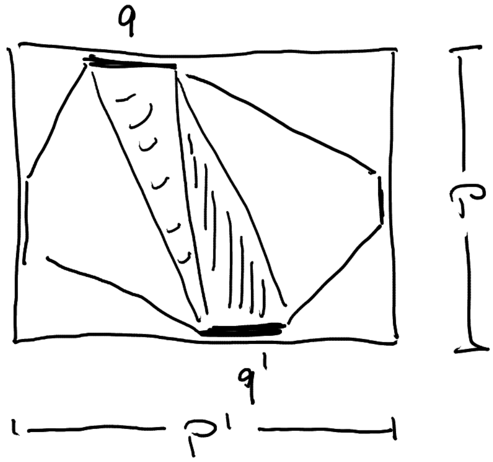
3.1

Scott's Thm P lattice polytope with $i \geq 1$ interior lattice pts

Then either

- $P \cong 3\Delta_2$, so $a = 9/2$, $i = 1$, $b = 9$ or
- $a \leq 2(i+1) \iff b \leq a+4$

proof place P into rectangle $R = [0,p'] \times [0,p]$
with p as small as possible (up to lattice transformations



At most $2(p-1)$ boundary lattice pts not on q, q'

$\Rightarrow$ $b \leq (q+1)+(q'+1)+2(p-1) = q+q'+2p$ (1)

$a \geq \frac{1}{2}p(q+q')$ (2)

(1)+(2) $\Rightarrow$ $2b-2a \leq 2(q+q'+2p) - p(q+q')$

$= (q+q'-4)(2-p)+8$ (3)

with strict inequality if P has a vertex not on q, q'

3.2

We do case distinction:

(I) $p = q + q' = 3$

(3) strict: then $b \leq a+4$ ✓

otherwise: (2) $\Rightarrow a = 9/2$

by Pick's Formula: $a \geq b/2$, so $b \leq 9$

if $b < 9$, then $b \leq a+4$

we are left with $i=1, b=9, a=9/2$

<u>Ex</u>: Check that this implies $P = 3\Delta_2$

(II) $p = 2$ or $q+q' \geq 4$

$\Rightarrow (q+q'-4)(2-p) \leq 0$, so $b \leq 8$ by (3)

(III) $p = 3$ and $q+q' \leq 2$

(1) $\Rightarrow b \leq 8$

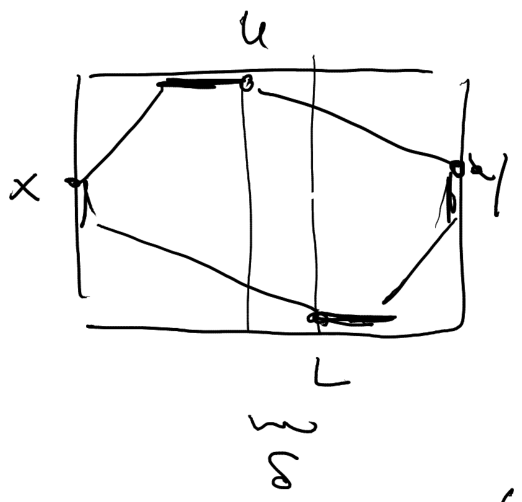
Pick's Formula: $b - a \leq b - b/2 \leq 4$.

(IV) $p \geq 4$ and $q+q' \leq 3$

choose $U \in q$, $L \in q'$ with

$\delta :=$ x-distance of U, L minimal

can assume U to the left of L (otherwise flip!)

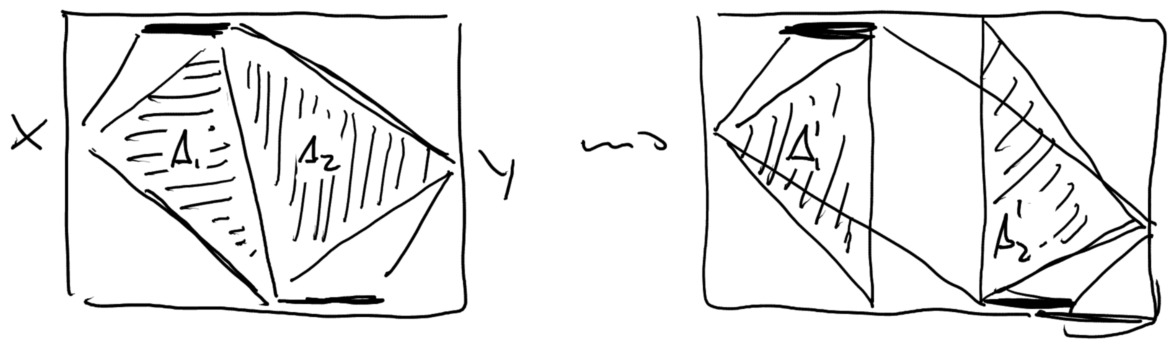


$v \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} v$ leaves q, q', p invariant,

so we can assume

$$\delta \le \frac{1}{2}(p-(q+q'))$$

(then we still have $p < p'$ as p was minimal)



$$a \ge a(\Delta_1)+a(\Delta_2) \ge a(\Delta_1')+a(\Delta_2') \ge \frac{1}{2} p(p'-\delta)$$

$$\ge \frac{1}{2} p\left(p' - \frac{1}{2}p + \frac{1}{2}(q+q')\right) \underset{p'>p}{\ge} \frac{1}{4} p(p+q+q')$$

combine this with (1):

$$4(b-a) \le 8p + 4q + 4q' - p(p+q+q')$$

$$= p(8-p) - (p-4)(q+q') \le 16 \quad \text{as } p \ge 4$$

$$\Rightarrow b \le a+4$$ ☒

The Thm defines a polyhedral set L

$i \ge 1 \qquad b \ge 3 \qquad b \le i + \frac{b}{2} - 1 + 4 = 2(i+3)$

s.th. any lattice polygon P with $i \ge 1$ is either $3\Delta_2$ or its pair (i,b) is in L.

Ex: try to realize all such pairs.

2. Lattices

3.4

Λ is an additive subgroup of $\mathbb{R}^d$ if

(1) $0 \in \Lambda$

(2) $x+y \in \Lambda$ for all $x, y \in \Lambda$

(3) $-x \in \Lambda$ — " — $x \in \Lambda$

Def $\Lambda \subseteq V$ lattice if Λ is a discrete additive subgroup Λ of V, i.e. for all $x \in \Lambda$ there is $\varepsilon > 0$ s.th.

$$B_\varepsilon(x) \cap \Lambda = \{x\}$$

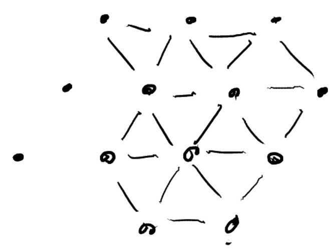
The rank of the lattice Λ is $\dim \operatorname{lin} \Lambda$

Examples (1) $\bigoplus \mathbb{Z} e_i \cong \mathbb{Z}^d$

(2) Let $H := \{ (x_0, \dots, x_d) \in \mathbb{R}^{d+1} \mid \sum x_i = 0 \} \cong \mathbb{R}^d$

and $A_d := \mathbb{Z}^{d+1} \cap H$.

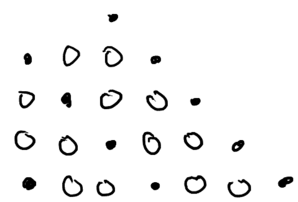
Then A_d is a lattice



A_2

(3) subgroups of lattices are lattices

e.g. $\{ x \in \mathbb{Z}^2 \mid x_1 + x_2 \equiv 0 \pmod 3 \}$



(4) For a subspace $L \subseteq \mathbb{R}^d$ and a lattice $\Lambda \subseteq \mathbb{R}^d$ the set $\Lambda_L := \Lambda \cap L$ is a lattice.

Def: A linearly independent set $B \subseteq \mathbb{R}^d$ lattice basis of Λ if it generates Λ:

$$\Lambda = \Lambda(B) := \{ \sum \lambda_i b_i \mid \lambda_i \in \mathbb{Z},\ b_i \in B \}$$

Example $\{ x \in \mathbb{Z}^2 \mid x_1 + x_2 \equiv 0 \bmod 3 \} = \Lambda(\{\binom{3}{0}, \binom{-1}{1}\})$

Prop: Let $b_1, \ldots, b_k \in \mathbb{R}^d$ be linearly independent. Then

$$\Lambda := \{ \sum \lambda_i b_i \mid \lambda_i \in \mathbb{Z} \}$$ is a lattice

proof: Ex.

We want to show that any lattice has a basis. This needs some preperations.

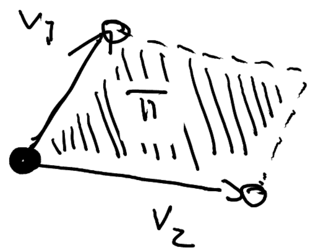
Def: $B := \{v_1, \ldots, v_d\}$ linearly independent. Then

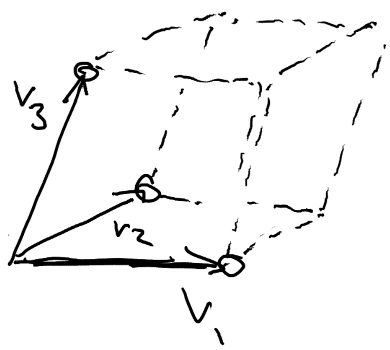
$$\Pi(B) := \{ \sum \lambda_i v_i \mid 0 \leq \lambda_i < 1 \}$$

is the <u>fundamental</u> <u>parallelepiped</u> of B

We denote its closure by

$$\overline{\Pi}(B) = \{ \sum \lambda_i v_i \mid 0 \leq \lambda_i \leq 1 \}$$





Prop: If $B = \{v_1, \dots, v_d\}$ is a basis of $\mathbb{R}^d$ then any $u \in \mathbb{R}^d$ has a unique representation
$u = a + v$ for $a \in \Lambda(B)$ and $v \in \Pi(B)$

proof: Ex ☒

$\Rightarrow$ translates of $\Pi(B)$ by $\Lambda(B)$ tile the space!

For the construction of a lattice basis we start with some linearly independent set of vectors $b_1, \dots, b_d \in \Lambda$
This gives a sequence of subspaces

$$L_0 := \{0\}, \quad L_k := \operatorname{lin}(b_1, \dots, b_k)$$

with $L_0 \subsetneq L_1 \subsetneq L_2 \subsetneq L_3 \subsetneq \dots \subsetneq L_d$

The basis $b_1, \dots, b_k$ of L_k does not necessarily generate $L_k \cap \Lambda$
$\leadsto$ successively replace $b_1, \dots, b_d$ with $u_1, \dots, u_d$ s.th. $u_1, \dots, u_k$ generates $\Lambda \cap L_k$

simple for b_1: Choose u_1 primitive s.th. $b_1 = g u_1$
Then u_1 generates $L_1 \cap \Lambda$.

How should we choose u_2?

Prop: Λ lattice, $v_1, \dots, v_k \in \Lambda$ linearly independent, $L := \operatorname{lin}(v_1, \dots, v_k)$
Then there is $v \in \Lambda \setminus L$, $x \in L$ s.th.

$$d(v, x) \le d(w, y) \quad \forall\ w \in \Lambda \setminus L, y \in L$$

→ use compactness of a ball around $\overline{\Pi}$ to turn this into a finite problem and enumerate

proof: Let $\overline{\Pi} := \overline{\Pi}(v_1, \dots, v_d)$

Let $a \in \Lambda \setminus L$ and $r := d(a, \overline{\Pi})$

Then $B_r(a) := \{ x \in \mathbb{R}^d \mid d(x, \overline{\Pi}) \leq r \}$

is compact and $(B_r(a) \setminus L) \cap \Lambda$ is finite and not empty

$\Rightarrow$ we can choose $v \in (B_r(a) \setminus L) \cap \Lambda$ and $x \in \overline{\Pi}$ realizing

$$d(v, x) = d(v, \overline{\Pi})$$

Let $w \in \Lambda \setminus L$, $y \in L$, $\overline{\Pi} := \overline{\Pi}(v_1, \dots, v_k)$

$$\Rightarrow y = \sum \lambda_i v_i = \underbrace{\sum \lfloor \lambda_i \rfloor v_i}_{=: z \in \Lambda} + \underbrace{\sum \{\lambda_i\} v_i}_{=: z' \in \overline{\Pi}}$$

$$\text{so } d(w, y) = d(\underbrace{w - z}_{\in \Lambda}, \underbrace{y - z}_{\in \overline{\Pi}})$$

$\boxtimes$

With this observation we can continue to construct our lattice basis:

Choose $u_k \in \Lambda \setminus L_{k-1}$ closest to L_{k-1}

Claim: $u_1, \dots, u_k$ is a lattice basis for $L_k \cap \Lambda$

3.8

$k=1$: ✓

$k>1$: Let $v = \sum \mu_i b_i \in L_k \cap \Lambda$
$u_k = \sum \eta_i b_i$ $\Big\}\ \mu_i, \eta_i \in \mathbb{R}$

we can assume that $\mu_i, \eta_i \geq 0$ (flipping does not change distance)

choose $l \in \mathbb{Z}_{\geq 0}$ s.th.

$$v' := v - l u_k = \sum_{i=1}^{k} \mu_i' b_i \quad \text{and} \quad 0 \leq \mu_k' < \eta_k$$

$$\Rightarrow \operatorname{dist}(v', L_{k-1}) = \operatorname{dist}(\mu_k' b_k, L_{k-1})$$
$$= \mu_k' \operatorname{dist}(b_k, L_{k-1})$$
$$< \eta_k \operatorname{dist}(b_k, L_{k-1})$$
$$= \operatorname{dist}(u_k, L_{k-1})$$

Now $v' \in \Lambda$ and closer to L_{k-1} as u_k $\Rightarrow v' \in \Lambda \cap L_{k-1}$

By induction:
$$v' = \sum_{i=1}^{k-1} \lambda_i u_i \quad \text{for } \lambda_i \in \mathbb{Z}$$
$$\Rightarrow v = l u_k + \sum_{i=1}^{k-1} \lambda_i u_i \ \text{ generated by } u_1, \dots, u_k$$

This proves

<u>Thm</u> Every lattice has a basis. ∎

3.9

Given two bases B, B' of a lattice,
we can represent each basis vector of B as an integral linear combination of B' and vice versa,
so writing the bases as columns of two matrices B, B':

$$B = B' \cdot S \ , \ B' = B \cdot T \quad \text{with } S, T \text{ integral}$$

$$\Rightarrow B = B T S \quad \rightarrow \quad TS = \mathbb{1} \ , \text{ so } |\det T| = |\det S| = 1$$

This implies that $|\det B| = |\det B'|$
We define

Def. Λ lattice with basis B. Then

$$\det \Lambda := \det B = \operatorname{vol} \Pi(B)$$

is the <u>determinant</u> of Λ

The construction of a basis in the theorem is not unique.
$\rightsquigarrow$ given two bases B, B', can we decide wether $\Lambda(B) = \Lambda(B')$?

We can use more generally any finite set $B = \{b_1, \dots, b_m\} \subseteq \mathbb{R}^d$
to generate $\Lambda(B) := \{ \sum \lambda_i b_i \mid \lambda_i \in \mathbb{Z} \}$

This is not necessarily a lattice (why?)

If $\Lambda(B)$ is a lattice, can we compute a basis?

$\rightsquigarrow$ need some kind of normal form (computation)
$\longrightarrow$ Hermite normal form (HNF)

The computation of the HNF is similar to Gauß elimination, but uses unimodular transformations to preserve the lattice.

$\leadsto$ search for unimodular T s.th. we can read off basis from BT

What are transformations that preserve the lattice?

(1) multiply column by -1: $T = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$

(2) swap columns i and j:

$$\begin{array}{c c} \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 0 & & 1 & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \\ & & & 1 & & 0 & \\ & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \leftarrow j \\ \\ \\ \\ \end{array} \\ \begin{array}{c} \qquad\qquad\qquad \uparrow \qquad\qquad \uparrow \\ \qquad\qquad\qquad i \qquad\qquad\; j \end{array} & \end{array}$$

(3) add k times the j-th column to the i-th column

$$\begin{array}{c c} \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & k & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} & \begin{array}{l} \\ \\ \\ \\ \leftarrow j \\ \\ \\ \end{array} \\ \begin{array}{c} \qquad\quad \uparrow \\ \qquad\quad i \end{array} & \end{array}$$

Def: $H \in \mathbb{R}^{d \times n}$ with full row rank d is in Hermite normal form if

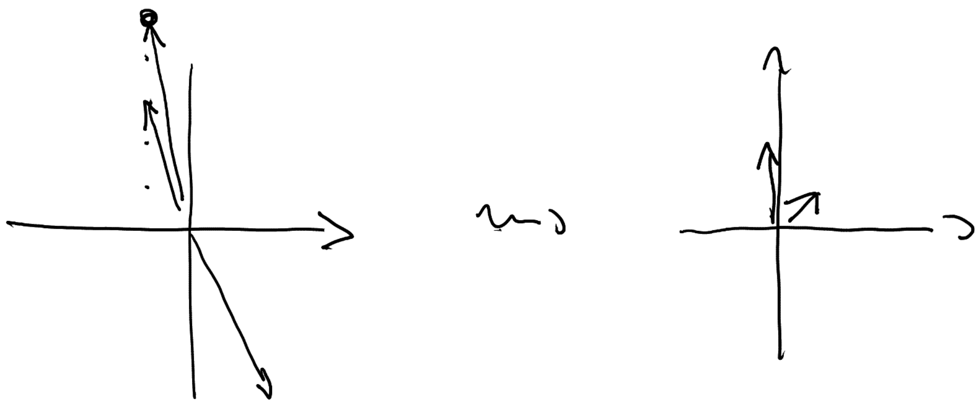
(1) $h_{ij} = 0$ for $j > i$

(2) $0 \leq h_{ij} < h_{ii}$ for $j < i$

Thm: $A \in \mathbb{Q}^{d\times n}$. Then there is a unimodular transformation T s.th. $H = AT$ is in HNF

Example:

$$\begin{pmatrix} -1 & -1 & 2 \\ 5 & 3 & -4 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix}$$



proof: Let g be the common denominator of the entries of A.

if H is an HNF of gA, then $\frac{1}{g}H$ is an HNF for A

$\rightsquigarrow$ it suffices to consider integer matrices A

We now prove this by induction over the rows of A:

Assume A has already the form

$$A = \begin{pmatrix} B & 0 \\ D & C \end{pmatrix}$$

with $B \in \mathbb{Z}^{k\times k}$, $k \geq 0$ in HNF

Let $(c_{11}, \dots, c_{1m-k})$ be the first row of C

with our elementary column transformations we can transform C s.th.

(1) $c_{11} \geq c_{12} \geq \dots \geq_{1,m-k} \geq 0$

(2) $c := c_{11} + c_{12} + \dots + c_{1m-k}$ is as small as possible

then: • $c_{11} > 0$ as A has full row rank

• $c_{12} = 0$ as otherwise we can subtract second from first column (and possibly reorder)

$\Rightarrow c_{12} = c_{13} = \dots c_{1,m-k} = 0$

the column operations extend to A without affecting B, Π.

$\leadsto$

$$A = \begin{array}{c} \left[\begin{array}{ccc} B & 0 & 0 \\ m & c_{11} & 0 \\ \Pi & c' & C' \end{array}\right] \\ \begin{array}{ccc} \underbrace{\quad}_{k} & \overset{\uparrow}{k+1} & \end{array} \end{array}$$

we can use $(k+1)$st column to adjust m s.th. all entries are nonnegative and smaller than c_{11} $\boxtimes$

Prop: The HNF of a matrix is unique (no proof)

We can use the HNF to solve several lattice problems:

(1) given any $b_1, \dots, b_m \in \mathbb{Q}^n$, find a lattice basis

3.B

(2) given bases B, B', check if

$$\Lambda(B) = \Lambda(B')$$

(3) given bases B, B', find the smallest lattice containing both $\Lambda(B)$ and $\Lambda(B')$

$\leadsto$ compute $HNF(B \mid B')$

(4) containment / membership:

B, B' bases : $\Lambda(B') \subseteq \Lambda(B) \iff HNF(B \mid B') = HNF(B)$

$v \in \Lambda(B)$: $HNF(B \mid v) = HNF(B)$

Remark Efficient computation of the HNF:

transform first row of C:

(1) swap a column with nonzero first element to first column, make c_{11} positive

(2) for all columns c_j with nonzero first element:

compute $\gcd(c_{11}, c_{1j}) = x c_{11} + y c_{1j}$

Replace first column with

$$x c_1 + y c_j$$

j-th column with

$$\frac{1}{g}(c_{1j} c_1 - c_{11} c_j)$$

Thm: We can compute the HNF in polynomial time $\boxtimes$

Remark: HNF for matrices that do not have full row rank:

If in the algorithm $c = 0$: Continue with next row.

$\to$ nonnegativity and max on diagonal only for nonzero rows!

Similarly we can use row transformations:

Thm (Smith Normal Form SNF)

$A \in \mathbb{Z}^{d \times n}$. Then there are unimod. transformations L, R s.th.

$$S := L A R$$

is a diagonal matrix

$$S = \begin{pmatrix} s_1 & & & 0 \\ & s_2 & & \\ & & \ddots & \\ 0 & & & s_d \end{pmatrix}$$

with $s_1 \mid s_2 \mid s_3 \mid \dots \mid s_d$ and $s_i \in \mathbb{Z}_{\geq 0}$

The matrix S is unique (but L, R are not!)

For the proof use both row and column transformations $\boxtimes$

Example

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

<u>Thm</u> (Basis of sublattice)

Λ' sublattice of Λ, $\operatorname{rk} \Lambda = d$

Then there is a lattice basis $u_1, \dots, u_d \in \Lambda$ of Λ and $s_1, \dots, s_d \in \mathbb{Z}_{\geq 0}$, $s_1 | s_2 | \dots | s_d$ s.th.

$$s_1 u_1, s_2 u_2, \dots, s_k u_k$$

is a basis of Λ', where $k := \max(i \mid s_i \neq 0)$

<u>proof</u> up to unimodular transformation we can assume that $\Lambda = \mathbb{Z}^d$.

Let $u_1, \dots, u_k$ be generators of Λ' and $A = \begin{pmatrix} | & & | \\ u_1 & \dots & u_k \\ | & & | \end{pmatrix}$

$\leadsto$ there are L, R unimodular s.th.

$$L A R = S \quad \text{SNF with } S = \begin{pmatrix} s_1 & & & 0 \\ & \ddots & & \\ & & s_k & \\ 0 & & & 0 \ddots 0 \end{pmatrix}$$

rewrite this as

$$AR = L^{-1} S$$

Then AR is a basis of Λ', and L^{-1} is a basis of Λ.

let $L^{-1} = (v_1, \dots, v_k, v_{k+1}, \dots, v_d)$

then $\mathcal{R} = (s_1 v_1, \dots, s_k v_k)$ $\boxtimes$

Let $\Lambda' \subseteq \Lambda$ be sublattice. For $x \in \Lambda$ we let

$$x + \Lambda' := \{x + y \mid y \in \Lambda'\}$$

be the coset of Λ modulo Λ'

The set of cosets is Λ / Λ' and the index of Λ' in Λ is $|\Lambda / \Lambda'|$

Cor $\Lambda' \subseteq \Lambda$ lattices of rank d and $v_1, \dots, v_d$ a basis of Λ'. The

$$|\Lambda / \Lambda'| = |\overline{\Pi}(v_1, \dots, v_d) \cap \Lambda| = \frac{\det \Lambda'}{\det \Lambda}$$

and the number of pts of Λ in a fundamental parallelepiped does not depend on the chosen basis.

proof: immediate from the previous thm $\boxtimes$

Cor: For a lattice Λ with basis $u_1, \dots, u_d$

$$\det \Lambda = |\overline{\Pi}(u_1, \dots, u_d) \cap \mathbb{Z}^d|$$ $\boxtimes$