CHAPTER 3

Representations of integers by general quadratic forms

In the present chapter, we generalize the previous discussions on the representations of integers to a general quadratic form in n variables. We refer to Appendix 11 for general terminology and facts about quadratic forms.

1. Quadratic forms over a lattice

Let $q : \mathbb{Q}^n \to \mathbb{Q}$ be a quadratic form whose polarization is noted $\langle ., . \rangle$: $\langle \mathbf{x}, \mathbf{x}' \rangle = q(\mathbf{x} + \mathbf{x}') - q(\mathbf{x}) - q(\mathbf{x}')$. We assume that q is non degenerate (ie. $rk(q) = n$ or equivalently $\text{disc}(q) \neq 0$).

Given $d \in \mathbb{Q}$ we are interested in the solutions of the equation

$$q(\mathbf{x}) = d, \ \mathbf{x} \in \mathbb{Q}^n \tag{3.1}$$

or equivalently the set of isometric embeddings

$$f : (\mathbb{Q}, dx^2) \hookrightarrow (\mathbb{Q}^n, q), \ q(f(x.1)) = dx^2$$

(by defining $f(1) = \mathbf{x}$). Picking $\mathcal{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ any[1] basis of $\mathbb{Q}^n$, this amounts to studying the solutions to the polynomial equation

$$Q_{\mathcal{B}}(x_1, \cdots, x_n) = d$$

where

$$Q_{\mathcal{B}}(x_1, \cdots, x_n) = q(x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n) = \sum_{i,j=1\cdots n} \frac{1}{2} m_{i,j} x_i x_j,$$
$$m_{i,j} = \langle \mathbf{e}_i, \mathbf{e}_j \rangle.$$

We will be interested in studying the set of solutions $\mathbf{x}$ to this equation whose coordinates $x_1, \cdots, x_n$ satisfy additional constraints of arithmetic type.T he most basic requirement is that the coordinates are all *integral* or in other terms we look for the solutions of (3.1) which are contained in the lattice

$$L = \mathbb{Z}\mathbf{e}_1 + \cdots + \mathbb{Z}\mathbf{e}_n.$$

Let us recall what a lattice is:

[1]for instance this could be the canonical basis $\{\mathbf{e}_{0,1} = (1, 0, , 0), \cdots, \mathbf{e}_{0,n}\}$ but it will turn useful to consider general bases as well

DEFINITION 3.1. *A lattice L in a finite dimensional vector space V over $\mathbb{Q}$ is a finitely generated $\mathbb{Z}$-module $L \subset V$ such that $\mathbb{Q}.L = V$ (since $\mathbb{Z}$ is a principal ideal ring, L is a free $\mathbb{Z}$-module of rank $\dim V$.). For $V = \mathbb{Q}^n$, we denote the lattice $\mathbb{Z}^n$ by L_0.*

A quadratic lattice (L, q) is a lattice equipped with the (restriction of) a quadratic form q.

This lead us to the notion representation *in a quadratic lattice*:

DEFINITION 3.2. *Let (V, q) be a finite dimensional quadratic space over $\mathbb{Q}$ and $L \subset V$ a quadratic lattice. A scalar $d \in \mathbb{Q}$ is representable by q in L (or by the quadratic lattice (L, q)) if there exists $\mathbf{x} \in L - \{0\}$ satisfying*

$$q(\mathbf{x}) = d.$$

The set of representations of d by q in L is noted $\mathrm{R}_q(d; L)$; for $V = \mathbb{Q}^n$ and $L_0 = \mathbb{Z}^n$ we will also use the notation $\mathrm{R}_q(d)$.

REMARK. Picking a $\mathbb{Z}$-basis $\mathcal{B}$ amounts to looking at the set of integral solutions of the polynomial equation

$$Q_{\mathcal{B}}(x_1, \cdots, x_n) = d.$$

If we pick a different $\mathbb{Z}$-basis $\mathcal{B}' = \{\mathbf{e}'_1, \cdots, \mathbf{e}'_n\}$ we obtain a possibly different polynomial equation, but the two problems are obviously equivalent.

REMARK. Instead of asking for integrality of the coordinates of the solutions to (3.1) we could look for more refined questions; for instance that the coordinates satisfy some system of congruences $x_i \equiv a_i \,(\mathrm{mod}\, b)_i$: this amounts to studying the restriction of q to the shifted lattice

$$(a_1, \cdots, a_n) + \bigoplus_{i=1\cdots n} \mathbb{Z} b_i \mathbf{e}_i.$$

Here we will stick to the most basis question.

Obviously a asking for a representation of d by (L, q) is equivalent to asking for an isometric embeddings

$$f : (\mathbb{Z}, dx^2) \hookrightarrow (L, q),\ q(f(x.1)) = dx^2,$$

by setting $f(1) = \mathbf{x}$ for $\mathbf{x} \in L$ a representation. This lead to the more general

DEFINITION 3.3. *Let (L, q) and (M, Q) be quadratic lattices, a representation of (L, q) by $(M; Q)$ is a $\mathbb{Z}$-linear map*

$$f : L \to M$$

such that for any $\mathbf{x} \in L$

$$Q(f(\mathbf{x})) = q(\mathbf{x}).$$

and to the more general problem considered by Siegel of studying the set of embeddings of a quadratic lattice into another.

1.1. Integral quadratic forms.

DEFINITION 3.4. *A quadratic lattice (L, q) is* integral *if*

$$q(L) \subset \mathbb{Z}.$$

Observe that given a general quadratic lattice (L, q), the coefficient of q in a basis of L, $m_{i,j}$ are rational numbers, and so there exists a positive integer N such that

$$q(L) \subset \frac{1}{N}\mathbb{Z}.$$

Up to replacing $q(\cdot)$ by $Nq(\cdot)$ we may reduce to the case where (L, q) is integral.

In terms of the Gramm matrix $M_{\mathcal{B}}(q) = (\langle \mathbf{e}_i, \mathbf{e}_j \rangle_{i,j}) = (m_{ij})_{i,j}$, q being integral on L is equivalent to

$$m_{ii} \in 2\mathbb{Z},\ m_{ij} \in \mathbb{Z}. \tag{3.2}$$

In other terms, the set of quadratic forms integral on L is identified with the lattice $\mathrm{Sym}_n(\mathbb{Z})$ of the space $\mathrm{Sym}_n(\mathbb{Q})$ of $n \times n$ rational symmetric matrices whose coordinates satisfy the integrality condition (3.2). Such symmetric matrices will be called *integral*.

DEFINITION 3.5. *An integral quadratic lattice (L, q) is primitive if L is maximal in the set of lattices $\{L',\ q(L') \subset \mathbb{Z}\}$, that is if there is no $L' \supset L$ such that $q(L') = L$.*

1.2. The discriminant. Recall that given $\mathcal{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_n\}$ a basis of V, the *discriminant of q* relative to $\mathcal{B}$ is defined as

$$\mathrm{disc}_{\mathcal{B}}(q) := \begin{cases} (-1)^{n/2} \det(M_{\mathcal{B}}(q)) & \text{if } n \text{ is even} \\ (-1)^{(n-1)n/2} \det(M_{\mathcal{B}}(q))/2 & \text{if } n \text{ is odd} \end{cases}.$$

where $M_{\mathcal{B}}(q) = (\langle \mathbf{e}_i, \mathbf{e}_j \rangle)$. Suppose that $\mathcal{B}$ is a $\mathbb{Z}$-basis of L. If $\mathcal{B}'$ is another $\mathbb{Z}$-basis of L, then $\det(M_{\mathcal{B}'}(q))$ differ from $\det(M_{\mathcal{B}}(q))$ by the square of the determinant of a matrix in $\mathrm{GL}_n(\mathbb{Z})$ whose value is ± 1, therefore $\mathrm{disc}_{\mathcal{B}}(q)$ depends only on the lattice L and not on the choice of a basis so we write it

$$\mathrm{disc}(q, L) = \mathrm{disc}_{\mathcal{B}}(q).$$

Observe that if $q_{|L}$ is integral, then $\mathrm{disc}(q, L)$ is an integer: for $M \in \mathrm{Sym}_k(\mathbb{Z})$, $\det(M)$ is an integer which is even if n is odd.

2. The Hasse principle

Let (L, q) be a non-degenerate integral quadratic lattice.

QUESTION. Under which conditions is the set $\mathrm{R}_q(d; L)$ non-empty ?

2.1. The theorem of Hasse-Minkowski. We start with the simpler problem of determining whether d is representable by q in $\mathbb{Q}^n$: whether the equation

$$q(\mathbf{x}) = d$$

has a (non-zero) solution in $\mathbb{Q}^n$.

The *Hasse-Minkowski* Theorem offers a necessary and sufficient condition:

THEOREM (Hasse-Minkowski). *A rational number $d \in \mathbb{Q}$ is representable by q over $\mathbb{Q}$ if and only if d is representable by q over $\mathbb{R}$ and over the field of p-adic numbers $\mathbb{Q}_p$ for any prime p. Which means that if k is any of the fields $\mathbb{R}$ or $\mathbb{Q}_p$, the equation*

$$q(\mathbf{x}) = d$$

admits a non-zero solution in k^n.

PROOF. The representability over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every p is obviously necessary. For a proof that it is sufficient, we refer to [**Ser73**, Thm.]. □

The Hasse-Minkowski theorem furnishes *practical algorithm* to decide, in finite time whether a rational d is representable by q : by multiplying the equation $q(\mathbf{x}) = d$ by a sufficiently large square. one may always assume that d is an integer and that q is integral. If q is of rank 1 there is no need of the theorem. If $\mathrm{rk}(q) = 2$, then q is either isotropic and represents every rational or is proportional to Nr_k the norm form of a quadratic field K and we is reduced to solve the equation $\mathrm{Nr}_K(z) = d'$ for d' some squarefree integer and z an algebraic integer.

If $\mathrm{rk}(q) \geq 3$

- checking whether d is representable over $\mathbb{R}$ is easy and depends on the signature of q and on the sign of d;
- for the p-adic field $\mathbb{Q}_p$, the Chevalley-Warning theorem along with Hensel's lemma show that d is always representable over $\mathbb{Z}_p$ if p is coprime with $\mathrm{disc}(q)$;
- for the finitely many remaining primes dividing $\mathrm{disc}(q)$, it is sufficient to check (again by Hensel's lemma), that the equation

  $$q(\mathbf{x}) \equiv d (\mathrm{mod}\ p^\alpha)$$

  has a solution in $(\mathbb{Z}/p^\alpha\mathbb{Z})^n$ for

  $$\alpha = 2[\mathrm{ord}_p(d)/2] + 2\,\mathrm{ord}_p(\mathrm{disc}(q)) + 1.$$

2.2. The integral Hasse principle. We now turn our attention to the question of the existence of representation in a given lattice L.

For R either the ring of real numbers $\mathbb{R}$ or the ring of p-adic integers $\mathbb{Z}_p$, set

$$L_R := L \otimes_{\mathbb{Z}} R.$$

DEFINITION 3.6. *We say that d is representable by q in L_R (or over R if the lattice L is understood) if the equation $q(\mathbf{x}) = d$ admits a non-zero solution in L_R.*

If d is representable by q in L_R for $R = \mathbb{R}$ and $R = \mathbb{Z}_p$ for every prime p we say that d is locally representable (by q) in L.

Being locally representable by L and obviously a necessary condition for being representable in L. It is natural to surmise that this condition is sufficient:

INTEGRAL HASSE PRINCIPLE. *If d is locally representable by q in L then d should be representable by q in L.*

We should from the start that the Integral Hasse Principle is *false* in general:

– When $n = 2$: for "most" quadratic forms q, there is a positive proportion of the integers d for the Integral Hasse Principle fails: let K be a quadratic field, $L = \mathcal{O} \subset K$ be an order and let $q = \mathrm{Nr}_{K/\mathbb{Q}}$ be its associated norm form. If the class number of $\mathcal{O}$ is greater than 1, the integral Hasse principle will fail for a positive proportion of the locally representable integers.

– When $n = 3, 4$, there are infinitely many examples of quadratic forms for which an infinite set of integers does not satisfy the Hasse principle: see [**Han04**] for instance.

On the positive side, one has the following

THEOREM 3.1. *Let q be a quadratic form over $\mathbb{Q}^n$ and L be a lattice on which q is integral. Let $d \neq 0$ be an integer, the integral Hasse principle holds (for d relative to the quadratic lattice (L, q)) whenever*

- *$n \geq 5$ and d is sufficiently large ($d \geq d(L, q)$ for some constant $d(L, q)$ depending on L, q).*
- *$n = 4$, d is sufficiently large and with bounded valuation at any prime p for which q is $\mathbb{Q}_p$-anisotropic.*
- *$n = 3$, d is sufficiently large, with bounded valuation at any prime p for which q is $\mathbb{Q}_p$-anisotropic and which does not belong to a finite, explicitable set of square classes $\{d_j\mathbb{Z}^2, \}_{j\in J_q}$ depending on L, q.*

To discuss the proof of this theorem in greater details, we need to introduce another notion: *the q-genus of a lattice.*

2.3. The genus of a lattice. Let d be locally representable by q in L. In particular d is representable in $\mathbb{R}^n$ and in $\mathbb{Q}_p^n$ for every prime p and by the Hasse-Minkowski theorem, there exists $\mathbf{x}_{\mathbb{Q}} \in \mathbb{Q}^n$ such that

$$q(\mathbf{x}_{\mathbb{Q}}) = d.$$

The problem is that $\mathbf{x}_{\mathbb{Q}}$ does not necessarily belong to L; at least we have the following

LEMMA 3.1. *For all but finitely many p, $\mathbf{x}_{\mathbb{Q}} \in L_p$*

PROOF. Let $\mathcal{B} = \{\mathbf{e}_i,\ i = 1 \cdots, n\}$ be a basis of L and write

$$\mathbf{x}_{\mathbb{Q}} = \sum_i x_i \mathbf{e}_i,\ x_i \in \mathbb{Q}.$$

If N is a non-zero multiple of all the denominators of the $\mathbf{x}_i$ we have

$$\mathbf{x} \in \frac{1}{N} L$$

and if p does not divide N, $N \in \mathbb{Z}_p^{\times}$ and

$$\mathbf{x}_{\mathbb{Q}} \in L_p.$$

□

Let S be the set of p such that $\mathbf{x}_{\mathbb{Q}} \notin L_p$, we know that for $p \in S$ there exist $\mathbf{x}_p \in L_p - \{0\}$ for which

$$q(\mathbf{x}_p) = d.$$

By Witt's theorem, for any such p there exist $s_p \in \mathrm{SO}(\mathbb{Q}_p)$ such that

$$s_p \mathbf{x}_p = \mathbf{x}_{\mathbb{Q}}.$$

Let $L'_p = L_p$ if $p \notin S$ and $L'_p = s_p L_p$ otherwise: L'_p is a lattice in $\mathbb{Q}_p^n$ which equals L_p for all $p \notin S$. Let

$$L' = \bigcap_p \mathbb{Q}^n \cap L'_p \subset \mathbb{Q}^n.$$

This is a $\mathbb{Z}$-module and claim that L' is a in fact a lattice: indeed for any $p \in S$ let $\alpha_p \in \mathbb{N}$ be such that

$$p^{\alpha_p} L_p \subset L'_p \subset p^{-\alpha_p} L_p$$

and $N = \prod_{p \in S} p^{\alpha_p}$, then

$$NL \subset L' \subset \frac{1}{N} L$$

so L' is a lattice. Moreover since $\mathbf{x}_{\mathbb{Q}} \in L'_p$ for every p, then

$$\mathbf{x}_{\mathbb{Q}} \in L'.$$

The two lattices L and L' are very closely connected:

DEFINITION 3.7. *Let (V, q) be a quadratic space over $\mathbb{Q}$; two lattices $L, L' \in V$ are locally isometric (for q), denoted*

$$L \sim_{loc} L'$$

if and only if for every prime p, there is $s_p \in \mathrm{SO}_q(\mathbb{Q}_p)$ (possibly the identity) such that

$$L'_p = s_p L_p.$$

Being locally isometric is an equivalence relation. The local isometry class of a lattice L is called the q-genus of L and is noted

$$\mathrm{genus}_q(L).$$

REMARK 3.1. Observe that, given two lattices L, L' one has $L_p = L'_p$ for all but finitely many p, therefore if $L \sim_{loc} L'$ then for all but finitely many p, $L'_p = L_p = s_p L_p$ or in other terms

$$s_p \in \mathrm{SO}_q(\mathbb{Q}_p) \cap \mathrm{GL}(L_p) = \mathrm{SO}_q(L_p)$$

say; here $\mathrm{GL}(L_p)$ denote the stabilizer of the lattice L_p in $\mathrm{GL}_n(\mathbb{Q}_p)$ (since $L_p = g_p \mathbb{Z}_p^n$ for some $g_p \in \mathrm{GL}_n(\mathbb{Q}_p)$, $\mathrm{GL}(L_p) = g_p \mathrm{GL}_n(\mathbb{Z}_p) g_p^{-1}$ is a conjugate to the stabilizer of $\mathbb{Z}_p^n$ in $\mathrm{GL}_n(\mathbb{Q}_p)$, which is precisely $\mathrm{GL}_n(\mathbb{Z}_p)$ the group of $n \times n$ matrices with entries in $\mathbb{Z}_p$ and whose determinant is in $\mathbb{Z}_p^\times$).

Suppose $L \sim_{loc} L'$; write $L'_p = s_p L_p$, $s_p \in \mathrm{SO}_q(\mathbb{Q}_p)$. Since $q(s_p \mathbf{x}) = q(\mathbf{x})$ we have for every p,

$$\mathrm{R}_q(d, L'_p) = s_p \mathrm{R}_q(d, L'_p);$$

therefore the question of studying representations by q in L_p and L'_p are equivalent for every p; in particular the set of d's which are locally represented by L and L' are identical.. Alternatively, given $\mathcal{B}$ a basis of L, $\mathcal{B}'_p = s_p \mathcal{B}$, is a $\mathbb{Z}_p$-basis of L'_p and the quadratic polynomials representing the quadratic form q is these two bases are the same:

$$Q_{\mathcal{B}}(x_1, \cdots, x_n) = q(\mathbf{x}) = q(s_p \mathbf{x}) = Q_{\mathcal{B}'}(x_1, \cdots, x_n).$$

From the discussion at the beginning of this section, we have proven the following

PROPOSITION 3.1 (Hasse-Minkowski : integral version). *An integer d is locally representable by q in L if an only if d representable by q in at least one lattice $L' \in \mathrm{genus}_q(L)$.*

2.4. Genus classes. There is a stronger equivalence relation on the space of lattices namely isometry:

DEFINITION 3.8. *Two lattices $L, L' \in V$ are (globally) isometric or simply isometric (for q), denoted*

$$L \sim_{\mathbb{Q}} L'$$

if there is $s_{\mathbb{Q}} \in \mathrm{SO}_q(\mathbb{Q})$ such that

$$L' = s_{\mathbb{Q}} L.$$

The isometry class of a lattice will be noted $[L]$

In particular if $L' = s_{\mathbb{Q}} L$

$$\mathrm{R}_q(d; L') = s_{\mathbb{Q}} \mathrm{R}_q(d; L).$$

Since two isometric lattices are locally isometric, the genus of q, $\mathrm{genus}_q(L)$ decomposes into a disjoint union of isometry classes, the *genus classes* of L. We denote by

$$[\mathrm{genus}_q(L)] = \{[L'],\ L' \in \mathrm{genus}_q(L)\}$$

the set of *genus classes*.

The following theorem which may be seen as a generalization of Gauss's finiteness theorem for the number of $\mathrm{SL}_2(\mathbb{Z})$ classes of binary quadratic forms is especially important:

THEOREM 3.2 (Hermite-Minkowski). *The set of genus classes* $[\mathrm{genus}_q(L)]$ *is finite. Its cardinality*

$$h_q(L) = |[\mathrm{genus}_q(L)]|$$

is called the q-*<class number of* L.

Let

$$\mathrm{gen}_q(L) = \{L_1 = L, \cdots, L_h\}$$

be a set of representatives of the genus classes of L containing L. As we have noted above if d is representable in some L' then it is representable in any lattice isometric to L', therefore by Proposition 3.1 we have the following

We have thus obtained the following approximation to the Integral Hasse Principle:

THEOREM 3.3. *If* d *is locally representable in* L*, there is at least one* $L_i \in \mathrm{gen}_q(L)$ *such that* d *is representable in* L'.

In particular, if the class number $h_q(L)$ *is equal to one, the Integral Hasse Principle holds.*

EXERCISE 3.1. *Show that the lattices* $\mathbb{Z}^4$ *and* $\mathbb{Z}^3$ *have class number* 1 *relative to the quadratic forms* q_4, det, q_3, *and* disc .

3. Equidistribution on union of hyperboloids

It is illuminating to view the validity of the Integral Hasse Principle (such as the statement of Theorem 3.1) as a form of equidistribution on the whole set of genus classes of L. Fix

$$\mathrm{gen}_q(L) = \{L_1 = L, \ldots, L_{h_q(L)}\},$$

a set of representative of the various genus classes and let

$$\mathrm{R}_q(d; \mathrm{gen}_q(L)) = \bigsqcup_{i=1\ldots h_q(L)} \mathrm{R}_q(d; L_i)$$

be the (set theoretic) *disjoint union* of the various representations of d in these representatives.

We consider the affine variety

$$V_{q,\pm 1}(\mathbb{R}) = \{\mathbf{x} \in \mathbb{R}^n,\ q(\mathbf{x}) = \pm 1\}$$

and let

$$V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R}) = \bigsqcup_{i=1\ldots h_q(L)} V_{q,\pm 1}(\mathbb{R}),$$

be the disjoint union of $h_q(L)$ copies of $V_{q,\pm 1}(\mathbb{R})$. For $\pm 1 = \mathrm{sign}(d)$ have a map projection

$$|d|^{-1/2} :\ \mathrm{R}_q(d; \mathrm{gen}_q(L)) \to V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R}), \tag{3.3}$$

induced by the various projection maps

$$\begin{array}{ccc} \mathrm{R}_q(d;L_i) & \hookrightarrow & V_{q,\pm 1}(\mathbb{R}) \\ \mathbf{x} & \mapsto & |d|^{-1/2}\mathbf{x} \end{array} .$$

We wish to investigate the distribution of the image , $|d|^{-1/2}\mathrm{R}_q(d;\mathrm{gen}_q(L))$ inside $V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R})$ as $d \to \infty$ (for d locally representable in L). For this we need to describe a mesure on $V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R})$. We repeat the description given in §6.1.

3.1. Measures on hyperboloids. By Witt's theorem, $V_{q,\pm 1}(\mathbb{R})$ is acted on transitively by $G := \mathrm{SO}_q(\mathbb{R})$; so, if we choose $\mathbf{x}_\infty \in V_{q,\pm 1}(\mathbb{R})$ we get an identification

$$V_{q,\pm 1}(\mathbb{R}) = G.\mathbf{x}_\infty \simeq G/H$$

given by

$$g \in G \mapsto \mathbf{x}_\infty.g^{-1} \in V_{q,\pm 1}.$$

Here $H = \mathrm{Stab}_{\mathbf{x}_\infty}(G_i)$ is an orthogonal group in $n-1$ variables (the special orthogonal group of the orthocomplement $\mathbf{x}_\infty^\perp \subset \mathbb{R}^n$). Now the choice of Haar measures on G and H yield quotient mesure $\mu_{G/H}$ hence via (**??**) a left G-invariant measure on $V_{q,\pm 1}(\mathbb{R})$ which we denote $\lambda_{q,\pm 1}$.

Remark. This measure is proportional to the measure which to an open set $\Omega \subset V_{q,\pm 1}(\mathbb{R})$ associate

$$\mu_{\mathbb{R}^n}(\mathcal{C}(\Omega))$$

where $\mathcal{C}(\Omega) = \{r.\mathbf{x},\ \mathbf{x} \in \Omega,\ r \in [0,1]\}$ is the solid angle in $\mathbb{R}^n$ supported by Ω.

We denote by $\lambda_{\mathrm{gen}_q(L),\pm 1}$ the sum of the measures $\lambda_{q,\pm 1}$ on the disjoint union $V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R})$. Similarly the counting measure on $\mathrm{R}_q(d;\mathrm{gen}_q(L))$ yields a measure $V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R})$ via the projection map 3.3. Explicitely for $\varphi = (\varphi_1, \cdots, \varphi_h) \in \mathscr{C}_c(V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R}))$,

$$\lambda_{\mathrm{gen}_q(L),\pm 1}(\varphi) = \sum_i \lambda_{q,\pm 1}(\varphi_i),\ \lambda_d(\varphi) = \sum_i \sum_{\mathbf{x}_i \in \mathrm{R}_q(L_i)} \varphi_i(\frac{\mathbf{x}_i}{|d|^{1/2}}).$$

We have the following equidistribution theorem:

Theorem 3.4. *Let (L,q) be a non-degenerate integral quadratic lattice in $n \geq 3$ variables. There exist a finite set of integers $\mathrm{Exp}(q)$, which is reduced to $\{0\}$ if $n \geq 4$ such that the following hold.*

As $d \to \infty$ amongst integers which are

- *locally integrally representable by q,*
- *coprime with the discriminant $\mathrm{disc}_L(q)$,*
- *not contained in the finite union of square classes $\mathrm{Exp}(q) \times (\mathbb{Q}^\times)^2$,*

the set

$$|d|^{-1/2}\mathrm{R}_q(d;\mathrm{gen}_q(L)) \subset V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R})$$

become equidistributed on $V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R})$ *w.r.t. the measure* $\lambda_{\mathrm{gen}_q(L),\pm 1}$*: for any* $\varphi, \varphi' \in \mathscr{C}_c(V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R}))$ *such that* $\lambda_{\mathrm{gen}_q(L),\pm 1}(\varphi') \neq 0$*, one has*

$$\sum_{\mathbf{x}\in \mathrm{R}_q(d;\mathrm{gen}_q(L))} \varphi'(|d|^{-1/2}\mathbf{x}) = (\lambda_{\mathrm{gen}_q(L),\pm 1}(\varphi') + o(1))|d|^{n/2-2+o(1)};$$

in particular, the above sum is non-zero if d *large enough, and the quotient given below is defined and has the following limit*

$$\frac{\sum_{\mathbf{x}\in \mathrm{R}_q(d;\mathrm{gen}_q(L))} \varphi(|d|^{-1/2}\mathbf{x})}{\sum_{\mathbf{x}\in \mathrm{R}_q(d;\mathrm{gen}_q(L))} \varphi'(|d|^{-1/2}\mathbf{x})} \to \frac{\lambda_{\mathrm{gen}_q(L),\pm 1}(\varphi)}{\lambda_{\mathrm{gen}_q(L),\pm 1}(\varphi')}.$$

In particular, choosing φ' to be supported on the first copy of $V_{q,\pm 1}(\mathbb{R})$ in $V_{\mathrm{gen}_q(L),\pm 1}(\mathbb{R})$ we obtain:

COROLLARY 3.1. *Let* (L, q) *be a non-degenerate integral quadratic lattice in* $n \geq 3$ *variables. The Integral Hasse Principle relative to* (L, q) *holds for the integers* d *which are sufficiently large, coprime to the discriminant* $\mathrm{disc}(q, L)$ *and outside a finite set of exceptional square classes (depending on* (L, q)*).*

REMARK. The coprimality with the discriminant of q condition can be relaxed a bit in these two statements: for instance it could be replaced by "absolutely bounded valuation at any prime dividing the discriminant". That a condition of that sort is necessary may be seem by looking at the set $\mathrm{R}_4(d_0 2^k)$ of representations of $d = 2^k d_0$ as a sum of 4 squares when $k \geq 3$: these are all obtained from the representations of $d_0, 2d_0, 4d_0$ by scaling by a power of 2.

REMARK. The requirement about the exceptional square classes is void for $n \geq 4$. It is void for $n = 3$ too if we require d to be squarefree.

4. From homogeneous spaces to arithmetic quotients

As for Theorem 2.4, the starting point of the proof is an equivalence between this equidistribution statement on (a disjoint union of) ellipsoids and an equidistribution statement on (a disjoint union of) quotient of an orthogonal group by a discrete arithmetic subgroup.

For this we start by observing that the sets $\mathrm{R}_q(d; L_i)$ have "trivial" symmetries: the group $\mathrm{SO}_q(L_i) = \mathrm{SO}_q(\mathbb{Q}) \cap \mathrm{GL}(L_i)$ obviously act on $\mathrm{R}_q(d; L_i)$ which decomposes into a disjoint union of $\mathrm{SO}_q(L_i)$-orbits

$$\bigsqcup_{[\mathbf{x}_i]\in[\mathrm{R}_q(d;L_i)]} \mathrm{SO}_q(L_i)\mathbf{x}_i$$

where $[\mathrm{R}_q(d; L_i)]$ denote the set of orbits, $[\mathbf{x}_i] = \mathrm{SO}_q(L_i).\mathbf{x}_i$ the orbit of some representation $\mathbf{x}_i \in R_{q_i}(d)$. We have the following finiteness result which generalize Gauss Theorem 2.2:

THEOREM 3.5. *The set of orbits* $[\mathrm{R}_q(d)]$ *is finite.*

Therefore we have

$$\mathrm{R}_q(d;\mathrm{gen}_q(L)) = \bigsqcup_i \bigsqcup_{[\mathbf{x}_i]\in[\mathrm{R}_q(d;L_i)]} \mathrm{SO}_q(L_i)\mathbf{x}_i.$$

Setting for $i = 1 \dots h_q(L)$,

$$\Gamma_i = \mathrm{SO}_q(L_i) \subset \mathrm{SO}_q(\mathbb{Q}),$$

and using the identification $V_{q,\pm 1}(\mathbb{R}) \simeq G/H$ we have

$$\mathrm{R}_q(d;\mathrm{gen}_q(L)) \simeq \bigsqcup_i \bigsqcup_{[\mathbf{x}_i]\in[\mathrm{R}_q(d;L_i)]} \Gamma_i g_{\mathbf{x}_i} H/H \subset \bigsqcup_i G/H$$

where

$$\mathbf{x}_i.g_{\mathbf{x}_i} = \mathbf{x}_\infty.$$

By duality this collection of Γ_i-orbits, $i = 1, \cdots, h_q(L)$ correspond to a collection of H-orbits on the union of the quotients $\Gamma_i\backslash G$

$$\bigsqcup_i \bigsqcup_{[\mathbf{x}_i]\in[\mathrm{R}_q(d;L_i)]} \Gamma_i\backslash\Gamma_i g_{\mathbf{x}_i} H \subset \bigsqcup_i \Gamma_i\backslash G =: (\Gamma\backslash G)_{\mathrm{gen}_q(L)}.$$

we now express the duality

Union of left Γ_i-orbits in $G/H \iff$ Union of right H-orbits on $\Gamma_i\backslash G$

at the level of measures (cf. Appendix 10): for each i, let $\mu_{\Gamma_i\backslash G}$ be the quotient of the Haar measure μ_G by the counting measure on the discrete group Γ_i and for each representation $\mathbf{x}_i$, let $\mu_{[\mathbf{x}_i]}$ be the measure supported along the H-orbit

$$\Gamma_i\backslash\Gamma_i g_{\mathbf{x}_i} H \subset \Gamma_i\backslash G$$

which is induced by μ_H. We form the finite sums

$$\mu_{\mathrm{gen}_q(L)} = \sum_i \mu_{\Gamma_i\backslash G} \text{ and } \mu_d = \sum_i \sum_{[\mathbf{x}_i]} \mu_{[\mathbf{x}_i]}.$$

The following is essentially a tautology:

PROPOSITION 3.2. *The measures* $\mu_{\mathrm{gen}_q(L)}$ *and* μ_d *are respectively dual to the measures* $\lambda_{\mathrm{gen}_q(L),\pm 1}$ *and* λ_d *in the following sense: for any* $\varphi = (\varphi_i)_i \in \mathscr{C}_c(\bigsqcup_i G)$, *let*

$$\varphi_H = (\varphi_{i,H})_i \in \mathscr{C}_c(\bigsqcup_i G/H), \text{ where } \varphi_{i,H} : gH/H \to \int_H \varphi_i(gh)d\mu_H(h)$$

$$\varphi_\Gamma = (\varphi_{i,\Gamma_i})_i \in \mathscr{C}_c(\bigsqcup_i \Gamma_i\backslash G), \text{ where } \varphi_{i,\Gamma_i} : \Gamma_i\backslash\Gamma_i g \to \sum_{\gamma_i\in\Gamma_i} \varphi(\gamma_i g).$$

We have

$$\lambda_{\mathrm{gen}_q(L),\pm 1}(\varphi_H) = \mu_{\mathrm{gen}_q(L)}(\varphi_\Gamma), \text{ and } \lambda_d(\varphi_H) = \mu_d(\varphi_\Gamma).$$

Since the spaces generated respectively by the functions of the form φ_H and φ_Γ for $\varphi \in \mathscr{C}_c(\bigsqcup_i G)$ are dense in $\mathscr{C}_c(\bigsqcup_i G/H)$ and $\mathscr{C}_c(\bigsqcup_i \Gamma_i\backslash G)$ we obtain that Theorem 3.4 is equivalent to

THEOREM 3.6. *Let (L,q) be a non-degenerate integral quadratic lattice in $n \geq 3$ variables. There exist a finite set of integers $\mathrm{Exp}(q)$, which is reduced to $\{0\}$ if $n \geq 4$ such that the following hold.*

As $d \to \infty$ amongst the integers which are

- *locally integrally representable by q,*
- *coprime to the discriminant $\mathrm{disc}(q,L)$,*
- *not contained in the finite union of square classes $\mathrm{Exp}(q)(\mathbb{Q}^\times)^2$,*

the measure μ_d supported on the set of of H-orbits

$$\bigsqcup_i \bigsqcup_{[\mathbf{x}_i]\in[\mathrm{R}_q(d;L_i)]} \Gamma_i\backslash\Gamma_i g_{\mathbf{x}_i} H \subset (\Gamma\backslash G)_{\mathrm{gen}_q(L)}.$$

converge to the measure $\mu_{\mathrm{gen}_q(L)}$ on $(\Gamma\backslash G)_{\mathrm{gen}_q(L)}$ in the following sense: for any $\varphi,\varphi' \in \mathscr{C}_c((\Gamma\backslash G)_{\mathrm{gen}_q(L)})$ such that $\mu_{\mathrm{gen}_q(L)}(\varphi') \neq 0$, one has,

$$\mu_d(\varphi') = (\mu_{\mathrm{gen}_q(L)}(\varphi') + o(1))|d|^{n/2-2+o(1)}; \tag{3.4}$$

in particular, that sum is non-zero if d large enough, so that the quotient below is defined and has the following limit

$$\frac{\mu_d(\varphi)}{\mu_d(\varphi')} \to \frac{\mu_{\mathrm{gen}_q(L)}(\varphi)}{\mu_{\mathrm{gen}_q(L)}(\varphi')}. \tag{3.5}$$

An additional feature of this equidistribution theorem is the following

THEOREM 3.7. *The measure $\mu_{\mathrm{gen}_q(L)}$ is finite (ie. $\mu_{\mathrm{gen}_q(L)} < 1$). The measure μ_d is also finite unless $n = 3$ and q is isotropic and $d\,\mathrm{disc}(q,L)$ is a square.*

PROOF. We have

$$\mu_{\mathrm{gen}_q(L)}(1) = \sum_{L_i\in\mathrm{gen}_q(L)} \mu_{\Gamma_i\backslash G}(1)$$

and

$$\mu_d(1) = \sum_{L_i\in\mathrm{gen}_q(L)} \sum_{[\mathbf{x}_i]\in\mathrm{SO}_q(L_i)\backslash\mathrm{R}_q(d;L_i)} \mu_{[\mathbf{x}_i]}(1).$$

By Theorems 3.2 and 3.5 it suffice to show that for each $i = 1\cdots, h_q(L)$, $\mu_{\Gamma_i\backslash G}$ and that each of the measure $\mu_{[\mathbf{x}_i]}$ are finite. This is a consequence the following result of Siegel which is by now a special case of the Borel-Harish-Chandra theorem (see theorem 4.1 in the next chapter):

THEOREM 3.8 (Siegel). *Let (L,q) be an non-degenerate integral quadratic lattice in $n \geq 2$ variables, then*

$$\mathrm{SO}_q(L) = \{g \in \mathrm{SO}_q(\mathbb{Q}),\ L.g \subset L\}$$

is a lattice in $G = \mathrm{SO}_q(\mathbb{R})$*: the quotient space* $\mathrm{SO}_q(L)\backslash \mathrm{SO}_q(\mathbb{R})$ *has finite volume (when equipped with the quotient of Haar measures) if and only if*

- $n \geq 3$*, or*
- $n = 2$ *and* q *is* $\mathbb{Q}$*-anisotropic (*q *does not represent* 0 *over* $\mathbb{Q}$*).*

Moreover for any n*, if* q *is anisotropic then* $\mathrm{SO}_q(L)\backslash \mathrm{SO}_q(\mathbb{R})$ *is compact.*

This clearly settle the case of $\mu_{\Gamma_i\backslash G}$. For the measure $\mu_{[\mathbf{x}_i]}$ we observe the homeomorphisms

$$\Gamma_i\backslash\Gamma_i g_{\mathbf{x}_i} H \simeq \Gamma_i\backslash\Gamma_i g_{\mathbf{x}_i} H g_{\mathbf{x}_i}^{-1} = \Gamma_{\mathbf{x}_i}\backslash \mathbf{H}_{\mathbf{x}_i}(\mathbb{R})$$

where $\mathbf{H}_{\mathbf{x}_i}(\mathbb{R}) = g_{\mathbf{x}_i} H g_{\mathbf{x}_i}^{-1}$ is the group of real points of the $\mathbb{Q}$-algebraic group

$$\mathrm{SO}_{q,\mathbf{x}_i} = \mathrm{Stab}_{\mathbf{x}_i}(\mathrm{SO}_q)$$

and

$$\Gamma_{\mathbf{x}_i} = \mathrm{SO}_q(L_i) \cap \mathrm{SO}_{q,\mathbf{x}_i}(\mathbb{R})$$

is the stabilizer of L_i inside that group. Moreover $\mathrm{SO}_{q,\mathbf{x}_i}$ is the special orthogonal group (in $n-1$ variables), of the quadratic space $(\mathbf{x}_i^\perp, q_{\mathbf{x}_i})$ obtained by restricting q to the hyperplane $\mathbf{x}_i^\perp$ and $\Gamma_{\mathbf{x}_i} = \mathrm{SO}_{q_{\mathbf{x}_i}}(L_{\mathbf{x}_i})$ is the stabilizer of the rank $n-1$-lattice $L_{\mathbf{x}_i} = \mathbf{x}_i^\perp \cap L_i$. Considering a basis formed of the vector $\mathbf{x}_i$ and or a basis of $\mathbf{x}_i^\perp$ and computing discriminants one finds that

$$\mathrm{disc}(q) = d\,\mathrm{disc}(q_{\mathbf{x}_i}) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

It follows from Siegel's theorem above that for $n > 3$ the measure μ_d is finite. For $n = 3$, the measure μ_d is finite if and only if some (hence every) quadratic form $q_{\mathbf{x}_i}$ is anisotropic (this is always the case if q itself is anisotropic). Recall (Appendix 11) that $q_{\mathbf{x}_i}$ is $\mathbb{Q}$-similar to the norm form on the quadratic algebra $\mathbb{Q}[X]/(X^2 - \mathrm{disc}(q_{\mathbf{x}_i}))$ which is isotropic if and only if $\mathrm{disc}(q_{\mathbf{x}_i})$ is a square class. Since $\mathrm{disc}(q_{\mathbf{x}_i}) \equiv d\,\mathrm{disc}(q) \pmod{(\mathbb{Q}^\times)^2}$, the measure μ_d is finite unless d belong to the square class of $\mathrm{disc}(q)$. □

From now on, we assume that we are in the situation where the measure μ_d is finite: either $n \geq 4$ or $n = 3$ and $d\,\mathrm{disc}_{\mathbb{Z}^n}(q) \neq \square$.

If q is anisotropic $(\Gamma\backslash G)_{\mathrm{gen}_q(L)}$ is compact and we may choose $\varphi' = 1$ (3.5), otherwise we may do so by an approximation argument: we obtain for any $\varphi \in \mathscr{C}_c((\Gamma\backslash G)_{\mathrm{gen}_q(L)})$

$$\frac{\mu_d(\varphi)}{\mu_d(1)} \to \frac{\mu_{\mathrm{gen}_q(L)}(\varphi)}{\mu_{\mathrm{gen}_q(L)}(1)}$$

as $d \to \infty$ amongst the set of integers d satisfying the conditions of Theorem 3.6.

In the next chapters we will discuss the proof of Theorems 3.7 and 3.6 by interpreting the spaces

$$(\Gamma\backslash G)_{\mathrm{gen}_q(L)} \text{ and } \bigsqcup_i \bigsqcup_{[\mathbf{x}_i]\in[\mathrm{R}_q(d;L_i)]} \Gamma_i\backslash\Gamma_i g_{\mathbf{x}_i} H$$

as *quotient of adelic points* of the algebraic orthogonal groups

$$\mathrm{SO}_q,\ \mathrm{SO}_{q,\mathbf{x}_i}\,.$$