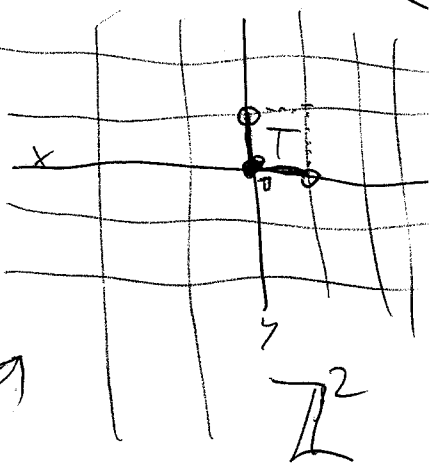
Lecture 7

$B = \{v_1, v_2, \dots, v_n\} \subset \mathbb{R}^n$ a base of ($\mathbb{R}$-vector space) $\mathbb{R}^n$, a lattice $\Lambda = \Lambda(B) \subset \mathbb{R}^n$ (in $\mathbb{R}^n$) is the set $\Lambda = \{\sum_{i=1}^{n} a_i v_i \mid a_i \in \mathbb{Z}\}$. The fundamental parallelepiped $T = T(B)$ of $\Lambda(B)$

$$\| \quad \{\sum_{i=1}^{n} \alpha_i v_i \mid \alpha_i \in [0,1)\}$$



($u \in \mathbb{R}^n$, $T+u := \{x+u \mid x \in T\}$.)

$v_1 = (1,0), v_2 = (0,1)$

Lemma $\Lambda = \Lambda(B)$ a lattice in $\mathbb{R}^n$, $T = T(B)$ its f. p. Then $\{T+u \mid u \in \Lambda\}$ is a partition of $\mathbb{R}^n$.

Proof. Every $\alpha \in \mathbb{R}$ has a unique expression as $\alpha = \lfloor \alpha \rfloor + \{\alpha\}$, $\mathbb{R}^n \ni v = \sum_1^n \alpha_i v_i = \sum_1^n (\lfloor \alpha_i \rfloor + \{\alpha_i\}) v_i$ ☒

($\lfloor \alpha \rfloor \in \mathbb{Z}$, $\{\alpha\} \in [0,1)$)

In other words $\forall p \in \mathbb{R}^n$ lies in exactly one shifted copy $T+u$ of T, where $u \in \Lambda$.

Proposition $\Lambda = \Lambda(B_1) = \Lambda(B_2)$ a lattice in $\mathbb{R}^n$. Then $\mathrm{Vol}(T(B_1)) = \mathrm{Vol}(T(B_2))$.

Proof.

($B = \{u_1, \dots, u_n\} \subset \mathbb{R}^n$ (not necessarily a basis), $M(B) := \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$ – the vectors u_i are in rows.)

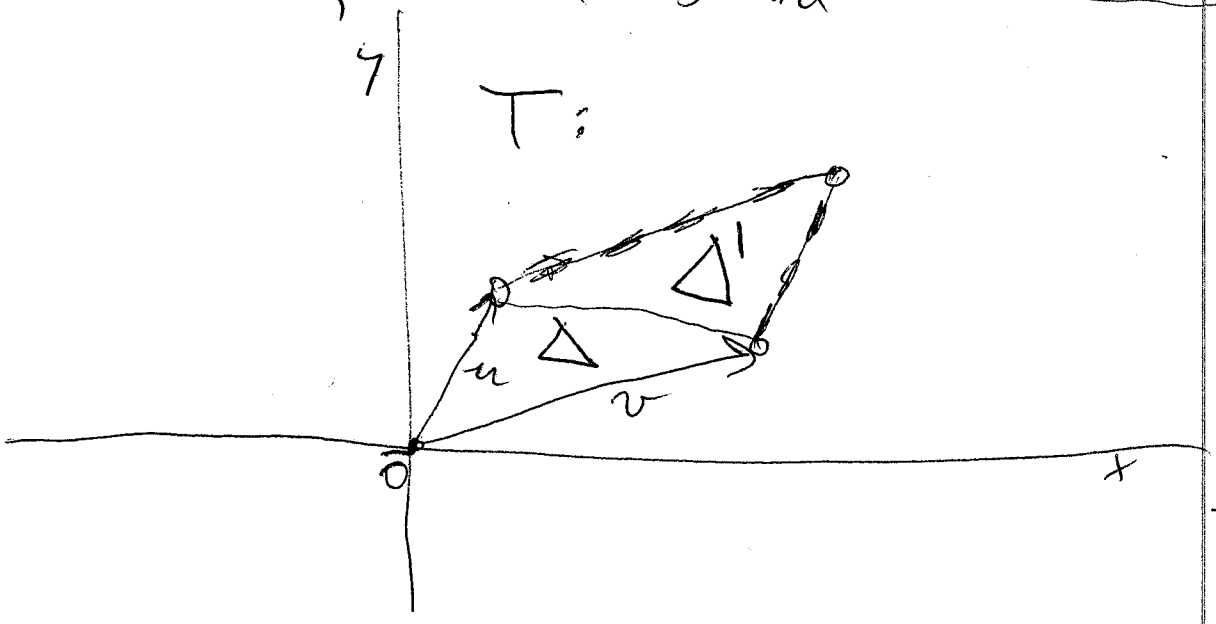
Volume of a parel. T (u $T(B)$) $= |\det(T(B))|$ - a fact.

Now let $B_1 = \{v_1, \dots, v_n\}$, $B_2 = \{w_1, \dots, w_n\}$ be bases, $V = T(B_1)$, $W = T(B_2)$. $\Delta(B_1) = \Delta(B_2) \rightsquigarrow$ $\boxed{V = AW}$ $\boxed{W = BV}$ for some matrices $A, B \in \mathbb{Z}^{n \times n}$. The matrices V and W are regular $\rightsquigarrow A = VW^{-1}$, $B = WV^{-1} \rightsquigarrow AB = BA = I$.

$\rightsquigarrow \underline{\det(A)\det(B) = \det(AB) = \det(I) = 1}$.

But $\det(A), \det(B) \in \mathbb{Z}$ (as $A, B \in \mathbb{Z}^{n \times n}$) $\rightsquigarrow A = B = \pm 1 \rightsquigarrow |\det(V)| = |\det(W)| \rightarrow \mathrm{vol}(T(B_1)) = \mathrm{vol}(T(B_2))$. ☒

Geometric proof of the (Cauchy–Farey) thm. on Farey fractions. Let $\frac{a}{b} < \frac{c}{d}$ be two neighbours in the list F_n, then $\frac{c}{d} - \frac{a}{b} = \frac{1}{bd} \iff \boxed{bc - ad = 1}$.



$u = (a, b)$
$v = (c, d)$
$B = \{u, v\}$
$T = T(B)$
$\Delta = \Delta(B) \subset \mathbb{Z}^2$

$\Delta = \{ w \in \mathbb{R}^2 \mid w = \alpha u + \beta v, 0 \le \alpha, \beta \le 1, \alpha + \beta \le 1 \}$.

($\Delta \cap \mathbb{Z}^2 = \{ \bar{0}, u, v \}$, because: ....

$\Delta' = u + v - \Delta \rightsquigarrow T = T(B) \cap \mathbb{Z}^2 = \{ \bar{0} \}$. $\rightsquigarrow$

.... $\rightsquigarrow \Lambda = \mathbb{Z}^2$, by the Lemma. By the Proposition $|\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}| = \mathrm{Vol}(T(\{(0,1),(1,0)\})) =$

$\mathrm{Vol}(T(B)) = |\det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}| = 1$

($\rightsquigarrow bc - ad = 1$. ☒

If $\Lambda = \Lambda(B)$ is a lattice in $\mathbb{R}^n$, we define the volume of Λ as

$$\boxed{\mathrm{Vol}(\Lambda) := \mathrm{Vol}(T(B))}.$$

Theorem (Minkowski, 1891) If $B \subset \mathbb{R}^n$ is a bounded, centrally symmetric and convex set and $\Lambda \subset \mathbb{R}^n$ is a lattice s.t. $2^n \mathrm{Vol}(\Lambda) < \mathrm{Vol}(B)$

$\Rightarrow B \cap \Lambda \neq \{\bar{0}\}$, i.e

$\exists u \in \Lambda \cap B, u \neq \bar{0}$.

Proof. $T :=$ f.p. of Λ

($B_z := T \cap (\frac{1}{2}B + z)$, $z \in \mathbb{R}^n$, $C_z := (T - z) \cap \frac{1}{2}B$.

$C_z = B_z - z$ $\rightsquigarrow \mathrm{Vol}(C_z) = \mathrm{Vol}(B_z - z)$.

$$\sum_{z\in\Lambda} \mathrm{Vol}(B_z) \overset{(1)}{=} \sum_{z\in\Lambda} \mathrm{Vol}(C_z) \overset{(2)}{=} \mathrm{Vol}\left(\tfrac{1}{2}B\right) \overset{(3)}{=} 2^{-n}\mathrm{Vol}(B) >$$

$> \mathrm{Vol}(\Lambda) = \mathrm{Vol}(T)$, but each $B_z \subset T$ $\rightsquigarrow \exists\, z_1, z_2 \in \Lambda$ s.t. $B_{z_1} \cap B_{z_2} \neq \emptyset$ $\rightsquigarrow \frac{1}{2}x_1 + z_1 = \frac{1}{2}x_2 + z_2$

$z_1 \neq z_2$ // $\frac{1}{2}B + z_1$ // $\frac{1}{2}B + z_2$

for some $x_i \in B$, $i = 1, 2$. $\rightsquigarrow$ $\frac{1}{2}(x_1 - x_2) = z_2 - z_1$ $\neq 0$

$\in B$, $x_1 \in \Lambda$, $-x_2$

Exercise 5: • Why $\mathrm{Vol}(B)$ exists? (two)

• Why are the sums above finite?

Lagrange II: $\forall n \in \mathbb{N}_0\ \exists\, x_i \in \mathbb{Z}$, $i = 1..4$: $\sum_1^4 x_i^2 = n$.

A geometric proof: (By Minkowski's thm.)

Chinese thm. on residues: (2) If $m_1, m_2, \dots, m_r \in \mathbb{N}$ are pairwise coprime and $n_1, \dots, n_r \in \mathbb{Z}$, then the system $x \equiv n_i \pmod{m_i}$, $i = 1..r$, has a (unique) solution x (unique mod $m_1 m_2 \dots m_r$)

Example $x \equiv 1\ (2)$, $x \equiv 1\ (3)$, $x \equiv 3\ (5)$ — $1, 7, \underline{13}, 73, 223, 283, \dots$

Lemma $\forall$ $\square$-free number $n \in \mathbb{N}$, $n = p_1 p_2 \cdots p_r$, the congruence $x^2 + y^2 + 1 \equiv 0 \pmod{n}$ has a solution.

Proof. We proved it for $n = p$. For $n = p_1 p_2 \cdots p_r$ it follows by the Ch. remainder thm. $\boxtimes$

Since $\forall n \in \mathbb{N}$ has (unique) expression as $n = s^2 u$ where $s, u \in \mathbb{N}$ & u is $\square$-free, it suffices to prove Lagrange's thm. just for $\square$-free numbers.

Let $n \in \mathbb{N}$ be $\square$-free, let $a, b \in \mathbb{N}$ be such that $a^2 + b^2 + 1 \equiv 0 \pmod{n}$. We take a lattice in $\mathbb{R}^4$, namely $\Lambda = \Lambda(\{u_1, u_2, u_3, u_4\})$ where

$$\begin{matrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{matrix} \begin{pmatrix} n & 0 & 0 & 0 \\ 0 & n & 0 & 0 \\ a & b & 1 & 0 \\ b & -a & 0 & 1 \end{pmatrix} \rightsquigarrow \mathrm{Vol}(\Lambda) = n^2.$$

For we take the convex body $B = K(r) = \{\bar{x} \in \mathbb{R}^4 \mid x_1^2 + \cdots + x_4^2 \leq r^2\}$, for an appropiate $r > 0$.

Fact: $\mathrm{Vol}(K(r)) = \frac{\pi^2 r^4}{2} \overset{?}{>} 2^4 n^2 = 2^{\dim} \mathrm{Vol}(\Lambda)$

$\Longleftrightarrow r^2 > \frac{4\sqrt{2}}{\pi} n = (1.80063\ldots) n$. We set $r^2 := 1.9\, n$.

Minkowski's thm.: $\exists\, z = \sum_1^4 a_i u_i \in \Lambda$, not all $a_i \in \mathbb{Z}$ are 0, s.t. $z \in K(r)$.

$\Updownarrow$

$$0 < |z|^2 \leq r^2 = 1 \cdot q_n < 2n$$

$\hookrightarrow = (a_1 n + a_3 a + a_4 b)^2 + (a_2 n + a_3 b - a_4 a)^2 + a_3^2 + a_4^2$

$= a_3^2 \underbrace{(a^2 + b^2 + 1)}_{\equiv 0} + a_4^2 \underbrace{(b^2 + a^2 + 1)}_{\equiv 0} + 2a_3 a_4 ab - 2a_3 a_4 ab +$

$+ h(nn) \equiv 0 \pmod{n}$! $n \mapsto n$, n is a sum of 4 $\square$s. ☒

Well, but this proof...?

- Hermann Minkowski

thank you!