MATH 225A: LECTURE 12
NOVEMBER 2, 2021
SCRIBE: VIR PATHAK

Theorem 5.4. *Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is generated over $\mathbb{Z}$ by r vectors $e_1, ..., e_r$ which are linearly independent over $\mathbb{R}$.*

Proof. Choose $\mathbf{e} = e_1, ..., e_r$ in H with $e_1, ..., e_r$ $\mathbb{R}$-linearly independent and with r maximal. Set

$$\wp_{\mathbf{e}} = \left\{ \sum_{i=1}^{r} \alpha_i e_i \mid \alpha_i \in [0,1] \right\}.$$

The set $\wp_{\mathbf{e}}$ is called the fundamental parallelogram of H with respect to the basis $e_1, ..., e_r$. We can immediately see that $\wp_{\mathbf{e}}$ is compact because it is homeomorphic to $\mathbb{R}^n$.

Take an $x \in H$. Then we can write x in the form

$$x = \sum_{i=1}^{r} \lambda_i e_i$$

for $\lambda_i \in \mathbb{R}$. If x cannot be written in this form, we can add x to $\{e_1, ..., e_r\}$, contradicting the maximality of r.

Now for $j \in \mathbb{Z}$ set

$$x_j := jx - \sum_{i=1}^{r} [\lambda_i j] e_i$$

where $[\cdot]$ denotes the integer part of a real number. From the above two equations, we have

$$x_j = \sum_{i=1}^{r} (\lambda_i j - [\lambda_i j]) e_i$$

for all $j \in \mathbb{Z}$. This implies that $x_j \in \wp_{\mathbf{e}}$. Moreover, we also see that $x_j \in H$ from the definition of x_j. So $x_j \in \wp_{\mathbf{e}} \cap H$.

Now we use the discreteness of H. Namely, recall that this means $H \cap \wp_{\mathbf{e}}$ is finite since $\wp_{\mathbf{e}}$ is compact. Now consider $j = 1$. By our definition of x_1, we have

$$x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$$

so x is in the $\mathbb{Z}$ span of a finite set. This tells us H is finitely generated over $\mathbb{Z}$. Next by the finiteness of $\wp_{\mathbf{e}} \cap H$, we can find $j \neq k$ such that $x_j = x_k$. Rearranging and expanding the equation $x_j = x_k$, we get

$$\sum_{i=1}^{r} \lambda_i (j-k) e_i = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) e_i.$$

Since the $\{e_i\}$ are $\mathbb{R}$-linearly independent, we must have

$$\lambda_i (j-k) = [j\lambda_i] - [k\lambda_i].$$

So we must have each $\lambda_i \in \mathbb{Q}$.

Now let x be any element in $\wp_{\mathbf{e}} \cap H$ with $x = \sum_{i=1}^{r} \lambda_i e_i$. Then by our work so far, we know that $x = \sum_{i=1}^{r} \lambda_i e_i$ where $\lambda_i \in \mathbb{Q}$ for each i. Now let

$$d = \mathrm{LCM}(\mathrm{denom}(\lambda_i)).$$

Then for any $x \in H$, we know

$$x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i \in \frac{1}{d} \sum_{i=1}^{r} \mathbb{Z} e_i.$$

So we may conclude that

$$H \subseteq \frac{1}{d} \sum_{i=1}^{r} \mathbb{Z} e_i.$$

This implies

$$\sum_{i=1}^{r} \mathbb{Z} e_i \subseteq H \subseteq \frac{1}{d} \sum_{i=1}^{r} \mathbb{Z} e_i.$$

Therefore we must have that H is finitely generated of rank r over $\mathbb{Z}$ on some linear combination of the vectors $\{\frac{1}{d} e_i\}$. This basis is linearly independent over $\mathbb{R}$ as desired. $\square$

Definition 5.5. *With the above notation, call H a lattice in $\mathbb{R}^n$ if $r = n$.*

Definition 5.6. *Let $\mathbf{e} = \{e_1, ..., e_r\}$ and $\mathbf{f}$ be a $\mathbb{Z}$ basis of H. Define*

$$Vol(H) := Vol(\wp_{\mathbf{e}}).$$

Note that a change of basis $\mathbf{e} \mapsto \mathbf{f}$ corresponds to a change of basis matrix in $GL_r(\mathbb{Z})$. So $Vol(\wp_{\mathbf{e}}) = Vol(\wp_{\mathbf{f}})$ since this matrix has a determinant whose absolute value is 1.

Theorem 5.7. *(Minkowski)*
Let H be an $\mathbb{R}^n$ lattice, and let $\mathcal{S} \subset \mathbb{R}^n$ be a measurable set with $Vol(\mathcal{S}) > Vol(H)$. Then there exists $x, y \in \mathcal{S}$ such that $x - y \in H \setminus \{0\}$ (i.e $x \neq y$).

Proof. By the previous theorem, we know there exists a $\mathbb{Z}$ basis $\mathbf{e} = \{e_1, ..., e_n\}$ for H. Notice that we can write $\mathbb{R}^n$ in the form

$$\mathbb{R}^n = \bigcup_{h \in H} (\wp_{\mathbf{e}} + h).$$

So we must have

$$\mathcal{S} = \bigcup_{h \in H} [(h + \wp_{\mathbf{e}}) \cap \mathcal{S}].$$

Note that for $h_1, h_2 \in H$, we have that $\wp_{\mathbf{e}} + h_1 \cap \wp_{\mathbf{e}} + h_2$ has measure zero.

It follows that

$$\begin{aligned} \mathrm{Vol}(\mathcal{S}) &= \sum_{h \in H} \mathrm{Vol}((h + \wp_{\mathbf{e}}) \cap \mathcal{S}) \\ &= \sum_{h \in H} \mathrm{Vol}(\wp_{\mathbf{e}} \cap (\mathcal{S} - h)). \end{aligned}$$

The above equality holds because volumes are translation invariant.

Next, suppose for a contradiction that all sets $\wp_{\mathbf{e}} \cap (\mathcal{S} - h)$ are disjoint. Then we see that

$$\mathrm{Vol}(\wp_{\mathbf{e}}) \geq \mathrm{Vol} \sum_{h \in H} (\wp_{\mathbf{e}} \cap (\mathcal{S} - h)) = \mathrm{Vol}(\mathcal{S}).$$

But this implies $\mathrm{Vol}(H) \geq \mathrm{Vol}(\mathcal{S})$ which contradicts our hypothesis. So the sets

$$\wp_{\mathbf{e}} \cap (\mathcal{S} - h)$$

are not disjoint. Therefore we can find $h \neq h'$ such that

$$\wp_{\mathbf{e}} \cap (\mathcal{S} - h) \cap (\mathcal{S} - h') \neq \varnothing.$$

So we must have that there exists $x, y \in \mathcal{S}$ such that $x - h = y - h'$. This implies $x - y = h - h' \neq 0$ (since $h \neq h'$). We conclude that $x - y \neq 0 \in H$. This completes the proof. $\square$

Definition 5.8. *We say that $\mathcal{S} \subseteq \mathbb{R}^n$ is symmetric if $x \in \mathcal{S}$ implies that $-x \in \mathcal{S}$.*

Definition 5.9. *We say that $\mathcal{S}$ is convex if for all $x, y \in \mathcal{S}$ and $\alpha \in [0,1]$ we have*

$$\alpha x + (1-\alpha)y \in \mathcal{S}.$$

Corollary 5.10. *(Blichfeldt)*
Let $\mathcal{S} \subseteq \mathbb{R}^n$ be a symmetric, convex, measurable subset, and suppose Vol($\mathcal{S} > 2^n$ Vol(H) (where H is as before). Then $\mathcal{S}$ contains a nonzero point of H.

Proof. Take $\mathcal{S}' = \frac{1}{2}S$. Then

$$\mathrm{Vol}(S') = \frac{1}{2^n}\mathrm{Vol}(\mathcal{S}) > \mathrm{Vol}(H).$$

So by Minkowski's theorem, we know there exists $y, z \in \mathcal{S}'$ such that

$$x := y - z = \frac{1}{2}(2y) + \frac{1}{2}(-2z) \in H \setminus \{0\}.$$

Next, note that $2y \in \mathcal{S}$ by definition, as is $2z$ so we have $-2z \in \mathcal{S}$ by symmetry. By convexity, we conclude that $x \in \mathcal{S}$. We see that $x \in (S \cap H) \setminus \{0\}$ as required. □

Embellishment 5.11. *With the above notation, suppose further that $\mathcal{S}$ is compact, but that Vol($\mathcal{S}$) $\geq 2^n$ Vol(H). Then we can still find a nonzero element in $S \cap H$.*

Proof. Since $\mathcal{S}$ is compact, it is closed and therefore complete. Now for each positive integer k, consider

$$\mathcal{S}_k = (1 + \frac{1}{k})\mathcal{S}.$$

Then we have

$$\mathrm{Vol}(\mathcal{S}_k) = (1 + \frac{1}{k})^n \mathrm{Vol}(\mathcal{S}) > 2^n \mathrm{Vol}(H).$$

So as before, we may find

$$x_k \in (S_k \cap H) \setminus \{0\}.$$

We see that $x_k \in (2\mathcal{S}) \cap H$ and this set is finite by the discreteness of H. Therefore there exists an x_m such that

$$x_m \in \bigcap_k \mathcal{S}_k.$$

Since $\mathcal{S}$ is closed and $\mathcal{S} = \cap_k \mathcal{S}_k$, we see that $x_m \in (\mathcal{S} \cap H) \setminus \{0\}$. $\square$

Now we introduce notation that will be used in the rest of the chapter. Let $K/\mathbb{Q}$ be a given number field and let

$$\{\sigma_i\}_{i=1}^n$$

be distinct embedding of K in $\mathbb{C}$, and $n = [K : \mathbb{Q}]$. Let s be the number of real embeddings (so $\sigma_i(K) \subseteq \mathbb{R}$). Moreover, let $2t$ be the number of complex embeddings (so $\sigma_i(K) \not\subseteq \mathbb{R}$.) Henceforth we suppose that $\sigma_1, ...\sigma_s$ are real and the set

$$\{\sigma_{s+1}, ..., \sigma_{s+t}, \sigma_{s+t+1}, ...\sigma_{s+2t}\}$$

is such that $\overline{\sigma_{s+j}} = \sigma_{s+j+t}$ where $\overline{\sigma_{s+j}}$ denotes (complex conjugation) $\circ\, \sigma_{s+j}$.

Define the fundamental embedding

$$\boldsymbol{\sigma} : K \hookrightarrow \mathbb{R}^s \times \mathbb{C}^t$$

given by

$$x \mapsto \prod_{i=1}^{s+t} x^{\sigma_i}$$

Note

$\boldsymbol{\sigma}$ is a homomorphism of $\mathbb{Q}$-algebras. Often we will identify $\mathbb{R}^s \times \mathbb{C}^t$ with $\mathbb{R}^n$ as vector spaces (but not rings).

Proposition 5.12. *Let $M \subset K$ be a $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ with basis $\{x_1, ..., x_n\}$. Then $\boldsymbol{\sigma}(M)$ is an $\mathbb{R}^n$-lattice with*

$$Vol(\boldsymbol{\sigma}(M)) = 2^{-t} |\det(x_i^{\sigma_j})|.$$