LECTURE 3, OPPENHEIM CONJECTURE I

RUNLIN ZHANG

CONTENTS

1. The statement 1
2. The space of lattices 1
3. Values of a quadratic form and orbits of its symmetric group 5
4. Computation of the Lie algebra 8
References 9

We recommend the last chapter of [BM00] for an elementary account of the proof of Oppenheim conjecture. See [Mar97, LM14, BGHM10] for history and more recent stories.

1. THE STATEMENT

The goal of this and the next lecture is to prove a weak Oppenheim conjecture. In this lecture we will reduce the proof to a dynamical statement whose proof is delegated to the next lecture. A stronger form will be treated later with the help of non-divergence of unipotent flows.

Theorem 1.1. *Let Q be a non-degenerate indefinite quadratic from with real coefficients in $N \geq 3$ variables. Assume that Q is not a scalar multiple of some quadratic form with rational coefficients. Then the closure of $Q(\mathbb{Z}^N \setminus \mathbf{0})$ contains 0.*

Remark 1.2. *This theorem says nothing nontrivial to the quadratic form $Q_1 = xy - \sqrt{2}z^2$ since $Q_1(1,0,0) = 0$. However, it is nontrivial for $Q_2 = x^2 + y^2 - \sqrt{2}z^2$ since the value of Q_2 at integral points can never be 0 unless $(x, y, z) = (0,0,0)$.*

Later we will specialize to the case when $N = 3$, from which the general case would follow. Details are left to the reader.

Remark 1.3. *Counter examples exist when $N = 2$. For instance consider the quadratic form $Q(x_1, x_2) := (x_1 - \sqrt{2}x_2)x_2$. Note that $\sqrt{2}$ is badly approximable which means that there exists $c > 0$ such that $\{\sqrt{2}x_2\}x_2 \geq c$ for all non-zero integer x_2 where $\{\cdot\}$ stands for the distance to the nearest integer. We will sketch a dynamical explanation below.*

Date: 202203.

2. The space of lattices

For a quadratic form Q in N variables, define for $k = \mathbb{R}, \mathbb{Q}, \mathbb{Z}$,

$$\mathrm{SO}_Q(k) := \left\{ g \in \mathrm{SL}_N(k) \,\middle|\, Q \circ g = Q \right\}. \tag{1}$$

The definition makes sense for Q irrational. It might happen that $\mathrm{SO}_Q(\mathbb{Z})$ is trivial. If M_Q is the symmetric matrix representing of Q, i.e. $Q(v) = v^{tr} M_Q v$ (v written as a column vector), then

$$\mathrm{SO}_Q(k) := \left\{ g \in \mathrm{SL}_N(k) \,\middle|\, g^{tr} M_Q g = M_Q \right\}. \tag{2}$$

One can compute the Lie algebra of $\mathrm{SO}_Q(\mathbb{R})$ as

$$\mathfrak{so}_Q = \left\{ X \in \mathfrak{sl}_n(\mathbb{R}) \,\middle|\, M_Q X + X^{tr} M_Q = 0 \right\}.$$

Where does it act on?

Definition 2.1. *A subgroup Λ of $\mathbb{R}^N$ is said to be a* ***(unimodular) lattice*** *if Λ is discrete and cocompact in $\mathbb{R}^N$ (with $\mathrm{Vol}(\mathbb{R}^N/\Lambda) = 1$).*

Here Vol is taken with respect to the standard Euclidean metric on $\mathbb{R}^N$.

Example 2.2. *$\mathbb{Z}^N$ is a unimodular lattice in $\mathbb{R}^N$.*

Example 2.3. *$\mathbb{Z}[\sqrt{2}]$ may be viewed as a lattice in $\mathbb{R}^2$ by the geometric embedding, i.e.*

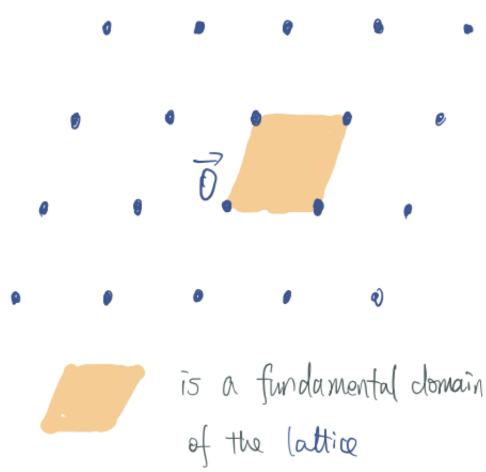
$$\Lambda := \{(x, y) \mid x, y \in \mathbb{Z}[\sqrt{2}],\ x = \sigma(y)\}$$

where σ is the nontrivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Example 2.4. *$\mathbb{Z}[\sqrt{-2}]$ may be viewed as a lattice in $\mathbb{R}^2$ by identifying it with $\mathbb{C}$, explicitly,*

$$\Lambda = \{(x, \sqrt{2}y) \mid x, y \in \mathbb{Z}\}.$$

Example 2.5. *You can get a unimodular lattice starting from a lattice by multiplying a scalar.*



Explicitly, for every discrete subgroup Λ of $\mathbb{R}^N$, one can find $v_1, \dots, v_n$ in $\mathbb{R}^N$ such that they are $\mathbb{R}$-linearly independent and $\Lambda = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \dots \oplus \mathbb{Z}v_n$. Such a set $\{v_1, \dots, v_n\}$ will be called a **basis** of Λ. And n is called the **rank** of Λ. Λ is a lattice iff $n = N$. Conversely, given n vectors $v_1, \dots, v_n$ that are $\mathbb{R}$-linearly independent, the subgroup $\mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$ is a discrete subgroup of $\mathbb{R}^N$.

$\mathrm{Vol}(\mathbb{R}^N/\Lambda) = |\det(v_1,..,v_N)| = \|v_1 \wedge ... \wedge v_N\|$. This is because

$$\{a_1 v_1 + ... + a_N v_N \mid a_i \in [0,1)\}$$

forms a strict fundamental domain for $\mathbb{R}^N/\Lambda$, namely, it is in bijection with $\mathbb{R}^N/\Lambda$ under the quotient map. Also, let us recall that

$$\mathrm{Vol}(\mathbb{R}^N/\Lambda) = \|v_1\| \cdot \mathrm{dist}(v_2, \mathbb{R}v_1) \cdot \mathrm{dist}(v_3, \mathbb{R}v_1 + \mathbb{R}v_2) \cdot ... \cdot \mathrm{dist}(v_N, \mathbb{R}v_1 + ... + \mathbb{R}v_{N-1}).$$

Thus Λ is a unimodular lattice iff $\det(v_1,...,v_N) = \pm 1$.

It is useful to be familiar with quotient construction in Euclidean spaces. More precisely, an **Euclidean space** is a finite-dimensional $\mathbb{R}$-linear space together with a non-degenerate positive definite quadratic form (or an "inner product", if you prefer). The "standard" $\mathbb{R}^N$ is nothing but the vector space $\mathbb{R}^N$ together with the form $Q_{std}(x_1,...,x_N) := x_1^2 + ... + x_N^2$. Once an Euclidean space is given, we can talk about distance, volume...

If W is a $\mathbb{R}$-subspace of $\mathbb{R}^N$, then we think of W as an Euclidean space by restricting the quadratic form to W. Since Q_{std} is positive definite, its restriction to every subspace is also positive definite. Also, the quotient $\mathbb{R}^N/W$ is also equipped with a natural Euclidean structure by identifying it with the orthogonal complement of W in $\mathbb{R}^N$. Alternatively, you can define the quotient metric on $\mathbb{R}^N/W$ and then argue that it comes from a quadratic form. These two methods give the same Euclidean structure on $\mathbb{R}^N/W$.

Definition 2.6. *Let X_N be the set of unimodular lattices in $\mathbb{R}^N$ equipped with the Chabauty topology.*

Alternatively, one may think of X_N as the set of all lattices of $\mathbb{R}^N$ up to $\mathbb{R}^*$-action.

A detailed treatment of Chabauty topology may be found in [BP92, Chapter E, Section 1]. For us, it suffices to know that under the Chabauty topology, a sequence $(\Lambda_n) \subset \mathrm{X}_N$ converges to $\Lambda \in \mathrm{X}_N$ iff one can find a basis $v_1^n, ..., v_N^n$ of Λ_n such that as $n \to \infty$, $(v_i^n)_n$ converges to some $v_i^\infty \in \mathbb{R}^N$ for every $i = 1,...,N$ and $\Lambda = \oplus_i \mathbb{Z} v_i^\infty$.

Note that for a sequence $(\Lambda_n) \subset \mathrm{X}_N$, if there are bases $(v_1^n,...,v_N^n)$ with $(v_i^n)_n$ converges to some $v_i^\infty \in \mathbb{R}^N$ for every i, then $\{v_1^\infty,...,v_N^\infty\}$ are automatically $\mathbb{R}$-linearly independent and they span a lattice Λ with covolume $\mathrm{Vol}(\mathbb{R}^N/\Lambda) = 1$.

$\mathrm{X_N}$ also admits a natural action of $\mathrm{SL}_N(\mathbb{R})$ and

Lemma 2.7. *The map $g \mapsto g.\mathbb{Z}^N$ from $\mathrm{SL}_N(\mathbb{R})$ to $\mathrm{X_N}$ descends to a homeomorphism $\mathrm{SL}_N(\mathbb{R})/\mathrm{SL}_N(\mathbb{Z}) \cong \mathrm{X_N}$.*

Proof. $\mathrm{SL}_N(\mathbb{Z})$ is equal to the stabilizer of $\mathbb{Z}^N$ in $\mathrm{SL}_N(\mathbb{R})$, this proves the injectivity.

For every $\Lambda \in \mathrm{X}_N$, find a basis $v_1,...,v_N$. Replacing v_1 by $-v_1$ if necessary, assume $M := (v_1,...,v_N)$ (v_i written as column vectors) has determinant 1. Then $M.\mathbb{Z}^N = \Lambda$. This proves the surjectivity.

We leave it to the reader to convince himself/herself that the map is open and continuous. □

Definition 2.8. *For a discrete subgroup $\Lambda \leq \mathbb{R}^N$ we define*

$$\delta(\Lambda) := \inf_{v \neq 0 \in \Lambda} \|v\| \tag{3}$$

where $\|\cdot\|$ is taken to be the standard Euclidean norm.

Clearly $\delta(\Lambda) > 0$.

You may interpret $\delta(\Lambda)$ as the length of the smallest geodesic in the quotient flat torus $\mathbb{R}^N/\Lambda$.

One can check that $\delta : \mathrm{X}_N \to \mathbb{R}_{>0}$ is continuous.

Lemma 2.9. *[Mahler's criterion]*

1. *A set $\mathscr{B} \subset \mathrm{X_N}$ does not have compact closure (we will simply write unbounded later) if for every $\varepsilon > 0$ there exists Λ with $\delta(\Lambda) \le \varepsilon$.*
2. *For every $\varepsilon > 0$, the set*
$$\{\Lambda \,|\, \delta(\Lambda) \ge \varepsilon\}$$
is compact in X_N.

Definition 2.10. *For a discrete subgroup Λ of $\mathbb{R}^N$, we let $\|\Lambda\| := \mathrm{Vol}(V/\Lambda)$ where V is the $\mathbb{R}$-linear span of Λ. For a lattice Λ of some Euclidean space V, we let $\|\Lambda\|_V = \mathrm{Vol}(V/\Lambda)$.*

As we have discussed, if $v_1, ..., v_n$ is a basis of Λ, then

$$\|\Lambda\| = \|v_1\| \cdot \mathrm{dist}(v_2, \mathbb{R}.v_1) \cdot ... \cdot \mathrm{dist}(v_n, \mathbb{R}v_1 + ... + \mathbb{R}v_{n-1}).$$

Let us also remark that $\mathrm{dist}(v_2, \mathbb{R}v_1) = \|v_2\|_{\mathbb{R}^N/\mathbb{R}v_1}$ and more generally

$$\mathrm{dist}(v_k, \mathbb{R}v_1 + ... + \mathbb{R}v_{k-1}) = \|v_k\|_{\mathbb{R}^N/(\mathbb{R}v_1+...+\mathbb{R}v_{k-1})}.$$

Proof. 1. follows from the continuity of δ. Let us prove 2.

Fix some $\varepsilon > 0$ and take $\Lambda \in \mathrm{X}_N$ satisfying $\delta(\Lambda) \ge \varepsilon$. It suffices to construct a basis of Λ with bounded distance to the origin.

Consider the projection $p : \mathbb{R}^N \to \mathbb{R}^N/\Lambda$. As $\mathrm{Vol}(\mathbb{R}^N/\Lambda) = 1$, p restricted to the subset $[-1,1]^N$ is not injective. This shows that for some $v_{\neq 0} \in \Lambda$, $\|v\| \le C_1(N)$ for some positive constant depending only on N. In particular, if we choose $v_1 \in \Lambda$ such that

$$\|v_1\| = \delta(\Lambda),$$

then $\|v_1\| \le C_1(N)$. Note that v_1 is primitive in the sense that v_1 is not an integral multiple of any vector in Λ other than $\pm v_1$.

Let π_1 be the projection from $\mathbb{R}^N$ to $V_1 := \mathbb{R}^N/\mathbb{R}v_1$. Since Λ_1 has rank $N-1$ and spans V_1, we have that Λ_1 is discrete and actually a lattice in V_1.

Note that

$$\begin{aligned}
1 = \|\Lambda\| &= \|v_1\| \cdot \mathrm{dist}(v_2, \mathbb{R}v_1) \cdot ... \cdot \mathrm{dist}(v_N, \mathbb{R}v_1 + ... + \mathbb{R}v_{N-1}) \\
&= \|\pi_1(v_1)\| \cdot \|v_2\|_{V_1} \cdot \mathrm{dist}(\pi_1(v_3), \mathbb{R}\pi_1(v_2)) \cdot ... \cdot \mathrm{dist}(\pi_1(v_N), \mathbb{R}\pi_1(v_2) + ... + \mathbb{R}\pi_1(v_{N-1})) \\
&= \|v_1\| \cdot \|\Lambda_1\|_{V_1} \ge \varepsilon \cdot \|\Lambda_1\|_{V_1} \\
&\implies \|\Lambda_1\|_{V_1} \le \varepsilon^{-1} =: C_2(\varepsilon)
\end{aligned}$$

Now choose $v_2 \in \Lambda \setminus \mathbb{R}v_1$ such that

$$\|\pi_1(v_2)\| = \delta_{V_1}(\Lambda_1).$$

A similar argument as above shows that $\|\pi_1(v_2)\| < C_3(N, \varepsilon)$. By modifying v_2 by some integral multiple of v_1, we may assume that $\|v_2\| < C_3(N, \varepsilon) = C_3$ with a possibly different C_3.

Next we want to argue that $\delta_{V_1}(\Lambda_1) > c_1(N, \varepsilon)$ for some constant $c_1(N, \varepsilon) > 0$ (we will soon see that can take $c_1 = 0.4\varepsilon$) depending only on N, ε. Say we have a nonzero vector in V_1 of length smaller than λ. Then we have a vector $v \in \Lambda$ such that $0 < \mathrm{dist}(v, \mathbb{R}v_1) < \lambda$. So if we write $v = x.v_1 + w$ for some w orthogonal to v_1 then $\|w\| \le \lambda$. Let n_x be the nearest integer to x, then $v' := (x - n_x)v_1 + w \in \Lambda$ has norm $\|v'\| \le |x - n_x| \|v_1\| + \lambda$. However $|x - n_x| \le 0.5$ so if we had chosen $\lambda = 0.4\varepsilon \le 0.4\delta(\Lambda)$, then $\|v'\| \le 0.9\delta(\Lambda)$, this is a contradiction.

Let π_2 be the natural projection $\mathbb{R}^N \to \mathbb{R}^N/(\mathbb{R}v_1 + \mathbb{R}v_2) =: V_2$. By abuse of notation, also denote the natural projection $V_1 \to V_2$ by π_2.

With similar arguments, $\Lambda_2 := \pi_2(\Lambda_1)$ is a lattice in V_2 and

$$\|\Lambda_1\|_{V_1} = \|\pi_1(v_2)\| \cdot \|\Lambda_2\|_{V_2} \implies \|\Lambda_2\|_{V_2} \le c_1^{-1} \cdot C_2 =: C_4(N,\varepsilon) =: C_4.$$

Also with similar arguments, $\delta_{V_2}(\Lambda_2) > c_2(N,\varepsilon)$. So we can find v_3, ... up to v_N with bounded norms. And one can check that each step you get a primitive subgroup of Λ and $\{v_1,...,v_N\}$ forms a basis of Λ. So we are done. □

A **primitive subgroup** of Λ is a subgroup Δ such that the $\mathbb{Q}$-span (or equivalently, the $\mathbb{R}$-span) of Δ intersecting with Λ gives back Δ.

The $\mathbb{Z}$-span of two primitive subgroups may not be primitive. e.g., consider $(1,1),(1,-1)$ in $\mathbb{Z}^2$, each of which is primitive, but they span a index 2 subgroup of $\mathbb{Z}^2$, hence not primitive.

I am grateful to Yuyang Jiao for pointing out a gap in the above proof in a previous version of the note.

3. Values of a quadratic form and orbits of its symmetric group

Now comes the equivalent formulation of weak Oppenheim. For a rational quadratic form Q, this would imply that $\mathrm{SO}_Q(\mathbb{Z})$ is not cocompact in $\mathrm{SO}_Q(\mathbb{R})$ if $Q(v)=0$ admits a solution in $v_{\neq 0} \in \mathbb{Z}^N$ (in which case we say Q is isotropic over $\mathbb{Q}$). When $N \ge 5$, a rational indefinite quadratic form is always isotropic over $\mathbb{Q}$ (see [O'M00, 63:19, 66:1])

Lemma 3.1. *For a non-degenerate quadratic form Q in N variables with real coefficients, the following two are equivalent:*

1. *the closure of $Q(\mathbb{Z}^N \setminus 0)$ contains 0;*
2. *the orbit closure of $\mathrm{SO}_Q(\mathbb{R})$ based on the identity coset is unbounded in $\mathrm{X_N}$, in other words, $\mathrm{SO}_Q(\mathbb{R}) \cdot \mathbb{Z}^N$ contains non-zero vectors of arbitrarily small length.*

Proof of $2 \implies 1$. By assumption and Mahler's criterion, there exists $g_n \in \mathrm{SO}_Q(\mathbb{R})$ and $u_n (\neq 0) \in \mathbb{Z}^N$ such that $g_n \cdot u_n$ tends to $\mathbf{0}$. Hence

$$Q(u_n) = Q(g_n \cdot u_n) \to 0.$$

And we are done. □

For the proof of Thm.1.1 this direction is sufficient. However we feel that it is conceptually better to do the converse, too. Actually, this provides a different way of understanding why Thm.1.1 fails $N=2$ – it suffices to find a bounded, yet non-closed orbit of the diagonal group A on $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$. And one can do this by constructing two closed orbits of A and a third orbit Ay such that in the forward direction, Ay approximates one closed orbit and in the backward direction Ax approximates the other. This relies on the fact that closed A-orbits are dense (for instance, one can find one by explicit construction and then consider all lattices commensurable to it) and an argument with local coordinates in stable/unstable/flow direction.

Why is this sufficient? Note that if Q is an indefinite rational quadratic form in two variable, then either Q is $\mathbb{Q}$-equivalent to $Q_0 = xy$ or $Q_1 = x^2 - by^2$ for some $b>0$ and $\sqrt{b} \notin \mathbb{Q}$. In the former case, the orbit of $\mathrm{SO}_Q(\mathbb{R})$ based at the identity coset diverges (that is, the orbit map is proper) and in the second case the orbit is compact, stabilizer of which comes from certain elements in $\mathbb{Q}(\sqrt{b})$.

You may wish to fill in the details on your own.

Now go back to the proof of $1 \implies 2$ of Lem.3.1. We need the following fact.

Lemma 3.2. *For every $r_{\neq 0} \in \mathbb{R}$, $\mathrm{SO}_Q(\mathbb{R})$ acts transitively on the level set*

$$V_r := \left\{ v \in \mathbb{R}^N \,\middle|\, Q(v) = r \right\}.$$

Proof. By linear algebra, up to change of $\mathbb{R}$-coordinate (i.e. up to $\mathrm{GL}_N(\mathbb{R})$), we may and do assume that Q takes the form

$$Q(x_1, ..., x_N) = (x_1^2 + ... + x_s^2) - (x_{s+1}^2 + ... + x_{s+t}^2) =: Q_1(x_1, ..., x_s) - Q_2(x_{s+1}, ..., x_{s+t})$$

for some $s + t = N$ and $s, t \in \mathbb{Z}_{\geq 0}$. The case when one of s, t is equal to 0 is left to the reader. In the following we shall assume the otherwise.

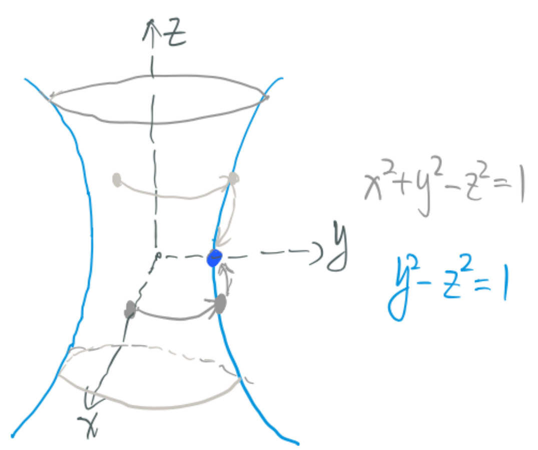
For $\boldsymbol{x} \in \mathbb{R}^N$, we write $v_x := (x_1, ..., x_s)$ and $w_x := (x_{s+1}, ..., x_N)$.

Now we fix r_0 and if V_{r_0} is empty there is nothing to prove. So assume otherwise and take $\boldsymbol{x}_0 \in V_{r_0}$. Let $r_1 := Q(v_{x_0})$ and $r_2 := Q(w_{x_0})$. Thus by transitivity in the (positive) definite case, we can find $k_i \in \mathrm{SO}_{Q_i}(\mathbb{R})$ (i=1,2) such that

$$k_1 \cdot v_{x_0} = (\sqrt{r_1}, 0, ..., 0)$$
$$k_2 \cdot w_{x_0} = (\sqrt{r_2}, 0, ..., 0).$$

Thus it remains to observe that $\mathrm{SO}_{(x_1^2 - x_{s+1}^2)}(\mathbb{R})$ (embedded in $\mathrm{SO}_Q(\mathbb{R})$ by leaving the rest of the coordinates unchanged) acts on the level set (excluding $\mathbf{0}$) of $x_1^2 - x_{s+1}^2$ transitively. Without loss of generality may replace the form $x_1^2 - x_{s+1}^2$ by xy. Then (attach the picture!) it should be clear that this is the case (the reader is reminded that the level sets are not connected, but the group $\mathrm{SO}_{(xy)}(\mathbb{R})$ is also not! It has 2 components). $\square$

Here is an illustration of the proof by pictures



Remark 3.3. *Q indefinite non-degenerate as above. When $N \geq 3$, $SO_Q(\mathbb{R})$ acts on $V_r \setminus \mathbf{0}$ transitively. When $N = 2$, $SO_Q(\mathbb{R})$ acts on $V_r \setminus \mathbf{0}$ with two orbits.*

Proof of $1 \implies 2$. By assumption for every $\varepsilon > 0$ there exists $u_{\varepsilon \neq 0} \in \mathbb{Z}^N$ such that $|Q(u_\varepsilon)| \leq \varepsilon$. On the other hand, there exists $u'_{\varepsilon \neq 0} \in \mathbb{R}^N$ such that

1. $Q(u_\varepsilon) = Q(u'_\varepsilon)$;
2. $\left\| u'_\varepsilon \right\| \leq \theta(Q, \varepsilon) = \theta$

where θ tends to 0 (for a fix Q) as ε does so. Now by the Lemma above, there exists $g_\varepsilon \in \mathrm{SO}_Q(\mathbb{R})$ with $u'_\varepsilon = g_\varepsilon \cdot u_\varepsilon$. Hence $\delta(g_\varepsilon \mathbb{Z}^N) \leq \theta$ and we see that $\mathrm{SO}_Q(\mathbb{R}) \cdot \mathbb{Z}^N$ is unbounded as $\varepsilon \to 0$ by Lem.2.9. $\square$

Now we specialize to $N = 3$.

In light of Lem.3.1, to prove Thm.1.1, it is sufficient to show that $\mathrm{SO}_Q(\mathbb{R}) \cdot \mathbb{Z}^3$ is unbounded. Find $g_0 \in \mathrm{SL}_3(\mathbb{R})$ such that $Q \circ g_0^{-1}$ is a scalar multiple of $Q_0 = 2x_1x_3 - x_2^2$. Then

$$\mathrm{SO}_{Q_0} = g_0 \,\mathrm{SO}_Q\, g_0^{-1}.$$

So sufficient to show that $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot g_0\mathbb{Z}^3$ is unbounded in X_3, which will follow from

Theorem 3.4. *Let $\Lambda \in \mathrm{X}_3$ be such that $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot \Lambda$ is bounded, then $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot \Lambda$ is closed, and hence compact.*

In some sense we cheated a little bit. Because we are going to use a trick that is specific to quadratic forms (really??). And the true dynamical result we are going to prove is (to be proved in the next lecture):

Theorem 3.5. *Let $\Lambda \in \mathrm{X}_3$ be such that $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot \Lambda$ is bounded, then either $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot \Lambda$ is closed and hence compact, or the closure of $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot \Lambda$ contains a $\{\boldsymbol{v}_s\}_{s\geq 0}$-orbit or a $\{\boldsymbol{v}_s\}_{s\leq 0}$-orbit. where*

$$\boldsymbol{v}_s := \exp\left(s \cdot \begin{bmatrix} 0 & 0 & 1 \\ & 0 & 0 \\ & & 0 \end{bmatrix} \right) = \begin{bmatrix} 1 & 0 & s \\ & 1 & 0 \\ & & 1 \end{bmatrix}.$$

Note that $\{\boldsymbol{v}_s\}$ is not contained in $\mathrm{SO}_{Q_0}(\mathbb{R})$.

Proof of Thm.3.4 and 1.1 assuming Thm.3.5. Say, we have a $\{\boldsymbol{v}_s\}_{s\geq 0}$-orbit (the other case is similar) based at Λ' for some $\Lambda' \in \overline{\mathrm{SO}_{Q_0}(\mathbb{R}).\Lambda}$. Write $\boldsymbol{x} = (x_1, x_2, x_3) \in \Lambda'$. Then

$$Q_0(\boldsymbol{v}_s.\boldsymbol{x}) = Q_0(x_1 + sx_3, x_2, x_3) = (2x_3^2)s + (2x_1x_3 - x_2^2).$$

First we can find some $\boldsymbol{x} \in \Lambda'$ such that $Q_0(\boldsymbol{x}) < 0$ and $x_3 \neq 0$ (I leave it to you to convince yourself that this is possible). Then there is some s (replace x_1 by $-x_1$ if necessary) with $Q_0(\boldsymbol{v}_s \cdot \boldsymbol{x}) = 0$. By Lem.3.1, this implies $\mathrm{SO}_{Q_0}(\mathbb{R})\boldsymbol{v}_s \cdot \Lambda \subset \overline{\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot \Lambda}$ is unbounded.

To prove Thm.1.1, by Lem.3.1, if $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot g_0.\mathbb{Z}^3$ is unbounded in X_3 then we are done. Now we assume otherwise. If $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot g_0.\mathbb{Z}^3$ is compact, or equivalently, $\mathrm{SO}_Q(\mathbb{R}).\mathbb{Z}^3$ is compact, then by Lem.3.6, Q is proportional to a rational quadratic form, contradiction. Thus we have a $\{\boldsymbol{v}_s\}_{s\geq 0}$ (the other case $s \leq 0$ is similar) orbit in the closure of $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot g_0.\mathbb{Z}^3$. Repeat the argument above, we find $s \in \mathbb{R}$ such that $Q_0(\boldsymbol{v}_s.x) = 0$ for some $x \in g_0\mathbb{Z}^3$. But $\boldsymbol{v}_s.g_0\mathbb{Z}^3$ is in the closure of $\mathrm{SO}_{Q_0}(\mathbb{R}) \cdot g_0.\mathbb{Z}^3$, implying that we can find $(v_n) \subset g_0\mathbb{Z}^3$, $(g_n) \subset \mathrm{SO}_{Q_0}(\mathbb{R})$ such that $g_n.v_n \to \boldsymbol{v}_s.x$. Hence

$$Q_0(v_n) = Q_0(g_n v_n) \to Q_0(\boldsymbol{v}_s.x) = 0.$$

Thus the closure of $Q(\mathbb{Z}^3) = Q_0(g_0.\mathbb{Z}^3)$ contains 0. $\square$

Lemma 3.6. *For a non-degenerate quadratic form Q, if $\mathrm{SO}_Q(\mathbb{Z})$ is cocompact in $\mathrm{SO}_Q(\mathbb{R})$, then Q is a multiple of a rational quadratic form.*

Note that if Q is NOT a multiple of a rational quadratic form, then for some non-zero coefficients α, β of Q, one has $\alpha/\beta \notin \mathbb{Q}$. Hence there exists $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ such that $\sigma(\alpha/\beta) \neq \alpha/\beta$, in particular, σQ is not proportional to Q.

So it suffices to complete

Step 1. for every $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$, show $\mathrm{SO}_Q(\mathbb{R})^\circ = \mathrm{SO}_{\sigma(Q)}(\mathbb{R})^\circ$;

Step 2. for every pair Q_1, Q_2 of non-degenerate quadratic forms of the same rank, show $\mathrm{SO}_{Q_1}(\mathbb{R})^\circ = \mathrm{SO}_{Q_2}(\mathbb{R})^\circ \implies Q_1 = \lambda Q_2$ for some $\lambda \in \mathbb{R}_{\neq 0}$.

Step 1. First note that

$$\mathrm{SO}_{\sigma(Q)}(\mathbb{R}) = \sigma(\mathrm{SO}_Q(\mathbb{R})) \supset \mathrm{SO}_Q(\mathbb{Z}).$$

Consider the linear representation

$$\mathrm{SL}_3(\mathbb{R}) \curvearrowright \mathrm{Sym} := \left\{\mathbb{R}-\text{Symmetric matrices}\right\}, \quad g\cdot M := gMg^{tr},$$

and the map (call it ϕ) $g \mapsto g\cdot\sigma(Q)$ from $\mathrm{SO}_Q(\mathbb{R})$ to Sym. Then ϕ factors through

$$\mathrm{SO}_Q(\mathbb{R})/\mathrm{SO}_Q(\mathbb{Z}) \to \mathrm{Sym}$$

and hence has compact (and bounded) image. Now we need two facts

1. $\mathrm{SO}_Q(\mathbb{R})^\circ$ is generated (as closed subgroup, this follows by a Lie algebra calculation) by one-parameter unipotent flows $\{\boldsymbol{u}_t := \exp \boldsymbol{u}t\}_{t\in\mathbb{R}}$ ($\boldsymbol{u}$ is some nilpotent matrix in $\mathfrak{so}_Q(\mathbb{R})$);
2. For every unipotent flow $\{\boldsymbol{u}_t\}$ and $M \in \mathrm{Sym}$, either $\{\boldsymbol{u}_t\cdot M\}$ is unbounded or M is fixed by $\{\boldsymbol{u}_t\}$. (if you do not believe this, do some explicit calculation with upper triangular unipotent flows)

But we already saw that $\mathrm{SO}_Q(\mathbb{R}).\sigma(Q)$ is bounded, thus $\mathrm{SO}_Q(\mathbb{R})^\circ$ fixes $\sigma(Q)$. So $\mathrm{SO}_Q(\mathbb{R})^\circ$ is contained in $\mathrm{SO}_{\sigma(Q)}(\mathbb{R})$. But they are both Lie subgroups of $\mathrm{SL}_3(\mathbb{R})$ of the same dimension, so we must have

$$\mathrm{SO}_Q(\mathbb{R})^\circ = \mathrm{SO}_{\sigma(Q)}(\mathbb{R})^\circ.$$

□

Step 2. By conjugation we assume $Q_1 = Q_0 = 2x_1x_3 - 2x_2^2$. One can compute that $\mathfrak{so}_{Q_0}(\mathbb{R})$ contains (and is generated by)

$$\begin{bmatrix} 1 & & \\ & 0 & \\ & & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ & 0 & 1 \\ & & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & & \\ 1 & 0 & \\ 0 & 1 & 0 \end{bmatrix}$$

(note that they do not form an $\mathfrak{sl}_2$-triple, you should multiply the first and the second (but not the third!) by 2) and hence $\mathrm{SO}_{Q_0}(\mathbb{R})$ contains

$$a_t := \begin{bmatrix} e^t & & \\ & 1 & \\ & & e^{-t} \end{bmatrix}, \quad u_s := \begin{bmatrix} 1 & s & s^2/2 \\ & 1 & s \\ & & 1 \end{bmatrix}, \quad u_s^- := \begin{bmatrix} 1 & & \\ s & 1 & \\ s^2/2 & s & 1 \end{bmatrix}. \tag{4}$$

Then a direct computation (at the level of Lie algebra is perhaps easier) shows that in order for $\mathfrak{so}_{Q_2}(\mathbb{R})$ to contain these elements, Q_2 must be a scalar multiple of Q_1 and we are done. □

4. Computation of the Lie algebra

By definition, writing $M_0 = \begin{bmatrix} & & 1 \\ & -1 & \\ 1 & & \end{bmatrix}$,

$$\mathfrak{so}_{Q_0} = \left\{X \in \mathfrak{sl}_3 \,\middle|\, M_0X + X^{tr}M_0 = 0\right\}.$$

Write $X = (x_{ij})$, then we are solving

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \begin{bmatrix} & & 1 \\ & -1 & \\ 1 & & \end{bmatrix} + \begin{bmatrix} x_{11} & x_{21} & x_{31} \\ x_{12} & x_{22} & x_{32} \\ x_{13} & x_{23} & x_{33} \end{bmatrix} \begin{bmatrix} & & 1 \\ & -1 & \\ 1 & & \end{bmatrix} = 0$$

$$\iff \begin{bmatrix} x_{31} & x_{32} & x_{33} \\ -x_{21} & -x_{22} & -x_{23} \\ x_{11} & x_{12} & x_{13} \end{bmatrix} + \begin{bmatrix} x_{31} & -x_{21} & x_{11} \\ x_{32} & -x_{22} & x_{12} \\ x_{33} & -x_{23} & x_{13} \end{bmatrix} = 0$$

$$\iff x_{31} = x_{22} = x_{13} = 0,\ x_{32} = x_{21},\ x_{33} + x_{11} = 0,\ x_{23} = x_{12}.$$

That is to say

$$\mathfrak{so}_{Q_0} = \left\{ \begin{bmatrix} x_{11} & x_{12} & 0 \\ x_{21} & 0 & x_{12} \\ 0 & x_{21} & -x_{11} \end{bmatrix} \right\}.$$

4.0.1. *Computation of its complement.* The notation $\mathfrak{so}_{Q_0}^{\perp}$ below is justified by the fact that it is indeed the orthogonal complement of $\mathfrak{so}_{Q_0}$ in $\mathfrak{sl}_3$ with respect to the killing form (Exercise: check this).

$$\mathfrak{so}_{Q_0}^{\perp} = \left\{ X \in \mathfrak{sl}_3 \,\middle|\, M_0 X - X^{tr} M_0 = 0 \right\}.$$

Write $X = (x_{ij})$, then we are solving

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \begin{bmatrix} & & 1 \\ & -1 & \\ 1 & & \end{bmatrix} - \begin{bmatrix} x_{11} & x_{21} & x_{31} \\ x_{12} & x_{22} & x_{32} \\ x_{13} & x_{23} & x_{33} \end{bmatrix} \begin{bmatrix} & & 1 \\ & -1 & \\ 1 & & \end{bmatrix} = 0$$

$$\iff \begin{bmatrix} x_{31} & x_{32} & x_{33} \\ -x_{21} & -x_{22} & -x_{23} \\ x_{11} & x_{12} & x_{13} \end{bmatrix} = \begin{bmatrix} x_{31} & -x_{21} & x_{11} \\ x_{32} & -x_{22} & x_{12} \\ x_{33} & -x_{23} & x_{13} \end{bmatrix}$$

$$\iff x_{32} = -x_{21}, x_{11} = x_{33} \text{ and } x_{23} = -x_{12}.$$

That is to say

$$\mathfrak{so}_{Q_0}^{\perp} = \left\{ \begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & -2x_{11} & -x_{12} \\ x_{31} & -x_{21} & x_{11} \end{bmatrix} \right\}.$$

REFERENCES

[BGHM10] Paul Buterus, Friedrich Götze, Thomas Hille, and Gregory Margulis, *Distribution of Values of Quadratic Forms at Integral Points*, arXiv e-prints (2010), arXiv:1004.5123.

[BM00] M. Bachir Bekka and Matthias Mayer, *Ergodic theory and topological dynamics of group actions on homogeneous spaces*, London Mathematical Society Lecture Note Series, vol. 269, Cambridge University Press, Cambridge, 2000. MR 1781937

[BP92] Riccardo Benedetti and Carlo Petronio, *Lectures on hyperbolic geometry*, Universitext, Springer-Verlag, Berlin, 1992. MR 1219310

[LM14] Elon Lindenstrauss and Gregory Margulis, *Effective estimates on indefinite ternary forms*, Israel J. Math. **203** (2014), no. 1, 445–499. MR 3273448

[Mar97] G. A. Margulis, *Oppenheim conjecture*, Fields Medallists' lectures, World Sci. Ser. 20th Century Math., vol. 5, World Sci. Publ., River Edge, NJ, 1997, pp. 272–327. MR 1622909

[O'M00] O. Timothy O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition. MR 1754311