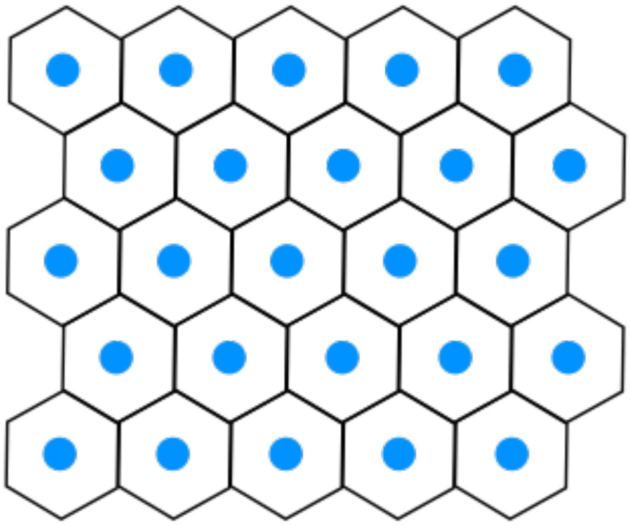
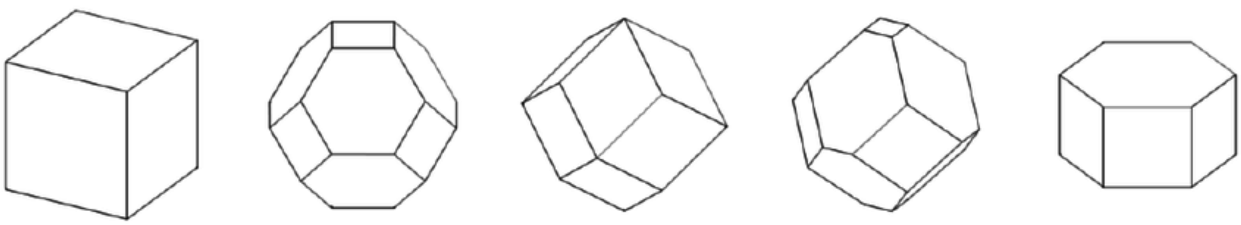
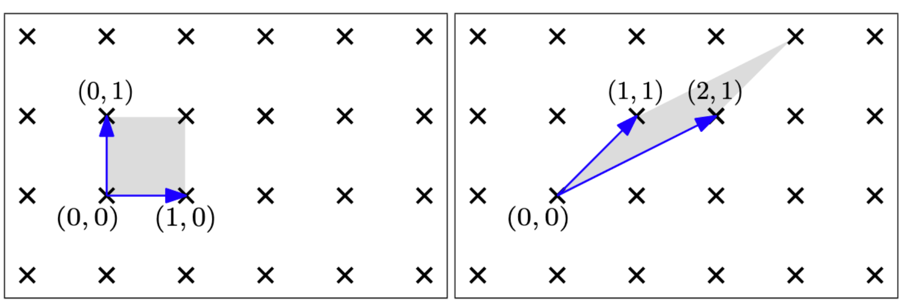


Voronoi cells honeycomb lattice

Some Voronoi cells for lattices in 3-d space



Some Voronoi cells for lattices in 3-d space



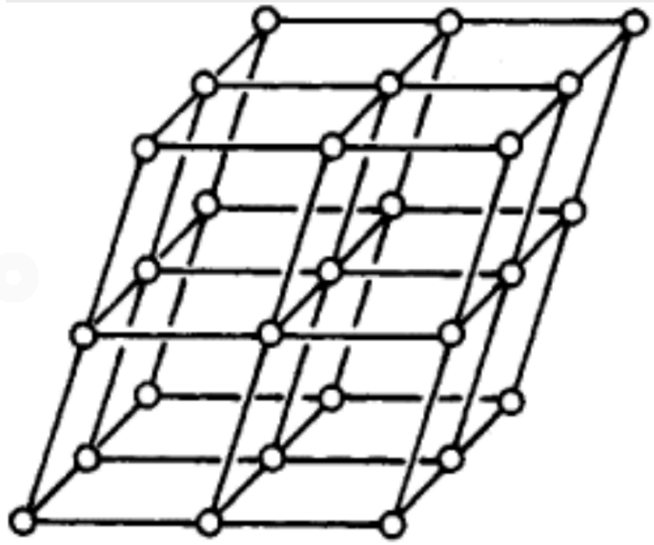
(a) A basis of $\mathbb{Z}^2$ (b) Another basis of $\mathbb{Z}^2$

(picture from Oded Regev's homepage).

Two fundamental parallelipipeds corresponding to two bases

$$\det\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = -1$$

Fundamental parallelepiped, 3d



Lattices lecture 1, Oct. 18 2020

http://math.tau.ac.il/~barakw/geo_numbers

Topic was founded by Hermann Minkowski

~1880 – 1909

In 1910 Minkowski's book "Geometrie der Zahlen" was published.

Connected to: convexity, number theory,

Diophantine approximation, dynamics, computer science and electrical engineering.

Definitions and basic algebraic data

Def A lattice in $\mathbb{R}^n$ is a subset $L \subset \mathbb{R}^n$ for which there is a linearly independent set $v_1, \dots, v_n$ (an $\mathbb{R}$-basis for $\mathbb{R}^n$) s.t. $L = \left\{ \sum_{i=1}^{n} a_i v_i : \begin{array}{l} a_i \in \mathbb{Z} \\ i=1,\dots,n \end{array} \right\} \overset{\text{notation}}{=} \mathrm{span}_{\mathbb{Z}}(v_i)$

notation

$$= \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_n$$

The collection $v_1, \dots, v_n$ is called a basis for L.

Examples 1. $n=2$ $\quad v_1 = e_1 = (1,0)$
$\quad v_2 = e_2 = (0,1)$

$$\mathbb{Z}^2 = \{(x,y) : x,y \in \mathbb{Z}\} = \mathrm{span}_{\mathbb{Z}}(v_1, v_2)$$

More generally $\mathbb{Z}^n = \mathrm{span}_{\mathbb{Z}}(e_1, \dots, e_n)$

This is the <u>integer lattice</u>.

2. $v_1 = e_1 \quad v_2 = e_1 + e_2 = (1,1)$.

$$\mathrm{span}_{\mathbb{Z}}(v_1, v_2) = \mathbb{Z}^2.$$

(so v_1, v_2 are the basis of $\mathbb{Z}^2$)

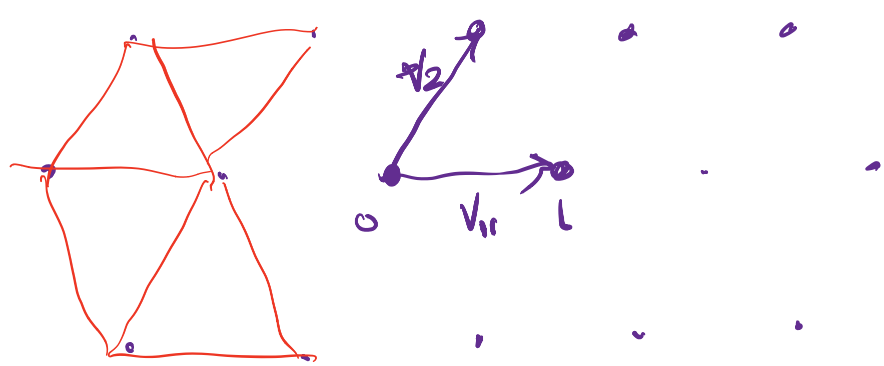
Denote $L = \mathrm{span}_{\mathbb{Z}}(v_1, v_2)$.

Since $v_1, v_2 \in \mathbb{Z}^2$, $L \subset \mathbb{Z}^2$.

$e_1 = v_1 \quad e_2 = v_2 - v_1 \in L$

$\mathbb{Z}^2 = \mathrm{span}_{\mathbb{Z}}(e_1, e_2) \subset L \implies L = \mathbb{Z}^2$.

3. $v_1 = e_1 \quad v_2 = \left(\cos\frac{\pi}{3}, \sin\frac{\pi}{3}\right)$



Sometimes called "honeycomb lattice" or

"hexagon lattice".

4. $A \in M_n(\mathbb{R})$ $\quad A \in GL_n(\mathbb{R}) =$

$\{A \in M_n(\mathbb{R}) : \det A \neq 0\}$

$$L = A\mathbb{Z}^n = \left\{ A\left(\sum_{i=1}^n a_i e_i\right) : a_i \in \mathbb{Z} \right\}$$

$$= \left\{ \sum_{i=1}^n a_i A(e_i) : a_i \in \mathbb{Z} \right\} =$$

$$= \operatorname{span}_{\mathbb{Z}}(Ae_1, \dots, Ae_n) = \operatorname{span}_{\mathbb{Z}}(\text{columns of } A).$$

<u>Cor of computation</u> any lattice is of this form. Because if $L = \operatorname{span}_{\mathbb{Z}}(v_1, \dots, v_n)$

define $A = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}$ = matrix whose columns are v_i's.

$\det A \neq 0$ because v_i lin. ind.

and by previous discussion $L = A(\mathbb{Z}^n)$.

<u>Q</u> How many different bases for the

same lattice? Let's start with $L = \mathbb{Z}^n$:

Prop: Let $GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det A = \pm 1\}$.

Then: (i) $GL_n(\mathbb{Z})$ is a group, and consists of all $A \in M_n(\mathbb{Z})$, invertible, $A^{-1} \in M_n(\mathbb{Z})$.

(ii) $A\mathbb{Z}^n = \mathbb{Z}^n \iff A \in GL_n(\mathbb{Z})$.

Pf: (i) Clearly $GL_n(\mathbb{Z})$ closed under matrix multiplication.

If $A \in GL_n(\mathbb{Z})$, by Cramer's rule implies

$$A^{-1} = \frac{1}{\det(A)} \mathrm{Adj}(A) \in M_n(\mathbb{Z}).$$

This proves $GL_n(\mathbb{Z})$ is a subgroup of $GL_n(\mathbb{R})$.

If $A \in M_n(\mathbb{Z})$, $A^{-1} \in M_n(\mathbb{Z})$

then $\underbrace{\det(A)}_{\in \mathbb{Z}} \cdot \underbrace{\det(A^{-1})}_{\in \mathbb{Z}} = \det(I_n) = 1$

$\Rightarrow \det(A) = \pm 1 \Rightarrow A \in GL_n(\mathbb{Z})$.

(ii) $\Leftarrow$ Let $A \in GL_n(\mathbb{Z})$. Then

$A(\mathbb{Z}^n) = \mathrm{span}_{\mathbb{Z}}(\text{columns of } A) \subset \mathbb{Z}^n$

By same logic $A^{-1}\mathbb{Z}^n \subset \mathbb{Z}^n$

apply to both sides: $\mathbb{Z}^n \subset A\mathbb{Z}^n$.

$\Rightarrow A\mathbb{Z}^n = \mathbb{Z}^n$.

$\Leftarrow$ $A\mathbb{Z}^n = \mathbb{Z}^n \Rightarrow$ columns of A are in $\mathbb{Z}^n$. $\Rightarrow A \in M_n(\mathbb{Z})$.

Applying A^{-1} to both sides

$\mathbb{Z}^n = A^{-1}\mathbb{Z}^n \Rightarrow A^{-1} \in M_n(\mathbb{Z}) \underset{(i)}{\Longrightarrow} A \in GL_n(\mathbb{Z})$.

<u>Cor 1</u> All bases of $\text{span}_{\mathbb{Z}}(v_1, \dots, v_n)$ are of the form $u_1, \dots, u_n$ where

(*) $u_j = \sum_{i=1}^{n} r_{ij} v_i$, where $(r_{ij}) \in GL_n(\mathbb{Z})$

In particular, for $\mathbb{Z}^n = \text{span}(e_1, \dots, e_n)$, $u_1, u_2, \dots, u_n$ is a basis if and only if $r_{ij} = \begin{pmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{pmatrix} \in GL_n(\mathbb{Z})$.

<u>Pf</u> $\text{span}_{\mathbb{Z}}(v_1, \dots, v_n) = \text{span}_{\mathbb{Z}}(u_1, \dots, u_n)$

$\Longleftrightarrow B\mathbb{Z}^n = A\mathbb{Z}^n$, where $B = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}$

$A = \begin{pmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{pmatrix}$

$\iff B^{-1}A\mathbb{Z}^n = \mathbb{Z}^n \iff B^{-1}A = \gamma$ for some $\gamma \in GL_n(\mathbb{Z})$

$\iff A = B\gamma$, for some $\gamma \in GL_n(\mathbb{Z})$.

$\iff$ (*) (note right-multiplying B by γ results in linear comb. with coeff in γ, of columns of B)

<u>Cor 2</u> There is a bijection

$\{\text{all lattices in } \mathbb{R}^n\} \longleftrightarrow GL_n(\mathbb{R}) / GL_n(\mathbb{Z})$

$G/\Gamma = \{g\Gamma : g \in G\}$ $\Gamma\backslash G = \{\Gamma g : g \in G\}$

coset space

<u>Pf</u> Follows from a general fact in group theory. Let G act on a space X

[i.e., have a map $G \times X \to X$, $(g, x) \mapsto gx$ satisfies

(i) $ex = x$ $\forall x \in X$

(ii) $g_1(g_2 x) = (g_1 g_2)x$]

Suppose action is <u>transitive</u>, i.e. $\forall x_1, x_2 \in X$
$\exists g \in G$ s.t. $g x_1 = x_2$.
Then for each $x_0 \in X$, the map
$G/G_0 \longrightarrow X$, given by $gG_0 \longmapsto g x_0$
where $G_0 = \{g \in G : g x_0 = x_0\}$ (stabilizer gp)
is a <u>bijection</u>. Use this in our setup
with $x_0 = \mathbb{Z}^n$, $G = GL_n(\mathbb{R})$, $G_0 = GL_n(\mathbb{Z})$.

<u>Cor 3</u> If $L = A\mathbb{Z}^n$, $A \in GL_n(\mathbb{R})$,
then $|\det(A)|$ depends only on L (not on A).
<u>Pf</u>: If $A_1\mathbb{Z}^n = L = A_2\mathbb{Z}^n$ then
$\exists \gamma \in GL_n(\mathbb{Z})$ s.t. $A_1\gamma = A_2$.
$\det(A_1) = \pm\det(A_2)$.

<u>Def</u> $|\det(A)|$ = covolume of L
notation $\longrightarrow = \operatorname{covol}(L)$
In literature: $d(L)$, $\det(L)$

Fundamental domain

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

Def A set $\Omega \subset \mathbb{R}^n$ is a <u>fundamental domain</u> <u>for L</u> if: (i) Ω is a Borel set.

(ii) For every $x \in \mathbb{R}^n$ there is a unique $y \in \Omega$ s.t. there is $\ell \in L$ with $y = x - \ell$.

Restatements of (ii): • $\bigsqcup_{\ell \in L} \ell + \Omega = \mathbb{R}^n$

disjoint union

• Ω is a collection of equivalence class representatives for the relation $x_1 \sim x_2 \Leftrightarrow x_1 - x_2 \in L$

• Ω is a collection of coset representatives for the quotient $\mathbb{R}^n / L$.

<u>Examples</u> 1. Let $\mathbb{Z}^n = L$. $\Omega = [0,1)^n$

$\forall x \in \mathbb{R}$, define $\lfloor x \rfloor = \max\{k \in \mathbb{Z} : k \leq x\}$

$\{x\} = x - \lfloor x \rfloor$ $\quad \{x\} \in [0,1)$ $\quad x = \lfloor x \rfloor + \{x\}$

Given $x = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^n$ Let $\ell = \begin{pmatrix} \lfloor y_1 \rfloor \\ \vdots \\ \lfloor y_n \rfloor \end{pmatrix} \in \mathbb{Z}^n$

$$x - \ell = y = \begin{pmatrix} \{y_1\} \\ \vdots \\ \{y_n\} \end{pmatrix} \in \Omega.$$

2. More generally, if $L = A(\mathbb{Z}^n)$, $A \in GL_n(\mathbb{R})$

Then $A([0,1)^n)$ is a fundamental domain for L. For (ii), given $x \in \mathbb{R}^n$, define

$\mathbb{Z}^n \ni x' = A^{-1}x$, $y' \in [0,1)^n$, $\ell' \in \mathbb{Z}^n$ s.t.

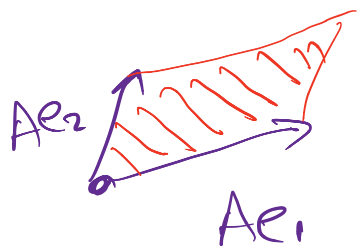
$$y' = x' - \ell'. \quad y = Ay' = x - \underset{\substack{\| \\ \ell \in L}}{A\ell'}$$

proves (ii) for $A([0,1)^n) = \Omega$, and L.

$\Omega = A([0,1)^n)$ is a parallelepiped, it's called the fundamental parallelepiped associated with the basis $Ae_1, \dots, Ae_n$.

$$A([0,1)^n) = \left\{ A\left(\sum_{i=1}^n c_i e_i\right) : \begin{array}{l} c_i \in [0,1) \\ i = 1, \dots, n \end{array} \right\}$$

$$= \left\{ \sum_{i=1}^{n} c_i A e_i : c_i \in [0,1) \right\}$$

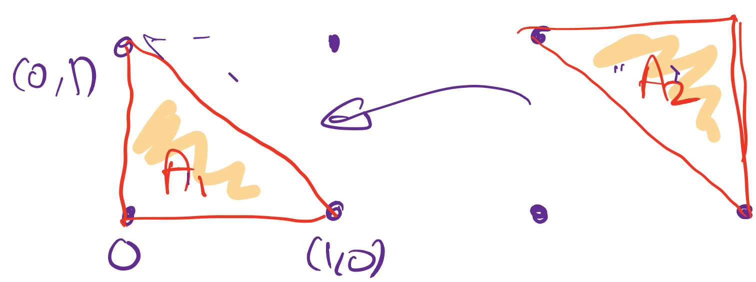


Lebesgue measure on $\mathbb{R}^n$

Recall from calculus: $\mathrm{Vol}(A([0,1)^n))$

$$= |\det(A)| = \mathrm{covol}(L).$$

Example: $L = \mathbb{Z}^2$



$A_1 \cup A_2$ is a fund. domain.

Prop If A and B are two fundamental domains for L then $\mathrm{Vol}(A) = \mathrm{Vol}(B)$.

Pf For each $b \in B$, define $\ell \in L$, $\ell = \ell(b)$, and $a \in A$, $a = a(b)$ by the requirement $a = b - \ell$. (by (ii) this is well-defined).

Define, for $\ell_0 \in L$, $B_{\ell_0} = \{b \in B : \ell(b) = \ell_0\}$.

B_{ℓ_0} is a Borel set. Because

$$B_{\ell_0} = B \cap (A + \ell_0).$$

By uniqueness in (ii), $B = \bigsqcup_{\ell \in L} B_\ell$

$$A = \bigsqcup_{\ell \in L} B_\ell - \ell.$$

So $\mathrm{Vol}(B) = \sum_{\ell \in L} \mathrm{Vol}(B_\ell) = \sum_{\ell \in L} \mathrm{Vol}(B_\ell - \ell)$

$$= \mathrm{Vol}(A).$$

<u>Def</u> A <u>fundamental polytope for a lattice</u> <u>L</u> is a set $K \subset \mathbb{R}^n$ which is the convex hull of a finite set

(i.e. $\exists x_1, \dots, x_p \in \mathbb{R}^n$ s.t. $K = \left\{ \sum_{i=1}^{p} a_i x_i : a_i \geq 0 \ \sum a_i = 1 \right\}$)

and $\mathbb{R}^n = \bigcup_{l \in L} K + l$ and interiors of $l + K$, $l \in L$ are disjoint.

<u>Example</u> $[0,1]^n$ is a fund. polytope for $\mathbb{Z}^n$, and $A([0,1]^n)$ is a fundamental polytope for $A\mathbb{Z}^n$.

<u>Example</u> Voronoi cell of L.

ℓ_2-norm in $\mathbb{R}^n$

$$K = \{x \in \mathbb{R}^n : \forall l \in L,\ \|x\| \le \|x - l\|\}$$

(points at least as close to 0 as to any other point of L). Notation: $\mathrm{Vor}(L)$.

<u>Prop</u> (ex) The Voronoi cell is a polytope.

Hint and a proof of convexity.

$$\mathrm{Vor}(L) = \bigcap_{l \in L} \underbrace{\{x \in \mathbb{R}^n : \|x\| \le \|x - l\|\}}$$ = intersection of convex sets.

closure of one of the connected components of $\mathbb{R}^n \setminus \{x \in \mathbb{R}^n : \|x\| = \|x - \ell\|\}$.

affine hyperplane

<u>Question</u>: is it true that any polytope that tiles $\mathbb{R}^n$ is a fundamental polytope for some lattice.

Example: $[0,\pi)^n$ fundamental polytope for $\pi\mathbb{Z}^n = \begin{pmatrix} \pi & & \\ & \ddots & \\ & & \pi \end{pmatrix} \mathbb{Z}^n$.

Prop: If $L_1 \subset L_2$ is an inclusion of lattices, Ω_2 is a fund. domain for L_2, and $\{x_i\}_{i\in J}$ are coset representatives for L_2/L_1, then

$$\Omega_1 = \bigsqcup_{i\in J} (\Omega_2 + x_i)$$ is a fund. domain

for L_1, and $|J| = D = [L_2 : L_1] =$ (*)

$$= \frac{\mathrm{covol}(L_1)}{\mathrm{covol}(L_2)} < \infty$$

Pf any $\ell_2 \in L_2$ can be written uniquely as $\ell_1 + x_i$, where $\ell_1 \in L_1$ $i \in J$

Clearly Ω_1 is a Borel and the union is disjoint (ex. using that $\{x_i\}$ are coset rep's and Ω_2 is a fund. domain).

Therefore $\mathrm{covol}(L_1) = \mathrm{Vol}(\Omega_1) =$

$$= D\,\mathrm{Vol}(\Omega_2) = D\,\mathrm{covol}(L_2)$$

Divide by $\mathrm{covol}(L_2)$ to get $(*)$

Cor If $L_1 \subset L_2$ is an inclusion of lattices and $D = [L_2 : L_1]$ then

$$L_1 \subset L_2 \subset D L_1$$

Sublattices and subgroups

Thm Suppose $L_1 \subset L_2$ are lattices in $\mathbb{R}^n$.

(a) Given a basis $v_1, \dots, v_n$ of L_2 there is a basis $u_1, \dots, u_n$ of L_1, s.t.

$$(*) \quad \begin{aligned} u_1 &= m_{11} v_1 \\ u_2 &= m_{21} v_1 + m_{22} v_2 \\ &\vdots \\ u_n &= m_{n1} v_1 + \dots + m_{nn} v_n \end{aligned}$$

where $m_{ij} \in \mathbb{Z}$, $n \geq i \geq j \geq 1$, $m_{ii} \neq 0$.

(b) Given a basis $u_1, \dots, u_n$ of L_1

there is a basis $v_1, \dots, v_n$ of L_2 s.t. $(*)$ holds for some (m_{ij}).

Pf of ⓐ: Let $D = [L_2 : L_1]$, then $\forall v \in L_2$, $Dv \in L_1$.

Hence we can find $u_1, \dots, u_n \in L_1$ and $\{m_{ij}\}$, of the form in $(*)$, but with $u_1, \dots, u_n$ not necessarily a basis of L_1. (Take $m_{ii} = D$, $m_{ij} = 0$ for $i \neq j$, $u_i = Dv_i$).

Now choose a solution of $(*)$ (i.e. choose $u_1, \dots, u_n$ and m_{ij}) s.t. m_{11} is as small as possible, and inductively, if $u_1, \dots, u_{i-1}$ have been chosen, take m_{ii} as small as possible.

With these choices we claim $u_1, \dots, u_n$ is a basis of L_1. Otherwise,

$\mathrm{span}_{\mathbb{Z}}(u_1,\dots,u_n) \subsetneq L_1$.

Let $c \in L_1 \setminus \mathrm{span}_{\mathbb{Z}}(u_1,\dots,u_n)$

Write $c = t_1 v_1 + \cdots + t_n v_n$ with $t_i \in \mathbb{Z}$.

Let k be the last index which is nonzero,

i.e. $c = t_1 v_1 + \cdots + t_k v_k$ $\quad t_k \neq 0$.

In addition choose $c \in L_1 \setminus \mathrm{span}_{\mathbb{Z}}(u_1,\dots,u_n)$

so that k is as small as possible.

Since $m_{kk} \neq 0$, there is an integer s

s.t. $|t_k - s m_{kk}| < m_{kk}$.

$$\underbrace{c - s u_k} = (t_1 - s m_{k1}) v + \cdots + (t_k - s m_{kk}) v_k$$

belongs to L_1. If $c - s u_k \in \mathrm{span}_{\mathbb{Z}}(u_1,\dots,u_n)$

then $c \in \mathrm{span}_{\mathbb{Z}}(u_1,\dots,u_n)$ contradiction

So $c - s u_k \in L_1 \setminus \mathrm{span}_{\mathbb{Z}}(u_1,\dots,u_n)$.

Since k is minimal, we can't

have $t_k - s m_{kk} = 0$.

This contradicts the minimality in the choice of m_{kk}.

Proof of (b): Let $u_1, \dots, u_n$ be a basis of L_1, $D = [L_2 : L_1]$ as before. $DL_2 \subset L_1$.

Applying (a), with $L_1 \subset L_2$ replaced with $DL_2 \subset L_1$. Get a basis $Dv_1, \dots, Dv_n$ of DL_2 s.t.

$$(**) \quad \begin{aligned} Dv_1 &= w_{11} u_1 \\ Dv_2 &= w_{21} u_1 + w_{22} u_2 \\ &\vdots \\ Dv_n &= w_{n1} u_1 + \dots + w_{nn} u_n \end{aligned} \qquad \begin{aligned} &w_{ij} \in \mathbb{Z} \\ &w_{ii} \neq 0 \end{aligned}$$

Solve $(**)$ for u_i, one row at a time, sequentially.

$$\begin{aligned} u_1 &= m_{11} v_1 \qquad\qquad m_{11} = \frac{1}{w_{11}} \in \mathbb{Q} \\ u_2 &= m_{21} v_1 + m_{22} v_2 \\ &\vdots \\ u_n &= m_{n1} v_n + \dots + m_{nn} v_n . \end{aligned}$$

Since there is a unique way of writing $x \in \mathbb{R}^n$ as a lin. comb. of $v_1, \dots, v_n$, and since $u_i \in L_1 < L_2 = \mathrm{span}_{\mathbb{Z}}(v_i)$,

$m_{ij} \in \mathbb{Z}$.

Cor 1 In the theorem, can arrange that

(i) $m_{ii} > 0$, and

(iia) $0 \le m_{ij} < m_{jj}$ (case ⓐ)

(iib) $0 \le m_{ij} < m_{ii}$ (case ⓑ).

Pf To obtain (i), if $m_{ii} > 0$, do nothing, if $m_{ii} < 0$ replace u_i with $-u_i$.

To obtain (iia) replace u_i with

$u_i' = t_{i1} u_1 + \dots + t_{ii-1} u_{i-1} + u_i$, where

t_i'-s are obtained as follows.

For any choice of t_{ij}, u_i''s are a basis of L_1.

u_i' also satisfy (*), with coefficients m_{ij}', which are computed as follows.

$m_{ii}' = m_{ii}$

$m'_{ij} = t_{ij} m_{jj} + t_{i,j+1} m_{j+1,j} + \dots + t_{i,i-1} m_{i-1,j} + m_{ij}$

where m_{ij} are coefficients for u_i in $(*)$.

For each i (successively) choose $t_{i,i-1}$, $t_{i,i-2}, \dots$ guaranteeing at each step that $0 \le m'_{ij} < m_{jj} = m'_{jj}$.

(check!) Case (iii) also an ex.

<u>Cor 2</u> Let $u_1, \dots, u_k \in L$ linearly independent, where $L \subset \mathbb{R}^n$ is a lattice. Then there is a basis $v_1, \dots, v_n$ of L

$$u_1 = m_{11} v_1 \qquad m_{ii} > 0 \quad m_{ij} \in \mathbb{Z}$$
$$u_2 = m_{21} v_1 + m_{22} v_2 \qquad 0 \le m_{ij} < m_{ii}$$
$$\vdots$$
$$u_k = m_{k1} v_1 + \dots + m_{kk} v_k \qquad k \ge i \ge j \ge 1.$$

Pf Choose $u_{k+1}, \dots, u_n \in L$ s.t.

$u_1, \dots, u_k, u_{k+1}, \dots, u_n$ are lin. ind.
and apply Cor 2 with $L_1 = \operatorname{span}(u_i)$

$L_2 = L$.

<u>Cor 3</u> Let $u_1, \dots, u_k$ linearly independent in a lattice L. The following are equivalent:

(i) there are $u_{k+1}, \dots, u_n \in L$ s.t. $u_1, \dots, u_n$ are a basis of L.

(ii) $\operatorname{span}_{\mathbb{Z}}(u_1, \dots, u_k) = L \cap \operatorname{span}_{\mathbb{R}}(u_1, \dots, u_k)$.

<u>Pf</u>: (i) $\Rightarrow$ (ii) the inclusion $\subset$ in (ii) is obvious. For the inclusion $\supset$, let $c \in L \cap \operatorname{span}_{\mathbb{R}}(u_1, \dots, u_k)$. Then $\exists b_1, \dots, b_k \in \mathbb{R}$ and $a_1, \dots, a_n \in \mathbb{Z}$ s.t.

$\sum_{i=1}^{n} a_i u_i = c = \sum_{i=1}^{k} b_i u_i$. Since the u_i's are lin. ind.,

$b_i = a_i \in \mathbb{Z}$ for $i = 1, \dots, k$ and $a_i = 0$ for $i > k$.

In particular $c \in \operatorname{span}_{\mathbb{Z}}(u_1, \dots, u_k)$

(ii) $\Rightarrow$ (i) Given $u_1, \dots, u_k$ let $v_1, \dots, v_n$ as in Cor. 2, with coefficients (m_{ij}).

Each of $v_1, \dots, v_k$ is in $\mathrm{span}_{\mathbb{R}}(u_1, \dots, u_k)$ and hence, by (ii), in $\mathrm{span}_{\mathbb{Z}}(u_1, \dots, u_k)$.

So, successively, $u_1 = m_{11} v_1$, $m_{11} > 0$

$v_1 \in \mathrm{span}_{\mathbb{Z}}(u_1)$

$\Rightarrow m_{11} = 1 \Rightarrow u_1 = v_1$

$u_2 = m_{21} v_1 + m_{22} v_2 = m_{21} u_1 + m_{22} v_2$ $\quad m_{22} > 0$

$= m_{21} u_1 + m_{22}(\alpha u_1 + \beta u_2)$ for some $\alpha, \beta \in \mathbb{Z}$

$\Rightarrow$ (equating coefficients) $1 = m_{22}\beta$, $m_{22} > 0$, $\beta \in \mathbb{Z}$

$\Rightarrow m_{22} = 1 \Rightarrow$ (Cor 1) $m_{21} = 0 \Rightarrow u_2 = v_2$

Repeating this argument inductively gives $u_1 = v_1, u_2 = v_2, \dots, u_k = v_k$.

So can take $u_i = v_i$, $i = 1, \dots, n$.

Cor 4 A vector $u \in L$ can be completed to a basis $u = u_1, u_2, \ldots, u_n$ of L

if and only if

$au \in L,\ a \in \mathbb{R} \Rightarrow a \in \mathbb{Z}$.

The line $\mathrm{span}(u)$ ~~intersects~~ L exactly along multiples of u.

Def If this holds, u is called a primitive vector of L.

If property of Cor 3 holds for $u_1, \ldots, u_k$, $\mathrm{span}_{\mathbb{Z}}(u_1, \ldots, u_k)$ is called a primitive subgroup of L

and $u_1, \ldots, u_k$ is called a primitive k-tuple.