27/10/14 W1D2

Geom. of Numbers - גיאומטריה של מספרים

Def. $v_1 \dots v_n \in \mathbb{R}^n$ lin. ind. - $\mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$ is a lattice with basis $v_1 \dots v_n$.

Prop: If $\overset{e_1, \dots e_n}{\cancel{v_1 \dots v_n}}$ is the st. basis and $A \in GL_n(\mathbb{Z}) \overset{\{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}}{=}$, $v_i = Ae_i$ is a basis of $\mathbb{Z}^n$. All bases have this property.

Proof $A\mathbb{Z}^n \subseteq \mathbb{Z}^n$. $A^{-1} \in GL_n(\mathbb{Z})$ too and $A^{-1}\mathbb{Z}^n \subseteq \mathbb{Z}^n$. $\mathbb{Z}^n = A^{-1}(A\mathbb{Z}^n) \subseteq \mathbb{Z}^n$ so $A\mathbb{Z}^n = \mathbb{Z}^n$.

If $v_1 \dots v_n$ is a basis $e_k = \sum b_{jk} v_j = \sum b_{jk} \sum a_{ij} e_i = \sum \left(\sum_j a_{ij} b_{jk}\right) e_i$. Therefore $AB = Id$. and $B = A^{-1}$, so $\det A = \pm 1$ as required.

What about other lattices? For any $P \in GL_n(\mathbb{R})$ one can form $P(\mathbb{Z}^n) = \{\sum a_i P e_i \mid a_i \in \mathbb{Z}\}$ with basis $Pe_i = v_i$. All lattices have this form $\begin{pmatrix} | & | & & | \\ v_1 & v_2 & \dots & v_n \\ | & | & & | \end{pmatrix}$

Cor. Any lattice is of form $P(\mathbb{Z}^n)$. Two bases v_i, u_j are obtained by $u_i = \sum a_{ij} v_j$ where $A \in GL_n(\mathbb{Z})$.

Cor. Lattices are in 1-1 correspondence with $\frac{GL_n(\mathbb{R})}{GL_n(\mathbb{Z})}$

Prob. A Lattice is discreet - $(\lambda_n) \in \Lambda$ s.t. $\lim \lambda_n$ exists $\exists n_0 \forall n > n_0 \; \lambda_n = \lambda_{n_0}$. For any compact $K \in \mathbb{R}^n$, $|\Lambda \cap K| < \infty$.

Proof. True for $\mathbb{Z}^n$ and conserved under homeomorphism (mult. by $P \in GL_n(\mathbb{R})$).

Prop. $\Lambda \subseteq \mathbb{R}^n$ is lattice $\longleftrightarrow$ discreet and group iso. to $\mathbb{Z}^n$.
($\leftarrow$ will be proved later)

Def measurable $\Omega \subseteq \mathbb{R}^n$ is called fundemental if for any $x \in \mathbb{R}^n$ $\exists! \lambda \in \Lambda$ s.t. $x + \lambda \in \Omega$. A unique, measurable choice of coset rep.

Prop: Any 2 fund. domains for Λ have equal volume.

Proof: let Ω_1, Ω_2 be fund. dom. For any $x \in \Omega_2$ $\exists! \lambda \in \Lambda$ ($=\lambda(x)$) s.t. $\lambda + x \in \Omega_1$. $\Omega_2 = \biguplus_{\lambda \in \Lambda} A_\lambda = \{x \in \Omega_2 \mid \lambda(x) = \lambda\}$. If $\lambda \neq \lambda'$, $(A_\lambda + \lambda) \cap (A_{\lambda'} + \lambda') = \emptyset$

since $\lambda(x)$ is unique. Now,

$$Vol(\Omega_2) = \sum_{\lambda\in\Lambda} Vol(A_\lambda) = \sum_{\lambda\in\Lambda} Vol(A_\lambda + \lambda) = Vol\Big(\bigcup_{\lambda\in\Lambda}(A_\lambda + \lambda)\Big) \leq Vol(\Omega_1).$$

From symmetry $Vol(\Omega_1) = Vol(\Omega_2)$.

Examples: if $\Lambda = \mathbb{Z}^n$, $\Omega = [0,1)^n$. If $x = (x_1, x_2 \dots x_n)$, $\lambda = (-\lfloor x_1 \rfloor, -\lfloor x_2 \rfloor \dots \lfloor x_n \rfloor)$.

$\left(\lfloor x \rfloor = \max_{\substack{n \leq x \\ n \in \mathbb{Z}}} n\right)$. Therefore $\{\sum a_i v_i \mid \forall 0 \leq a_i < 1\}$ is fund. dom. for Λ with basis $v_1, \dots v_n$ ($P(\Omega)$, where $P = \begin{pmatrix} v_1 & \dots & v_n \end{pmatrix}$).

Cor. For $\Lambda = \{\sum a_i v_i \mid a_i \in \mathbb{Z}\}$, $\{\sum a_i v_i \mid 0 \leq a_i < 1\}$ is the fund. cell / parallelpiphead for $v_1 \dots v_n$. $Vol(\Omega_{v_i}) = |\det\begin{pmatrix} v_1 & \dots & v_n \end{pmatrix}|$. By prev. prop. $d(\Lambda) := Vol(\Omega_{v_i})$ (or sometimes $cov(\Lambda)$ - covolume) is indep. of choice of basis and is the vol. of any fund. dom. for Λ.

Def. A lattice Λ is unimodular if its covolume is 1.

The set of unimodular lattices is $\mathcal{L}_n$ and is in natural bijection with $\{A \in GL_n(\mathbb{R}) \mid \det A = \pm 1\} / GL_n(\mathbb{Z})$ and $SL_n(\mathbb{R}) / SL_n(\mathbb{Z})$. $A \cdot SL_n(\mathbb{Z}) \to A\mathbb{Z}^n$.

Minkowski's First Thm. Let A be a centrally symmetric convex set in $\mathbb{R}^n$ and $\Lambda \subseteq \mathbb{R}^n$ a lattice, if $Vol(A) > 2^n d(\Lambda)$ (or $=$ and A is compact), then $A \cap \Lambda$ contains a nonzero point.

Blicfield's Lemma $Vol(A) > d(\Lambda) \to$ there are (*) $a_1 \neq a_2 \in A$ s.t. $a_1 - a_2 \in \Lambda$.

proof define $\lambda(a)$, A_λ as before. The sets $A_\lambda + \lambda$ must intersect for $\lambda \neq \lambda' \in \Lambda$.

Strengthening If A is compact and $Vol(A) = d(\Lambda)$, (*) holds. So, no fund. dom. is compact.

proof: $A_t = (1 + \frac{1}{t})A$, $B = \bigcup_{t\in[1,2]} tA$ contains any A_t, and is compact. By lemma $a_1^{(k)} \neq a_2^{(k)} \in A_k$ $a_1 - a_2 = \lambda_k \in B - B$ which is compact. $\lim_{i\to\infty} \lambda_{k_i}$ exists for some subsequence k_i so $\lambda_{k_{n_i}}$ is constant from some point λ, therefore $\lim_{j\to\infty} a_1^{(k_{i_j})} = a_1$, $\lim_{j\to\infty} a_2^{(k_{i_j})} = a_2$ for some i_j, and $a_1 - a_2 = \lambda \in \Lambda$.

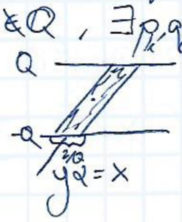
<u>proof</u> (Minkowski's first) (reminder – A is convex $\leftrightarrow$ $x,y \in A \Rightarrow ax+(1-a)y \in A$ for any $a\in[0,1]$. A is cent. symm. if $a\in A \to -a\in A$.)

Let $A_0 = \frac{1}{2}A$. A_0 satisfies Blichfield's lemma, so $a_1 - a_2 \in \Lambda/\{0\}$ s.t. $a_1 = \frac{x}{2}, a_2 = \frac{y}{2}$ where $x,y\in A$. so $a_1 - a_2 = \frac{1}{2}x + \frac{1}{2}(-y) \in \Lambda/\{0\}$. But $-y\in A$ so $\frac{1}{2}x+\frac{1}{2}(-y)\in A$.

<u>remark</u> $2^n d(\Lambda)$ is tight – think about $(-1,1)^n$ and $\Lambda = \mathbb{Z}^n$, or $[-1+\varepsilon, 1-\varepsilon]^n$ (again in $\Lambda=\mathbb{Z}^n$). If A is a (euclidean) ball, finding the sharp const. is open (solved for $n=1,\dots,8$, and 24). Also for many other families of shapes and norms.

<u>Applications</u> 1) Diophantine approx. – Dirichlet's thm. $\overset{[-]}{\alpha}\in\mathbb{R}^{[n]}$, $Q>1$, there exist $\overset{[-]}{p}\in\mathbb{Z}^{[n]}, q\in\mathbb{N}$ s.t. $\left|\overset{[-]}{\alpha}-\frac{\overset{[-]}{p}}{q}\right|_{[\infty]} \leq \frac{1}{qQ^{[1/n]}}$, $q\le Q$.

<u>cor</u> if $\alpha\notin\mathbb{Q}$, $\exists p_k, q_k$ as before s.t. $\left|\alpha-\frac{p_k}{q_k}\right| \frac{1}{q_k^2}$, $q_k\nearrow\infty$.

using 

$A=\{\overset{[-]}{(x,y)} \mid |x|<Q \wedge |y\alpha - x|_{[\infty]} < \frac{1}{Q^{[1/n]}}\}$, $\Lambda=\mathbb{Z}^{[n+1]}$