GEOMETRY OF NUMBERS B

Tapani Matala-aho, Aalto University, 2022

Abstract

Geometry of numbers is a powerful tool in studying Diophantine inequalities. In geometry of numbers a basic question is to find a non-zero lattice vector from a convex subset in a n-dimensional space, say in $\mathbb{R}^n$. Hermann Minkowski answered this challenge with his convex body theorems. In these lectures we shall discuss how to apply Minkowski's theorems to prove classical Diophantine inequalities.

Jacobian

Let $\overline{f} : \mathbb{R}^n \to \mathbb{R}^n$ be a function with $\overline{f}(\overline{x}) = (f_1(\overline{x}), \ldots, f_n(\overline{x}))^t$, where all the partial derivatives

$$\frac{\partial f_i(\overline{x})}{\partial x_j}, \quad i, j = 1, \ldots, n,$$

exist.

The Jacobian matrix of $\overline{f}$ is defined by

$$J(\overline{f}(\overline{x})) := \begin{bmatrix} \frac{\partial f_1(\overline{x})}{\partial x_1} & \cdots & \frac{\partial f_1(\overline{x})}{\partial x_n} \\ \cdot & \cdot & \\ \cdot & \cdot & \\ \frac{\partial f_n(\overline{x})}{\partial x_1} & \cdots & \frac{\partial f_n(\overline{x})}{\partial x_n} \end{bmatrix} \tag{1}$$

Jacobian

The determinant

$$\det J(\overline{f}(\overline{x})) = \begin{vmatrix} \frac{\partial f_1(\overline{x})}{\partial x_1} & \dots & \frac{\partial f_1(\overline{x})}{\partial x_n} \\ \cdot & \cdot & \\ \cdot & \cdot & \\ \frac{\partial f_n(\overline{x})}{\partial x_1} & \dots & \frac{\partial f_n(\overline{x})}{\partial x_n} \end{vmatrix} \tag{2}$$

of the Jacobian matrix will be called Jacobian.

Integration by a change of variables

For $\overline{f}:\mathbb{R}^n \to \mathbb{R}^n$ we write

$$\overline{y} = (y_1, \ldots, y_n)^t = \overline{f}(\overline{x}) = (f_1(\overline{x}), \ldots, f_n(\overline{x}))^t, \tag{3}$$

Suppose $\overline{f}:\mathcal{B} \to \overline{f}(\mathcal{B})$ is injective and $G:\mathbb{R}^n \to \mathbb{R}$ an integrable function. Then

$$\int\limits_{\overline{y}\in\overline{f}(\mathcal{B})} G(\overline{y})\, dy_1 \ldots dy_n = \int\limits_{\overline{x}\in\mathcal{B}} G\left(\overline{f}(\overline{x})\right) \det J(\overline{f}(\overline{x}))\, dx_1 \ldots dx_n. \tag{4}$$

Volume

By a volume $\mathrm{vol}\,\mathcal{C}$ of a subset $\mathcal{C} \subseteq \mathbb{R}^n$ we mean the absolute value of the Riemann (or Lebesgue) integral

$$\mathrm{vol}\,\mathcal{C} := \left| \int_{\overline{x} \in \mathcal{C}} dx_1 \ldots dx_n \right|, \tag{5}$$

if it exists.

Volume of n-dimensional p-ball

Let $p \in \mathbb{R}^+$. In $\mathbb{R}^n$ the n-dimensional p-ball of radius $r \in \mathbb{R}_{\geq 0}$ is defined by

$$\begin{aligned} \mathcal{B}_p^n(r) &:= \left\{ \overline{x} \in \mathbb{R}^n \,\middle|\, \|\overline{x}\|_p \leq r \right\} \\ &= \left\{ (x_1, \ldots, x_n) \in \mathbb{R}^n \,\middle|\, |x_1|^p + \ldots + |x_n|^p \leq r^p \right\}. \end{aligned}$$

Its volume is given by

$$\operatorname{vol} \mathcal{B}_p^n(r) = 2^n r^n \frac{\Gamma(1+1/p)^n}{\Gamma(1+n/p)}, \tag{6}$$

Volume of n-dimensional p-ball

where $\Gamma(z)$ is the gamma function defined by

$$\Gamma(x+1) := \int_0^\infty e^{-s} s^x \, ds$$

for $x \in \mathbb{R}^+$. It satisfies the functional equation $\Gamma(x+1) = x\Gamma(x)$ for $x \in \mathbb{R}^+$. In particular, $\Gamma(1/2) = \sqrt{\pi}$. Some interesting cases:

	p	vol $\mathcal{B}_p^n(r)$	
Octahedron	1	$\frac{2^n r^n}{n!}$	
Ball	2	$\frac{\pi^{n/2} r^n}{\Gamma(1+n/2)}$	
Cube	∞	$2^n r^n$	

Convex body

Definition 1

A non-empty subset $\mathcal{C} \subseteq \mathbb{R}^n$ is *convex*, if for any pair of points $\overline{a}, \overline{b} \in \mathcal{C}$ holds

$$\{s\overline{a} + (1-s)\overline{b} |\ 0 \leq s \leq 1\} \subseteq \mathcal{C}.$$

A bounded convex subset $\mathcal{C} \subseteq \mathbb{R}^n$ is called a *convex body*. A subset $\mathcal{C}$ is *central symmetric* (symmetric wrt origin) if $\mathcal{C} = -\mathcal{C}$.

Remark 1

In these notes we don't expect that a convex body is necessarily closed.

Convex body

In a convex set $\mathcal{C}$ arbitrary two points $\overline{a}, \overline{b}$ can be joined with a line segment belonging entirely in $\mathcal{C}$.

Example 2

Let $\lambda \in \mathbb{R}_{\geq 0}$ and assume that $\mathcal{C}$ is a central symmetric convex body. Then the dilation

$$\lambda\mathcal{C} := \{\lambda\overline{a} |\ \overline{a} \in \mathcal{C}\}$$

is also a central symmetric convex body.

Convex body

Example 3

Octahedron is an n-dimensional 1-ball of radius $r \in \mathbb{R}_{\geq 0}$ defined by

$$\begin{aligned}\mathcal{B}_1^n(r) &:= \left\{\overline{x} \in \mathbb{R}^n \,\middle|\, \|\overline{x}\|_1 \leq r\right\} \\ &= \left\{(x_1, \ldots, x_n)^t \in \mathbb{R}^n \,\middle|\, |x_1| + \ldots + |x_n| \leq r\right\}.\end{aligned}$$

Show that $\mathcal{B}_1^n(r)$ is a central symmetric convex body.

Example 4

If $s \geq 1$, then it can be shown that $\mathcal{B}_s^n(r)$ is a central symmetric convex body.

Lattice

In these lectures we consider lattices which are free $\mathbb{Z}$-modules in $\mathbb{R}^n$.

Definition 5

Let $n \in \mathbb{Z}^+$ and let $\bar{l}_1, ..., \bar{l}_r \in \mathbb{R}^n$ be linearly independent over $\mathbb{R}$, then the linear hull

$$\Lambda = \langle \bar{l}_1, ..., \bar{l}_r \rangle_{\mathbb{Z}} = \mathbb{Z}\bar{l}_1 + ... + \mathbb{Z}\bar{l}_r \subseteq \mathbb{R}^n$$

over $\mathbb{Z}$ is called a lattice in $\mathbb{R}^n$.

The set $\{\bar{l}_1, ..., \bar{l}_r\}$ is called a base of Λ with $\operatorname{rank} \Lambda = r$.

If $\operatorname{rank} \Lambda = n$, then Λ is called a full lattice.

Lattice, Gram determinant

Remark 2

The lattice $\Lambda = \langle \bar{l}_1, ..., \bar{l}_r \rangle_{\mathbb{Z}}$ *is a* $\mathbb{Z}$*-module.*

Lemma 3

Let $L = [\bar{l}_1, ..., \bar{l}_r]$*, then*

$$\det(L^t L) = \det[\bar{l}_i \cdot \bar{l}_j]_{1 \leq i,j \leq r} \geq 0, \tag{7}$$

where $\cdot$ *is the standard inner product in* $\mathbb{R}^n$*.*

The determinant $\det[\bar{l}_i \cdot \bar{l}_j]_{1 \leq i,j \leq r}$ is called Gram determinant.

Determinant of a lattice

Definition 6

The determinant of a lattice Λ is defined by

$$\det(\Lambda) := \sqrt{\det(L^t L)}, \quad L = [\bar{l}_1, ..., \bar{l}_r]. \tag{8}$$

where the columns $\bar{l}_1, ..., \bar{l}_r$ of the matrix L are the basis vectors $\bar{l}_1, ..., \bar{l}_r$ of Λ.

Lemma 4

For a full lattice we have

$$\det(\Lambda) = |\det\ L| = \left|\det[\bar{l}_1, ..., \bar{l}_n]\right|. \tag{9}$$

Determinant of a lattice

Let

$$\overline{e}_1 := (1, 0, \ldots, 0, 0)^t, \ldots, \overline{e}_n := (0, 0, \ldots, 0, 1)^t$$

denote the standard basis in $\mathbb{R}^n$.

Example 7

The integer lattice

$$\mathbb{Z}^n = \mathbb{Z}\overline{e}_1 + ... + \mathbb{Z}\overline{e}_n \tag{10}$$

has determinant $\det(\Lambda) = 1$.

Fundamental domain

Fundamental domain is defined by

$$\mathcal{F} := \mathcal{F}(\bar{l}_1, \ldots, \bar{l}_r) := \{x_1\bar{l}_1 + \ldots + x_n\bar{l}_r \mid 0 \leq x_i < 1\}.$$

And its translates are given by

$$\mathcal{F}_j := \overline{h}_j + \mathcal{F}$$

with respect to an enumeration

$$\Lambda = \{\overline{h}_j \mid j = 0, 1, \ldots\}$$

of the lattice Λ.

Fundamental domain: det = vol

Lemma 5

Every $\overline{x} \in \mathbb{R}^n$ has unique representation

$$\overline{x} = \overline{h}_j + \overline{f}, \quad \overline{h}_j \in \Lambda, \ \overline{f} \in \mathcal{F}. \tag{11}$$

Theorem 6

Let Λ be a full lattice. Then

$$\det(\Lambda) = \operatorname{vol} \mathcal{F} \tag{12}$$

or

$$\left|\det[\overline{\ell}_1, ..., \overline{\ell}_n]\right| = \operatorname{vol} \{x_1\overline{\ell}_1 + \ldots + x_n\overline{\ell}_n \mid 0 \leq x_i < 1\}. \tag{13}$$

Linear transformation

Let $\overline{L}: \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation and write

$$\overline{\ell}_i := \overline{L}\overline{e}_i = \alpha_{1i}\overline{e}_1 + \alpha_{2i}\overline{e}_2 + \ldots + \alpha_{ni}\overline{e}_n, \quad i = 1, \ldots, n. \tag{14}$$

Then

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \ldots & \alpha_{2n} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \ldots & \alpha_{3n} \\ . & . & . & \ldots & . \\ \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \ldots & \alpha_{nn} \end{bmatrix} = [\overline{\ell}_1, \ldots, \overline{\ell}_n] = L \tag{15}$$

determines $\overline{L}$'s matrix with respect to standard basis $\overline{e}_1, \ldots, \overline{e}_n$.

Linear transformation

Further,

$$\overline{L}\overline{x} = x_1\overline{L}\overline{e}_1 + \ldots + x_n\overline{L}\overline{e}_n = x_1\overline{\ell}_1 + \ldots + x_n\overline{\ell}_n, \tag{16}$$

for $\overline{x} = (x_1, \ldots, x_n)^t = x_1\overline{e}_1 + \ldots + x_n\overline{e}_n \in \mathbb{Z}^n$, so that we get a lattice

$$\begin{aligned}\Lambda = \overline{L}\mathbb{Z}^n &= \mathbb{Z}\overline{\ell}_1 + \mathbb{Z}\overline{\ell}_2 + \ldots + \mathbb{Z}\overline{\ell}_n \\ &= \mathbb{Z}\begin{bmatrix}\alpha_{11}\\ \alpha_{21}\\ \alpha_{31}\\ \vdots\\ \alpha_{n1}\end{bmatrix} + \mathbb{Z}\begin{bmatrix}\alpha_{12}\\ \alpha_{22}\\ \alpha_{32}\\ \vdots\\ \alpha_{n2}\end{bmatrix} + \ldots + \mathbb{Z}\begin{bmatrix}\alpha_{1n}\\ \alpha_{2n}\\ \alpha_{3n}\\ \vdots\\ \alpha_{nn}\end{bmatrix}.\end{aligned} \tag{17}$$

$\det = \det = \mathrm{vol}$

Vice versa: The lattice in (17) determines the linear map in (14) via the matrix L in (15).

Assume $\det L \neq 0$. Then the linear map $\overline{L}$ is bijective and determines a full lattice $\Lambda := \overline{L}(\mathbb{Z}^n)$, because

$$\det \Lambda = \left|\det[\overline{\ell}_1, ..., \overline{\ell}_n]\right| = |\det L| \neq 0. \tag{18}$$

In addition, by (12) and (18) we have

Theorem 7

$$\det \Lambda = |\det L| = \mathrm{vol}\,\mathcal{F}. \tag{19}$$

Linear transformation stretches volumes

From now on, we may use the same symbol L for the linear map $\overline{L}$ and its matrix L. For example $\det \overline{L} = \det L$.

Theorem 8

Linear transformation, say $L: \mathbb{R}^n \to \mathbb{R}^n$, stretches volumes by a factor $|\det L|$, namely

$$\mathrm{vol}\, L\mathcal{C} = |\det L| \cdot \mathrm{vol}\, \mathcal{C}. \tag{20}$$

Proof. Let $L: \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation and write

$$\overline{y} = (y_1, \ldots, y_n)^t = L\overline{x} = (L_1(\overline{x}), \ldots, L_n(\overline{x}))^t.$$

Linear transformation stretches volumes

We compute $\overline{y} = L\overline{x}$ by using their matrices

$$\overline{y} = L\overline{x} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \dots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}. \tag{21}$$

Hereby

$$\begin{bmatrix} L_1(\overline{x}) \\ L_2(\overline{x}) \\ \vdots \\ L_n(\overline{x}) \end{bmatrix} = \begin{bmatrix} \alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1n}x_n \\ \alpha_{21}x_1 + \alpha_{22}x_2 + \ldots + \alpha_{2n}x_n \\ \vdots \\ \alpha_{n1}x_1 + \alpha_{n2}x_2 + \ldots + \alpha_{nn}x_n \end{bmatrix}. \tag{22}$$

Linear transformation stretches volumes

So we are ready to compute the Jacobian as follows

$$
\begin{aligned}
\det J(L(\overline{x})) &= \begin{vmatrix} \frac{\partial L_1(\overline{x})}{\partial x_1} & \cdots & \frac{\partial L_1(\overline{x})}{\partial x_n} \\ . & . & \\ . & . & \\ \frac{\partial L_n(\overline{x})}{\partial x_1} & \cdots & \frac{\partial L_n(\overline{x})}{\partial x_n} \end{vmatrix} \\
&= \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \dots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \dots & \alpha_{nn} \end{vmatrix} = \det L.
\end{aligned} \tag{23}
$$

Linear transformation stretches volumes

In computing the volume integrals the map L is restricted by $L: \ \mathcal{C} \to L\mathcal{C}$.

By the change of variables

$$\begin{aligned} \int\limits_{\overline{y} \in L\mathcal{C}} dy_1 \dots dy_n &= \int\limits_{\overline{x} \in \mathcal{C}} \det J(L(\overline{x}))\, dx_1 \dots dx_n \\ &\overset{(23)}{=} \int\limits_{\overline{x} \in \mathcal{C}} \det L\, dx_1 \dots dx_n = \det L \int\limits_{\overline{x} \in \mathcal{C}} dx_1 \dots dx_n. \end{aligned} \tag{24}$$

Hence, by taking absolute values we get

$$\operatorname{vol} L\mathcal{C} = \left| \det L \right| \cdot \operatorname{vol} \mathcal{C}. \quad \square \tag{25}$$

Volume of the fundamental domain/Proof of Theorem 6

Proof of Theorem 6. We need to show that

$$\left|\det[\overline{\ell}_1, ..., \overline{\ell}_n]\right| = \mathrm{vol}\,\{x_1\overline{\ell}_1 + \ldots + x_n\overline{\ell}_n \mid 0 \leq x_i < 1\}. \tag{26}$$

Define an n-cube

$$\square := \{(x_1, \ldots, x_n)^t \mid 0 \leq x_i < 1\}. \tag{27}$$

We have

$$\mathcal{F} = L\square := \{x_1\overline{\ell}_1 + \ldots + x_n\overline{\ell}_n \mid 0 \leq x_i < 1\}. \tag{28}$$

Therefore we can use the same linear map and notations as in Theorem 8.

Volume of the fundamental domain/Proof of Theorem 6

Now $\mathcal{C} = \square$ and

$$\operatorname{vol} \square = \int_{\overline{x} \in \square} dx_1 \ldots dx_n = \int_0^1 \ldots \int_0^1 dx_1 \ldots dx_n = 1. \tag{29}$$

By (20) and (9) it follows

$$\operatorname{vol} \mathcal{F} = \operatorname{vol} L\square = |\det L| \cdot \operatorname{vol} \square = \det \Lambda. \quad \square \tag{30}$$

Linear transformation

Define further $\Omega := T\Lambda$, where $T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear transformation.

Then

$$\det \Omega = |\det T| \cdot \det \Lambda. \tag{31}$$

In particular,

$$\det \Lambda = |\det L| \cdot \det \mathbb{Z}^n. \tag{32}$$

Linear transformation

Lemma 9

Linear transformation, say $L: \mathbb{R}^n \to \mathbb{R}^n$, *preserves*

A. compactness,

B. symmetry and

C. convexity.

Proof of A. Let A be the matrix of L defined in (15). Then

$$\|L\overline{x}\|_2 \leq \|A\|_2 \, \|\overline{x}\|_2 = \sqrt{\sum \alpha_{ij}^2} \, \|\overline{x}\|_2 := f \, \|\overline{x}\|_2. \tag{33}$$

Linear transformation

Let $\mathcal{B} \subseteq \mathbb{R}^n$ be a compact set. By (33) the linear map L is continuous, therefore it maps the closed set $\mathcal{B}$ onto a closed set $L\mathcal{B}$. The set $\mathcal{B}$ is bounded, say $\|\overline{x}\|_2 \leq M$, for all $\overline{x} \in \mathcal{B}$. Thus

$$\|L\overline{x}\|_2 \leq f\, \|\overline{x}\|_2 \leq fM \quad \forall\, \overline{x} \in \mathcal{B}. \tag{34}$$

In all, $L\mathcal{B}$ is compact. □

Linear transformation

Lemma 10

Let $L: \mathbb{R}^n \to \mathbb{R}^n$ *be a one to one linear transformation.*

Then $L^{-1}: \mathbb{R}^n \to \mathbb{R}^n$ *is one to one linear transformation.*

Let $\mathcal{C} \subseteq \mathbb{R}^n$ *be a central symmetric convex body, then*

$\mathcal{B} := L^{-1}\mathcal{C} \subseteq \mathbb{R}^n$ *is a central symmetric convex body, too.*

Further $\Lambda := L(\mathbb{Z}^n)$ *is a full lattice.*

Area of ellipse

Let $a, b \in \mathbb{R}^+$. Notations $\overline{x} = (x, y), \overline{X} = (X, Y) \in \mathbb{R}^2$. Consider the area of the disk

$$\mathcal{E} := \left\{ \overline{x} \,\middle|\, \frac{x^2}{a^2} + \frac{y^2}{b^2} \leq 1 \right\}. \tag{35}$$

First we define a linear map L by setting

$$L(x, y) := \left(\frac{x}{a}, \frac{y}{b} \right), \tag{36}$$

which satisfies

$$L = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{bmatrix}, \quad \det L = \frac{1}{ab}. \tag{37}$$

Area of ellipse

Write now

$$\mathcal{D} := \{\overline{X} \,\Big|\, X^2 + Y^2 \leq 1\}. \tag{38}$$

By surjectivity, L maps $\mathcal{E}$ onto $\mathcal{D}$ or

$$L\mathcal{E} = \{(\alpha, \beta) = L\overline{x}, \overline{x} \in \mathcal{E} \,\Big|\, \alpha^2 + \beta^2 \leq 1\} = \mathcal{D}. \tag{39}$$

Because

$$\pi = \operatorname{vol} \mathcal{D} = \det L \cdot \operatorname{vol} \mathcal{E} = \frac{1}{ab} \operatorname{vol} \mathcal{E} \tag{40}$$

we get

$$\operatorname{vol} \mathcal{E} = ab\pi. \tag{41}$$

Area of the ellipse $Ax^2 + Bxy + Cy^2 \le D$

Let $A, B.C, D \in \mathbb{R}$. Notations $\overline{x} = (x, y), \overline{X} = (X, Y) \in \mathbb{R}^2$. Determine $\operatorname{vol} \mathcal{E}$, where

$$\mathcal{E} := \left\{ \overline{x} \,\middle|\, Ax^2 + Bxy + Cy^2 \le D \right\}. \tag{42}$$

Immediately

$$\begin{aligned} \mathcal{E} &= \left\{ \overline{x} \,\middle|\, \left(Ax + \frac{By}{2} \right)^2 + \left(AC - \left(\frac{B}{2} \right)^2 \right) y^2 \le AD \right\} \\ &= \left\{ \overline{x} \,\middle|\, \left(\frac{A}{\sqrt{AD}} x + \frac{B}{2\sqrt{AD}} y \right)^2 + \left(\frac{\sqrt{AC - \left(\frac{B}{2}\right)^2}}{\sqrt{AD}} y \right)^2 \le 1 \right\} \end{aligned} \tag{43}$$

Area of the ellipse $Ax^2 + Bxy + Cy^2 \leq D$

Define a linear map L by setting

$$L(x,y) := \left(\frac{A}{\sqrt{AD}}x + \frac{B}{2\sqrt{AD}}y, \frac{\sqrt{AC - \left(\frac{B}{2}\right)^2}}{\sqrt{AD}}y \right), \tag{44}$$

which satisfies

$$L = \begin{bmatrix} \frac{A}{\sqrt{AD}} & \frac{B}{2\sqrt{AD}} \\ 0 & \frac{\sqrt{AC - \left(\frac{B}{2}\right)^2}}{\sqrt{AD}} \end{bmatrix}, \quad \det L = \frac{\sqrt{AC - \left(\frac{B}{2}\right)^2}}{D}. \tag{45}$$

Area of the ellipse $Ax^2 + Bxy + Cy^2 \le D$

...Hence by

$$\pi = \operatorname{vol} \mathcal{D} = \det L \cdot \operatorname{vol} \mathcal{E} = \frac{\sqrt{AC - \left(\frac{B}{2}\right)^2}}{D} \operatorname{vol} \mathcal{E} \tag{46}$$

we get

$$\operatorname{vol} \mathcal{E} = \frac{D\pi}{\sqrt{AC - \left(\frac{B}{2}\right)^2}} = \frac{2D\pi}{\sqrt{4AC - B^2}}. \tag{47}$$