Space of unimodular lattices in $\mathbb{R}^n$, I.

Saturday, January 10, 2015
1:17 AM

Let's recall Oppenheim conjecture:

- $Q(x,y,z)$ is a quadratic form which is NOT proportional to a rational quadratic form
- Q is of signature $(2,1)$.

$\Rightarrow \overline{Q(\mathbb{Z}^3)} = \mathbb{R}$.

Remark. Changing Q to cQ we can assume $\det Q = -1$.

So $\exists g_0 \in SL_3(\mathbb{R})$ s.t., $\forall v \in \mathbb{R}^3$, $Q(\vec{v}) = Q_0(g_0 \vec{v})$

where $Q_0(x,y,z) = x^2 + y^2 - z^2$.

$\Rightarrow Q(\mathbb{Z}^3) = Q_0(g_0 \mathbb{Z}^3)$.

This means instead of working with different quadratic forms, we can work with only $\underline{Q_0}$; in the expense of varying the lattice.

Let me also recall that, for any quadratic form Q, we can consider its group of symmetries i.e.

$$SO_Q(\mathbb{R}) := \{ h \in SL_n(\mathbb{R}) \mid Q(h\vec{v}) = Q(\vec{v}) \}.$$

For the standard form $\quad x_1^2 + \cdots + x_m^2 - x_{m+1}^2 - \cdots - x_{m+n}^2$

this group is denoted by $\underline{SO(m,n)}$.

So for any $h \in SO(2,1)$ we have

$$Q(\mathbb{Z}^3) = Q_0(h g_0 \mathbb{Z}^3).$$

Let's focus on the original conjecture:

$$0 \text{ is a limit point of } Q(\mathbb{Z}^3). \qquad (*)$$

By the contrary assumption, $\exists\, \delta_0 > 0$ s.t.

$$\forall h \in SO(2,1),\ v \in \mathbb{Z}^3 \setminus \{0\}$$

$$|Q_0(h g_0 v)| > \delta_0$$

In particular, $\exists\, \delta_0' > 0$ s.t. $\forall h \in SO(2,1)$,

$$\min_{0 \neq v \in \mathbb{Z}^3} \| h g_0 v \| \geq \delta_0'. \qquad (**)$$

Def. $\forall \Lambda \subseteq \mathbb{R}^n$ discrete subgp, let $\quad \delta(\Lambda) = \min_{0 \neq v \in \Lambda} \|v\|$.

Hence $(**)$, $\quad \delta(hg_0 \mathbb{Z}^3) > \delta_0'$

for any $h \in SO(2,1)$.

It seems we cannot avoid studying all the lattices of $\mathbb{R}^n$ at the same time.

<u>Theorem</u>. Suppose $G \subseteq \mathbb{R}^n$ is a closed subgroup. Then $\exists\, V \subseteq \mathbb{R}^n$, $v_1, \dots, v_k \in \mathbb{R}^n$ s.t.

(1) V is a subspace and $V \subseteq G$.

(2) $G/V = \bigoplus_{i=1}^{k} \mathbb{Z}\,\overline{v_i}$ is a discrete subgroup of $\mathbb{R}^n/V$.

(3) $\overline{v_i}$'s are $\mathbb{R}$-linearly independent.

In particular, $G = V \oplus \bigoplus_{i=1}^{k} \mathbb{Z} v_i$, and

$$\dim V + k \leq n.$$

<u>Recall</u>. We have proved that, if G is a closed subgp of $\mathbb{R}$, then either $G = \mathbb{Z}\alpha$ or $G = \mathbb{R}$.

<u>Lemma</u>. $G \subseteq \mathbb{R}^n$, closed and connected

$\Rightarrow$ G is a subspace.

Pf. • W.L.O.G. we can assume the vector space gen. by G is $\mathbb{R}^n$.

• $\forall \varepsilon$, let $G_\varepsilon := \overline{\langle G \cap B_\varepsilon \rangle} \subseteq G$

$\Rightarrow G_\varepsilon$ is closed.

$$G_\varepsilon = \bigcup_{x \in G_\varepsilon} \Big[\underbrace{(G \cap B_\varepsilon) + x}_{\text{open in } G} \Big] \text{ is open in } G.$$

$\Rightarrow G_\varepsilon = G$.

• So $\forall \varepsilon > 0$ $\exists\, w_1, \dots, w_n \in G$ s.t. $\|w_i\| < \varepsilon$ and $\bigoplus \mathbb{R} w_i = \mathbb{R}^n$.

• $\vec{v} \in \mathbb{R}^n \Rightarrow \vec{v} = \sum \alpha_i w_i = \sum \lfloor \alpha_i \rfloor w_i + O(\varepsilon)$

$\Rightarrow G$ is $O(\varepsilon)$-dense in $\mathbb{R}^n \Rightarrow G = \mathbb{R}^n$. ∎

Lemma. $G \subseteq \mathbb{R}^n$ discrete $\Rightarrow G = \bigoplus_{i=1}^{k} \mathbb{Z} v_i$ for some $v_i \in \mathbb{R}^n$.

Pf. Let V be the $\mathbb{R}$-span of G. So $\exists\, \omega_i \in G$ s.t. $V = \bigoplus_{i=1}^{k} \mathbb{R} \omega_i \supseteq G \supseteq \bigoplus_{i=1}^{k} \mathbb{Z} \omega_i$.

If $\left| G / \bigoplus_{i=1}^{k} \mathbb{Z}\omega_i \right| = \infty$, then $G / \bigoplus_{i=1}^{k} \mathbb{Z}\omega_i$ has a

If $\left|G/\bigoplus_{i=1}^{k}\mathbb{Z}\omega_i\right| = \infty$, then $G/\bigoplus_{i=1}^{k}\mathbb{Z}\omega_i$ has a non-constant Cauchy sequence $\{g_n + \bigoplus_{i=1}^{k}\mathbb{Z}\omega_i\}$ as $\bigoplus \mathbb{R}\omega_i / \bigoplus \mathbb{Z}\omega_i$ is compact. So $\exists\, \lambda_n \in \bigoplus_{i=1}^{k}\mathbb{Z}\omega_i$ s.t. $\{g_n + \lambda_n\}$ is a non-constant Cauchy seq. of G. Since G is a discrete group, $g_n + \lambda_n$ is constant for large enough $\underline{n}$, which is a contradiction.

So $G/\bigoplus_{i=1}^{k}\mathbb{Z}\omega_i$ is a finite abelian group. Hence G is a finitely generated torsion-free group. Hence G is a free abelian group $G = \bigoplus_{i=1}^{k'}\mathbb{Z}\, v_i$. And since $\bigoplus_{i=1}^{k}\mathbb{Z}\omega_i$ is a finite index subgroup of G, $k = k'$ and v_i's are linearly independent over $\mathbb{R}$. $\blacksquare$

<u>Remark</u>. Later we will describe a "reduction process" through which one can construct a basis for Λ. This reduction is very important in <u>geometry of numbers</u> and <u>arithmetic groups</u>.

In particular, one does not need to use the structure of finitely generated $\mathbb{Z}$-modules.

Lemma. $G \subseteq \mathbb{R}^n$ closed subgroup which contains NO line.

$\Rightarrow$ 0 is NOT a limit point of G.

Pf. Suppose to the contrary that $\exists\, v_i \in G \setminus \{0\}$ s.t. $v_i \to 0$. Since the sphere is a compact set, after passing to a subsequence we can assume

$$\frac{v_i}{\|v_i\|} \longrightarrow u.$$

$$\Rightarrow \forall \varepsilon > 0,\ i \underset{\varepsilon}{\gg} 1,\quad u = \frac{v_i}{\|v_i\|} + O(\varepsilon)$$

for any $k \in \mathbb{Z}^{\geq 1}$.

$$\Rightarrow \frac{1}{k} u = \left\lfloor \frac{1}{k\|v_i\|} \right\rfloor v_i + \left\{ \frac{1}{k\|v_i\|} \right\} v_i + O(\varepsilon)$$

$v_i \to 0$

$$\Longrightarrow \frac{1}{k}u = \left\lfloor \frac{1}{k\|v_i\|} \right\rfloor v_i + \left\{ \frac{1}{k\|v_i\|} \right\} v_i + O(\varepsilon)$$

$$\xRightarrow{v_i \to 0} \frac{1}{k}u = \left\lfloor \frac{1}{k\|v_i\|} \right\rfloor v_i + O(\varepsilon) \qquad \text{if} \quad i \gg_{\varepsilon} 1.$$

$$\Longrightarrow \left.\begin{array}{l} \underbrace{\left\lfloor \frac{1}{k\|v_i\|} \right\rfloor v_i}_{v_i \in G} \longrightarrow \frac{1}{k}u \end{array}\right\} \Rightarrow \frac{1}{k}u$$

$\Longrightarrow G \cap \mathbb{R}u \supseteq \{\frac{1}{k}u \mid k \in \mathbb{Z}^{>0}\}$ is NOT discrete

$\Longrightarrow \mathbb{R}u \subseteq G$, which is a contradiction. ∎

Pf of theorem.

$G \subseteq \mathbb{R}^n$ closed subgroup $\Rightarrow G^\circ$ is a closed connected subgroup of $G \Rightarrow G^\circ = V$ is a subspace.

$\Rightarrow G/G^\circ \subseteq \mathbb{R}^n/V$ is a closed subgroup and contains NO line

$\Rightarrow G/G^\circ$ is discrete $\Rightarrow$ we are done. ∎

Definition. $\Lambda \subseteq G$ is called a lattice if

① Λ is discrete,

② G/Λ has finite volume w.r.t. Haar measure.

Corollary. $\Lambda \subseteq \mathbb{R}^n$ is a lattice $\Longleftrightarrow \Lambda = g\mathbb{Z}^n$

for some $g \in GL_n(\mathbb{R})$.

. There are bijections

$\Omega(\mathbb{R}^n) :=$ Space of lattices in $\mathbb{R}^n \longleftrightarrow GL_n(\mathbb{R})/GL_n(\mathbb{Z})$.

$\Omega^{(1)}(\mathbb{R}^n) :=$ Space of unimodular lattices in $\mathbb{R}^n$, i.e. $\mathrm{vol}(\mathbb{R}^n/\Lambda) = 1$ $\longleftrightarrow SL_n(\mathbb{R})/SL_n(\mathbb{Z})$.

<u>Lemma</u>. Let $\Lambda \in \Omega(\mathbb{R}^n)$. Then

$$\lim_{T\to\infty} \frac{|\Lambda \cap B_T|}{\mathrm{vol}(B_T)} = \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Lambda)}.$$

<u>Pf.</u> We know that $\Lambda = \mathbb{Z}\vec{v}_1 \oplus \cdots \oplus \mathbb{Z}\vec{v}_n$. Let

$$\mathcal{F} := \left\{ \sum_{i=1}^{n} \alpha_i v_i \;\middle|\; -1/2 \le \alpha_i < 1/2 \right\}$$

Then ① $\mathrm{vol}(\mathcal{F}) = |\det[\vec{v}_1 \cdots \vec{v}_n]| = \mathrm{vol}(\mathbb{R}^n/\Lambda)$

② $\mathbb{Z}^n = \bigcup_{\lambda\in\Lambda} \lambda + \mathcal{F}$

③ $\lambda_1 + \mathcal{F} \cap \lambda_2 + \mathcal{F} = \emptyset$ if $\lambda_1 \neq \lambda_2$.

$\Rightarrow \forall \vec{v} \in \mathbb{R}^n$, $\vec{v} - \vec{x} \in \Lambda$ for some $\vec{x} \in \mathcal{F}$.

$\Rightarrow B_T \subseteq (\Lambda \cap B_{T+M_0} + \mathcal{F})$ where $M_0 = \max_{v\in\mathcal{F}} \{\|v\|\}$.

$$\Rightarrow \quad B_{T-M_0} \subseteq (\Lambda \cap B_T) + \mathcal{F} \subseteq B_{T+M_0}$$

$$\Rightarrow \quad \mathrm{vol}(B_{T-M_0}) \leq |\Lambda \cap B_T|\, \mathrm{vol}(\mathcal{F}) \leq \mathrm{vol}(B_{T+M_0})$$

$$\Rightarrow \quad \frac{1}{\mathrm{vol}(\mathcal{F})} \cdot \left(\frac{T-M_0}{T}\right)^n \leq \frac{|\Lambda \cap B_T|}{\mathrm{vol}(B_T)} \leq \frac{1}{\mathrm{vol}(\mathcal{F})} \cdot \left(\frac{T+M_0}{T}\right)^n$$

$$\Rightarrow \quad \lim_{T\to\infty} \frac{|\Lambda \cap B_T|}{\mathrm{vol}(B_T)} = \frac{1}{\mathrm{vol}(\mathcal{F})} = \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Lambda)}. \quad \blacksquare$$

<u>Topology on $\Omega(\mathbb{R}^n)$</u>: It is enough to understand convergent series: we say $\Lambda_m \to \Lambda \iff$ For any ball $B(r)$ centered at the origin we have

$$\Lambda_m \cap B(r) \longrightarrow \Lambda \cap B(r), \text{ i.e.}$$

$\forall \varepsilon > 0$, $m \gg_\varepsilon 1$, $\quad \Lambda \cap B(r) \subseteq \varepsilon\text{-nbhd of } \Lambda_m \cap B(r)$

and $\quad \Lambda_m \cap B(r) \subseteq \varepsilon\text{-nbhd of } \Lambda \cap B(r)$.

<u>Theorem</u>: $\Theta : GL_n(\mathbb{R})/GL_n(\mathbb{Z}) \longrightarrow \Omega(\mathbb{R}^n)$,

$$\Theta(g\, GL_n(\mathbb{Z})) := g\,\mathbb{Z}^n$$

is a homeomorphism. (we are taking the quotient topology on $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$.)

<u>Pf</u>. $g_m GL_n(\mathbb{Z}) \longrightarrow g\, GL_n(\mathbb{Z}) \Rightarrow \exists\, \gamma_m \in GL_n(\mathbb{Z})$,

$g_m \gamma_m \longrightarrow g.$

- $g\mathbb{Z}^n \cap B(r)$ is a finit set $\{g\vec{v}_1, \dots, g\vec{v}_k\}$

Suppose $\varepsilon < \frac{1}{2} \min \{r - \|g v_i\|\}$, and $\max \|v_i\| \le M$.

Then for $m \gg_{\varepsilon, M} 1$ we have

$$\| g_m \gamma_m v_i - g v_i \| \le \varepsilon \qquad \text{for} \quad 1 \le i \le k$$

$\Rightarrow$ ① $g_m \gamma_m v_i \in B(r)$

② $\{g v_1, \dots, g v_k\} \subseteq \varepsilon\text{-nbhd of } \{g_m \gamma_m v_1, \dots, g_m \gamma_m v_k\}$

$$\Rightarrow g\mathbb{Z}^n \cap B(r) \subseteq \varepsilon\text{-nbhd of } g_m \gamma_m \mathbb{Z}^n \cap B(r)$$
$$= \varepsilon\text{-nbhd of } g_m \mathbb{Z}^n \cap B(r).$$

$\forall \vec{\omega}_0 \in g_m \mathbb{Z}^n \cap B(r) \Rightarrow \vec{\omega}_0 = g_m \gamma_m \vec{v}_0$ and $\|\vec{\omega}_0\| < r$
$\vec{v}_0 \in \mathbb{Z}^n$

$$\Rightarrow \| g\vec{v}_0 - \vec{\omega}_0 \| \le \| g - g_m \gamma_m \| \, \|\vec{v}_0\|$$
$$\le \| g - g_m \gamma_m \| \, (2\|g^{-1}\| r) \qquad \text{if } m \gg 1$$
$$\le \varepsilon \qquad \text{if } m \gg_{\varepsilon} 1.$$

Suppose $\varepsilon < r - \|\vec{\omega}_0\|$. Hence $g\vec{v}_0 \in g\mathbb{Z}^n \cap B(r)$.

$\Rightarrow g\mathbb{Z}^n \cap B(r) \subset \varepsilon\text{-nbhd of } g\mathbb{Z}^n \cap B(r)$

if $m \gg_{\varepsilon} 1$.

$\Rightarrow \quad g_m \mathbb{Z}^n \longrightarrow g\mathbb{Z}^n$.

Now suppose $g_m \mathbb{Z}^n \to g\mathbb{Z}^n$; let $v_1, \dots, v_n$ be the columns of $g \Rightarrow g\mathbb{Z}^n = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$.

$\Rightarrow \forall \varepsilon > 0, \ m \gg_{\varepsilon} 1,$

$$\varepsilon > \underset{\text{Hausdorff distance}}{Hd}\left(g\mathbb{Z}^n \cap B(2\max\|v_i\|), g_m\mathbb{Z}^n \cap B(2\max\|v_i\|)\right)$$

• Let $\delta(\Lambda) := \min\{\|v\| \mid v \in \Lambda \setminus \{0\}\}$.

$\Rightarrow \quad \delta(g_m\mathbb{Z}^n) \xrightarrow[m \to \infty]{} \delta(g\mathbb{Z}^n)$

$\Rightarrow B(\frac{1}{4}\delta(g\mathbb{Z}^n)) \cap g_m\mathbb{Z}^n = \{0\}$ if $m \gg 1$.

• So $\forall v \in \mathbb{Z}^n$, $m \gg_{\|v\|} 1$, $\exists!\, T_m(v) \in \mathbb{Z}^n$ s.t.

$$\| g_m T_m(v) - gv\| \le \frac{1}{4}\delta(g\mathbb{Z}^n).$$

$\Rightarrow \lim_{m \to \infty} g_m T_m(v) = gv$ for any $v \in \mathbb{Z}^n$.

So, for any $v \in \mathbb{Z}^n$, $\exists!\, \{T_m(v)\}_{m=m(v)}^{\infty} \subseteq \mathbb{Z}^n$

s.t. $\lim g_m T_m(v) = gv$. ⊛

s.t. $\lim_{m\to\infty} g_m T_m(v) = g v.$ ⊛

$\forall \vec{v}\in\mathbb{Z}^n, k\in\mathbb{Z}$, $k T_m(v)$ satisfies ⊛ $\Rightarrow T_m(kv)=kT_m(v)$

if $m \gg_{v,k} 1$.

Similarly $\forall v_1,v_2\in\mathbb{Z}^n$, $T_m(v_1+v_2)=T_m(v_1)+T_m(v_2)$

if $m\gg_{v_1,v_2} 1$.

So $\underline{\forall N\in\mathbb{Z}^{\geq 1}}$, if $m\gg_N 1$, for any $|a_i|\le N$,

$$T_m\Big(\sum_{i=1}^n a_i\vec{e}_i\Big) = \sum_{i=1}^n a_i\, T_m(\vec{e}_i).$$

Let $\gamma_m := [T_m(e_1) \ \cdots \ T_m(e_n)] \in M_n(\mathbb{Z})$. So

$$\lim_{m\to\infty} g_m\gamma_m = \Big[\lim_{m\to\infty} g_m T_m(e_1) \ \cdots \ \lim_{m\to\infty} g_m T_m(e_n)\Big]$$

$$= g.$$

<u>Claim</u>. If $m\gg 1$, then $\gamma_m\in GL_n(\mathbb{Z})$.

<u>Pf of claim</u>. Since $\det g_m \det\gamma_m \longrightarrow \det g\neq 0$ and

$\det\gamma_m\in\mathbb{Z}$, for $m\gg 1$ $\det\gamma_m\neq 0$.

Suppose $v\in\mathbb{Z}^n$ and $v\notin\gamma_m(\mathbb{Z}^n)\Rightarrow$

$$v = \sum_{i=1}^{n} \alpha_i \, T_m(e_i) \quad \text{for} \quad \alpha_i \in \mathbb{Q}.$$

$$\Rightarrow \exists \; \alpha_i \in \mathbb{Q} \cap [-1/2, 1/2) \text{ s.t. } 0 \neq v' = \sum_{i=1}^{n} \alpha_i \, T_m(e_i) \in \mathbb{Z}^n. \; (*)$$

$$\Rightarrow g_m v' = \sum_{i=1}^{n} \alpha_i \, g_m T_m(e_i) \Longrightarrow \| g_m v' \| \ll 1 \quad \text{if } m \gg 1.$$

$$\Rightarrow \exists \; v'' \in \mathbb{Z}^n \text{ s.t. } \| g_m v' - g v'' \| < \varepsilon \quad \text{if} \quad m \gg 1.$$

$$\Rightarrow v' = T_m(v'') \quad \text{if} \quad m \gg 1.$$

If $m \gg 1$, $T_m(v'') \in \sum_{i=1}^{n} \mathbb{Z} \, T_m(e_i)$. Hence by $(*)$ $v' = 0$, which is a contradiction.

So $g_m \gamma_m \longrightarrow g$ and $\gamma_m \in GL_n(\mathbb{Z})$, which implies $g_m GL_n(\mathbb{Z}) \longrightarrow g \, GL_n(\mathbb{Z})$. ∎

An simpler argument implies

$$SL_n(\mathbb{R}) / SL_n(\mathbb{Z}) \xrightarrow{\sim} \Omega^{(1)}(\mathbb{R}^n).$$

$$g \, SL_n(\mathbb{Z}) \longmapsto g \mathbb{Z}^n.$$