§2. The space of lattices

<u>Recall</u> a lattice in $\mathbb{R}^n$ (row vectors) is a subgroup L of the form

$$L = \bigoplus_{j=1}^{n} \mathbb{Z} v_j \quad \text{for some basis } v_1, \dots, v_n \text{ of } \mathbb{R}^n.$$

$$X_n = \{\text{lattices of } \mathbb{R}^n\} \leftrightarrow GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R})$$

$$\mathbb{Z}^n g \leftrightarrow \text{coset of } g$$

$$X_n^{(1)} = \left\{ \begin{matrix} \text{unimodular} \\ \text{lattices in } \mathbb{R}^n \end{matrix} \right\} \leftrightarrow SL_n(\mathbb{Z}) \backslash SL_n(\mathbb{R})$$

<u>Two other actions</u> $\qquad \begin{pmatrix} z & & \\ & \ddots & \\ & & z \end{pmatrix}$

<u>Scaling</u> $\mathbb{R}^\times \cong$ center of $GL_n(\mathbb{R})$ acts on X_n

each scaling class of lattices contains a unique unimodular representative, so $X_n / \mathbb{R}^\times \cong X_n^{(1)}$

<u>rotation</u> we have actions $X_n \curvearrowleft O(n)$ rotations of $\mathbb{R}^n$

$X_n^{(1)} \curvearrowleft SO(n) = O(n) \cap SL_n(\mathbb{R})$

So we may form the orbit spaces

$$X_n / O(n) = \{\text{lattices up to rotation}\}$$

$$X_n^{(1)} / SO(n) \cong X_n / \mathbb{R}^\times SO(n) = \{\text{lattices up to rotation + scaling}\}$$

<u>$n=1$</u> $\mathbb{Z} \subseteq \mathbb{R}$ is the only unimodular lattice $\quad \# X_1^{(1)} = 1$

$$X_1 = \{\alpha \mathbb{Z} : \alpha > 0\} \cong \mathbb{R}_+^\times$$

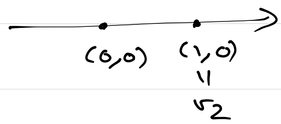
$\underline{n=2}$ Let's classify lattices in $\mathbb{R}^2$ up to rotation + scaling.

("$X_2 / \mathbb{R}^\times SO(2) = X_2^{(1)} / SO(2)$")

Let $L \leq \mathbb{R}^2$ be a lattice ($\Rightarrow$ discrete).

Choose a <u>shortest vector</u> $v_2 \in L$ (nonzero vector of minimal length).

By rotating + scaling, we may assume $v_2 = (1,0)$.



Note that v_2 is <u>primitive</u>: $\mathbb{R}v_2 \cap L = \mathbb{Z}v_2$

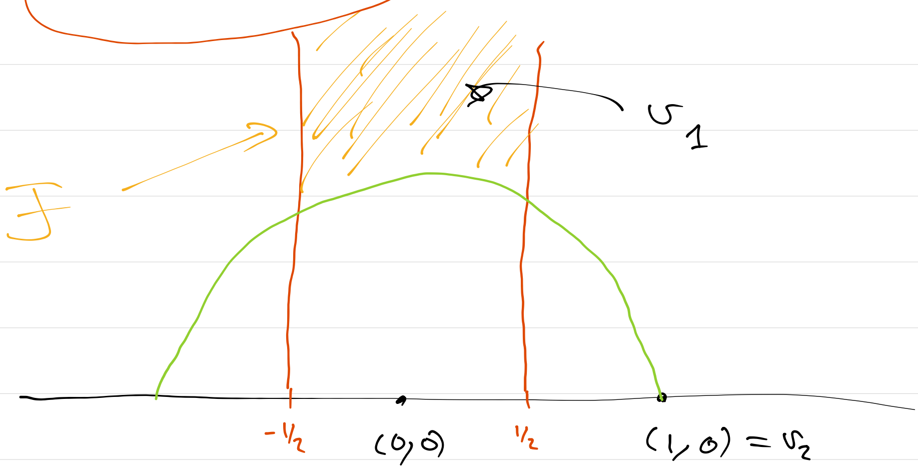
(else $\mathbb{R}v_2 \cap L = \frac{1}{N}\mathbb{Z}v_2$, $N>1$, and so $\frac{1}{N}v_2$ is shorter)

Choose $v_1 \in L - \mathbb{Z}v_2$ of minimal length.
$v_1 = (x,y)$

By replacing v_1 by $-v_1$ if necessary, we may assume $y>0$.

Because v_2 is shortest, $|v_1| \geq 1$.

Also, $-1/2 \leq x \leq 1/2$ (else $v_1 - v_2$ OR $v_1 + v_2$ is shorter than v_1)



Up to "boundary issues," $\mathcal{F}$ classifies $X_2 / \mathbb{R}^\times SO(2)$.

Iwasawa decomposition for $GL_n(\mathbb{R})$

Let $v_1, \dots, v_n$ of $\mathbb{R}^n$ be a basis.
Let $v_i' :=$ orthogonal projection of v_i to $\langle v_{i+1}, \dots, v_n \rangle^{\perp}$.
Then $v_1', \dots, v_n'$: orthogonal basis of $\mathbb{R}^n$ s.t.

$$v_i = v_i' + \sum_{j>i} c_{ij} v_j'.$$

Write $a_i := |v_i'| \in \mathbb{R}_+^\times$, $v_i' = a_i v_i''$.
Then $\{v_i''\}$: orthonormal basis of $\mathbb{R}^n$.

In terms of matrices, write $g = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$.

Then $g = uak$, where

$$u = \begin{pmatrix} 1 & c_{12} & c_{13} & * \\ & 1 & c_{23} & \\ & & 1 & \\ 0 & & & \ddots \\ & & & & 1 \end{pmatrix}, \quad a = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}$$

$$k = \begin{pmatrix} v_1'' \\ v_2'' \\ \vdots \\ v_n'' \end{pmatrix} \in O(n) =: K$$

$G := GL_n(\mathbb{R})$, $N = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$, $A = \begin{pmatrix} * & & \\ & \ddots & \\ & & * \end{pmatrix}$

$A \supset A^+ = \left\{ \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} : a_j > 0 \right\}$

$G = NAK$

$N \times A^+ \times K \to G$

$(u, a, k) \longmapsto uak$ is a diffeomorphism.

Siegel domains

(☆): ∃ multiple conventions

Let $L \subseteq \mathbb{R}^n$ be a lattice.

Defn A basis $v_1, \dots, v_n$ for L will be called reduced (☆) if, w/ notation as above,

- $|c_{ij}| \leq 1/2$ $\quad \forall\, 1 \leq i < j \leq n$
- $|a_i / a_{i+1}| \geq \frac{\sqrt{3}}{2}$. $\quad \forall\, 1 \leq i \leq n-1$

Note $\left(1/2, \sqrt{3}/2\right)$ are unimportant for us. $\quad 1/2 < \infty$, $\frac{\sqrt{3}}{2} > 0$.

Theorem (Minkowski) (i) Every lattice admits a reduced basis.

(ii) If $v_1, \dots, v_n$ and $u_1, \dots, u_n$ are reduced bases for the same lattice L, then

$$|v_j'| \asymp |v_j| \asymp |u_i| \asymp |u_i'|,$$

where "$A \asymp B$" means $c_1 B \leq A \leq c_2 B$ where $0 < c_1 < c_2$ depend at most upon n.

Thus "$a_1, \dots, a_n$ are well-defined up to constants."

(iii) If $v_1, \dots, v_n$: reduced basis, then $\underset{\substack{\asymp \\ |v_1| \cdots |v_n|}}{a_1 \cdots a_n} = \operatorname{vol}(\mathbb{R}^n / L)$.

(iv) Let $C \geq 1$ be large in terms of n.
Suppose $v_1, \dots, v_n$: reduced basis for L. Let $i \in \{1, \dots, n-1\}$.
Suppose $a_i / a_{i+1} > C$. Then

$$\mathbb{Z} v_{i+1} \oplus \mathbb{Z} v_{i+2} \oplus \cdots \oplus \mathbb{Z} v_n$$

depends only upon L, not upon the choice of reduced basis.

(v) Let $v_1, \dots, v_n$: reduced basis of L.
Let $T \in GL_n(\mathbb{R})$ such that $v_j T = v_j' \;\forall j$.
Then T and its inverse have operator norm $\ll 1$ ($\leq C$, depending only upon n)
In other words, $\forall v \in \mathbb{R}^n$, $\|v\| \asymp \|vT\|$.

Case $n=2$ Suppose $v_2 = (1,0)$ and $v_1 = (x,y)$ are a basis of a lattice L. This basis is reduced $\Longleftrightarrow |x| \le 1/2$, $y \ge \sqrt{3}/2$.

Indeed, $\quad v_2' = v_2, \qquad v_1' = (0,y)$

$a_2 = 1 \qquad a_1 = y,$

$v_1 = v_1' - x\, v_2', \qquad a_1/a_2 = y$

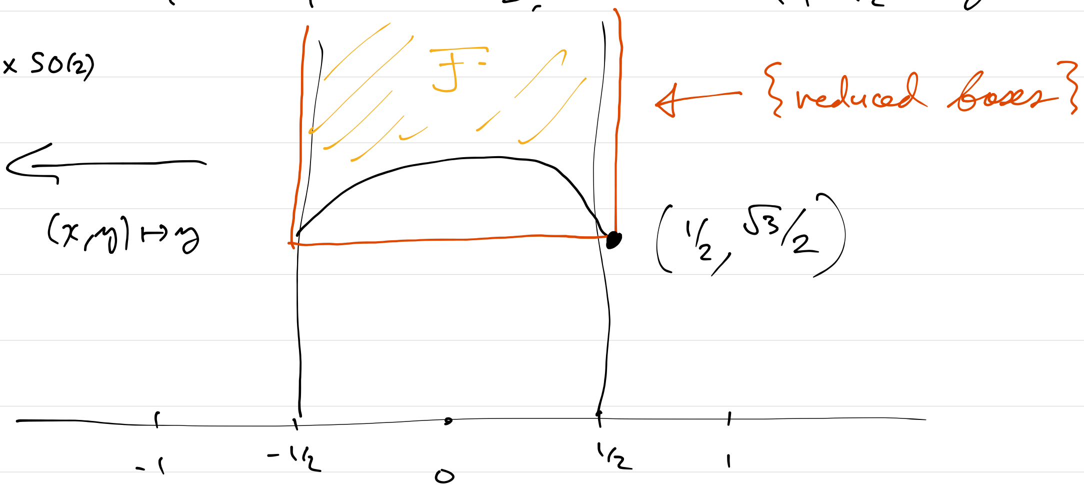
- fiber in $X_2^{(1)}$ looks like $\mathbb{Z}\backslash\mathbb{R} \times SO(2)$

1

- fiber is compact

$\longleftarrow$

$(x,y) \mapsto y$



Proof of Theorem

(i): Let L: lattice.

Choose $v_n \in L$: shortest vector. $(\Rightarrow \text{primitive})$

Let $L_{n-1} :=$ projection of L to $\langle v_n \rangle^{\perp}$

: rank $n-1$ lattice $\cong \mathbb{Z}^{n-1}$

Let $v_{n-1}' \in L_{n-1}$ be a shortest vector.

Lift it to a vector $v_{n-1} \in L$ of shortest length.

$(L \twoheadrightarrow L_{n-1})$

Then, by the same argument as when $n=2$, we see that

$$v_{n-1} = v_{n-1}' + c v_n', \qquad v_n' := v_n,$$

then $|c| \leq 1/2$. (Else replace v_{n-1} by $v_{n-1} \pm v_n$.)

By the $n=2$ picture, $|v_{n-1}'| \geq \frac{\sqrt{3}}{2} |v_n'|$.

Now set $L_{n-2} :=$ projection of L to $\langle v_{n-1}, v_n \rangle^{\perp}$,

and choose a shortest vector $v_{n-2}' \in L_{n-2}$.

Lift it to $v_{n-2} \in L$, and write

$$v_{n-2} = v_{n-2}' + a v_{n-1}' + b v_n', \qquad a, b \in \mathbb{R}.$$

By replacing v_{n-2} by $v_{n-2} + l v_{n-1}$ for suitable $l \in \mathbb{Z}$, we may assume $|a| \leq 1/2$.

By translating v_{n-2} by an integer multiple of v_n, we may assume $|b| \leq 1/2$.

Then $|a|, |b| \leq 1/2$. Also, $v_{n-2}' + a v_{n-1}' =$ projection of v_{n-2} to $\langle v_n \rangle^{\perp}$,

so $|v_{n-1}'| \leq |v_{n-2}' + a v_{n-1}'|$ by minimality $|v_{n-1}'|$.

Exercise deduce that $|v_{n-2}'| \geq \frac{\sqrt{3}}{2} |v_{n-1}'|$. Continue.

Remaining parts (ii)–(v) left as exercises (see notes).

<u>Exercise</u> Prove the Mahler compactness criterion:
for a subset $S \subseteq X_n^{(1)}$, the following are equivalent:

(i) S is precompact (i.e., has compact closure, "is bounded")

(ii) $\exists\, \delta > 0$ s.t. $|v| \geq \delta \quad \forall\, 0 \neq v \in L \in S$.

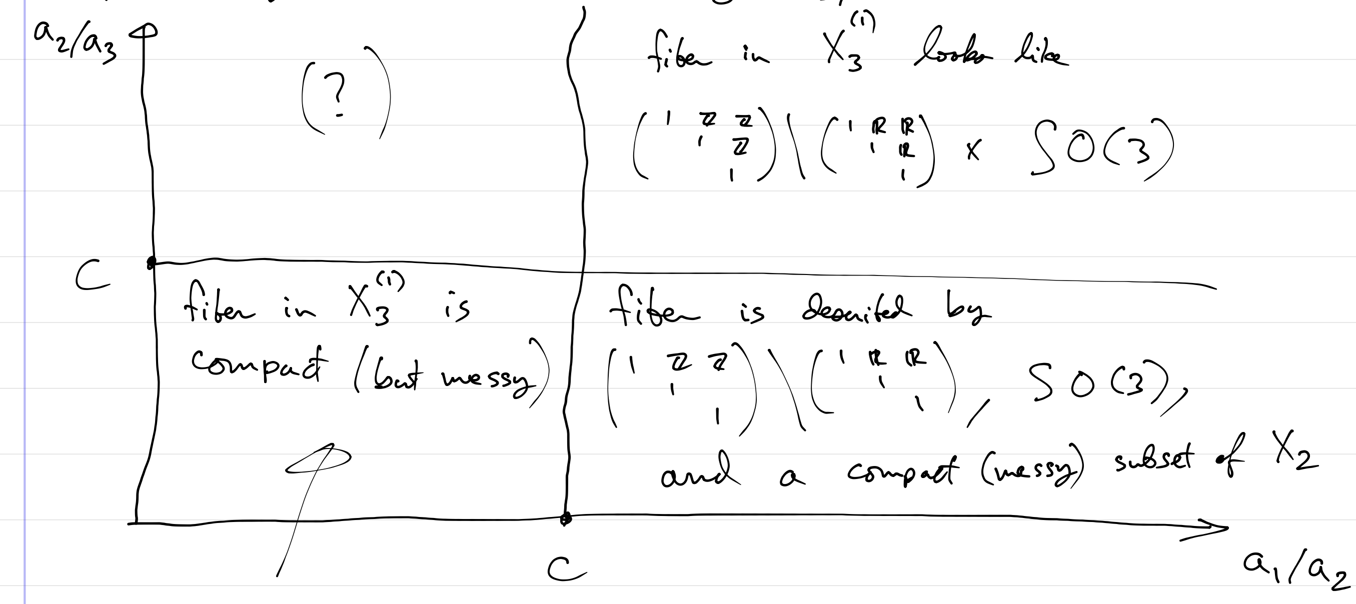
"The only way for a sequence (L_j) of unimodular lattices to tend off to ∞ is if $\exists\, 0 \neq v_j \in L_j$ s.t. $|v_j| \to 0$."

<u>$n=3$</u> Recall that if C is large, then ($\forall$ reduced bases v_1, v_2, v_3 of a lattice L)

(i) $a_1/a_2 > C \implies \langle v_2, v_3 \rangle$ depends only upon L

(ii) $a_2/a_3 > C \implies \langle v_3 \rangle$ —— // ——.

In case (i), then v_1 is determined up to sign and translation by v_2, v_3.



analogue of for $n=2$

Haar measure

On any locally compact group G, $\exists !$ (up to scaling) left (resp. right) measure $d^L g$ ($d^R g$) that is invariant by left (right) multiplication by G.

(to be continued)

Question Let $d\mu$: inv. prob. measure on $X_n^{(1)}$.

Let $\Omega \subseteq \mathbb{R}^n$: bounded open subset.

What is
$$\int_{L \in X_n^{(1)}} \#(\underbrace{L \cap \Omega}_{\{v \in L \,:\, v \in \Omega\}}) \, d\mu(L) \; ?$$

Note $\#(L \cap \Omega)$ can be arbitrarily large:

$$\forall \Omega \neq \phi \quad \exists L_j \quad \text{s.t.} \quad \#(L_j \cap \Omega) \to \infty.$$

We'll answer this next time.