Extreme ~~Ex~~ Let $p_1, \dots, p_k$ be distinct prime numbers.
Then $L = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k})$ is a Galois ext. of $\mathbb{Q}$ with Galois group $G = (\mathbb{Z}/2\mathbb{Z})^k$. The largest cyclic subgroups of $G$ ~~are isomorphic~~ have size 2.

$L = \mathbb{Q}(\underbrace{\sqrt{p_1} + \dots + \sqrt{p_k}}_{\alpha :=})$. Let $f \in \mathbb{Z}[X]$ be the min. pol. of $\alpha \in \mathcal{O}_L$

For any $p \nmid \operatorname{disc}(f)$, the pol. $f \bmod p$ splits either ~~into~~ into $2^k$ linear factors (if $|D| = 1$) or into $2^{k-1}$ quadratic factors (if $|D| = 2$).

Rmk "~~For~~ a random monic pol. $f \in \mathbb{Z}[X]$ of degree $n$, with probability
a) $f$ is irreducible.
b) The Galois closure of $\mathbb{Q}[X]/(f)$ over $\mathbb{Q}$ has Galois group $S_n$
c) For a random prime $p$, $f \bmod p$ is irreducible with probability $\frac{1}{n}$."

(The proof of c) uses the <u>Chebotarev density theorem</u>.)

# 13. Lattice reduction

**Def** A lattice $\Lambda \subset \mathbb{R}^n$ is a set of the form

$$\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n = \{a_1v_1 + \dots + a_nv_n \mid a_1, \dots, a_n \in \mathbb{Z}\}$$

with linearly independent vectors $v_1, \dots, v_n$.

Such $v_1, \dots, v_n$ are called a <u>basis</u> of $\Lambda$.

**Rmk** We can encode a basis $(v_1, \dots, v_n)$ of $\Lambda$ as a matrix

$$\begin{pmatrix} - v_1 - \\ \vdots \\ - v_n - \end{pmatrix} \in GL_n(\mathbb{R}).$$

A change of basis corresponds to left multiplication by an element of $GL_n(\mathbb{Z})$.

Hence, we obtain a bijection

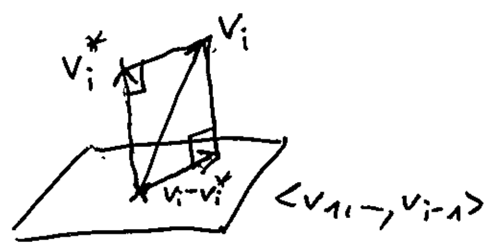
$$\{\Lambda \subset \mathbb{R}^n \text{ lattice}\} \Longleftrightarrow GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R}).$$

**Goal** For a given lattice $\Lambda$ with basis $(v_1, \dots, v_n)$, find a basis $(w_1, \dots, w_n)$ consisting of "nearly as short as possible" vectors $w_1, \dots, w_n$.

**Def** Let $v_1, \dots, v_n$ be a basis of $\mathbb{R}^n$.
For $i = 1, \dots, n$, let $v_i^*$ be the component of $v_i$ orthogonal to the subspace $\langle v_1, \dots, v_{i-1} \rangle$, i.e.:

$$v_i^* \perp v_1, \dots, v_{i-1}$$

and $v_i - v_i^* \in \langle v_1, \dots, v_{i-1} \rangle$.




Write $v_i = v_i^* + \sum_{j=1}^{i-1} \mu_{ij} v_j^*$
with $\mu_{ij} \in \mathbb{R}$ (for $j < i$).

The vectors $v_1^*, \dots, v_n^*$ are the <u>Gram-Schmidt basis</u> for $v_1, \dots, v_n$.

The numbers $\mu_{ij}$ $(j<i)$ are the <u>Gram-Schmidt coefficients</u>

<u>Lemma 13.1</u> a) $\langle v_1, \dots, v_i \rangle = \langle v_1^*, \dots, v_i^* \rangle$ for $i = 1, \dots, n$.
In part., $v_1^*, \dots, v_n^*$ form a basis of $\mathbb{R}^n$.

b) $v_i^* \perp v_j^*$ for all $i \neq j$.

c) $$\mu_{ij} = \frac{v_i \cdot v_j^*}{|v_j^*|^2}.$$

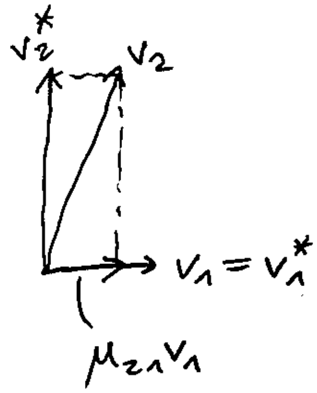
d) $$|v_i|^2 = |v_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \, |v_j^*|^2.$$

e) $$\begin{pmatrix} - v_1 - \\ \vdots \\ - v_n - \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ \mu_{21} & \ddots & \\ \vdots & & \\ \mu_{n1} & \cdots \ \mu_{n,n-1} & 1 \end{pmatrix} \begin{pmatrix} - v_1^* - \\ \vdots \\ - v_n^* - \end{pmatrix}$$

**Pf** a) induction over $i$
b) clear from a)
c) projection formula
d) Pythagoras.
e) clear

$\square$

Ex ($n=2$)



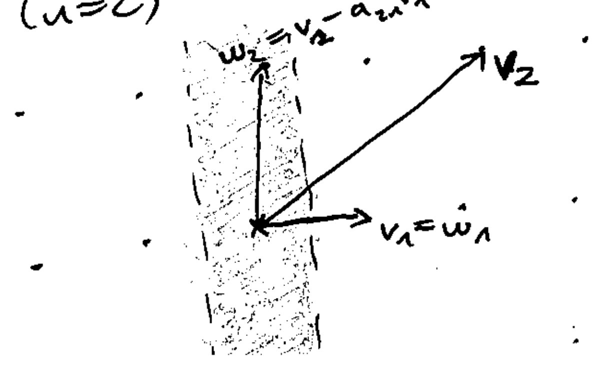

**Thm 13.3** Let $v_1, \dots, v_n$ be a basis of $\mathbb{R}^n$. There are integers $a_{ij} \in \mathbb{Z}$ $(j<i)$ such that the G-S coeff. for the basis $w_1, \dots, w_n$ given by $w_i = v_i - \sum_{j=1}^{i-1} a_{ij} v_j$ satisfy $|\mu_{ij}| \le \frac{1}{2}$ for all $j<i$.
They can be computed using $\mathcal{O}(n^3)$ operations in $\mathbb{R}$.

Rmks a)
$$\begin{pmatrix} - w_1 - \\ \vdots \\ - w_n - \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ a_{ij} & & 1 \end{pmatrix} \begin{pmatrix} - v_1 - \\ \vdots \\ - v_n - \end{pmatrix}$$

b) $w_i^* = v_i^*$ for $i = 1, \dots, n$.

Pf of Thm For $i = 1, \dots, n$:
For $j = i-1, \dots, 1$:
Subtract an appropriate integer multiple of row $j$ from row $i$ to make $|\mu_{ij}| \le \frac{1}{2}$.
$\square$

Ex ($n=2$)



Thm 13.4 Let $n=2$. The following algorithm computes a basis $w_1, w_2$ of $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2$ such that $w_1$ is a shortest nonzero vector in $\Lambda$:

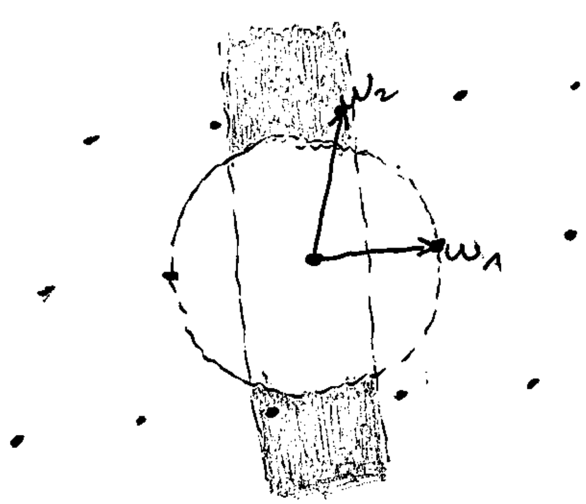
Alg 1) Replace $v_1, v_2$ by the basis computed in Thm 13.3 such that $|\mu_{21}| \leq \frac{1}{2}$.

2) If $|v_1| \leq |v_2|$:
Return $w_1 = v_1$, $w_2 = v_2$.

~~otherwise~~
If $|v_1| > |v_2|$:
Swap $v_1, v_2$ and return to step 1.

Pf correctness: Assume the alg. returned $w_1, w_2$.

Clearly, ~~Ther~~ $w_1, w_2$ still form a basis of $\Lambda$.
We have $|\mu_{21}| \leq \frac{1}{2}$ and $|w_1| \leq |w_2|$.




That ~~is~~ there is no shorter nonzero vector in $\Lambda$ than $w_1$ is "clear from the picture".

Formally:

$$|b_1 w_1 + b_2 w_2|^2$$
$$= b_1^2 |w_1|^2 + b_2^2 |w_2|^2 + 2 b_1 b_2 \underbrace{(w_1 \cdot w_2)}_{\mu_{21}|w_1|^2}$$
$$\geq \underbrace{(b_1^2 + b_2^2 - b_1 b_2)}_{\geq 1} |w_1|^2 \geq |w_1|^2$$

for all $(0,0) \neq (b_1, b_2) \in \mathbb{Z}^2$.

algorithm terminates: $|v_1|$ gets smaller in every iteration. But $\Lambda$ has only finitely many vectors of length less than the original $|v_1|$. $\square$

**Thm 13.5** Assume $v_1, v_2 \in \mathbb{Z}^2$ and the coordinates $c$ of $v_1, v_2$ satisfy $|c| \le B$. Then, the algorithm from Thm 13.4 takes $\mathcal{O}(\log B)$ steps (for large $B$).
($\Rightarrow$ polynomial running time in size of the input!)

**Pf** Rephrase the alg. as follows:

w.l.o.g. $|v_1| \ge |v_2|$.

$u_1 := v_1, \quad u_2 := v_2.$

$u_{i+2} := u_i - k_i u_{i+1}$ with $k_i = \text{round}\left(\dfrac{u_i \cdot u_{i+1}}{|u_{i+1}|^2}\right) \in \mathbb{Z}$

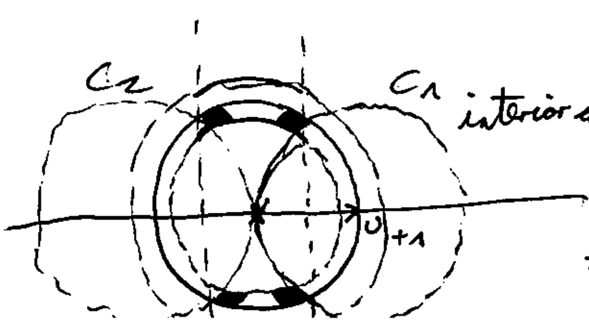
until $|u_{j+1}| > |u_j|$.

Then, we return $w_1 = u_j$, $w_2 = u_{j+1}$.

Clearly, $|u_1| \ge |u_2| > \dots > |u_j|$. Let $\delta = \frac{11}{10}$.

Claim: $\cancel{|u_i| > \delta |u_{i+1}|}$
For all $1 \le i \le j-3$, we have $|u_i| > \delta |u_{i+2}|$.

Pf Assume $|u_i| \le \delta |u_{i+2}|$.
$\Rightarrow |u_i| \le \delta |u_{i+1}|$ and $|u_{i+1}| \le \delta |u_{i+2}|$.




$u_{i+2}$ lies in the vertical strip and in the interior of the inner annulus.
$u_i$ lies in the outer annulus.
$u_{i+2} \in u_i + \mathbb{Z} u_{i+1}$.
$\Rightarrow u_{i+2}$ lies in the shaded region.

In particular, $v_{i+2}$ doesn't lie in the interior of the balls $C_1$ or $C_2$.

$\Rightarrow$ The projection of $v_{i+1}$ onto $v_{i+2}$ has length $\leq \frac{1}{2}|v_{i+2}$

$\Rightarrow v_{i+3} = v_{i+1}$.

$\Rightarrow |v_{i+3}| = |v_{i+1}| > |v_{i+2}|$

$\Rightarrow j = i+2$ $\unicode{x21af}$ $\square$

The claim implies that the total number of steps is $O(\log_\delta B)$ because $|v_1|^2 \leq O(B)$ and each $|v_i|^2$ is an integer. $\square$