion is clear for $\dim(V) = 1,2$. Assume $\dim(V) > 2$ and the assertion to be proven for all smaller dimensions. We have always $s(V) = s(V_1)(a,\det_B(V_1))_F$ by the multiplicative properties of the symbol $(\ \ ,\ \ )_F$. If $\dim(V_1)$ is even, we have $cw(V) = cw(V_1)(-a,(-1)^{\dim(V)/2}\det_B(V))_F$, if $\dim(V_1)$ is odd, we have $cw(V) = cw(V_1)(a,(-1)^{(\dim(V)-1)/2}\det_B(V))_F$. Upon inserting the relations given for V_1 by the inductive assumption and comparing the factors we obtain the assertion. □

REMARK 7.29. Let (V,Q) be a non degenerate quadratic space of dimension $n = 2m$ or $n = 2m+1$ over F and W a hyperbolic space of dimension $2m$ over F, put $\tilde{V} = W$ if $\dim(V) = 2m$ is even and $\tilde{V} \cong W \perp [1]$ if $\dim(V)$ is odd. Then $cw(V) = cw(V \perp \tilde{V})$ and $cw(V \perp \tilde{V})$ is the Brauer class of the Clifford algebra of $V \perp \tilde{V}$. One could use this construction to define the Clifford-Witt invariant without a distinction of cases between even and odd dimensions. Witt defined his invariant in [**40**] similarly but used a space $V' \cong [-1] \perp \cdots \perp [-1]$ of dimension n instead of our $\tilde{V}$.

7.4. Classifying invariants over local and global fields

LEMMA 7.30. *Let $F = F_v$ be a local field of characteristic $\neq 2$ with valuation v. The subgroup of the Brauer group $Br(F)$ generated by the classes of quaternion algebras is isomorphic to $\{\pm 1\}$ if $F \ncong \mathbb{C}$ and is trivial for $F = \mathbb{C}$.*
Under this isomorphism the Brauer class of the algebra $(a,b)_F$ is mapped to the Hilbert symbol $(a,b)_v$.

PROOF. The case $F = \mathbb{C}$ is trivial, for $F = \mathbb{R}$ it is well known that the Hamilton quaternions are up to isomorphy the only quaternion division algebra over F. We therefore assume that F is not archimedean in the sequel. By Theorem 5.31 there is a unique isometry class of anisotropic quadratic spaces of dimension 4 over F,and this space has determinant 1 and is universal. It is therefore isometric to $[1] \perp [-a] \perp [-b] \perp [ab]$ for some $a, b \in F^\times$ and is hence the quadratic space given by the quaternion algebra $(a, b)_F$ with the quaternion norm as quadratic form. This quaternion algebra is therefore the unique quaternion division algebra over F. □

REMARK 7.31. For a local field F we identify the the Brauer class of the quaternion algebra $(a, b)_F$ with the Hilbert symbol $(a, b)_v \in \{\pm 1\}$.

THEOREM 7.32. *Over a local field F of characteristic $\neq 2$ regular quadratic spaces (V, Q) are classified up to isometry by dimension, determinant, and Clifford-Witt (or Hasse) invariant.*
In particular, for given dimension and determinant there exist at most two isometry classes of regular quadratic spaces over F.

PROOF. Dimension 1 is trivial, dimension 2 follows from Lemma 7.10 and Example 7.17, dimension 3 from Lemma 7.11 and Example 7.17, both without any assumption on F.
Assume now that $\dim(V) = \dim(W) = n > 3$ and that the assertion is true for spaces of dimension smaller than n. The spaces $V \perp [-1], W \perp [-1]$ are isotropic, having dimension ≥ 5, hence V, represent 1 and can be written as $W \cong [1] \perp V', W \cong [1] \perp W'$ with $s(V') = s(W'), \det(V') = \det(W')$ the inductive assumption implies $V' \cong W'$, and the assertion follows. □

THEOREM 7.33. *Let $F = F_v$ be a non archimedean local field of characteristic $\neq 2$, let (V, Q) be a non degenerate quadratic space over F of dimension ≥ 2, not isometric to a hyperbolic plane.*
Then there exists a non degenerate quadratic space (W, Q') over F of the same dimension and determinant as (V, Q) with $s(W) = -s(V)$ (hence $cw(W) = -cw(W)$).

PROOF. If $\dim(V) = 2$ we put $(V, Q) \cong [a, b]$ and have $s(V) = cw(V) = (a, b)_v$, by assumption $-ab$ is not a square in F. If $-ab$ is a unit choose c to be a prime element π in F, if $-ab$ is (up to squares) a prime element, let $c \in F$ be a unit for which $F(\sqrt{c})$ is the (unique) unramified quadratic extension of F.
In both cases we have $(ca, cb)_v = (ca, -ab)_v = (c, -ab)_v (a, b)_v$ with $(c, -ab)_v = -1$, so $(W, Q') \cong [ca, cb]$ is as desired.
Let now $\dim(V) \geq 3$ and let c be the non square unit of F given above, let $U \cong [1, \pi], U' \cong [c, c\pi]$, where π is a prime element, we have $\det(U) = \det(U')$ and $cw(U) = -cw(U')$.
The space $V \perp U$ has dimension ≥ 5 and is hence isotropic and universal, so it represents c and can be written as $V_1 \perp [c]$, where V_1 has dimension 4 and is hence universal as well, so it represents $c\pi$. we can therefore write

$U \perp V \cong U' \perp V'$, where V' has the same dimension and determinant as V but opposite Clifford-Witt invariant. □

COROLLARY 7.34. *For $n \geq 3$ there exists a (up to isometry unique) regular quadratic space over the non archimedean local field F with* $\mathrm{char}(F) \neq 2$ *with given determinant and Clifford-Witt invariant.*

PROOF. Obvious. □

THEOREM 7.35. *Let F be a number field, fix $n \in \mathbb{N}$ and let non degenerate quadratic spaces (V_v, Q_v) of dimension n over F_v be given for all places v of F, denote by S_v resp. cw_v the Hasse resp. Clifford-Witt invariants for the completion F_v.*
Then a quadratic space (V, Q) over F with all completions isometric to the given spaces (V_v, Q_v) exists if and only if one has

a) *There exists $d \in F$ with $d(F_v^\times)^2 = \det(V_v)$ for all places v of F.*
b) *The Hasse invariants $s_v(V_v)$ (equivalently: The Clifford-Witt invariants) are equal to 1 for almost all places v.*
c) *The product of the Hasse (or the Clifford-Witt) invariants $s_v(V_v)$ (resp. $cw_v(V_v)$ over all places v is 1.*

PROOF. The necessity of the conditions follows immediately from the reciprocity theorem for the Hilbert symbol. We have to prove the existence of the global space if the conditions for the local spaces are satisfied; this is trivial for $n = 1$.
Let $n \geq 2$ and write $(V_v, Q_v) \cong [a_1^{(v)}, \dots, a_n^{(v)}]$ for all v in the set of places Σ_F of F. Let $T \subseteq \Sigma_F$ be a finite set containing all archimedean places and all places v with $s_v(V_v) = -1$. By the weak approximation theorem of algebraic number theory we find $a_1, \dots, a_{n-1} \in F$ such that a_i is in the square class of $a_i^{(v)}$ at all $v \in T$ for $1 \leq i \leq n-1$.
The space $W \cong [a_1, \dots, a_{n-1}, da_1a_2 \dots a_{n-1}]$ over F of determinant $d(F^\times)^2$ satisfies $W_v \cong V_v$ for all $v \in T$ and hence $s_v(W_v) = s_v(W_v)$ for all $v \in T$.
The set $S = \{v \in \Sigma_F \mid s_v(W_v) = -s_v(V_v)\}$ is therefore a finite subset of $\Sigma_F \setminus T$ satisfying $W_v \cong V_v$ for all $v \notin S$, since for these v both spaces have Hasse invariant 1 (and the same determinant). On the other hand, for $v \in S$ the spaces V_v and W_v have the same determinant and are not isometric, so that in particular neither of these spaces over F_v can be a hyperbolic plane.
If $S \neq \emptyset$ we have $S = \{v \in \Sigma_F \setminus T \mid s_v(W_v) = -1\}$, and one sees

$$\prod_{v \in S} s_v(W_v) = \prod_{v \in S} s_v(W_v) \prod_{v \notin S} s_v(V_v) = \prod_{v \in \Sigma_F} s_v(W_v) = 1,$$

so that S has even cardinality.
Again by weak approximation we find $\beta \in F^\times$ which is a square at all archimedean places and not a square at all $v \in S$, and by the Hilbert reciprocity law we can find $\alpha \in F^\times$ satisfying $(\alpha, \beta)_v = -1$ if and only if $v \in S$.
Let U, U' be binary quadratic spaces over F with $U \cong [1, -\beta], U' \cong [\alpha,$-$alpha\beta]$. We have $s_v(U') = (\alpha, -\alpha\beta)_v = (\alpha, -1)_v(\alpha, -\beta)_v = (\alpha, \beta)_v$ for $v \notin S$, hence $U_v \cong U'_v$ for $v \notin S$ and $U_v \ncong U'_v$ for $v \in S$.

For $n \geq 3$ and $v \in S$ we obtain as in the proof of Theorem 7.32 that U'_v is represented by $U_v \perp W_v$. If $n = 2$ holds, the space $U_v \perp W_v$ represents α since it is universal, and we can write $U_v \perp W_v \cong [\alpha, c_1, c_2, c_3]$. If $-\alpha\beta$ were not represented by $[c_1, c_2, c_3]$, the space $[c_1, c_2, c_3, \alpha\beta]$ would be anisotropic, hence of square determinant, so we had $\alpha\beta \in c_1c_2c_3(F^\times)^2$. From this we find $\det(U_v \perp W_v) = \alpha c_1c_2c_3(F^\times)^2 = \beta(F^\times)^2 = -\det(U_v)$, which implies that W_v is a hyperbolic plane, a contradiction. So U'_v is represented by $U_v \perp W_v$ in the case $n = 2$ too. Since $U_v \cong U'_v$ for all $v \notin S$ we see that U' is represented by $U \perp W$ locally everywhere, and by the Minkowski Hasse local global principle we can write $U \perp W \cong U' \perp W'$ with some space W' over F of dimension n and determinant d which satisfies $s_v(W'_v) = s_v(V_v)$ for all $v \in \Sigma_F$ as desired. □

COROLLARY 7.36. *For any given signature (n_+, n_-) there exists at most one genus of even unimodular $\mathbb{Z}$-lattices. Such a genus exists if and only if one has $n_+ \equiv n_-$ mod 8.*

PROOF. An even unimodular $\mathbb{Z}$-lattice Λ of signature (n_+, n_-) has determinant $(-1)^{n_-}$. The isometry class of Λ_p is by Hensel's lemma determined by the isometry class of its reduction $\Lambda_p/p\Lambda_p$ as (regular) quadratic space over $\mathbb{F}_p$, which for odd p is determined by the determinant. This shows that the isometry class of the completion of the space V supporting Λ is determined by the signature at all places of $\mathbb{Q}$ except perhaps at the prime $p = 2$. But then the Hilbert reciprocity law implies that the Hasse invariant at 2 is also determined, which by Theorem 7.32 implies that there is only one possibility for the isometry class of the completion V_2 at the prime 2, and by the Minkowski-Hasse theorem the class of V is determined by the fixed signature. Finally, an even unimodular lattice has $\mathbb{Z}_p$-maximal completions at all primes p, and since all $\mathbb{Z}_p$-maximal lattices on the same space V_p are isometric, the genus of such a lattice is uniquely determined, if it exists.
For the existence question we have by the Hilbert reciprocity law that $s_2(V_2) = (-1)^{\frac{n_-(n_--1)}{2}}$. Moreover, the space V_2 supports an even unimodular lattice of determinant $(-1)^{n_-}$ and dimension $n_- + n_+ = n$ if and only if $n = 2m$ is even and V_2 is hyperbolic, in which case its Hasse invariant is $(-1)^{\frac{m(m-1)}{2}}$. This is equivalent to $n_- \equiv m$ mod 4, hence to $n_+ + n_- = 2m \equiv 2n_-$ mod 8, which is finally equivalent to $n_+ \equiv n_-$ mod 8 as asserted. □

REMARK 7.37. There exist several different proofs of the last corollary. The existence of such a lattice also follows from the explicit construction of the positive definite E_8 root-lattice.

CHAPTER 8

The Maßformel of Smith, Minkowski and Siegel

In this chapter we continue the study of quadratic lattices over a ring of integers R in a global field F of characteristic different from 2, in particular over the ring of integers of a number field. We keep the notations of chapter 6. If $R = R_T$ for some fixed set T of places of F we will usually omit T in the notations. A (quadratic) R-module Λ for such an R can always be viewed as a lattice on the vector space $V = \Lambda \otimes_R F$ over F, with the natural extension of the quadratic form Q and its associated symmetric bilinear form b to V.

As a consequence of the Minkowski-Hasse theorem we had seen in Theorem 6.15 that a lattice M which is represented locally everywhere by the lattice Λ is represented globally by some lattice in the genus of Λ. Siegel's Maßformel (or mass formula or measure formula), also called Siegel's main theorem for (integral) quadratic forms, gives a quantitative version of this statement, expressing a weighted average over the genus of Λ of the numbers or measures of representations of M by the lattices in the genus as a product of local data. This extended earlier work of Smith and of Minkowski on the average of the inverses of the numbers of isometric automorphisms of the lattices in a genus.
We take the occasion to add a comment on the naming of the formula: In Siegel's three fundamental articles "Über die analytische Theorie der quadratischen Formen" [**32, 33, 34**] written in german in Annals of Mathematics, Siegel calls it the Massformel, following earlier terminology of Eisenstein und Minkowski, who defined and investigated the "Maß eines Genus" (english: the measure of a genus). Since the printer of the Annals apparently had no type for the special german letter ß, the word was not printed as Maßformel but as above as Massformel, which in later english texts changed to mass formula. It is, however, concerned with measure (german: Maß), and not with mass (german: Masse) and would better be translated as measure formula if one doesn't want to use the original german word.

8.1. Class and genus of a representation

DEFINITION 8.1. Let R be a commutative ring and $\phi_i : (M, Q') \to (\Lambda_i, Q_i)$ for $i = 1, 2$ be representations of quadratic R-modules. One says that ϕ_1, ϕ_2 belong to the same *class of representations* or that they are equivalent over

R if there is an isometry $\psi : (\Lambda_1, Q_1) \to (\Lambda_2, Q_2)$ with $\phi_2 = \psi \circ \phi_1$; one writes then $\phi_2 \in \mathrm{cls}(\phi_1)$.
If R is a ring of integers of the global field F and M and the Λ_i are R-lattices, the representations ϕ_1, ϕ_2 are said to belong to the same *genus (more precisely: R-genus or T-genus for $R = R_T$) of representations* if their coefficient extensions to the completions R_v are equivalent over R_v for all $v \in \Sigma_F \setminus T$ and their extensions to F_v are equivalent over F_v for the $v \in T$, one writes then $\phi_2 \in \mathrm{gen}(\phi_1)$ or $\phi_2 \in \mathrm{gen}_T(\phi_1)$.

Obviously, genera of representations consist of full classes of representations and the relations of belonging to the same class or to the same genus of representations are equivalence relations. If ϕ is a primitive representation then all representations in its class and in its genus are primitive.
Representations in the same class are by isometric quadratic modules. Similarly, representations in the same genus are representations by lattices in the same genus of lattices.
An isometry $\rho : M \to M'$ of quadratic modules induces a natural bijection between the representations of M and those of M' which respects classes and genera of representations. In particular, if $\phi : (M, Q') \to (\Lambda, Q)$ is a representation we can instead consider the inclusion mapping $i = i_\phi : (\phi(M), Q|_{\phi(M)}) \to (\Lambda, Q)$ of the lattice $\phi(M)$ in the class of M, it is sometimes called a special representation. Obviously, the inclusion mappings $i_1 : M \to \Lambda_1, i_2 : M \to \Lambda_2$ are in the same class if and only if there exists an isometry $\psi : \Lambda_1 \to \Lambda_2$ with $\psi|_M = \mathrm{Id}_M$.
If the ground ring R is $\mathbb{Z}$, representations are sometimes treated in matrix language, we give the definitions in that setting and provide the link to the lattice setting:

DEFINITION 8.2. Let $r \le n \in \mathbb{N}$. For symmetric matrices $S \in M_n(\mathbb{Z}), T \in M_r(\mathbb{Z})$ and $X \in M_{n,r}(\mathbb{Z})$ of rank r with $T = {}^tXSX$ we say that (X, S) is a representation of T. The representation is called primitive if X can be completed to a matrix in $GL_n(\mathbb{Z})$.

a) The representations $(X, S), (X', S')$ are in the same class if there exists $A \in GL_n(\mathbb{Z})$ with $S' = {}^tASA, X = AX'$.
b) The representations $(X, S), (X', S')$ are in the same genus if there exist for all primes p (including $p = \infty$) matrices $A_p \in GL_n(\mathbb{Z}_p)$ with $S' = {}^tA_pSA_p, X = A_pX'$.

REMARK 8.3.
For $S = S'$ the representations $(X, S), (X', S)$ are in the same class if and only if X, X' are in the same orbit under the action of the group of automorphisms of S.

LEMMA 8.4. *Let $\phi : M \to \Lambda, \psi : M \to \Lambda'$ be representations, let $T = (b(u_i, u_j))$ be the Gram matrix of K with respect to the $\mathbb{Z}$-basis $\{u_1, \dots, u_m)$ and S, S' the Gram matrices of Λ, Λ' with respect to the bases $\{v_1, \dots, v_n)$,*

$(v'_1, \dots, v'_n)$, *write* $\phi(u_j) = \sum_i x_{ij} v_i, \psi(u_j) = \sum_i x'_{ij} v'_i, X = (x_{ij}), X' = (x'_{ij}) \in M_{n,r}(\mathbb{Z})$.

a) *One has* $T = {}^t X S X = {}^t X' S' X'$.
b) ϕ *is primitive if and only if* (X, S) *is primitive.*
c) ϕ, ψ *are in the same class if and only if* $(X, S), (X', S')$ *are in the same class.*
d) ϕ, ψ *are in the same genus if and only if* $(X, S), (X', S')$ *are in the same genus.*

PROOF. This is easily checked. □

LEMMA 8.5. *Let* (M, Q') *and* (Λ_j, Q_j) *for* $j = 1, 2$ *be quadratic* $R = R_T$*-lattices on the quadratic spaces* $(W, Q'), (V_1, Q_1), (V_2, Q_2)$ *over the global field* F *with a ring of integers* $R = R_T$ *with* (W, Q') *or* (V_j, Q_j) *regular for* $j = 1, 2$, *assume that* (Λ_1, Q_1) *and* (Λ_2, Q_2) *are in the same genus. Let* $\phi_j : M \to \Lambda_j$ *for* $j = 1, 2$ *be representations.*
Then there is a lattice Λ' *on* V_1 *and a representation* $\phi' : M \to \Lambda'$ *in the class of the representation* ϕ_2.
If one has here $M \subseteq \Lambda_1$ *and* ϕ_1 *is the inclusion mapping* i_{M,Λ_1} *from* M *into* Λ_1, *the representation* ϕ' *above can also be chosen to be the inclusion* $i_{M,\Lambda'}$ *of* M *into* Λ'.

PROOF. If (W, Q') is regular, the representations may be viewed as representations into the regular spaces $V_j / \operatorname{rad}(V_j)$, we may therefore assume that the (V_j, Q_j) are regular. By assumption (V_1, Q_1) is isometric to (V_2, Q_2) over all completions F_v, by the Minkowski-Hasse theorem there exists an isometry $\sigma : V_2 \to V_1$ over F. Then $\phi' := \sigma \circ \phi_2 : M \to \Lambda' := \sigma(\Lambda_2)$ is a representation in the class of ϕ_2 as requested.
If we assume now that M is a sublattice of Λ_1 and that ϕ_1 is the inclusion mapping, we choose $\sigma : V_2 \to V_1$ and $\phi' = \sigma \circ \phi_2$ as above. The isometric map $\phi' : M \to \Lambda' \subseteq V_1$ extends to an isometry from the vector space $W \subseteq V_1$ over F generated by M onto the space W' generated by $\phi'(M) \subseteq V_1$. We denote by ρ' its inverse and find by Witt's extension theorem an isometry $\rho \in O(V_1, Q_1)$ extending ρ'. The map $\phi'' = \rho \circ \phi' : M \to \Lambda'' := \rho(\Lambda') \subseteq V_1$ is then the identity on W, so that ϕ'' and Λ'' are as requested. □

THEOREM 8.6. *Let* R *be the ring of integers of the number field* F, *let* M *be an* R*- lattice on the non degenerate quadratic space* (W, Q') *over* F. *Then for any given dimension* n *and fixed* $d \in \mathbb{N}$ *there are only finitely many classes of representations of* (M, Q') *into* (Λ, Q), *where* Λ *is an integral* R*-lattice on a non degenerate quadratic space* (V, Q) *of dimension* n *over* F *such that the norm of the volume ideal of* (Λ, Q) *equals* d.

PROOF. We can restrict attention to inclusions $M \to \Lambda$. With $V = W \perp U$ we put $K = \Lambda \cap U$. By Theorem 2.16 (which, as noticed in Section 2.3) stays valid for lattices over $\mathfrak{o}$ we have $\mathfrak{v}_b K \mid \mathfrak{v}_b(M) \mathfrak{v}_b \Lambda$ by b) of that Theorem. By the version of Theorem 6.10 for number rings (see the remark after that theorem) there are only finitely many possibilities for the isometry class of K, denote representatives by (K_i, Q_i) and by U_i the F-space generated by K_i, put $V_i = W \perp U_i$. If $\psi : K \to K_i$ is an isometry, the inclusion of M into the lattice $(\mathrm{Id}_W, \psi)(\Lambda) \subseteq M^\# \perp K_i^\# \subseteq V_i$ (where the duals are taken with regard to the spaces of the lattices M, K_i) is in the class of the inclusion $M \to \Lambda$ and has image in one of the finitely many lattices lying between $M \perp K_i$ and $M^\# \perp K_i^\#$. Taken together, the given inclusion $M \to \Lambda$ is in the class of one of finitely many inclusions, as asserted. □

It is of interest to study representations of degenerate lattices as well, e.g. representations of 0. Indeed with a suitable primitivity condition we can extend the finiteness statement above to that situation.

DEFINITION 8.7. Let $\phi : M \to \Lambda$ be a representation of lattices on quadratic spaces $(W, Q'), (V, Q)$ and extend ϕ to an isometric map (also denoted by ϕ) from W to V.
The representation ϕ is said to be of *imprimitivity bounded by* $c \in \mathbb{N}$ if one has $(\phi(W) \cap \Lambda : \phi(M)) \leq c$. We also call the index $(\phi(W) \cap \Lambda : \phi(M))$ the *imprimitivity index* of the representation ϕ.

REMARK 8.8.
a) Since there exists $a \in R$, $a \neq 0$ with $a(\phi(W) \cap \Lambda) \subseteq \phi(M)$, the imprimitivity index is always finite if $R = R_T$ is a ring of integers in the global field F, or more generally an integral domain with finite residue class rings R/Ra.
b) If $R = R_T$ is a ring of integers in the global field F, almost all imprimitivity indices of the completions ϕ_v of a representation ϕ are equal to 1, and the imprimitivity index of ϕ equals the product over the $v \in \Sigma_F \setminus T$ of the imprimitivity indices of the completions ϕ_v.
c) Obviously ϕ is primitive if and only if it is of imprimitivity bounded by 1. Since representations in the same class have the same imprimitivity index and the imprimitivity index can assume arbitrarily large values for representations of a degenerate lattice, it is clear that a finiteness statement as in the theorem above can not hold for representations of degenerate lattices unless one imposes a bound on the imprimitivity index.

THEOREM 8.9. *Let M be an R- lattice on the quadratic space (W, Q') over the number field F with ring of integers R. Then for any given dimension n and fixed $c, d \in \mathbb{N}$ there are only finitely many classes of representations of (M, Q') into (Λ, Q) of imprimitivity bounded by c, where Λ is an integral lattice on a non-degenerate quadratic space (V, Q) of dimension n over F such that the norm of the volume ideal of (Λ, Q) equals d.*
In particular, any genus of representations of (M, Q') into a non-degenerate lattice contains only finitely many classes.

PROOF. Again we have to consider only inclusions $i_{M,\Lambda} : M \to \Lambda$. We can moreover restrict attention to primitive representations: If $i_{M\Lambda} : M \to$

Λ is (without loss of generality) an inclusion of imprimitivity index bounded by c and $M' = W \cap \Lambda$, then M is one of the finitely many sublattices of M' of index $\le c$, so if there are only finitely many possibilities for the class of the inclusion $i_{M',\Lambda}$, the same holds for the class of $i_{M,\Lambda}$.
For simplicity we treat the case $\mathbb{R} = \mathbb{Z}$ first and indicate the necessary changes for general R in the end.
We assume first that $\mathrm{rad}(M) = M$, i.e., $Q|_W = 0$, (M, Q) is totally isotropic. With $\tilde{b}^{(W)} : V \to W^*$ as usual $\tilde{b}^{(M)}(\Lambda)$ is a sublattice of full rank of M^* (which we identify with $\{f \in W^* \mid f(M) \subseteq R\}$), so there are a basis $(y_1^*, \dots, y_r^*)$ of M^* and $c_1, \dots c_r \in R$ with $c_i \mid c_{i+1}$ such that the $c_i y_i^*$ form a basis of $\tilde{b}^{(M)}(\Lambda)$. We choose $z_i \in c_i^{-1}\Lambda \subseteq V$ with $\tilde{b}^{(M)}(z_i) = y_i^*$ and denote by $(x_1, \dots, x_r)$ the basis of M dual to $(y_1^*, \dots, y_r^*)$, by primitivity of M it can be extended to a basis of Λ. We have then $b(x_i, \Lambda) = c_i\mathbb{Z}$ and see by looking at the Gram matrix of this basis of Λ that $c_1 \dots c_r$ divides $\det(\Lambda)$. Since $\det(\Lambda)$ is fixed this leaves only finitely many possibilities for the c_i.
The $c_i z_i$ are determined only modulo elements of the orthogonal complement $K \supseteq M$ of M in Λ, so changing $c_i z_i$ by vector in $\sum_{j=1}^{i} \mathbb{Z}x_j \subseteq M$ for $1 \le i \le r$ we can achieve $0 \le b(c_i z_i, c_j z_j) \le c_i$ for $j \le i$. The lattice $M' = M + \sum_{i=1}^{r} \mathbb{Z}c_i z_i \subseteq \Lambda$ is then a non degenerate sublattice of Λ of rank $2r$ whose Gram matrix with respect to the basis $(x_1, \dots, x_r, z_1, \dots, z_r)$ is from a finite supply, so there are only finitely many possible isometry classes for M'. Moreover, for each of these M' there are only finitely many possible classes of inclusions $M \to M'$. By the previous theorem each of the possible non degenerate M' has only finitely many classes of inclusions into lattices Λ of rank n and determinant d.
To sum up, each inclusion $M \to \Lambda$ is in the class of one of the finitely many composite inclusions $M \to M' \to \Lambda$ constructed above, which proves the assertion in the case of totally isotropic M over $\mathbb{Z}$.
For general M we write $M = \mathrm{rad}(M) \perp M_1$ with non degenerate (M_1, Q). By the previous theorem there are only finitely many classes of inclusions $i_{M_1,\Lambda} : M_1 \to \Lambda$ with Λ integral of rank n and determinant d, these lead to finitely many possible isometry classes for the orthogonal complement K of M_1 in Λ. Our result in the totally isotropic case implies that we have to consider only finitely many classes of inclusions $\mathrm{rad}(M) \to K$. Finally, any inclusion $i_{M,\Lambda} : M \to \Lambda$ can be written as $(i_{\mathrm{rad}(M),K}, i_{M_1,\Lambda})$ as above, so there are only finitely many classes of such inclusions, as asserted.
The case of general R requires some modifications in the argument for the totally isotropic case since we have used the existence of bases at several points.
We have now $M^* = \bigoplus \mathfrak{a}_i y_i^*, \tilde{b}^{(M)}(\Lambda) = \bigoplus \mathfrak{c}_i \mathfrak{a}_i y_i^*$ with linearly independent $y_i * \in W^*$, fractional ideals $\mathfrak{a}_i$ from a fixed set of representatives of the ideal classes in R and integral ideals $\mathfrak{c}_i \subseteq R$. We choose again $z_i \in (\mathfrak{a}_i\mathfrak{c}_i)^{-1}\Lambda \subseteq V$ with $\tilde{b}^{(W)}(z_i) = y_i^*$ and $x_1, \dots, x_r \in W$ with $y_i^*(x_j) = \delta_{ij} = b(z_i, x_j)$. We have then $M = \bigoplus_{i=1}^{r} \mathfrak{a}_i^{-1} x_i$ and $b(x_i, \Lambda) = \mathfrak{a}_i\mathfrak{c}_i$. Over each completion all

the ideals are principal, so we can argue locally as in the case $R = \mathbb{Z}$ to see that $\mathfrak{c}_1 \dots \mathfrak{c}_r$ divides the volume ideal of Λ, thus there are again only finitely many possibilities for these ideals. Changing the z_i as above modulo $\mathfrak{c}_i^{-1}\mathfrak{a}_i^{-1}\sum_{j=1}^{i}\mathfrak{a}_j^{-1}x_j \subseteq$ we can change $b(z_i, z_j) \in (\mathfrak{a}_i\mathfrak{a}_j\mathfrak{c}_i\mathfrak{c}_j)^{-1}$ modulo $(\mathfrak{c}_i\mathfrak{a}_i\mathfrak{a}_j)^{-1}$ for $j \le i$, which allows us to reduce the $b(z_i, z_j)$ to a finite set of representatives of $(\mathfrak{a}_i\mathfrak{a}_j\mathfrak{c}_i\mathfrak{c}_j)^{-1}$ modulo $(\mathfrak{c}_i\mathfrak{a}_i\mathfrak{a}_j)^{-1}$. There are hence only finitely many possibilities for the isometry class of $M \oplus \sum_{i=1}^{r}\mathfrak{a}_i\mathfrak{c}_i z_i \subseteq \Lambda$, and the rest of the proof proceeds as above. □

THEOREM 8.10. *Let $R = R_v$ be the ring of integers in the local non archimedean field $F = F_v$, let M be an R-lattice on the quadratic space (W, Q') over F, let $c \in \mathbb{N}$. Then there are only finitely many classes of representations of imprimitivity bounded by c into non degenerate quadratic lattices (Λ, Q) of fixed rank n and determinant d.*

PROOF. As in the global case we can restrict attention to primitive inclusions $i_{M,\Lambda} : M \to \Lambda$. By considering the possible Jordan decompositions of Λ of fixed rank and determinant one sees that there are only finitely many possibilities for the isometry class of Λ. The rest of the proof goes through as in the global case. □

COROLLARY 8.11. *For M as in the theorem and Λ fixed there are only finitely many classes of representations of M by Λ.*
All representations of M by Λ for which the image of M is regularly embedded into Λ are in the same $R = R_v$-class, in particular, if M is regular, there is only one class of representations of M by Λ.

PROOF. The finiteness assertion is a consequence of the theorem. The assertion for regularly embedded M follows from Theorem 1.43. □

THEOREM 8.12. *Let $R = R_T$ be a ring of integers in the global field F, let M be a lattice on the quadratic $F-$ space (W, Q') and Λ an R-lattice on the regular quadratic space (V, Q). Assume that there exists a representation of M into Λ.*

a) *Let $\phi : M \to \Lambda'$ be a representation of M by a lattice Λ' in the genus of Λ. Then for all primes $v \in \Sigma_F \setminus T$ there is a representation $\psi_v : M_v \to \Lambda_v$ in the same R_v-class as $\phi_v : M_v \to \Lambda'_v$.*
b) *The map associating to the genus of the representation $\phi : M \to \Lambda'$ of M by a lattice Λ' in the genus of Λ the family $(\overline{\psi_v})_v$ of the R_v-classes $\overline{\psi_v}$ of the ψ_v from a) defines a bijection from the set of genera of representations of M by a lattice Λ' in the genus of Λ to the set of all families $(\overline{\psi_v})_{v\in\Sigma_F\setminus T}$, where the $\overline{\psi_v}$ are R_v-classes of representations of M_v by Λ_v almost all of which are the class of the inclusion $M_v \to \Lambda_v$.*
c) *Let $h_v(M_v, \Lambda_v)$ denote the number of R_v-classes of representations of M_v by Λ_v and $h_v^*(M_v, \Lambda_v)$ the number of R_v-classes of primitive representations of M_v by Λ_v. Then the number of genera of primitive representations of M by a lattice Λ' in the genus of Λ equals*

$\prod_v h_v^*(M_v, \Lambda_v)$. Moreover, if (W, Q') is regular, the number of genera of representations of M by a lattice Λ' in the genus of Λ equals $\prod_v h_v(M_v, \Lambda_v)$.

PROOF. Let $\phi : M \to \Lambda'$ be a representation of M by the lattice Λ' in the genus of Λ. Replacing M by $\phi(M)$ we may assume that ϕ is the inclusion $i_{M,\Lambda}$, and we can by Lemma 8.5 find a lattice $\Lambda'' \subseteq V$ containing M such that the inclusion $i_{M,\Lambda''} : M \to \Lambda''$ is in the class of ϕ. With an isometry $\rho_v : \Lambda''_v \to \Lambda_v$ we obtain for $v \in \Sigma_F \setminus T$ the local representation $\psi_v = \rho_v \circ i_{M_v,\Lambda''_v} : M_v \to \Lambda_v$ in the class of ϕ_v. For almost all v we have $\Lambda_v = \Lambda''_v$ so that we may choose $\rho_v = \mathrm{Id}_{V_v}$ and $\psi_v = i_{M_v,\Lambda_v} : M_v \to \Lambda_v$, which proves a).
One sees that the family of the classes of the ψ_v depends only on the genus of ϕ, so that we obtain a map from the set of genera of representations of M into a lattice in the genus of Λ to the set of families $(\overline{\psi_v})_{v\in\Sigma_F\setminus T}$, where the $\overline{\psi_v}$ are classes of representations of M_v into Λ_v almost all of which are the class of the inclusion $i_{M_v,\Lambda_v} : M_v \to \Lambda_v$. It is obvious that this map is injective. To show the surjectivity, let a family $(\overline{\psi_v})_v$ as above be given. For each of the finitely many v for which ψ_v is not in the class of the inclusion i_{M_v,Λ_v} we can by Witt's extension theorem find an isometry $\tau_v : V_v \to V_v$ with $\tau_v|_{M_v} = \psi_v$. There is a unique lattice $\Lambda' \supseteq M$ on V with $\Lambda'_v = \tau^{-1}\Lambda_v$ for these finitely many v and $\Lambda'_v = \Lambda_v$ for all other $v \in \Sigma_F$. The inclusion $i_{M,\Lambda'} : M \to \Lambda'$ is then the desired preimage of the family $(\overline{\psi_v})_v$, which proves b). For c) we notice first that almost all Λ_v are regular, hence Remark 1.34 implies that for any family of primitive $\psi_v : M_v \to \Lambda_v$ almost all $\psi_v(M_v)$ are regularly embedded into Λ_v. By Corollary 8.11 almost all ψ_v from such a family are then in the class of the inclusion $i_{M_v,\Lambda_v} : M_v \to \Lambda_v$, and we see that all families $(\overline{\psi_v})_v$ of classes of primitive representations are in the image of the map constructed in b). Since the preimage of the set of these primitive families consists of the genera of primitive representations the first part of c) follows.
Assume now that (W, Q') is regular. Then for almost all v the determinant of M is a unit in R_v, hence for almost all v all representations $\psi_v : M_v \to \Lambda_v$ are primitive. Since almost all Λ_v are regular, Remark 1.34 implies that for any family of $\psi_v : M_v \to \Lambda_v$ almost all $\psi_v(M_v)$ are regularly embedded into Λ_v, and by Corollary 8.11 almost all ψ_v are in the class of the inclusion $i_{M_v,\Lambda_v} : M_v \to \Lambda_v$. The image of the map constructed in b) is hence the set of all families $(\overline{\psi_v})_v$, and almost all of the $h_v(M_v, \Lambda_v)$ are equal to 1. This proves the second part of c). □

The next theorem transfers the study of the classes in the genus of a fixed representation into the study of double cosets in adelic orthogonal groups.

THEOREM 8.13. *Let R be a ring of integers in the global field F, let W be a subspace of the regular quadratic space (V, Q) over F, if W is regular let U denote the orthogonal complement of W in V. Write $O_U(F), O_V(F), O_W(F)$*

for the orthogonal groups of the spaces $(U,Q),(V,Q),(W,Q)$ *and* $O_U(\mathbb{A}_F)$, $O_V(\mathbb{A}_F), O_W(\mathbb{A}_F)$ *for their adelizations, consider the (adelic) orthogonal groups of* U, W *as subgroups of the (adelic) orthogonal group of* V *(acting trivially on the respective orthogonal complement). Write* $O_{V,W}(F) = \{\sigma \in O_V(F) | \sigma|_W = \mathrm{Id}_W\}$ *(with* $O_{V,W}(F)$ *identified with* $O_U(F)$ *if* W *is regular) and analogously* $O_{V,W}(\mathbb{A}_F)$.

Let Λ *be an* R*-lattice on* V *and* $M \subseteq \Lambda$ *a lattice on* W *and denote by* $i_{\Lambda'} = i_{M,\Lambda'}$ *the inclusion map of* M *into any lattice* Λ' *on* V *containing* M.

Then $O_{W,F}(\mathbb{A}_F)$ *acts transitively on the set of inclusions* $i_{M,\Lambda'}$ *in the genus of the inclusion* $i_{M,\Lambda}$ *by* $i_{M,\Lambda} \mapsto i_{M,\phi(\Lambda)}$ *for* $\phi \in O_{V,W}(\mathbb{A}_F)$. *This action induces a transitive action on the set of classes of representations in the genus of* $i_{M,\Lambda}$.

The stabilizer of $i_{M,\Lambda}$ *is the group*

$$O_{V,W}(\mathbb{A}_F;\Lambda) := O_{V,W}(\mathbb{A}_F) \cap O_\Lambda(\mathbb{A}_F) = \{\phi \in O_{V,W}(\mathbb{A}_F) \mid \phi(\Lambda) = \Lambda\}.$$

For $\phi, \phi' \in O_{V,W}(\mathbb{A}_F)$ *the inclusions* $i_{M,\phi(\Lambda)}, i_{M,\phi'(\Lambda)}$ *are in the same class if and only if*

$$O_{V,W}(F)\phi O_{V,W}(\mathbb{A}_F;\Lambda) = O_{V,W}(F)\phi' O_{V,W}(\mathbb{A}_F;\Lambda),$$

i.e., one has a bijection between classes of representations in the genus of $i_{M,\Lambda}$ *and double cosets* $O_{V,W}(F)\phi O_{V,W},(\mathbb{A}_F;\Lambda)$ *with* $\phi \in O_{V,W}(\mathbb{A}_F)$.

PROOF. This follows from Lemma 8.5 □

8.2. Representation and measures in the adelic orthogonal group

Let (V,Q) be a quadratic space over the number field F, let Λ be a lattice on V. The adelic (special) orthogonal group $O_V(\mathbb{A}) = \{\phi = (\phi_v)_{v\in\Sigma_F} \mid \phi_v \in O_V(F_v), \phi_v(\Lambda) = \Lambda$ for almost all $v\}$ (resp. $SO_V(\mathbb{A})$) of (V,Q) carries the restricted direct product topology coming from the topological groups $SO_V(F_v)$, i.e., one has a basis of open sets of the form $\prod_v U_v$, where each U_v is open in $O(F_v)$ and almost all U_v are equal to $O_V(F_v;\Lambda) = \{\phi \in O(F_v) \mid \phi(\Lambda) = \Lambda\}$. With respect to this topology $O_V(\mathbb{A})$ is known to be a locally compact group and as such carries an up to scalar multiplication unique left invariant measure or *Haar measure* [**5**]. Moreover, if (V,Q) is non degenerate (which we assume in the sequel), the group is semisimple and the Haar measure is biinvariant. We normalize the Haar measure on the adele group $\mathbb{A} = \mathbb{A}_F$ by requiring that $\mathbb{A}_F/F$ has measure 1. Using some algebraic geometry a Haar measure on $G(\mathbb{A})$ can be defined (for any linear algebraic group G defined over F) as a converging product $\mu = \prod_v \mu_v$ over all places of F of local Haar measures, using a left differential form ω (a so called gauge form) on G defined over F; a gauge form is unique up to F-multiples. The local integrals and measures are then defined by identifying coordinate neighborhoods in $G(F_v)$ with subsets of $F_v^{\dim G}$ and the Haar measure on $\mathbb{A}_F^{\dim G}$ induced from the Haar measure on $\mathbb{A}_F$ fixed above. Changing ω by a factor c changes the local measures μ_v by the factor $|c|_v$, so that the product formula of algebraic number theory implies that the Haar measure on the adelic orthogonal group attached to a gauge form ω defined over F is independent of the choice of the gauge form ω. This unique Haar measure μ on G attached to a gauge form is then called the *Tamagawa measure* μ, and it makes sense to define the *Tamagawa number* of G as $\tau(G) = \mu(G(F)\backslash G(\mathbb{A}))$. It is known that $\tau(G) = 1$ for connected simple simply connected groups and that $\tau(SO_V) = 2$ for non degenerate (V, Q) independent of the (non degenerate) quadratic space (V, Q). We will take this for granted in the sequel, details can be found in [**39, 25**]. It will be convenient to write

$$O_V(\mathbb{A}_f) = \{\phi = (\phi_v)_{v\in(\Sigma_F\backslash\infty} \mid \phi_v \in O_V(F_v), \phi_v(\Lambda) = \Lambda \text{ for almost all } v\}$$

for the subgroup of *finite adeles* in the adelic orthogonal group and $O_V(F_\infty) = \prod_{v\in\infty} O(F_v)$ for the archimedean component of $O_V(\mathbb{A})$, we have then $O_V(\mathbb{A}) = O_V(F_\infty) \times O_V(\mathbb{A}_f)$. We may also view both $O_V(F_\infty)$ and $O_V(\mathbb{A}_f)$ as subgroups of $O_V(\mathbb{A})$ by setting the respective other components equal to 1. Analogous notations are used for the special orthogonal group.

We have to explain in more detail what we mean by $\mu(G(F)\backslash G(\mathbb{A}))$.

DEFINITION 8.14. Let G be a group acting transitively on the topological space S which carries a G-invariant Borel measure. A Borel set $\mathcal{F} \subseteq S$ is called a *fundamental domain* for the action of G if S is the disjoint union of its translates $g\mathcal{F}$ for $g \in G$. The measure of $\mathcal{F}$ is then also called the measure of the homogeneous space $G\backslash S$.

REMARK 8.15.
a) Frequently one requires a fundamental domain to be connected and to satisfy some smoothness condition on the boundary. This will play no role in our case, so we omit such conditions.
b) It is known that two fundamental domains for the action of G on S have the same measure, so the measure of $G\backslash S$ is a well defined quantity.

DEFINITION 8.16. Let (V, Q) be a quadratic space over F and let Λ be an R-lattice on V, let $N \in \mathbb{N}$.
Then

$$\begin{aligned} H &:= O_V(F; \Lambda, N\Lambda) \\ &:= \{\phi \in O_V(F) \mid \phi(x) \equiv x \bmod N\Lambda \text{ for all } x \in \Lambda\} \subseteq O_V(F; \Lambda) \end{aligned}$$

is called a *principal congruence subgroup* in $O_V(F)$.
Principal congruence subgroups in $O_V(F_v), O_V(\mathbb{A}), O_V(\mathbb{A}_f)$ (where v is a non archimedean place of F) and in the corresponding special orthogonal groups are defined analogously.
A subgroup H of $O_V(F)$ (resp. $O_V(F_v), O_V(\mathbb{A}), O_V(\mathbb{A}_f)$ or the respective special orthogonal groups) is called a congruence subgroup if it contains a principal congruence subgroup with finite index.

REMARK 8.17.
a) Since for $\phi \in O_V(F)$ one has $O_V(F; \phi\Lambda, N\phi\Lambda) = \phi O_V(F; \Lambda, N\Lambda)\phi^{-1}$, all conjugates of congruence subgroups are congruence subgroups (globally, locally, adelically).

b) In the non archimedean local and in the adelic case (restricted to the finite adeles $\mathbb{A}_f$) the congruence subgroups are precisely the compact open subgroups of $O_V(F_v), O_V(\mathbb{A}_f)$, they form a basis of open neighborhoods of the identity element.
c) A congruence subgroup H of $O_V(\mathbb{A})$ is of the shape $H = O_V(F_\infty)\times H_f$, where H_f is a congruence subgroup of $O_V(\mathbb{A}_f)$.

LEMMA 8.18. *Let (V, Q) be a non degenerate quadratic space over the number field F with ring of integers R, let Λ be a lattice on V. Let $V = U \perp W$ be an orthogonal splitting of V into non degenerate subspaces of (V, Q). Then $O_U(F; \Lambda)$ is a congruence subgroup of $O_U(F)$. The analogous assertion is true for the non archimedean local and adelic (special) orthogonal groups.*

PROOF. Let $K_1 = U \cap \Lambda$ and denote by $K_2 \supseteq K_1$ the orthogonal projection $\mathrm{pr}_U(\Lambda)$ of Λ to U, let $N \in \mathbb{N}$ satisfy $NK_2 \subseteq N_1$. For $\phi \in O_U(F; K_2, NK_2)$ we have then $\phi(z) - z \in \Lambda$ for all $z \in K_2$. We consider $x = y + z \in \Lambda$ with $y \in W, z \in K_2$ and extend ϕ to all of V by letting it act trivially on W, obtaining $\phi(x) = x + (\phi(z) - z) \in \Lambda$. This gives $O_U(F; K_2, NK_2) \subseteq O_U(F; \Lambda) \subseteq O_U(F; K_2)$, so $O_U(F; \Lambda)$ is a congruence group. The proof carries over to the non archimedean local and to the adelic situation without change. □

LEMMA 8.19. *Let Λ_1, Λ_2 be lattices on V and $N_1, N_2 \in \mathbb{N}$. Then the principal congruence subgroups $O_V(F; \Lambda_1, N_1\Lambda_1), O_V(F; \Lambda_2, N_2\Lambda_2)$ are commensurable, i.e., their intersection has finite index in both of them.*
The same assertion holds for non archimedean local and adelic congruence subgroups of the (special) orthogonal group.

PROOF. It is enough to prove the assertion for $N_1 = N_2 = 1$ since $O_V(F; \Lambda, N\Lambda)$ has finite index in $O_V(F; \Lambda)$ for any N.
One can find nonzero $a, b \in \mathbb{Z}$ with $ab\Lambda_1 \subseteq a\Lambda_2 \subseteq \Lambda_1$. Then $O_V(F; \Lambda_1, ab\Lambda_1)$ is contained in $O_V(F; \Lambda_2) \cap O_V(F; \Lambda_1)$ and has finite index in $O_V(F; \Lambda_1)$. In the same way one sees that the intersection has finite index in $O_V(F; \Lambda_2)$. It is clear that the proof works for the non archimedean local and the adelic case as well. □

REMARK 8.20. For the applications towards Siegel's theorem the Haar measure on local and adelic (special) orthogonal groups is actually needed only for measurable sets which are finite unions of translates of congruence subgroups (often called *congruence sets*). Since all congruence subgroups have finite index over intersections of finitely many of them, any congruence set is a finite union of cosets of a single congruence subgroup H, i.e., it is of the shape $\cup_{i=1}^r \phi_i H$ and has measure $r\mu(H)$. In [**19**] this is used to define an invariant measure (or more correctly: an invariant measuring function) on congruence sets in the non archimedean local situation by setting $\mu(H_0) = 1$

for some fixed congruence subgroup H_0, defining

$$\mu(H) := \frac{(H : H_0 \cap H)}{(H_0 : H_0 \cap H)}$$

for congruence subgroups H and $\mu(\cup_{i=1}^r \phi_i H) = r\mu(H)$ for an arbitrary congruence set; the latter number is easily seen to be independent of the representation of the congruence set as a finite union of cosets. It is also clear that on congruence sets it agrees with the Haar measure normalized to $\mu(H_0) = 1$ and that any such left invariant measuring function must be a scalar multiple of this μ.
Moreover, it is not difficult to prove that it is also right invariant without using this property for the Haar measure: For $\phi \in O_V(F)$ the function μ' on congruence sets given by $\mu'(X) := \mu(X\phi)$ is a left invariant measuring function as well, hence $\mu' = c(\phi)\mu$ with $c(\phi \circ \psi) = c(\phi)c(\psi)$. Since the orthogonal group is generated by reflections τ which satisfy $\tau^2 = \mathrm{Id}_V$, one must have $c(\phi)$=1 for all ϕ. The problem is then to choose the normalizations of the local measures in such a way that their product over all places (including the archimedean ones, where the measure has to be defined by analytic means) is the (uniquely normalized) Tamagawa measure.
It should be noted that in this way one can also define a biinvariant measuring function on the set of all finite unions of cosets of congruence subgroups of the global orthogonal group $O_V(F)$ for a number field F. For the congruence subgroups this is then up to a constant multiple the inverse of the measure of a fundamental domain for the action of the congruence subgroup on $O_V(F_\infty)$ by left translations.

THEOREM 8.21. *Let (V, Q) be a non degenerate quadratic space over the number field F with ring of integers R, let H be a congruence subgroup of $O_V(\mathbb{A})$, assume that a fundamental domain $\mathcal{F}_\infty$ for the action of $O_V(F) \cap H$ by left translations on $O_V(F_\infty)$ is given, write $H_f = H \cap O_V(\mathbb{A}_f)$ for the finite part of H.*
Then $\mathcal{F}_\infty \times H_f$ is a fundamental domain both for the action of $O_V(F)$ on $O_V(F)H$ and for the action of $O_V(F) \cap H$ on H.

PROOF. For $\sigma_1, \sigma_2 \in O_V(F)$ one has $\sigma_1(\mathcal{F}_\infty \times H_f) \cap \sigma_2(\mathcal{F}_\infty \times H_f) = \emptyset$ since otherwise one had $\sigma_2^{-1}\sigma_1 \in O_V(F) \cap H$ with $\sigma_2^{-1}\sigma_1\mathcal{F}_\infty \cap \mathcal{F}_\infty \neq \emptyset$, in contradiction to the assumption that $\mathcal{F}_\infty$ is a fundamental domain for the action of $O_V(F) \cap H$ on $O_V(F_\infty)$.
Since one has

$$\begin{aligned} H = O_V(F_\infty) \times H_f &= \uplus_{\sigma \in H \cap O_V(F)} \sigma(\mathcal{F}_\infty \times H_f) \\ O_V(F)H &= \cup_{\sigma \in O_V(F)} \sigma(\mathcal{F}_\infty \times H_f), \end{aligned}$$

the assertion follows. $\square$

REMARK 8.22. If F is totally real and (V, Q) totally definite, the group $O_V(F_\infty)$ is compact and $O_V(F) \cap H$ is finite, so that it is not difficult to find

a fundamental domain $\mathcal{F}_\infty$ of finite measure as assumed above. One has then $\mu(O_V(F_\infty)) = |H \cap O_V(F)| \cdot \mu(\mathcal{F}_\infty)$.
Siegel has shown [**35**] that in the indefinite case a fundamental domain of finite volume exists too, a more general version of this statement for arithmetic groups is due to Borel and Harish-Chandra, see [**3**].

COROLLARY 8.23. *In the situation of the theorem let $\phi = (\phi_\infty, \phi_f) \in O_V(\mathbb{A})$ and assume that $\mathcal{F}_{\infty,\phi}$ is a fundamental domain for the action of $O_V(F) \cap \phi H \phi^{-1}$ on $O_V(F_\infty)$ by left translation.*
Then $\mathcal{F}_{\infty,\phi} \times \phi_f H_f$ is a fundamental domain for the action of $\phi H \phi^{-1} \cap O_V(F)$ on $O_V(F_\infty) \times \phi_f H_f$ and for the action of $O_V(F)$ on the double coset $O_V(F)\phi H \subseteq O_V(\mathbb{A})$.

PROOF. Obvious. □

REMARK 8.24. The considerations above remain valid if we replace throughout the orthogonal group O_V by the special orthogonal group SO_V.

THEOREM 8.25 (Siegel's main theorem on quadratic forms, first version). *Let (V, Q) be a non degenerate quadratic space over the number field F with ring of integers R, let H be a congruence subgroup of $SO_V(\mathbb{A})$ and let*

$$SO_V(\mathbb{A}) = \uplus_{i=1}^r SO_v(F)\phi_i H$$

be a finite disjoint coset decomposition. Assume that fundamental domains $\mathcal{F}_{\infty,\phi_i}$ for the action of $SO_V(F) \cap \phi_i H \phi_i^{-1}$ by left translations on $SO_V(F_\infty)$ are given for $1 \leq i \leq r$ and let μ be the Tamagawa measure on $SO_V(\mathbb{A})$, factored as $\mu = \mu_\infty \cdot \mu_f$ with Haar measures μ_∞ on $SO_V(F_\infty)$ and $\mu_f = \prod_{v \notin \infty} \mu_v$ on $SO_V(\mathbb{A}_f)$.
Then one has

$$\sum_{i=1}^r \mu_\infty(\mathcal{F}_{\infty,i}) = \frac{2}{\mu_f(H_f)}.$$

In particular, if F is totally real and (V, Q) totally definite and if in addition $H_f = \prod_{v \notin \infty} H_v$ one has

$$\sum_{i=1}^r \frac{1}{|SO_V(F) \cap \phi_i H \phi_i^{-1}|} = \frac{2}{\mu_\infty(SO_V(F_\infty)) \prod_{v \notin \infty} \mu_v(H_v)}.$$

PROOF. This follows from decomposing $\mu(SO_V(F)\backslash SO_{\mathbb{A}}(V))$ into the sum of the $\mu(SO_V(F)\backslash SO_V(F)\phi_i H)$. □

8.3. Computation of the local measures, non-archimedean places

In this section F is a non archimedean local field with ring of integers R, prime element π, maximal ideal $P = (\pi)$ and residue field $R/P = \mathbb{F}_q$.
We want to express the local measures in terms of numbers of solutions of certain congruences. An important tool will be a quantitative refinement of Theorem 5.15 (Hensel's Lemma):

LEMMA 8.26. *Let (V, Q) and (W, Q') be finite dimensional quadratic spaces over F with associated symmetric bilinear forms b, b' and let L, M be lattices of ranks ℓ, m in V, W respectively. Let $k \in \mathbb{N}$ be such that $P^k Q'(M) \subseteq P$.*
Let $f : L \to W$ be an R-linear map with $b(f(L), M) \subseteq R$ and write $\widetilde{b'}_f$ for the linear map from W to $\mathrm{Hom}_R(L, F)$ with $\widetilde{b'}_f(z)(x) = b'(f(x), z)$ for all $x \in L$.
Assume that one has

a) $L^* = \widetilde{b'}_f(M) + PL^*$
b) $Q'(f(x)) \equiv Q(x) \bmod P^k$ *for all* $x \in L$

Then the number of modulo $P^{k+1}M$ distinct R- linear maps $f' : L \to W$ with $f'(x) \equiv f(x) \bmod P^k M$ and $Q'(f'(x)) \equiv Q(x) \bmod P^{k+1}$ for all $x \in L$ is equal to $q^{\ell m - \frac{\ell(\ell+1)}{2}}$.
All of these also satisfy the condition $L^* = \widetilde{b'}_{f'}(M) + PL^*$

PROOF. As in the proof of Theorem 5.15 we write $f' = f + g$ where g maps L into $P^k M$ and satisfies

$$\widetilde{b'}_f(g(y))(x) \equiv -\beta(x, y) \bmod P^{k+1}$$

for all $x, y \in L$.
Now, for any $\mathbb{F}_q$-linear map $\bar{h} : L/PL \to M/PM$ we can define an $\mathbb{F}_q$-valued quadratic form $\bar{Q}_{\bar{h}}$ on L/PL by

$$\bar{Q}_{\bar{h}}(\bar{x}) := -\bar{b}((\overline{f(x)}, \bar{h}(x)),$$

and the modulo P^{k+1} distinct maps g as above can be obtained as $g = \pi^k h$, where $h : L \to M$ is considered modulo P. As in the proof of Theorem 5.15 we see that the linear map $\bar{h} \mapsto \bar{Q}_{\bar{h}}$ from $\mathrm{Hom}_{\mathbb{F}_q}(L/PL, M/PM)$ to the space X of $\mathbb{F}_q$-valued quadratic forms on L/PL is surjective. Since $\mathrm{Hom}_{\mathbb{F}_q}(L/PL, M/PM)$ has dimension ℓm and the space X has dimension $\frac{\ell(\ell+1)}{2}$, the assertion follows. □

COROLLARY 8.27. *Let Λ be a lattice on the non degenerate quadratic space (V, Q) over F of dimension n, let $k \in \mathbb{N}$ be such that $P^k Q(\Lambda^\#) \subseteq P$ holds. Then with $O_V(F; \Lambda, P^k\Lambda^\#) = \{\phi \in O_V(F; \Lambda) \mid \phi(x) - x \in P^k\Lambda^\#$ for all $x \in \Lambda\}$ and $A(\Lambda, \Lambda \bmod P^k\Lambda^\#) := |\{\phi \in \mathrm{Hom}_R(\Lambda, \Lambda/P^k\Lambda^\#) \mid Q(\phi(x)) \equiv Q(x) \bmod P^k$ for all $x \in \Lambda\}|$ one has*

$$(O_V(F; \Lambda, P^k\Lambda^\#) : O_V(F; \Lambda, P^{k+1}\Lambda^\#)) = q^{n\frac{n-1}{2}}$$

and

$$(O_V(F; \Lambda) : O_V(F; \Lambda, P^k\Lambda^\#)) = A(\Lambda, \Lambda \bmod P^k\Lambda^\#).$$

If μ is a Haar measure on $O_V(F)$ one has

$$\frac{\mu(O_V(F; \Lambda, P^k\Lambda^\#))}{\mu(O_V(F; \Lambda, P^{k+1}\Lambda^\#))} = q^{\frac{n(n-1)}{2}}.$$

PROOF. This follows directly from Theorem 5.15 and the lemma. □

PROPOSITION 8.28. *Let (V, Q) be a non degenerate quadratic space over F of dimension n, let Λ be an R- lattice on V with $Q(\Lambda) \subseteq R$. Identify* $\mathrm{End}_F(V)$ *with $M_n(F)$ and* $\mathrm{End}_R(\Lambda)$ *with $M_n(R)$ with respect to some fixed R-basis of Λ, equip F with the (additive) Haar measure μ_F under which R has measure* 1.

Let $\omega_{\mathcal{X}} = \bigwedge_{i,j} dx_{ij}$ denote the gauge form on $\mathcal{X} := \mathrm{End}_F(V)$ which induces (with the given choice of μ_F and the given coordinate mappings) the Haar measure $\mu_{\mathcal{X}}$ on $\mathcal{X}$ with $\mu_{\mathcal{X}}(\mathrm{End}_R(\Lambda)) = 1$.
Let μ_S denote the Haar measure on $\mathcal{S} := M_n^{\mathrm{sym}}(F)$ with $\mu(M_n^{\mathrm{sym}}(R)) = 1$, denote by ω_S the gauge form on $\mathcal{S}$ inducing μ_S and write $\mathcal{S}^* = \{S \in \mathcal{S} \mid S = {}^tXS_0X$ for an $X \in GL_n(F)\}$.
Denote by $S_0 \in \mathcal{S}$ the Gram matrix of Λ with respect to the given basis of Λ and put $\mathcal{X}_S^{(S_0)} := \{X \in \mathcal{X} \mid {}^tXS_0X = S\}$ for $S \in \mathcal{S}$.
Then there exists a differential form ω of degree $\frac{n(n-1)}{2}$ on $\mathcal{X}$ such that for the measure $\mu_S^{(S_0)}$ associated to the restriction of ω to $\mathcal{X}_S^{(S_0)}$ (for $S \in \mathcal{S}^*$) one has

$$\int_{\mathcal{X}} f(X)d\mu_{\mathcal{X}} = \int_{\mathcal{S}^*} \Big(\int_{\mathcal{X}_S^{(S_0)}} f(X) d\mu_S^{(S_0)} \Big) d\mu_S$$

for any integrable function f on $\mathcal{X}$.
The measure $\mu_{S_0} := \mu_{S_0}^{(S_0)}$ is then a Haar measure on $\mathcal{X}_{S_0}^{(S_0)} = O_V(F)$, induced by the gauge form $\omega|_{\mathcal{X}_{S_0}^{(S_0)}}$ on $O_V(F)$.

PROOF. This follows from the theory of differential forms on algebraic varieties and their associated measures. An explicit construction is given in [**2**]. □

REMARK 8.29. If we replace Q by cQ and hence S_0 by cS_0, we change μ_{S_0} to $\mu_{cS_0} = |c|_v^{-\frac{n(n+1)}{2}} \mu_{S_0}$. Similarly, changing the Gram matrix S_0 to $S_0' = {}^tUS_0U$ with $U \in GL_n(F)$ changes the measure by a factor of $|\det(U)|_v^{-n-1}$ (the map sending $S \in M_n^{\mathrm{sym}}(F)$ to ${}^tUSU$ is easily seen to have determinant $(\det(U))^{n+1}$).

PROPOSITION 8.30. *With notations as above one has for $k \in \mathbb{N}$ satisfying $P^kQ(\Lambda^\#) \subseteq P$, $P^k\Lambda^\# \subseteq \Lambda$:*

$$\begin{aligned} \mu_{S_0}(O_V(F;\Lambda)) &= |2|_v^{-n} q^{-kn\frac{n-1}{2}} A(\Lambda, \Lambda \bmod P^k\Lambda) \\ &= |2|_v^{-n} q^{-kn\frac{n-1}{2}} |\det_b(\Lambda)|_v^{-n} A(\Lambda, \Lambda \bmod P^k\Lambda^\#). \end{aligned}$$

PROOF. We prove the first equality, the second one is then a trivial consequence.
We take for f the characteristic function of $\{\phi \in \mathrm{End}_R(\Lambda) \mid Q(\phi(x)) \equiv Q(x) \bmod P^k$ for all $x \in \Lambda\}$ and notice that this property depends only on ϕ modulo $P^k\Lambda$ (in fact, only on ϕ modulo $P^k\Lambda^\#$). If X is the matrix associated to ϕ this is equivalent to ${}^tXS_0X \equiv S_0 \bmod P^k$, where the diagonal entries,

which are even, are congruent modulo $2P^k$; we write ${}^tXS_0X \equiv_{\mathrm{ev}} S_0$ for this property in the sequel.
We have then (omitting superscripts (S_0) in the sequel) for $S \in \mathcal{S}^*$

$$\int_{\mathcal{X}_S} f(X)d\mu_{\mathcal{X}_S} = \begin{cases} 0 & S \not\equiv_{\mathrm{ev}} S_0 \bmod P^k \\ \mu_{S_0}(O_V(F;\Lambda)) & S \equiv_{\mathrm{ev}} S_0 \bmod P^k \end{cases}.$$

From the previous proposition we get then

$$\int_{\mathcal{X}} f(X)d\mu_{\mathcal{X}} = \mu_{S_0}(O_V(F;\Lambda)) \int_{S\equiv_{\mathrm{ev}}S_0 \bmod P^k} d\mu_{\mathcal{S}}.$$

The integral on the right hand side without the extra congruence condition on the diagonal elements equals $q^{-kn\frac{n+1}{2}}$, the extra congruence condition gives an additional factor of $|2|_v^n$, so that we arrive at

$$\int_{\mathcal{X}} f(X)d\mu_{\mathcal{X}} = \mu_{S_0}(O_V(F;\Lambda))|2|_v^n q^{-kn\frac{n+1}{2}}.$$

We compare this with

$$\begin{aligned} \int_{\mathcal{X}} f(X)d\mu_{\mathcal{X}} &= \mu_{\mathcal{X}}(\{X \in M_n(R) \mid {}^tXS_0X \equiv_{\mathrm{ev}} S_0 \bmod P^k\} \\ &= q^{-kn^2} A(\Lambda, \Lambda \bmod P^k\Lambda), \end{aligned}$$

using that the validity of the congruence here depends only on X modulo $P^kM_n(R)$, and obtain the assertion. □

REMARK 8.31. a) The formula above is valid for any k satisfying the assumptions. The independence of the right hand side of k (as long as k satisfies the assumptions) can also be obtained as a consequence of our quantitative form of Hensel's lemma,

b) The proof shows that the factor $|2|_v^{-n}$ does not occur if one replaces the condition $Q(\phi(x)) \equiv Q(x) \bmod P^k$ in the definition of $A(\Lambda, \Lambda \bmod P^k\Lambda^\#)$ by the condition ${}^tXS_0X \equiv S_0 \bmod P^k$, where X is the matrix of ϕ with respect to the given basis. This power of 2 occurring for dyadic places v therefore does not occur in treatments working with the symmetric bilinear form only instead of the quadratic form.

COROLLARY 8.32. *With notations as above let Λ_0 be a fixed lattice on V with Gram matrix S_0, write $\mu = \mu_{S_0}$ for the Haar measure on $O_v(F)$ as above. Then we have for any lattice Λ on V with $\Lambda \subseteq \Lambda^\#$ and $k \in \mathbb{N}$ with $P^kQ(\Lambda^\#) \subseteq P$, $P^k\Lambda^\# \subseteq \Lambda$*

$$\mu(O_V(F;\Lambda)) = |2|_v^{-n}(\Lambda : P^k\Lambda^\#)^{\frac{1-n}{2}} A(\Lambda, \Lambda \bmod P^k\Lambda^\#)|\det S_0|_v^{-\frac{n+1}{2}}$$

and

$$\mu(O_V(F, \Lambda, P^k\Lambda^\#))(\Lambda : P^k\Lambda^\#)^{\frac{n-1}{2}} = |2|_v^{-n}|\det S_0|_v^{-\frac{n+1}{2}}$$

independent of the choice of Λ.

PROOF. We fix a basis of Λ and write the Gram matrix of Λ as ${}^tUS_0S$ with $U \in GL_n(F)$. Using $\mu = |\det(U)|_v^{n+1}\mu_S$ and $(\Lambda : P^k\Lambda^\#) = q^{kn}|\det_b(\Lambda)|_v$ we can then rewrite the formula from the proposition as

$$\begin{aligned}\mu(O_V(F;\Lambda)) &= |2|_v^{-n}|\det(U)|_v^{n+1}(\Lambda : P^k\Lambda^\#)^{\frac{1-n}{2}}|\det_b(\Lambda)|_v^{-\frac{n+1}{2}}A(\Lambda,\Lambda \bmod P^k\Lambda^\#)\\ &= |2|_v^{-n}(\Lambda : P^k\Lambda^\#)^{\frac{1-n}{2}}|\det(S_0)|_v^{-\frac{n+1}{2}}A(\Lambda,\Lambda \bmod P^k\Lambda^\#).\end{aligned}$$

The second formula follows from this upon inserting

$$(O_V(F;\Lambda) : O_V(F;\Lambda, P^k\Lambda^\#)) = A(\Lambda,\Lambda \bmod P^k\Lambda^\#).$$

□

8.4. Computation of local measures, definite archimedean places

We postpone the discussion of the local measure on the orthogonal group $O_{(V,Q)}(F)$ in the case that that $F = \mathbb{C}$ or that $F = \mathbb{R}$ and Q is indefinite and assume in this section that $F = F_v = \mathbb{R}$ and that (V, Q) is a positive definite quadratic space over F. Since Q and $-Q$ lead to the same orthogonal group this covers the negative definite case as well.

We choose as in the previous section a basis of V and denote by S_0 the Gram matrix of (V, Q) with respect to this basis. As in the non archimedean case we construct a Haar measure $\mu = \mu_{S_0}$ on $O_V(F)$. For this, we first take on $F = \mathbb{R}$ the Lebesgue measure. We identify $\mathcal{S} = M_n^{\mathrm{sym}}(F)$ with $\mathbb{R}^{\frac{n(n+1)}{2}}$ and obtain as measure $\mu_{\mathcal{S}}$ on $\mathcal{S}$ induced by the differential form $\bigwedge_{i\le j} ds_{ij}$ the Lebesgue measure on $\mathbb{R}^{\frac{n(n+1)}{2}}$. From this we obtain as in the non-archimedean case measures $\mu_S^{(S_0)}$ on $\mathcal{X}_S^{(S_0)}$ for each $S \in \mathcal{S}$. Identifying $O_V(F)$ with $\mathcal{X}_{S_0}^{(S_0)}$ we set $\mu = \mu_{S_0} = \mu_{S_0}^{(S_0)}$, this Haar measure on $O_V(F)$ is induced (with notations as in the non-archimedean case) by the gauge form $\omega|_{\mathcal{X}_{S_0}^{(S_0)}}$.

Again as there we see that $S_0' = {}^tUS_0U$ for $U \in GL_n(F)$ leads to $\mu_{S_0'} = |\det U|_v^{-n-1}\mu_{S_0}$. In particular, if we write $S_0 = {}^tUU$ with $U \in GL_n(F)$ we obtain $\mu_{S_0} = |\det(S_0)|_v^{-\frac{n+1}{2}}\mu_{1_n}$, where 1_n denotes the identity matrix.

Fixing $S_0 = 1_n$ we omit superscripts (S_0) in the sequel. To proceed similarly as in the non-archimedean case we choose now $f(X) = \exp(-\mathrm{tr}({}^tXX)$ as our test function f on $\mathrm{End}(V) = M_n(\mathbb{R})$ and have $\int_{\mathcal{X}} f(X)d\mu_{\mathcal{X}} = \pi^{\frac{n^2}{2}}$, using $\int_{-\infty}^{\infty}\exp(-x^2)dx = \sqrt{\pi}$.

In order to make the measure $\mu_{\mathcal{S}}$ on $\mathcal{S}^*$ explicit we parametrize $\mathcal{S}$ by the set of lower triangular matrices $X = (x_{ij})_{i,j}$, mapping X to $S = {}^tXX$. We have then by a straightforward calculation

$$\omega_{\mathcal{S}} := \bigwedge_{i\le j} ds_{ij} = 2^n\prod_{i=1}^n x_{ii}^i \bigwedge_{i\ge j} dx_{ij},$$

and μ_S is the measure induced by this differential form. The equation $\omega_{\mathcal{X}} = \omega \wedge \omega_S$ gives then

$$\omega = 2^{-n} \prod_{i=1}^{n} x_{ii}^{-i} \bigwedge_{i<j} dx_{ij}$$

up to summands containing one of the dx_{ij} with $i \geq j$. For the computation of

$$\int_{\mathcal{X}} f(X) d\mu_{\mathcal{X}} = \int_{S^*} \Big(\int_{\mathcal{X}_S^{(S_0)}} f(X) d\mu_S^{(S_0)} \Big) d\mu_S$$

we notice that for $S = {}^tXX \in S^*$ we have $\mathcal{X}_S = O_V(F)X$. The integrand in the inner integral above is constant on $\mathcal{X}_S$, and the volume of $O_V(F)X$ with respect to the restriction of ω to $\mathcal{X}_S$ is $\det(X)^{-1}$ times the volume of $O_V(F)$. This can be checked by looking at $X = \lambda 1_n$ for some $\lambda \neq 0$ since the quotient of these volumes is some character of $GL_n(F)$ and hence a function of the determinant only. We arrive at

$$\begin{aligned} \pi^{\frac{n^2}{2}} &= \int_{M_n(F)} f(X) \\ &= \int_{S^*} \Big(\int_{\mathcal{X}_S^{(S_0)}} f(X) d\mu_S^{(S_0)} \Big) d\mu_S \\ &= \mu_{1_n}(O_V(F)) \int \prod_{i=1}^{n} 2^n x_{ii}^{i-1} \exp(-\sum_{i\leq j} x_{ij}^2) \bigwedge_{i\geq j} dx_{ij}. \end{aligned}$$

We use again $\int_{-\infty}^{\infty} \exp(-x^2)dx = \sqrt{\pi}$ for the integration with respect to the variables x_{ij} with $i > j$, for the integration with respect to the x_{ii} we use $\int_{-\infty}^{\infty} 2x^i \exp(-x^2)dx = \Gamma(\frac{i+1}{2})$ and obtain

$$\mu_{1_n}(O_V(F)) = \pi^{\frac{n(n+1)}{4}} \prod_{i=1}^{n} (\Gamma(\frac{i}{2}))^{-1}$$

and hence

$$\mu_{1_n}(SO_V(F)) = \frac{1}{2} \pi^{\frac{n(n+1)}{4}} \prod_{i=1}^{n} (\Gamma(\frac{i}{2}))^{-1}.$$

REMARK 8.33. a) The differential forms considered in this section are the same as in the non-archimedean situation of the previous section.

b) By the well known formula $\mathrm{vol}(S^{n-1}) = 2\pi^{\frac{n}{2}}(\Gamma(\frac{n}{2}))^{-1}$ for the volume of the $(n-1)$-dimensional unit sphere we can express the measure of $SO_V(F)$ also as

$$\mu_{1_n}(SO_V(F)) = 2^{-n} \prod_{i=2}^{n} \mathrm{vol}(S^{i-1}).$$

8.5. The global Tamagawa measure

We now put together the local computations. For this, let F be a totally real number field of degree r over $\mathbb{Q}$ with discriminant D_F and different $\mathcal{D}_F$, let $\mu_{F_{\mathbb{A}}} = \prod_{v\in\Sigma_F} \mu_{F_v}$ be the invariant measure on $\mathbb{A}_F$ with $\mu_{F_{\mathbb{A}}}(\mathbb{A}_F/F) = 1$. We choose the usual normalization of the μ_{F_v} with $\mu_{F_v}(R_v) = |\mathcal{D}_F|_v^{\frac{1}{2}}$ for all non archimedean v and μ_{F_v} equal to the Lebesgue measure for the real places of F. In particular, for non archimedean v the measure on F_v used now is $|\mathcal{D}_F|_v^{\frac{1}{2}}$ times the measure used in Section 8.3, and since $SO_V(F_v)$ has dimension $n(n-1)/2$, the measure on $SO_V(F_V)$ is changed by a factor $|\mathcal{D}_F|_v^{\frac{n(n-1)}{4}}$.

By the product formula the product of these factors over all non archimedean places of F is then $|D_F|^{-\frac{n(n-1)}{4}}$, where $|D_F|$ is the ordinary absolute value of the field discriminant.

Let (V, Q) be a totally definite quadratic space over F, let Λ_0 be a fixed free lattice on V with Gram matrix S_0 with respect to a fixed basis. Using our present choice of the measures μ_{F_v} on the F_v we define local measures $\mu_v = (\mu_{S_0})_v$ on $SO_V(F_v)$ and obtain the Tamagawa measure $\mu_{\mathbb{A}}$ on $SO_V(\mathbb{A})$. Combining our local results with the first version of the Minkowski-Siegel theorem we obtain:

THEOREM 8.34 (Siegel's main theorem on quadratic forms, second version). *Let Λ be an integral lattice on V, denote by $\Lambda_1, \dots, \Lambda_h$ representatives (on V) of the proper (with respect to $SO(V)$) integral equivalence classes in the genus of (Λ, Q).*

For non archimedean v and $k = k_v$ satisfying $P_v^k Q(\Lambda_v) \subseteq P_v$, $P_v^k \Lambda_v^\# \subseteq \Lambda_v$ put

$$\alpha_v(\Lambda) = \frac{1}{2}|2|_v^{-n} q_v^{-k\frac{n(n-1)}{2}} |\det_b(\Lambda_v)|_v^{\frac{1-n}{2}} A(\Lambda_v, \Lambda_v \bmod P_v^k \Lambda_v^\#)$$

where q_v is the order of the residue field R_v/P_v. Then one has

$$\sum_{i=1}^{h} \frac{1}{|SO_V(F;\Lambda_i)}| = |D_F|^{\frac{n(n-1)}{4}} 2^{r+1} \pi^{-r\frac{n(n+1)}{4}} \prod_{i=1}^{n} (\Gamma(\frac{i}{2}))^r \prod_{v\notin\infty} (\alpha_v(\Lambda))^{-1}.$$

PROOF. In our first version of Siegel's main theorem we use $H = SO_V(\mathbb{A}_F; \Lambda)$ and have $SO_V(F) \cap \phi_i H \phi_i^{-1} = SO(F; \Lambda_i)$ with $\phi_i \Lambda = \Lambda_i$. The local measures occurring there have been computed in the two preceding sections, with the normalization of the Haar measure discussed above introducing the extra factor $|D_F|^{\frac{n(n-1)}{4}}$. We notice that the product of the factors $|\det(S_0)|_v^{-\frac{n+1}{2}}$ over all places v is equal to 1 by the product formula and obtain the assertion. □

REMARK 8.35. a) The $\alpha_v(\Lambda)$ are called the *local densities* for Λ.

b) The factors $|2|_v^{-n}$ occurring non trivially in the α_v for the dyadic places v of F (i.e., the places where the v-value of 2 is not 1) combine in the product to a total factor of 2^{nr}. It is therefore not unusual to omit these factors in the definition of the local densities at the non archimedean places and instead to insert a factor of 2^n for each of the real places.

c) It is easily checked that $\sum_{i=1}^{h} \frac{1}{|SO_V(F;\Lambda_i)}| = 2\sum_{i=1}^{h'} \frac{1}{|O_V(F;\Lambda'_i)}|$, where $\Lambda'_1, \dots, \Lambda'_{h'}$ are a set of representatives of the isometry classes in the genus of Λ (with respect to $O_V(F)$), since for any Λ_i admitting no automorphism of determinant -1 the isometry class of Λ_i splits into two proper isometry classes. The latter sum is called the *measure* or *Maß*, often also written as "mass", $m(\Lambda) = m(\mathrm{gen}(\Lambda))$ of the genus of Λ. We have then

$$m(\mathrm{gen}(\Lambda)) = |D_F|^{\frac{n(n-1)}{2}} 2^r \pi^{-r\frac{n(n+1)}{4}} \prod_{i=1}^{n} (\Gamma(\frac{i}{2}))^r \prod_{v \notin \infty} (\alpha_v(\Lambda))^{-1}.$$

Another way to check this is to consider the subgroup

$$SO_V(\mathbb{A}_F) \cup \{\phi = (\phi_v)_{v\in\Sigma_F} \in O_v(\mathbb{A}_F) \mid \det(\phi_v) = -1 \text{ for all } v \in \Sigma_F\}$$

of $O_V(\mathbb{A}_F)$ in which $SO_V(\mathbb{A}_F)$ has index 2. A fundamental domain for the action of $SO_V(F)$ on $SO_V(\mathbb{A}_F)$ is then also a fundamental domain for the action of $O_V(F)$ on this group.

If $H \subseteq SO_V(\mathbb{A}_F)$ is a congruence subgroup of $SO_V(\mathbb{A}_F;\Lambda)$ for a lattice Λ as above and we have a double coset decomposition $SO_V(\mathbb{A}_F) = \cup_{j=1}^{t} SO_V(F)\psi_j H$, we can use our two versions of Siegel's theorem to express the sum of the inverses of the $|SO_v(F) \cap \psi_j H \psi_j^{-1}|$ by the left hand side of the theorem above and the index of H in $SO_V(\mathbb{A}_F;\Lambda)$.
For example we get the following result first proven by van der Blij in classical matrix notation:

COROLLARY 8.36. *Let Λ be a lattice as above and fix $x_0 \in \Lambda^\#$, write $SO_V(F, x_0+\Lambda) = \{\phi \in SO_V \mid \phi)x_0+\Lambda) = x_0+\Lambda\}$ and define $SO_V(\mathbb{A}_F, x_0+\Lambda)$ analogously. Then $SO_V(\mathbb{A}_F, x_0+\Lambda)$ is a congruence subgroup of $SO_V(\mathbb{A}_F, \Lambda)$.
For a lattice $\Lambda' \in \mathrm{gen}(\Lambda)$ and $x \in (\Lambda')^\#$ say that $x + \Lambda'$ is in the proper class of $x_0 + \Lambda$ if there exists $\phi \in SO_V(F)$ with $\phi(x_0 + \Lambda) = x + \Lambda'$ and that that $x+\Lambda'$ is in the proper genus of $x_0+\Lambda$ if there exists $\phi \in SO_V(\mathbb{A}_F)$ with $\phi_v(x_0 + \Lambda) = x + \Lambda'_v$ for all $v \in \Sigma_F$.
Let $\{x_j + \Lambda'_j\}$ be a set of representatives of the (finitely many, say t) classes in the genus of $x_0 + \Lambda$ and write s_v for the index of $SO_V(F_v, x_0 + \Lambda)$in $SO_V(F;\Lambda)$.
Then $s_v = 1$ for almost all v, and with $s = \prod_v s_v$ we have*

$$\sum_{j=1}^{t} \frac{1}{|SO_V(F; x_j + \Lambda'_j)}| = s \sum_{i=1}^{h} \frac{1}{|SO_V(F;\Lambda_i)|}.$$

PROOF. Obvious. □

EXAMPLE 8.37. Let $F = \mathbb{Q}$ and let Λ be an even unimodular $\mathbb{Z}$-lattice on the positive definite quadratic space (V, Q) over $\mathbb{Q}$ (i.e., we have $Q(\Lambda) \subseteq \mathbb{Z}$

and $\det_b(\Lambda) = 1$). It is known that such lattices only occur with rank $n = 2m$ divisible by 8 and that the E_8 root lattice represents the unique isometry class of such lattices in dimension 8.
For the computation of the local factors we can take $k = k_p = 1$ for all primes p, which gives

$$\alpha_p(\Lambda) = |2|_p^{-n} q^{-\frac{(n(n-1)}{2}} |SO_{\Lambda/p\Lambda}(\mathbb{F}_p)|,$$

where the factor $|2|_p^{-n}$ is equal to 2^n for $p = 2$ and equal to 1 for the odd primes p.
Since the quadratic space $\Lambda/p\Lambda$ over $\mathbb{F}_p$ is an orthogonal sum of $m = \frac{n}{2}$ hyperbolic planes we have (see Section 13 of [**19**])

$$|SO_{\Lambda/p\Lambda}(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}}(1 - p^{-m}) \prod_{i=1}^{m-1} (1 - p^{-2i}),$$

which gives

$$\prod_p (\alpha_p(\Lambda))^{-1} = 2^{-n} \zeta(m) \prod_{i=1}^{m-1} \zeta(2i).$$

For $n = 8$ this gives

$$\prod_p (\alpha_p(\Lambda))^{-1} = \frac{\pi^{16}}{2^{11} 3^8 5^3 7}$$

using the well known values $\zeta(2) = \frac{\pi^2}{6}, \zeta(4) = \frac{\pi^4}{90}, \zeta(6) = \frac{\pi^6}{945}$. The remaining factor $2^2 \pi^{-\frac{n(n+1)}{4}} \prod_{i=1}^n \Gamma(\frac{i}{2})$ evaluates to

$$\frac{3^3 5}{2^2 \pi^{16}},$$

and we obtain $|SO_V(\mathbb{Q}; \Lambda)| = |SO(E_8)| = 2^{13} 3^5 5^2 7$, which is indeed in agreement with the known value for the order of the special orthogonal group of the E_8 root lattice.
The same computation in rank 16 can be used to prove that there are only two isometry classes of even unimodular lattices of rank 16, represented by the lattices $E_8 \perp E_8$ and D_{16}^+ discussed in Section 6.4.
The measure (or Maß) of the unique genus of even unimodular lattices then grows rapidly with the rank and is of the order of magnitude of $4 \cdot 10^7$ already in rank 32, which implies that the number of isometry classes is at least 80 million in this rank, so that an explicit classification is no longer possible or useful. The even unimodular lattices of rank 24 have been classified, there are exactly 24 isometry classes.

Having established the maßformel for the measure of a genus we now need some preparations for the formula for representation measures (Darstellungsmaße).

LEMMA 8.38. *Let (V, Q) be a non degenerate quadratic space over the non-archimedean local field $F = F_v$ with an orthogonal splitting $V = U \perp W$ into nonzero non degenerate subspaces U, W, write n, u, w for their respective dimensions. Let Λ be an integral lattice on V and $M = W \cap \Lambda$ a primitive sublattice of Λ on W, denote by $i_{M,\Lambda} : M \to \Lambda$ the inclusion map of M into Λ. Let $k \in \mathbb{N}$ satisfy $P^k Q(\Lambda^\#) \subseteq P$, $P^k\Lambda^\# \subseteq \Lambda$. Then*

$$\frac{(O_V(F;\Lambda) : O_V(F;\Lambda, P^k\Lambda^\#))}{(O_U(F;\Lambda) : O_U(F;\Lambda, P^k\Lambda^\#))} = A(i_{M,\Lambda}, \Lambda \bmod P^k\Lambda^\#),$$

where $A(i_{M,\Lambda}, \Lambda \bmod P^k\Lambda^\#)$ denotes the number of R-linear maps $\phi : M \to \Lambda/P^k\Lambda^\#$ with $\phi = \psi \bmod P^k\Lambda^\#$ for an isometry $\psi : M \to \Lambda$ in the class of $i_{M,\Lambda}$.

PROOF. By the isomorphism theorem of group theory we have

$$(O_U(F;\Lambda) : O_U(F;\Lambda, P^k\Lambda^\#)) = (O_U(F;\Lambda)O_V(F;\Lambda, P^k\Lambda^\#) : O_V(F;\Lambda, P^k\Lambda^\#)),$$

and get

$$\frac{(O_V(F;\Lambda) : O_V(F;\Lambda, P^k\Lambda^\#)}{(O_U(F;\Lambda) : O_U(F;\Lambda, P^k\Lambda^\#))} = (O_V(F;\Lambda) : O_U(F;\Lambda)O_V(F;\Lambda, P^k\Lambda^\#)).$$

We put $O_V(F;\Lambda,(M, P^k\Lambda^\#)) := \{\phi \in O_V(F;\Lambda) \mid \phi(x) - x \in P^k\Lambda^\# \text{ for all } x \in M\}$ and claim that $O_U(F;\Lambda)O_V(F;\Lambda, P^k\Lambda^\#) = O_V(F;\Lambda, M, P^k\Lambda^\#)$ holds.

The inclusion from left to right is trivial, for the other direction let $\phi \in O_V(F;\Lambda,(M, P^k\Lambda^\#))$ be given. Since M is primitive in Λ there exists a primitive sublattice $K \subseteq \Lambda$ with $\Lambda = M \oplus K$, write $\sigma = \phi \oplus \mathrm{Id}_K$ which is a linear map, but not necessarily an isometry. For $x = y + z \in \Lambda$ with $y \in M, z \in K$ we have $y' := \sigma(y) - y = \phi(y) - y \in P^k\Lambda^\#$ and hence $Q(\sigma(x)) = Q(y + y' + z) \equiv Q(x) \bmod P^k$, and for $x \in M$ we even have $Q(\sigma(x)) = Q(\phi(x))$.
By Hensel's Lemma there exists an isometric map $\rho : \Lambda \to \Lambda^\#$ with $\rho(x) \equiv \sigma(x) \bmod P^k\Lambda^\#$ for all $x \in \Lambda$, from which we see that $\rho \in O_V(F;\Lambda, M, P^k\Lambda^\#)$ holds. More precisely, going through the proof of Theorem 5.15 we see that the bilinear form β used there can be chosen to satisfy $\beta(x, y) = 0$ for all $y \in M$. If $(e_1, \dots, e_n)$ is a basis of Λ for which the first w vectors form a basis of M and the remaining u vectors form a basis of K, we can then choose the linear map g in that proof to satisfy $g(e_1) = \cdots = g(e_w) = 0$ and hence $g|_M = 0$, i.e., the isometric map ρ mentioned above can be constructed in such a way that it satisfies $\rho|_M = \phi|_M$.
We have therefore $\phi\rho^{-1} \in O_U(F;\Lambda)$, which proves the claimed equality.

The quotient of group indices in the assertion of the Lemma is therefore equal to $(O_V(F;\Lambda) : O_V(F;\Lambda,(M, P^k\Lambda^\#)))$. But obviously $\phi, \psi \in O_V(F;\Lambda)$ are in the same coset modulo $O_V(F;\Lambda,(M, P^k\Lambda^\#))$ if and only if they induce the same map $M \to \Lambda/P^k\Lambda^\#$, which proves the assertion. □

LEMMA 8.39. *With notations as before let S_0 be the Gram matrix of (V, Q) with respect to some fixed basis of V and analogously T_0 a Gram matrix of*

(W, Q), denote by μ_V, μ_U the Haar measures on $O_V(F), O_U(F)$ constructed with respect to these Gram matrices as in Section 8.3.
Then one has

$$\frac{\mu_V(O_V(F;\Lambda,P^k\Lambda^\#))}{\mu_U(O_U(F;\Lambda,P^k\Lambda^\#))} = q^{kw\frac{1-u-n}{2}} |\det_b(M)|_v^{\frac{1-u}{2}} |\det_b(\Lambda)|_v^{-\frac{w}{2}} \frac{|\det(S_0)|_v^{-\frac{n+1}{2}} |2|_v^{-n}}{|\det(T_0)|_v^{-\frac{u+1}{2}} |2|_v^{-u}}.$$

PROOF. We denote by L the orthogonal projection of Λ onto U. By Lemma 1.64 we have $L^\# = \Lambda^\# \cap U$ and by Theorem 2.16 $\det_b(\Lambda) = \det_b(M)\det_b(L)$, which implies $(\Lambda : P^k\Lambda^\#) = (M : P^kM^\#)(L : P^kL^\#)$.
We claim that

$$O_U(F;\Lambda,P^k\Lambda^\#) = O_U(F;L,P^kL^\#).$$

The inclusion from left to right is trivial, for the other direction let $\phi \in O_U(F;L,P^kL^\#)$ and $x = y + z \in \Lambda$ with $y \in W, z \in L$. We see that $\phi(x) = y + \phi(z) = y + z + z'$ with $z' \in P^kL^\# = P^k\Lambda^\# \cap U$, which implies $\phi(x) - x \in P^k\Lambda^\#$ for all $x \in \Lambda$ and proves our claim.

We can now apply Corollary 8.32 and obtain

$$\begin{aligned}
\frac{\mu_V(O_V(F;\Lambda,P^k\Lambda^\#))}{\mu_U(O_U(F;\Lambda,P^k\Lambda^\#))} &= \frac{(\Lambda : P^k\Lambda^\#)^{\frac{1-n}{2}}}{(L : P^kL^\#)^{\frac{1-u}{2}}} \frac{|2|_v^{-n}|\det(S_0)|^{-\frac{n+1}{2}}}{|2|_v^{-u}|\det(T_0)^{-\frac{u+1}{2}}} \\
&= (\Lambda : P^k\Lambda^\#)^{-\frac{w}{2}} (M : P^kM^\#)^{\frac{1-u}{2}} \frac{|2|_v^{-n}|\det(S_0)|^{-\frac{n+1}{2}}}{|2|_v^{-u}|\det(T_0)^{-\frac{u+1}{2}}} \\
&= q^{kw\frac{1-u-n}{2}} |\det_b(M)|_v^{\frac{1-u}{2}} |\det_b(\Lambda)|_v^{-\frac{w}{2}} \frac{|2|_v^{-n}|\det(S_0)|^{-\frac{n+1}{2}}}{|2|_v^{-u}|\det(T_0)^{-\frac{u+1}{2}}}.
\end{aligned}$$

□

PROPOSITION 8.40. *With notations as above let*

$$\alpha_v(i_{M,\Lambda}) := \frac{|\det(S_0)|_v^{\frac{n+1}{2}} \mu_V(O_V(F;\Lambda))}{|\det(T_0)|_v^{\frac{u+1}{2}} \mu_U(O_U(F;\Lambda))}$$

and write $\alpha_v^*(\Lambda, M)$ for the sum of the $\alpha_v(i_{M,\Lambda_i})$, where the inclusions i_{M,Λ_i} run through a set of representatives of the classes of primitive representations of M by lattices Λ_i on V in the class of Λ. Similarly, write $A^*(M, \Lambda \bmod P^k\Lambda)$ for the same sum of the $A(i_{M,\Lambda_i}, \Lambda \bmod P^k\Lambda)$. Then $A^*(M, \Lambda/P^k\Lambda^\#)$ is equal to the number of R-linear maps $\phi : M \to \Lambda/P^k\Lambda^\#$ satisfying $Q(\phi(x)) \equiv Q(x) \bmod P^k$ for all $x \in \Lambda$ for which $\phi(M)$ is a direct summand in $\Lambda/P^k\Lambda^\#$ and we have

$$\alpha_v(i_{M,\Lambda}) = q^{kw\frac{1-u-n}{2}} |\det_b(M)|_v^{\frac{1-u}{2}} |\det_b(\Lambda)|_v^{-\frac{w}{2}} |2|_v^{u-n} A(i_{M,\Lambda}, \Lambda \bmod P^k\Lambda^\#),$$

$$\alpha_v^*(\Lambda, M) = q^{kw\frac{1-u-n}{2}} |\det_b(M)|_v^{\frac{1-u}{2}} |\det_b(\Lambda)|_v^{-\frac{w}{2}} |2|_v^{u-n} A^*(M, \Lambda \bmod P^k\Lambda^\#).$$

PROOF. The first assertion is a direct consequence of the two lemmas above.
For the second assertion we observe that the quotient in the second lemma above is independent of the class of the representation at hand. The assertion therefore follows upon summation over the classes of primitive representations. □

REMARK 8.41. The $\alpha_v^*(\Lambda, M)$ are called the *primitive local representation densities*.

THEOREM 8.42 (Siegel's main theorem for representations, definite case). *Let F be a totally real number field of degree r over $\mathbb{Q}$ and $(V, Q), (W, Q')$ totally definite quadratic spaces over F with* $\dim(W) = w < \dim(V) = n$. *Let Λ be a lattice on V and M a lattice on W' that is represented locally everywhere primitively by Λ, let (without loss of generality) $\phi : M \to \Lambda$ be a primitive representation of M by Λ, let $\Lambda_1, \dots, \Lambda_h$ be a set of representatives of the proper classes in the genus of Λ.*

a) *For a lattice $\Lambda_j \in \mathrm{gen}(\Lambda)$ let $r(\mathrm{gen}(\phi), \Lambda_j)$ denote the number of representations of M by Λ_j which are in the genus of the representation ϕ (all of which are primitive), let*
$$r(\mathrm{gen}(\phi)) = \frac{\sum_{j=1}^h \dfrac{r(\mathrm{gen}(\phi), \Lambda_j)}{|SO_V(F; \Lambda_j)|}}{\sum_{j=1}^h \dfrac{1}{|SO_V(F; \Lambda_j)|}}.$$
Then
$$r(\mathrm{gen}(\phi)) = |D_F|^{-\frac{(n+u-1)(n-u)}{4}} \pi^{\frac{r(n+u+1)(n-u)}{4}} \prod_{j=u+1}^{n} (\Gamma(\frac{j}{2}))^{-r} \prod_{v \notin \infty} \alpha_v(\phi).$$

b) *Let $r^*(\Lambda_j, M)$ denote the number of primitive representations of M by Λ_j, let*
$$r^*(\mathrm{gen}(\Lambda), M) = \frac{\sum_{j=1}^h \dfrac{r^*(\Lambda_j, M)}{|SO_V(F; \Lambda_j)|}}{\sum_{j=1}^h \dfrac{1}{|SO_V(F; \Lambda_j)|}}.$$
Then
$$r^*(\mathrm{gen}(\Lambda), M) = |D_F|^{-\frac{(n+u-1)(n-u)}{4}} \pi^{\frac{r(n+u+1)(n-u)}{4}} \prod_{j=u+1}^{n} (\Gamma(\frac{j}{2}))^{-r} \prod_{v \notin \infty} \alpha_v^*(\Lambda, M).$$

If one replaces proper classes by classes and SO_V by O_V in the definitions of $r^*(\mathrm{gen}(\phi)), r^*(\mathrm{gen}(\Lambda), M)$*, these numbers remain unchanged.*

PROOF. We know that we can restrict attention to inclusion mappings i_{M,Λ_j}. Let such an i_{M,Λ_j} be given. Then $SO_V(F; \Lambda)$ operates transitively on the set of representations of M by Λ_j which are in the proper class of i_{M,Λ_j}, and the stabilizer of i_{M,Λ_j} is $SO_U(F;\Lambda_j)$. If we sum here over all classes of representations of M by Λ_j which are in the genus of i_{M,Λ_j} (representing each such class by an inclusion) we find

$$\frac{r(\mathrm{gen}(\phi),\Lambda_j)}{|SO_V(F;\Lambda_j)|}=\frac{1}{SO_U(F;\Lambda_j)}.$$

With a double coset decomposition

$$SO_U(\mathbb{A}_F)=\bigcup_{j=1}^{t} SO_U(F)\phi_j SO_U(\mathbb{A}_F;\Lambda)$$

we can write here $SO_U(F;\phi_j(\Lambda))=SO_U(F)\cap\phi_j SO_U(\mathbb{A}_F;\Lambda)\phi_j^{-1}$, and our first version of Siegel's main theorem, applied to the congruence subgroup $H=SO_U(\mathbb{A}_F;\Lambda)$ of $SO_U(\mathbb{A}_F)$ gives

$$\sum_{j=1}^{h}\frac{r(\mathrm{gen}(\phi),\Lambda_j)}{|SO_V(F;\Lambda_j)|}=\frac{2}{\mu_{U,\infty}(SO_U(F_\infty))\prod_{v\notin\infty}\mu_{U,v}(SO_U(F_v;\Lambda))},$$

where the $\mu_{U,v}$ are the local factors of the Tamagawa measure for $SO_U(\mathbb{A}_F)$. We divide this equation by the equation given by the first version of Siegel's main theorem for the congruence subgroup $SO_V(\mathbb{A}_F,\Lambda)$ of $SO_V(\mathbb{A}_F)$ and obtain, in view of the definition of the $\alpha_v(i_{M,\Lambda})$ and inserting the measures of the infinity components already computed, the assertion in a). Notice that the factors $|\det(S_0)|_v^{-\frac{n+1}{2}}, |\det(T_0)|_v^{-\frac{u+1}{2}}$ occurring in the local measures for all places v including the archimedean ones cancel out because of the product formula.
The assertion in b) then follows upon summation over the genera of primitive representations.
That changing from SO to O doesn't change anything is obvious since numerator and denominator both change by a factor of 2. □

REMARK 8.43. As in Theorem 8.34 the factors $|2|_v^{u-n}$ occurring non trivially in the α_v for the dyadic places v of F (i.e., the places where the v-value of 2 is not 1) combine in the product to a total factor of $2^{r(n-u)}=2^{rw}$. It is again not unusual to omit these factors in the definition of the local densities at the non archimedean places and instead to insert a factor of $2^{n-u}=2^w$ for each of the real places.

EXAMPLE 8.44. We let $(\Lambda,Q)=I_4$ be the four dimensional cube lattice whose Gram matrix is diagonal with diagonal entries 2. The lattice is unimodular over $\mathbb{Z}_p$ for all odd primes p, for $p=2$ we have $\Lambda_2^\#=\frac{1}{2}\Lambda$ with $Q(\Lambda_2^\#)\mathbb{Z}=\frac{1}{4}\mathbb{Z}$, so that we can choose $k=k_2=3$ at the prime 2. For M we choose the 1-dimensional lattice with Gram matrix $2t$ for some $t\in\mathbb{N}$. For odd primes p we have to count the primitive solutions modulo p of $\sum_{i=1}^4 x_i^2=t$, where primitive is here the same as nonzero modulo p. This is most easily done writing the completion Λ_p as a sum of two hyperbolic planes, we find (see also Section 13 of [**19**]) $p^3 - p = p(p^2 - 1)$ for $p \nmid t$ and $p^3 + p^2 - p - 1 = (p+1)(p^2 - 1)$.

At the prime 2 we have to count the number of solutions of $\sum_{i=1}^4 x_i^2 \equiv t \bmod 8$ where the x_i are considered modulo 4 and where at least one of the x_i is odd. For $t = 1$ we have $\sum_{i=1}^4 x_i^2 \equiv 1 \bmod 8$ if and only if precisely one of the x_i is odd and either one or all of the remaining variables are zero modulo 4, which gives a total of $4 \cdot 2 \cdot (3+1) = 32$ solutions. Since the lattice (Λ_2, tQ) is easily seen to be isometric to (Λ_2, Q) over $\mathbb{Z}_2$ for all odd t, one obtains the same result for all odd t, alternatively one can count the solutions for those t directly as well. For t congruent to 2 or 6 modulo 8 precisely 2 of the x_i have to be odd and we obtain 48 solutions, for $t \equiv 4 \bmod 8$ all x_i have to be odd and we obtain 16 solutions, for $t \equiv 0 \bmod 8$ there are no solutions.

For $t = 1$ our formula gives then with $\alpha_2(I_4, t) := \alpha_2(\Lambda, M) = 1$ and $\alpha_p(I_4, t) := \alpha_p(\Lambda, M) = (1 - p^{-2})$ for $p \neq 2$ and using $\zeta(2) = \frac{\pi^2}{6}$

$$\begin{aligned} r(1, I_4) &= \pi^2 \prod_p \alpha_p(\Lambda, M) \\ &= \pi^2 \frac{4}{3} \zeta(2)^{-1} \\ &= 8, \end{aligned}$$

in agreement with the obvious count for this number.

For $p \nmid t$ we have the same values of α_p as above, for $p \mid t$ and $2 \neq p$ we have $\alpha_p^*(I_4, t) = \frac{p+1}{p} |t|_p^{-1} \alpha_p(I_4, 1)$, for $p = 2$ we obtain

$$\alpha_2^*(I_4, t) = \begin{cases} 3 & t \equiv 2, 6 \bmod 8 \\ 2 & t \equiv 4 \bmod 8 \end{cases}$$

and hence with $t = 2^s t'$, $s \nmid t'$

$$r^*(I_4, t) = t' \prod_{2 \neq p \mid t} \frac{p+1}{p} \begin{cases} 8 & 2 \nmid t \\ 24 & t \equiv 2, 6 \bmod 8 \\ 16 & t \equiv 4 \bmod 8 \end{cases}.$$

The formula for the number $r(I_4, t) = \sum_{d^2 \mid t} r^*(I_4, \frac{t}{d^2})$ of all representations of t by I_4 looks smoother, we obtain

$$r(I_4, t) = 8 \sum_{d \mid t, 4 \nmid d} d,$$

a formula which was first obtained by Jacobi with the help of a study of the analytic properties of the theta series $\sum_{t=0}^{\infty} r(I_4, t) \exp(\pi i t z)$.

So far we have only considered primitive representations, let us now turn towards imprimitive representations.

LEMMA 8.45. *With notations as before let M' be an integral lattice on W and denote by $M_1, \dots, M_t$ the integral overlattices of M'.*
Then $r(\Lambda, M') = \sum_{i=1}^t r^*(\Lambda, M_i)$.

PROOF. Obvious. □

LEMMA 8.46. *With notations as above let v be a non archimedean place of F and write $A(M', M; \Lambda \bmod P^k\Lambda^\#)$ for the number of R-linear maps $\phi : M' \to \Lambda/P^k\Lambda^\#$ satisfying $\phi(M) = \phi(W) \cap \Lambda$ and $Q(\phi(x)) \equiv Q(x) \bmod P^k$ for all $x \in M'$, let $\alpha_v(\Lambda; M', M)$ be obtained from $A(M', M; \Lambda \bmod P^k\Lambda^\#)$ as we obtained $\alpha_v^*(\Lambda; M)$ from $A^*(M; \Lambda \bmod P^k\Lambda^\#)$ above.*
Then for large enough k

$$A(M', M; \Lambda \bmod P^k\Lambda^\#) = (M : M')^{1-u} A^*(M; \Lambda/P^k\Lambda^\#),$$

and one has

$$\alpha_v(\Lambda; M', M) = \alpha_v^*(\Lambda; M).$$

PROOF. The second formula follows from the first one. By the elementary divisor theorem there is a basis $f_1, \dots, f_w$ of M such that $\pi_v^{s_1} f_1, \dots, \pi_v^{s_w} f_w$ with some $0 \le s_1 \le \cdots \le s_w$ is a basis of M', where π_v is a prime element of R_v. Let T denote the Gram matrix of Q with respect to the f_i.
Let $\phi : W \to V$ be an R-linear (hence F-linear) map such that $\phi(M) \subseteq \Lambda$ is primitive. Then ϕ restricted to M' is an isometry modulo P^k if and only if the Gram matrix $T^{(\phi, M')}$ of (M', Q) with respect to the $\phi(\pi_v^{s_i} f_i)$ satisfies $t_{ij}^{(\phi,M')} \equiv_{ev} \pi_v^{s_i+s_j} t_{ij} \bmod P^k$, where $\equiv_{ev}$ denotes as earlier that the congruence is modulo $2P^k$ for $i = j$. Equivalently, we may write $t_{ij}^{(\phi,M)} \equiv_{ev} t_{ij} \bmod P^{k-(s_i+s_j)}$, where $T^{(\phi,M)}$ denotes the Gram matrix of (M, Q) with respect to the $\phi(f_i)$. The number of modulo P^k different such Gram matrices T_ℓ is $\prod_{i \le j} q^{s_i} q^{s_j} = (M : M')^{w+1}$.
The proof of Hensel's Lemma (Theorem 5.15) shows that for large enough k the number of modulo $P^k\Lambda^\#$ distinct R-linear maps $\psi : M \to \Lambda$ for which $\psi(M)$ is primitive in Λ and $T^{(\psi,M)} \equiv_{ev} T_\ell \bmod P^k$ for one of these T_ℓ holds is $(M : M')^{w+1} A^*(M; \Lambda \bmod P^k\Lambda^\#)$. In other words, all these matrices occur equally often among the Gram matrices modulo P^k associated to refinements modulo $P^k\Lambda^\#$ of the maps counted by $A^*(M; \Lambda \bmod P^{k-2s_w}\Lambda^\#)$. Furthermore, each of these ψ yields upon restriction to M' one of the maps ϕ counted in $A(M', M; \Lambda \bmod P^k\Lambda^\#)$, and each of those ϕ occurs as the restriction of $(M' : M)^n$ different ψ. Summing up and noticing $1 - u = 1 + w - n$ we see that indeed

$$A(M', M; \Lambda \bmod P^k\Lambda^\#) = (M : M')^{1-u} A^*(M; \Lambda/P^k\Lambda^\#),$$

holds.
Inserting this result into the formula relating the $\alpha_v(\quad), \alpha_v^*(\quad)$ with the $A(\quad), A^*(\quad)$ one obtains the second part of the assertion. □

REMARK 8.47. For both lemmas the argument above is valid for the case $W = V$ as well.

THEOREM 8.48. *With notations as above one has*

$$r(\mathrm{gen}(\Lambda), M') = \frac{\sum_{j=1}^{h} \dfrac{r(\Lambda_j, M')}{|SO_V(F;\Lambda_j)|}}{\sum_{j=1}^{h} \dfrac{1}{|SO_V(F;\Lambda_j)|}}$$

satisfies

$$r(\mathrm{gen}(\Lambda), M') = |D_F|^{-\frac{(n+u-1)(n-u)}{4}} \pi^{\frac{r(n+u+1)(n-u)}{4}} \prod_{j=u+1}^{n} (\Gamma(\frac{j}{2}))^{-r} \prod_{v \notin \infty} \alpha_v(\Lambda, M').$$

In the case $V = W$ (i.e, $u = 0$ in the formula above) one has to adjust here the definition of $\alpha_v(\Lambda, M')$ by a factor $\frac{1}{2}$ on the right hand side.

PROOF. The first of the above lemmas expresses the number of representations of M' by Λ in terms of the primitive representation numbers of the integral overlattices of M'. The resulting sum of numbers of primitive representations can then be expressed using the primitive local densities α_v^* for these overlattices, and application of the second lemma finishes the proof. Notice that the factor $\frac{1}{2}$ already occurred in the formula for the Maß (measure) of a genus, it occurs here for the same reason. $\square$

CHAPTER 9

Spin Group and Strong Approximation

In this chapter F is a field of characteristic not 2 and (V, Q) is a non degenerate quadratic space over F. In the definition of the Clifford group we will follow the by now standard twisted approach introduced by Atiyah and Bott, modifying the original definition of Chevalley.

9.1. Clifford group and spin group

DEFINITION 9.1. The Clifford group $\Gamma(V, Q) = \Gamma_V$ is defined by

$$\Gamma_V := \{x \in C(V, Q)^\times \mid C(-\operatorname{Id})(x)vx^{-1} \in V \text{ for all } v \in V\}.$$

LEMMA 9.2. *Γ_V acts on V by $x.v = C(-\operatorname{Id})(x)vx^{-1}$, and the homomorphism $\rho : \Gamma_V \to GL(V)$ defined by this group action has kernel $F^\times \subseteq \Gamma_V$.*

PROOF. It is obvious that $x.v = C(-\operatorname{Id})(x)vx^{-1}$ defines a group action of Γ_V on V If $\mathbf{x} \in \Gamma_V$ is in the kernel of ρ we write $x = x_0 + x_1$ with $x_i \in C_i(V, Q)$ and have $x_0v - x_1v = vx_0 + vx_1$ and isolating the components in the grading we see $x_0v = vx_0, x_1v = -vx_1$. This implies $x_0z = zx_0$ for all $z \in C(V, Q)$ and $x_1z_j = (-1)^j u_j x_1$ for $z_j \in C_j(V, Q)$. We see that x is in the graded center of $C(V, Q)$ as defined in Remark 7.23, and since this graded center is trivial we obtain the assertion. □

DEFINITION AND LEMMA 9.3. *For $x \in \Gamma_V$ one has*

$$n(x) := \bar{x}x \in F$$

and $\bar{x}x = x\bar{x}$. Moreover, n is a group homomorphism from Γ_V to $F^\times$ satisfying $n(x) = -Q(x)$ for $x \in V$ with $Q(x) \neq 0$.
We call $n(x)$ the norm or the Clifford norm of x.

PROOF. We apply the standard involution $x \mapsto \bar{x}$ of $C(V, Q)$ to the equation $C(-\operatorname{Id})(x)vx^{-1} = w \in V$ to get $\bar{x}^{-1}vC(-\operatorname{Id})\bar{x} = w$. From this we get $v = C(-\operatorname{Id})(\bar{x}x)v(\bar{x}x)^{-1})$, i.e., $\bar{x}x$ is in the kernel of the homomorphism ρ above and therefore in $F^\times$.
We see then $x(\bar{x}x) = (\bar{x}x)x$ and thus $\bar{x}x = x\bar{x}$, which easily gives that n is a group homomorphism. The definition of $\bar{x}$ finally implies $n(x) = -Q(x)$ for $x \in V$ with $Q(x) \neq 0$. □

LEMMA 9.4. *For $x \in V$ with $Q(x) \neq 0$ we have $x \in \Gamma_V$ and $\rho(x)(v) = \tau_x(v)$ for all $v \in V$.*

PROOF. We have

$$\begin{aligned} C(-\operatorname{Id})(x)vx^{-1} &= -xv\frac{x}{Q(x)} \\ &= \frac{(vx - b(x,v))x}{Q(x)} \\ &= v - \frac{b(x,v)}{Q(x)}x \\ &= \tau_x(v) \end{aligned}$$

for all $v \in V$. □

THEOREM 9.5. *The homomorphism $\Gamma_V/F^\times \to GL(V)$ induced by ρ is an isomorphism onto $O_V(F)$.*

PROOF. Let $v \in V$ with $Q(v) \neq 0$. We have

$$-Q(C(-\operatorname{Id})(x)vx^{-1}) = n(C(-\operatorname{Id})(x)vx^{-1}) = -n(C(-\operatorname{Id})(x))Q(v)n(x)^{-1}$$

since n is a group homomorphism and $v \in \Gamma_V$ by the previous lemma. But $\overline{C(-\operatorname{Id})(x)} = C(-\operatorname{Id})(x)$ implies $n(C(-\operatorname{Id})(x)) = n(x)$ and we obtain $Q(\rho(x)(v)) = Q(v)$ for all anisotropic v. If $v \in V$ is isotropic with $w = \rho(x)(v)$, we have $v = \rho(x^{-1})(w)$, so w has to be isotropic as well, and we see that indeed $\rho(x) \in O_V(F)$.
To see that ρ is surjective we recall that by Witt's generation theorem 1.32 $O_V(F)$ is generated by symmetries τ_x with anisotropic x, which are in the image of ρ by the previous lemma. □

COROLLARY 9.6. *Any $x \in \Gamma_V$ is homogeneous, i. e., it is either in $C_0(V,Q)$ or in $C_1(V,Q)$. More precisely, it can be written as a monomial $v_1 \dots v_r$ with $v_i \in V$ and $\det(\rho(x)) = (-1)^r$.*

PROOF. Obvious. □

DEFINITION 9.7. The Spin group $\operatorname{Spin}(V,Q) = \operatorname{Spin}_V(F)$ of (V,Q) is $\{x \in \Gamma_V \cap C_0(V,Q) \mid n(x) = 1\}$. The group $\operatorname{Pin}_V(F)$ is $\{x \in \Gamma_V \mid n(x) = 1\}$.
The group $O'_V(F) \subseteq SO_V(F)$ is the image of $\operatorname{Spin}_V(F)$ under ρ.

LEMMA 9.8. *The group $O'_V(F)$ contains the commutator subgroup of $O_V(F)$.*

PROOF. This is obvious since $(\tau_{y_1} \circ \dots \circ \tau_{y_r})^{-1} = \tau_{y_r} \circ \dots \circ \tau_{y_1}$ holds. □

9.2. Spinor norm, spinor genus, and strong approximation

DEFINITION 9.9. Let $\phi \in SO_V(F)$, $\phi = \rho(x)$ with $x \in \Gamma_V \cap C_0(V,Q)$. The *spinor norm* $\theta(\phi)$ of ϕ is the square class $n(x)(F^\times)^2$.

LEMMA 9.10. *Let $\phi = \tau_{y_1} \circ \dots \circ \tau_{y_r} \in SO_V(F)$ with anisotropic vectors $y_i \in V$. Then $\theta(\phi) = Q(y_1)\dots Q(y_r)(F^\times)^2$.*
In particular, the square class $Q(y_1)\dots Q(y_r)(F^\times)^2$ is independent of the choice of a product decomposition $\phi = \tau_{y_1} \circ \dots \circ \tau_{y_r} \in SO_V(F)$.

PROOF. Obvious. □

REMARK 9.11. If one scales the quadratic form Q by a factor $c \in F^{\times}$, the orthogonal group obviously doesn't change, and the spinor norm of a $\phi \in SO_V(F)$ doesn't change either. It is of course possible to define the spinor norm for orthogonal transformations of determinant -1 as well, but it will then not be invariant under scaling of the quadratic form.

EXAMPLE 9.12.

a) Let $F = \mathbb{R}$ and (V, Q) be positive definite. Then $\theta(\phi) = (\mathbb{R}^{\times})^2$ for all $\phi \in SO_V(F)$ since all the $Q(v)$ are positive, and the restriction of the homomorphism ρ to $\mathrm{Spin}_V(\mathbb{R})$ is surjective. Since its kernel is $\{\pm 1\}$, the spin group is in this case a double cover of the special orthogonal group.
b) If F is $\mathbb{C}$ or another algebraically closed field, the surjectivity of $\rho|_{\mathrm{Spin}_V(F)}$ is obvious and we have again a double covering of $SO_V(F)$ by $\mathrm{Spin}_V(F)$. In particular, in the sense of the theory of algebraic groups, the spin group (as an algebraic group) is a double cover of the special orthogonal group. If F is a field that is not algebraically closed, e. g. $F = \mathbb{Q}$, the image $O'_V(F)$ of the F-points $\mathrm{Spin}_V(F)$ can nevertheless be smaller than $SO_V(F)$.

DEFINITION 9.13. Let F be a number field, let Λ, Λ' be lattices on V.
Λ' is said to be in the *spinor genus* of Λ and one writes $\Lambda' \in \mathrm{spn}(\Lambda)$ if there are $\sigma \in O_V(F)$ and $\phi = (\phi_v)_{v \in \Sigma_F} \in O'_V(\mathbb{A}_F)$ with $\Lambda' = \sigma(\phi(\Lambda))$.
If here σ can be chosen in $SO_V(F)$ we say that Λ' is in the proper spinor genus $\mathrm{spn}^+(\Lambda)$.

REMARK 9.14. It is clear that lattices in the same spinor genus are a fortiori in the same genus and that a spinor genus consists of full isometry classes. It turns out that in some cases the concepts of spinor genus and isometry class coincide.

THEOREM 9.15 (Strong approximation). *Let F be a global field and (V, Q) be a non degenerate quadratic space over F, let $S \subseteq \Sigma_F$ be a finite set of places such that (V_v, Q_v) is isotropic for at least one $v \in S$.*
Then Spin_V *admits strong approximation with respect to S, i, e.,*
$\mathrm{Spin}_V(F) \prod_{v \in S} \mathrm{Spin}_V(F_v)$ *is dense in* $\mathrm{Spin}_V(\mathbb{A}_F)$.

PROOF. This has been proven for all almost simple simply connected classical groups over number fields by Kneser in [**20**], a first form of the result is due to Eichler [**11**]. For the general proof and historical remarks see [**30**]. □

REMARK 9.16. The group $\mathrm{Spin}_V(\mathbb{A}_F)$ of adelic points of the spin group is as usual the restricted direct product of the $\mathrm{Spin}_V(F_v)$ with respect to a family of compact subgroups H_v for the non archimedean places v of F, which can be taken (equivalently) as

$$H_v = \mathrm{Spin}_V(F_v; \Lambda) := \{x \in \mathrm{Spin}_V(F_v) \mid \rho(x)(\Lambda) \subseteq \Lambda\}$$

for a fixed (but arbitrary) lattice Λ on V or as $H_v = \{\sum_j \alpha_j z_j \in \mathrm{Spin}_V(F_v) \mid \alpha_j \in R_v\}$, where the z_j comprise some fixed basis of $C_0(V, Q)$ as vector space over F and R_v is the valuation ring of F_v. A basis of open neighborhoods of 1 in $\mathrm{Spin}(\mathbb{A}_F)$ is then given by the $\prod_v U_v$, where each U_v is open in $\mathrm{Spin}_v(F_v)$ and may be chosen to be a principal congruence subgroup of $\mathrm{Spin}_v(F_v)$ for non archimedean v, and where $U_v = H_v$ for almost all v.

To give the strong approximation property a more concrete shape we formulate the following corollary:

COROLLARY 9.17. *Let F and $S \subseteq \Sigma_F$ be as in the theorem, assume that S contains all archimedean places of F and let $v_1, \dots, v_r \in \Sigma_F \setminus S$ be given. Let moreover $g_j \in \mathrm{Spin}_V(F_{v_j})$, $\phi_j \in O'_V(\mathbb{F}_{v_j})$ and $s_j \in \mathbb{N}$ be given for $1 \leq j \leq r$. Let $\mathrm{Spin}_V(F_v; \Lambda, \pi^{s_j}\Lambda) \subseteq \mathrm{Spin}_V(F_v, \Lambda)$ for a lattice Λ on V denote the congruence subgroup consisting of all $g \in \mathrm{Spin}_V(F_v)$ satisfying $\rho(x) - x \in \pi^{s_j}\Lambda$ for all $x \in \Lambda$. Then*

a) *There exists $g \in \mathrm{Spin}_V(F)$ with $g \in g_j\mathrm{Spin}_V(F_{v_j}; \Lambda, \pi_v^{s_j}\Lambda)$ for $1 \leq j \leq r$ and $g \in \mathrm{Spin}_V(F_v; \Lambda)$ for all $v \notin (S \cup \{v_1, \dots, v_r\})$.*
b) *There exists $\sigma \in O'_V(F)$ satisfying $\sigma \in \phi_j(O'_V(F_v) \cap SO_V(F_v; \Lambda, \pi^{s_j}\Lambda)$ for $1 \leq j \leq r$ and $\sigma \in SO_V(F_v; \Lambda)$ for all $v \in \Sigma_F \setminus (S \cap \{v_1, \dots, v_r\})$.*

PROOF. This is obtained by writing out the statement of the theorem in terms of the topology of $\mathrm{Spin}_V(\mathbb{A}_F)$. □

THEOREM 9.18 (Eichler). *Let F be a number field and Λ a lattice on the non degenerate quadratic space (V, Q) over F, assume that (V_v, Q_v) is indefinite for at least one archimedean place of F.*
Then the (proper) spinor genus of Λ consists of only one (proper) class.

PROOF. Let Λ' be a lattice on V in the spinor genus of Λ, we may assume that $\Lambda' = \phi(\Lambda)$ for some $\phi = (\phi_v)_v \in O'_V(\mathbb{A}_F)$. Let $S = \infty$ denote the set of archimedean places of F and denote by $v_1, \dots, v_r$ the finitely many $v \in \Sigma_F \setminus S$ with $\Lambda'_v \neq \Lambda$.
By Corollary 9.17 there exists $\sigma \in O'_V(F)$satisfying $\sigma \in \phi_{v_j}SO_V(F_v; \Lambda)$ for $1 \leq j \leq r$ and $\phi \in SO_V(F_v; \Lambda)$ for all non archimedean $v \notin \{v_1, \dots, v_r\}$. We have then $\sigma(\Lambda_v) = \Lambda'_v$ for all non archimedean v, hence $\sigma(\Lambda) = \Lambda'$, and Λ' is in the class of Λ. The argument for the proper spinor genus is identical. □

The main advantage of the concept of spinor genus is that questions about spinor genera can essentially be decided on a local level. We want to show next that the number of spinor genera in a given genus of lattices can be explicitly computed as an index of idele groups. For this we need some lemmas.

LEMMA 9.19. *Let $F = F_v$ be a non archimedean local field for which 2 is a unit in the valuation ring $R = R_v$ (a nondyadic local field). Let Λ be a unimodular lattice on the non degenerate quadratic space (V, Q) over F of dimension ≥ 2. Then $\theta(SO_V(F; \Lambda)) = R^\times (F^\times)^2$.*

PROOF. As in the proof of Theorem 1.32 one proves by induction on $\dim(V)$ that $O_V(F;\Lambda)$ is generated by symmetries τ_x with respect to vectors $x \in \Lambda$ with $Q(x) \in R^\times$; indeed in all places where we had the condition that $Q(z) \neq 0$ for some vector z we can replace it here by $Q(z) \in R^\times$, the fact that 2 and hence 4 is a unit in R is crucial for this. Since a unimodular R-lattice of rank ≥ 2 represents all units (here we use again that 2 is a unit), the assertion follows. □

DEFINITION AND LEMMA 9.20. *Let (V, Q) be a non degenerate quadratic space over the number field F, let $\phi = (\phi_v)_v \in SO_V(\mathbb{A}_F)$. Then $\theta(\phi_v) \cap R_v^\times \neq \emptyset$ for almost all places v of F, and there is an idele $\alpha = (\alpha_v)_v \in J_F$ with $\alpha_v \in \theta(\phi_v)$ for all $v \in \Sigma_F$, and all such ideles form a square class modulo J_F^2.*
This square class $\alpha J_F^2 \subseteq J_F$ is denoted by $\theta(\phi)$ and is called the idele spinor norm of ϕ.

PROOF. Let Λ be a lattice on V. Since $\phi_v \in SO_V(F_v;\Lambda_v)$ holds for almost all v and Λ_v is unimodular for almost all v, the assertion follows from the previous lemma. □

THEOREM 9.21. *Let (V, Q) and F be as before, Λ a lattice on V, let $\phi = (\phi_v)_v \in SO_V(\mathbb{A}_F)$.*
Then $\phi(\Lambda)$ is in the proper spinor genus of Λ if and only if

$$\theta(\phi) \in \theta(SO_V(F))\theta(SO_V(\mathbb{A}_F;\Lambda))$$

holds.
The number of proper spinor genera in the genus of Λ is equal to the group index

$$(J_F^V : \theta(SO_V(F))\theta(SO_V(\mathbb{A}_F;\Lambda))),$$

where $J_F^V = \theta(SO_V(\mathbb{A}_F))$.

PROOF. $\phi(\Lambda) \in \mathrm{spn}^+(\Lambda)$ is equivalent to $\phi \in SO_V(F)O'_V(\mathbb{A}_F)SO_V(\mathbb{A}_F;\Lambda)$. This is again equivalent to $\theta(\phi) \in \theta(SO_V(F))\theta(SO_V(\mathbb{A}_F;\Lambda))$, notice for this that in $SO_V(F)O'_V(\mathbb{A}_F)SO_V(\mathbb{A}_F;\Lambda)$ the order of the factors can be exchanged since $O'_V(\mathbb{A}_F)$ contains all commutators in $SO_V(\mathbb{A}_F)$.
The number of proper spinor genera is equal to the number of double cosets in the decomposition

$$SO_V(\mathbb{A}_F) = \bigcup_j SO_V(F)\phi_j O'_V(\mathbb{A}_F)SO_V(\mathbb{A}_F;\Lambda).$$

By the same argument as above, the map associating to the double coset $SO_V(F)\phi O'_V(\mathbb{A}_F)SO_V(\mathbb{A}_F;\Lambda)$ the coset of $\theta(\phi)$ in the factor group

$$J_F^V/\theta(SO_V(F))\theta(SO_V(\mathbb{A}_F;\Lambda))$$

is a bijection. □

We can make the last formula a little more explicit:

LEMMA 9.22. *Let J_F^V be as in the theorem and assume* $\dim(V) \geq 3$. *Then*

$$J_F^V = \{\alpha = (\alpha_v)_v \in J_F \mid \alpha_v > 0 \textit{ for all real } v \textit{ with } (V_v, Q_v) \textit{ definite}\}$$

and $\theta(SO_V(F)) = F^\times \cap J_F^V$.

PROOF. For archimedean v it is obvious that $\theta(SO_V(F_v)) = F^\times$ if v is complex or (V_v, Q_v) indefinite and that $\theta(SO_V(F_v))$ consists of the positive elements of $F_v^\times = \mathbb{R}^\times$ if v is real and (V_v, Q_v) definite.
Let now v be non archimedean. If $\dim(V) \geq 4$ holds, the completion (V_v, Q_v) is universal and hence $\theta(SO_V(F_v)) = F^\times$. Let $\dim(V) = 3$ and $a \in F_v^\times$, by scaling the quadratic form we may assume that $\det_B(V)$ is the square class of a prime element. If a is a unit in R_v, we have $-a \notin \det_B(V_v)$, hence the 4-dimensional space $V_v \perp [-a]$ over F_v has determinant $\neq (F_v^\times)^2$ and must be isotropic, which implies $a \in Q(V_v)$. On the other hand, $\det_B(V) = \pi_v (F_v^\times)^2$ for a prime element π_v of R_v implies that at least one prime element is in $Q(V_v)$, and we see that $\theta(SO_V(F_v)) = F_v^\times$.
For the statement about the global spinor norm group $\theta(SO_V(F))$ the inclusion $\theta(SO_V(F)) \subseteq F^\times \cap J_F^V$ is clear.
Denote by T the set of all real places v for which (V_v, Q_v) is definite. Let $\dim(V) \geq 4$ and let $a \in F^\times$ be positive at all $v \in T$, let $0 \neq b \in Q(V)$. Then ab is positive and hence in $Q(V_v)$ at all $v \in T$, and $ab \in Q(V_v)$ for the remaining $v \in \Sigma_F$ since $(V_v, Q_v$ is universal for these v. By the Minkowski-Hasse Theorem we have $ab \in Q(V)$, hence $ab^2 \in \theta(SO_V(F))$ and $a \in \theta(SO_V(F))$.
Let now $\dim(V) = 3$ and a be as above, by scaling the quadratic form we may assume $\det_B(V) = (F^\times)^2$. Denote by S the finite set of all non archimedean v for which (V_v, Q_v) is anisotropic. Using weak approximation we choose $b \in F^\times$ such that $b \notin (F_v^\times)^2, -ab \notin (F_v^\times)^2$ hold for all $v \in S \cup T$, in particular, $-b$ and hence $-ab$ are negative at all $v \in T$. The 4-dimensional spaces $W_1 = V \perp [-b], W_2 = V \perp [-ab]$ are then isotropic over all completions F_v, and the Minkowski-Hasse Theorem implies $b \in Q(V), ab \in Q(V)$, from which we obtain $a \in \theta(SO_V(F))$. □

LEMMA 9.23. *Let $F = F_v$ be a non archimedean local field,* $\mathrm{char}(F) \neq 2$, *let (V, Q) be a non degenerate quadratic space of dimension ≥ 3 over F and Λ be a maximal lattice on V.*
Then $\theta(SO_V(F_v; \Lambda)) \supseteq R_v^\times$.

PROOF. If (V, Q) is anisotropic Λ is the set of all $x \in V$ with $Q(x) \in R$ by Theorem 5.27 and hence $SO_V(F_v; \Lambda) = SO_V(F_v)$, which implies $\theta(SO_V(F_v; \Lambda)) = F_v^\times$. Otherwise we can write $\lambda = H \perp \Lambda'$ with a hyperbolic plane H by Theorem 2.19 and we see $\theta(SO_V(F_v; \Lambda)) \supseteq R_v^\times$ as asserted since already the orthogonal group of H has all units as spinor norms. □

THEOREM 9.24. *Let (V, Q) be a non degenerate quadratic space over $\mathbb{Q}$. Then all $\mathbb{Z}$-maximal lattices on V belong to the same proper spinor genus. In particular, for any signature (n_+, n_-) with $n_+ \neq 0 \neq n_-$ there exists at most one class of even unimodular $\mathbb{Z}$-lattices of this signature.*

PROOF. Since $\mathbb{Q}$ has class number 1 this follows from Theorem 9.21 and the lemmas following it. $\square$

REMARK 9.25. The spinor norm groups of the automorphism groups of local lattices have been computed, following the initial work of Eichler and Kneser, in great detail by Hsia, Earnest, and Beli. In particular, it has been proven that the spinor norm group of a unimodular $\mathbb{Z}_2$-lattice of rank ≥ 3 contains (as in the case of maximal lattice treated above) all units, so that a genus of unimodular $\mathbb{Z}$-lattices (odd or even) contains only one proper spinor genus.

9.3. Neighboring lattices and anzahlmatrices

THEOREM 9.26. *Let F be a number field and (V, Q) a non degenerate quadratic space. Let $v_0 \in \Sigma_F$ be a non archimedean place such for which (V_{v_0}, Q) is isotropic, let Λ_1, Λ_2 be lattices on V in the same spinor genus. Then there exists a lattice Λ_2' in the isometry class of Λ_2 with $(\Lambda_2)_v' = (\Lambda_1)_v$ for all $v \in \Sigma_F \setminus \{v_0\}$.*

PROOF. without loss of generality we can assume that there exist $\phi \in O_V'(\mathbb{A}_F)$ with $\Lambda_2 = \phi(\Lambda_1)$. Let $S := \infty \cup \{v_0\} \subseteq \Sigma_F$, denote by $v_1, \dots, v_n$ the finitely many places $v \in \Sigma_F$ with $(\Lambda_1)_v \neq (\Lambda_2)_v$. By Corollary 9.17 there exist $\sigma \in O_V'(F)$ with $\sigma \in \phi_{v_j}^{-1} O_V'(F_{v_j}; \Lambda_2)$ for $1 \leq j \leq n$ and $\sigma \in O_V'(F_v; \lambda_2)$ for all $v \notin S \cup \{v_1, \dots, v_n\}$.
Then $\sigma(\Lambda_2) =: \Lambda_2'$ is as required. □

REMARK 9.27. The lattices Λ_1, Λ_2 or the space (V, Q) supporting them are called arithmetically indefinite (“arithmetisch indefinit”) following Eichler, who introduced this idea in [**12**].

DEFINITION 9.28 (Kneser). Let (V, Q) be a non degenerate quadratic space over the number field F and let $v \in \Sigma_F$ be a non archimedean place of F and P the associated maximal ideal in the ring of integers R of F.
Lattices Λ, Λ' on V are called v-neighbors or P-neighbors if one has

$$\Lambda/(\Lambda \cap \Lambda') \cong R/P \cong \Lambda'/(\Lambda \cap \Lambda').$$

If $\Lambda = \Lambda_1, \dots, \Lambda_h$ is a set of representatives of the isometry classes of lattices in the genus of Λ denote by $N_v(\Lambda_i, \Lambda_j) = N_P(\Lambda_i, \Lambda_j)$ the number of lattices in the isometry class of Λ_j which are P-neighbors of Λ_i.
The $h \times h$ matrix $(N_P(\Lambda_i, \Lambda_j))_{i,j}$ is called P-neighborhood matrix of the genus of Λ.

REMARK 9.29. The P-neighborhood matrix defined above is a special case of the anzahlmatrix associated to a fixed system of elementary divisors for an ideal complex as defined by Eichler in [**11**].

As noticed by Eichler the anzahlmatrices satisfy a certain symmetry relation. We formulate and prove this in a slightly more general context:

PROPOSITION 9.30 (Eichler,[**11**]). *Let F be a number field or a non archimedean local field with ring of integers R, let (V, Q) be a regular quadratic space over F.*
Let $\sim_1, \sim_2$ be two relations on the set of lattices on V such that for all $\phi \in O_V(F)$ and all lattices Λ_1, Λ_2 on V one has $\phi(\Lambda_2) \sim_1 \Lambda_1$ if and only if $\phi^{-1}(\Lambda_1) \sim_2 \Lambda_2$ holds. Assume moreover that for all lattices Λ on V there are only finitely many lattices Λ' on V satisfying $\Lambda' \sim_1 \Lambda$ or $\Lambda' \sim_2 \Lambda$.
For $i = 1, 2$ let $N_i(\Lambda_1, \Lambda_2)$ denote the number of lattices M on V which are isometric to Λ_2 and satisfy $M \sim_i \Lambda_1$.

Then $N_1(\Lambda_1,\Lambda_2)=0$ *if and only if* $N_2(\Lambda_2,\Lambda_1)=0$*, and if both are nonzero one has*

$$\frac{N_1(\Lambda_1,\Lambda_2)}{N_2(\Lambda_2,\Lambda_1)}=\frac{(O_V(F;\Lambda_1)\,:\,O_V(F;\Lambda_1)\cap O_V(F;\Lambda_2))}{(O_V(F;\Lambda_2)\,:\,O_V(F;\Lambda_1)\cap O_V(F;\Lambda_2))}.$$

PROOF. Let lattices Λ_1,Λ_2 be given with $\Lambda_2\sim_1\Lambda_2$, hence (setting $\phi=\mathrm{Id}_V$ in the assumption) $\Lambda_1\sim_2\Lambda_2$ and let $\phi_1(\Lambda_2),\dots\phi_q(\Lambda_2)$ with $\phi_i\in O_V(F)$ denote the different lattices M in the class of Λ_2 with $M\sim_1\Lambda_1$. The cosets $\phi_iO_V(F;\Lambda_2)$ are then distinct and uniquely determined and their union is equal to $X:=\{\phi\in O_V(F)\mid\phi(\Lambda_2)\sim_1\Lambda_1$. Let $\psi_1(\Lambda_1),\dots,\psi_r(\Lambda_1)$ denote the different lattices K in the class of Λ_1 with $K\sim_2\Lambda_2$. The cosets $\psi_kO_V(F;\Lambda_1)=O_V(F;\psi_k(\Lambda_1))\psi_k$ are then also distinct and uniquely determined. and their union is equal to $Y=\{\psi\in O_V(F)\mid\psi(\Lambda_1)\sim_2\Lambda_2\}$. Moreover, by our assumption on the relations $\sim_1,\sim_2$ we see that Y is just the set of inverses of the elements of X. Let

$$G=O_V(F;\Lambda_2)\cap O_V(F;\phi_1^{-1}(\Lambda_2))\cap\cdots\cap O_V(F;\phi_r^{-1}(\Lambda_2))$$

and consider coset decompositions

$$\begin{aligned}O_V(F;\Lambda_2)&=\bigcup_{\mu}^{s}\sigma_\mu G\\ O_V(F;\psi_k\Lambda_1)&=\bigcup_{\nu}^{t}G\rho_{k\nu}.\end{aligned}$$

Notice that remark 8.20 on the elementary construction of a biinvariant Haar measure on congruence sets implies $(O_V(F;\psi_k\Lambda_1)\,:\,G)=(O_V(F;\psi_{k'}\Lambda_1)\,:\,G)$ for all k,k', so that the index ν above indeed runs over the same set $1\le\nu\le t$ for all k. We have $\phi_i\sigma_\mu G=\phi_{i'}\sigma_{\mu'}G$ if and only if $i=i',\mu=\mu'$ hold and $G\rho_{k\nu}\psi_k=G\rho_{k'\nu'}\psi_{k'}$ if and only if $k=k',\nu=\nu'$. Since $\phi\mapsto\phi^{-1}$ defines a bijection of $X=\bigcup_{i,\mu}\phi_i\sigma_\mu G$ onto $Y=\bigcup_{k,\nu}G\rho_{k\nu}\psi_k$ we obtain $qs=rt$, which is the assertion. □

COROLLARY 9.31. *With notations as above write* m_j *for the measure* $\mu_\infty(O_V(F;\Lambda_j)\backslash(O_V(F_\infty)))$ *of the volume of a fundamental domain in* $O_V(F_\infty)$ *under the action of the arithmetic subgroup* $O_V(F;\Lambda_j)$*, where* $F_\infty=\prod_{v\in\infty}F_v$ *and* μ_∞ *is a (fixed) Haar measure on* $O_V(F_\infty)$ *.*
Then one has

$$m_iN_P(\Lambda_i,\Lambda_j)=m_jN_P(\Lambda_i,\Lambda_j).$$

In particular, if (V,Q) *is totally definite, one has*

$$|O_V(F;\Lambda_j)|N_P(\Lambda_i,\Lambda_j)=|O_V(F;\Lambda_i)|N_P(\Lambda_i,\Lambda_j).$$

Moreover, the P*-neighborhood matrices for different maximal ideals commute pairwise and the algebra generated by the* P*-neighborhood matrices for all maximal ideals* P *can be diagonalized simultaneously.*

PROOF. Upon letting $\sim_1=\sim_2$ be the relation "is P-neighbor of", the first assertion follows from the proposition because of

$$\frac{m_i}{m_j} = \frac{(O_V(F;\Lambda_j) : O_V(F;\Lambda_i) \cap O_V(F;\Lambda_j)}{(O_V(F;\Lambda_i) : O_V(F;\Lambda_i) \cap O_V(F;\Lambda_j)}.$$

The assertion in the totally definite case is just a reformulation using the finiteness of the automorphism groups of the lattices in that case.
The last part of the assertion is obvious since by the first part all matrices in question can be simultaneously transformed into symmetric matrices by conjugation with a diagonal matrix. □

COROLLARY 9.32. *With notations as above let $\Lambda_1 \subseteq \Lambda_2$. Let q be the number of sublattices of Λ_1 which are isometric to Λ_2 and r be the number of overlattices of Λ_2 which are isometric to Λ_1. Then*

$$\frac{q}{r} = \frac{(O_V(F;\Lambda_1) : O_V(F;\Lambda_1) \cap O_V(F;\Lambda_2))}{(O_V(F;\Lambda_2) : O_V(F;\Lambda_1) \cap O_V(F;\Lambda_2))}.$$

PROOF. With $M \sim_1 L$ if and only if $M \subseteq L$, $L \sim_2 M$ if and only if $L \supseteq M$ this follows directly from the proposition. □

REMARK 9.33. Eichler proves in [**11**] analogous results for anzahlmatrices of ideal complexes with fixed elementary divisor systems. These can be obtained from our proposition in the same way as Corollary 9.31 using similitude groups instead of groups of isometries. The assertion of Corollary 9.32 can be obtained from Eichler's results, it has been formulated and used for classification results about positive definite lattices by B. B. Venkov and is sometimes called Venkov's theorem. From our general setting it is clear that analogous results (with unitary isometry groups instead of orthogonal groups) hold for hermitian lattices.

THEOREM 9.34. *Let (V, Q) be a positive definite quadratic space over $\mathbb{Q}$ of dimension ≥ 5, let Λ, Λ' be unimodular $\mathbb{Z}$-lattices on V which are in the same genus, let $p \in \mathbb{N}$ be a prime.*
Then there exists a chain $\Lambda = \Lambda_0, \Lambda_1, \ldots, \Lambda_r$ of unimodular lattices on V such that Λ_i, Λ_{i+1} are p-neighbors for $0 \leq i < r$ and Λ_r is in the isometry class of Λ'.
If $p = 2$ the condition that Λ, Λ' should be in the same genus can be omitted.

PROOF. From Remark 9.25 it follows that the genus of λ consists of only one spinor genus. By theorem 9.26 we can therefore assume that $\Lambda_\ell = \Lambda'_\ell$ for all primes $\ell \neq p$. If $\Lambda \neq \Lambda'$ there exists $x \in \Lambda', x \notin \Lambda$ with $px \in \Lambda$. Since px is then primitive in Λ we have $b(px, \Lambda) \nsubseteq p\mathbb{Z}_p$. It follows that $\Lambda_x := \{y \in \Lambda \mid b(x, y) \in \mathbb{Z}\}$ is a sublattice of Λ of index p, and setting $\Lambda_1 := \mathbb{Z}x + \Lambda_x$ we obtain another unimodular $\mathbb{Z}$-lattice Λ_1 on V which is a p-neighbor of Λ.
From $\Lambda \cap \Lambda' \subseteq \Lambda_x \subseteq \Lambda_1$ we see $\Lambda \cap \Lambda' \subseteq \Lambda' \subseteq \Lambda_1$, and this inclusion is proper since $x \notin \Lambda \cap \Lambda', x \in \Lambda'\Lambda_1$. By induction on $(\Lambda : \Lambda \cap \Lambda') = (\Lambda' : \Lambda \cap \Lambda')$ the assertion follows. □

REMARK 9.35. a) If $p = 2$ and Λ, Λ' are both even all members of the chain constructed above are even as well.

b) Starting from a given unimodular $\mathbb{Z}$-lattice Λ one can algorithmically determine all p-neighbors of it. Continuing this until representatives of all classes in the genus of Λ have been found one can classify genera of positive definite lattices. This is Kneser's neighboring lattice method from [**21**]. It has been generalized by various authors and is now part of some computer algebra packages, in particular MAGMA.

Bibliography

[1] M. Atiyah, MacDonald: Introduction to Commutative Algebra, Addison-Wesley, Reading Mass. 1969

[2] S. Böge: Schiefhermitesche Formen über Zahlkörpern und Quaternionenschiefkörpern, J. f. die reine u. angew. Math. (Crelles Journal) 221.

[3] A. Borel, Harish-Chandra: Arithmetic subgroups of algebraic groups. Ann. of Math. (2) 75 (1962), 485–535.

[4] N. Bourbaki: Algèbre Commutative, Reprint of the 1998 original. Springer-Verlag, Berlin, 2007.

[5] N. Bourbaki: Integration, Paris 1965

[6] J. W. S. Cassels: Rational Quadratic Forms, London Mathematical Society Monographs, 13. Academic Press, London-New York, 1978.

[7] C. Chevalley: L'Arithmétique dans les Algèbres de Matrices, Hermann, Paris 1936

[8] C. Curtis, I. Reiner: Representation Theory of Finite Groups and Associative Algebras, Wiley 1966

[9] J. Dieudonné: La Géométrie des Groupes Classiques, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5. Springer-Verlag, Berlin-New York, 1971

[10] A. G. Earnest, J. S.Hsia: Spinor norms of local integral rotations. II. Pacific J. Math. 61 (1975), no. 1, 71–86

[11] M. Eichler: Quadratische Formen und Orthogonale Gruppen, Grundlehren d. math. Wiss. 63, Springer Verlag 1952.

[12] M. Eichler: Die Ähnlichkeitsklassen indefiniter Gitter. Math. Z. **55** (1952), 216–252.

[13] D. Eisenbud: Commutative Algebra. With a view toward algebraic geometry. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995

[14] J. Ellenberg, A. Venkatesh: Local-global principles for representations of quadratic forms. *Invent. Math.* **171** (2008), 257–279.

[15] J. S. Hsia: Spinor norms of local integral rotations I, Pacific J. Math. 57 (1975), 199–206.

[16] J. S. Hsia: Representations by spinor genera. *Pacific J. Math.* **63** (1976), 147–152.

[17] P. Humbert: Réduction de formes quadratiques dans on corps algébrique fini, Comm. Math. Helv. 23 (1949), 50-63.

[18] I. Kaplansky: Modules over Dedekind rings and valuation rings, Trans. Amer. Math. Soc. 72 (1952), 327–340.

[19] M. Kneser: Quadratische Formen. Quadratische Formen. Revised and edited in collaboration with Rudolf Scharlau. Springer-Verlag, Berlin, 2002.

[20] M.Kneser: Starke Approximation in algebraischen Gruppen I, J. Reine Angew. Math. 218 (1965), 190–203.

[21] M. Kneser: Klassenzahlen definiter quadratischer Formen, Arch. Math. 8 (1957), 241–250.

[22] M. -A. Knus: Quadratic and Hermitian forms over Rings, Hermitian forms over rings. Grundlehren der Mathematischen Wissenschaften 294. Springer-Verlag, Berlin, 1991.

[23] M. Kneser: Klassenzahlen indefiniter quadratischer Formen. *Arch. Math.* **7** (1956) 323 – 332.

[24] M. Kneser: Darstellungsmaße indefiniter quadratischer Formen. *Math. Z.* **77** (1961), 188–194.

[25] R. Kottwitz: Tamagawa numbers, Ann. of Math. (2) 127 (1988), 629-646

[26] T. Y. Lam: Introduction to Quadratic Forms over Fields, Graduate Studies in Math. 67, AMS, Providence 2004

[27] A. K. Lenstra, H. W. Lenstra, H. W, L. Lovász: Factoring polynomials with rational coefficients. Math. Ann. 261 (1982), no. 4, 515–534.

[28] O. T. O'Meara: Introduction to Quadratic Forms. Introduction to quadratic forms. Die Grundlehren der mathematischen Wissenschaften, Bd. 117 Springer-Verlag, Berlin-Göttingen-Heidelberg 1963

[29] H. Minkowski: Sur la reduction des formes quadratiques positives quaternaires, Ges. Abh. I (1911), 149-156

[30] V. Platonov, A. Rapinchuk: Algebraic groups and number theory. Translated from the 1991 Russian original by Rachel Rowen. Pure and Applied Mathematics, 139. Academic Press, Inc., Boston, MA, 1994.

[31] W. Scharlau: Quadratic and Hermitian Forms. Grundlehren der Mathematischen Wissenschaften 270. Springer-Verlag, Berlin, 1985.

[32] C. L. Siegel: Über die analytische Theorie der quadratischen Formen, Ann. of Math (2) 36 (1935), 527-606

[33] C. L. Siegel: Über die analytische Theorie der quadratischen Formen II, Ann. of Math (2) 37 (1936), 230-263

[34] C. L. Siegel: Über die analytische Theorie der quadratischen Formen III, Ann. of Math (2) 38 (1937), 212-291

[35] C. L. Siegel: Einheiten quadratischer Formen: Abh. Math. Sem. Hansischen Univ. 13 (1940), 209–239.

[36] P. Tammela: Minkowski's fundamental reduction domain for positive quadratic forms of seven variables. J. of Soviet Math. 16 (1981), 836-857

[37] B. L. van der Waerden: Die Reduktionsthorie der positiven quadratischen Formen, Acta math. **96** (1956)

[38] C. T. C. Wall: Graded Brauer groups, J. f. d. reine und angew. Mathematik **213**, 1964

[39] A. Weil: Adeles and Algebraic Groups, Birkhäuser/Springer 1982 (PM 23)

[40] E. Witt: Theorie der quadratischen Formen in beliebigen Körpern, J. f. d. reine und angew. Mathematik **176**

[41] S. Zemel: On lattices over valuation rings of arbitrary rank, J. of Algebra 423 (2015), 812-852