Lecture 14, 11.12.

A subset $C \subseteq \mathbb{R}^n$ is called

a) centrally symmetric if $c \in C \Rightarrow -c \in C \quad \forall c \in C$

b) convex if $c, c' \in C \Rightarrow \{tc' + (1-t)c \mid 0 \le t \le 1\} \subseteq C \quad \forall c, c' \in C$.

Thm 6.18

Let Λ be a lattice. Suppose $C \subseteq \mathbb{R}^n$ is convex and centrally symmetric and either

a) $vol(C) > 2^n d(\Lambda)$

b) $vol(C) = 2^n d(\Lambda)$ and C is compact

Then C contains a non-zero lattice point of Λ.

Proof: Assume a). It is enough to show that there are distinct $x_1, x_2 \in \Lambda$ with

$$\left(\tfrac{1}{2}C + x_1\right) \cap \left(\tfrac{1}{2}C + x_2\right) \neq \emptyset.$$

Namely, we then have $\quad \frac{1}{2}c_1 + x_1 = \frac{1}{2}c_2 + x_2$

for some $c_1, c_2 \in C$, hence $\Lambda \ni x_1 - x_2 = \frac{1}{2}c_2 - \frac{1}{2}c_1 \in C$, where we use that C is convex and centrally symmetric.

So, suppose that all the sets $\frac{1}{2}C + x$, $x \in \Lambda$, would be pairwise disjoint. Let ϕ be the fundamental domain of Λ. Then also all the sets $\phi \cap (\frac{1}{2}C + x)$, $x \in \Lambda$, are pairwise disjoint. Hence,

$$vol(\phi) \ge \sum_{x \in \Lambda} vol\left(\phi \cap \left(\tfrac{1}{2}C + x\right)\right)$$

Translating $\phi \cap (\frac{1}{2}C + x)$ by $-x$ gives the set $(\phi - x) \cap \frac{1}{2}C$, and this has the same volume. Since the $\phi - x$, $x \in \Lambda$, cover all of $\mathbb{R}^n$ (and thus of $\frac{1}{2}C$), we have

$$vol\left(\tfrac{1}{2}C\right) = \sum_{x \in \Lambda} vol\left((\phi - x) \cap \tfrac{1}{2}C\right)$$

Hence, ②

$$vol(\phi) \geq \sum_{x\in\Lambda} vol\left(\phi \cap \left(\tfrac{1}{2}C + x\right)\right) = \sum_{x\in\Lambda} vol\left((\phi - x)\cap \tfrac{1}{2}C\right) = vol\left(\tfrac{1}{2}C\right) = \frac{1}{2^n} vol(C) \;\lightning$$

$\square$

Case b). Take any sequence $(\varepsilon_n)_{n\in\mathbb{N}}$ with $\varepsilon_n > 0$, $\varepsilon_n \geq \varepsilon_{n+1}$, $\lim \varepsilon_n = 0$.

$$vol\left((1+\varepsilon_n)C\right) > vol(C) = 2^n d(\Lambda)$$

Hence, by a), $(1+\varepsilon_n)C$ contains a non-zero lattice point

$$x_n \in \Lambda \cap (1+\varepsilon_n)C \subset \Lambda \cap (1+\varepsilon_1)C$$

Since C, and thus $(1+\varepsilon_1)C$, is compact, the sequence (x_n) contains a converging subsequence. By Cor 6.17, the limit x is a lattice point of Λ (non-zero since Λ discrete). We furthermore have

$$x \in \bigcap_{n\in\mathbb{N}} (1+\varepsilon_n)C = C. \quad \square$$

6.7 Successive minima

The length of a shortest vector in Λ is only the first level of interesting information about Λ.

Def 6.19

Let $\lambda_1(\Lambda)$ be the norm of a shortest non-zero $v_1 \in \Lambda$.

Let $\lambda_2(\Lambda)$ " " $v_2 \in \Lambda$ that is linearly indep from v_1.

$\xrightarrow{\text{inductively}} \lambda_i(\Lambda), \ldots$

Can alternatively define this as

$$\lambda_i(\Lambda) := \min\{\lambda > 0 \mid \exists\, v_1, \ldots, v_i \in \Lambda \ \mathbb{R}\text{-linearly independent and } \|v_j\| \leq \lambda \ \forall j\}$$

We obviously have $\lambda_1(\Lambda) \leq \lambda_2(\Lambda) \leq \ldots \leq \lambda_n(\Lambda)$.

The $\lambda_i(\Lambda)$ are called the <u>successive minima</u> of Λ.

Lemma 6.20

There are linearly independent $v_1, \ldots, v_n \in \Lambda$ such that $\|v_i\| = \lambda_i(\Lambda)$ for $i = 1, \ldots, n$.

For such vectors, if $x = \sum x_i v_i \in \Lambda$, $x_i \in \mathbb{Z}$, then $\|x\| \geq \lambda_r(\Lambda)$, $r = \max\{i \mid x_i \neq 0\}$.

Proof:

We can inductively find such vectors.

Let $v \in \Lambda$ be any non-zero vector. By Cor 6.17 there are only finitely many lattice vectors w with $\|w\| \leq \|v\|$. Hence, there is $v_1 \in \Lambda$ with $\|v_1\| = \lambda_1(\Lambda)$.

Now assume $v_1, \dots, v_i$ are linearly independent with $\|v_j\| = \lambda_j(\Lambda)$ for all $j = 1, \dots, i$.

By definition, there are $w_1, \dots, w_{i+1}$ linearly independent such that $\|w_j\| \leq \lambda_{i+1}(\Lambda)$ for all $j = 1, \dots, i+1$.

There must be some ℓ such that $v_1, \dots, v_i, w_\ell$ are linearly independent.

We have $\|w_\ell\| \leq \lambda_{i+1}(\Lambda)$.

If $\|w_\ell\| = \lambda_{i+1}(\Lambda)$, we can take $v_{i+1} := w_\ell$ and are done.

So, suppose $\|w_\ell\| < \lambda_{i+1}(\Lambda)$.

Let r be minimal with $\lambda_r(\Lambda) \leq \|w_\ell\| < \lambda_{r+1}(\Lambda)$, so $r \leq i$.

Then $v_1, \dots, v_r, w_\ell$ are $r+1$ linearly independent vectors with $\|\cdot\| < \lambda_{r+1}(\Lambda)$ ↯

Second claim: $x = x_r v_r + \sum_{i=1}^{r-1} x_i v_i$ is linearly independent from $v_1, \dots, v_{r-1}$,

hence $\|x\| \geq \lambda_r(\Lambda)$. □

Recall from §6.6 that

$$\frac{\lambda_1(\Lambda)^n}{d(\Lambda)} \leq \sqrt{\gamma_n}^{\,n}, \quad \gamma_n \text{ the Hermite constant}$$

Now, we can even bound:

Thm 6.21 (Minkowski's second theorem)

$$\frac{\prod_{i=1}^{n} \lambda_i(\Lambda)}{d(\Lambda)} \leq \sqrt{\gamma_n}^{\,n}$$

Proof:

Let $v_1, \dots, v_n \in \Lambda$ be linearly independent with $\|v_i\| = \lambda_i(\Lambda)$ (exists by Lemma 6.20)

Let Q be the Gram matrix of Λ. Using the quadratic supplement we can (4)
write for $x = \sum_{i=1}^{n} x_i v_i$:

$$\|x\|^2 = Q(x) = z_1(x_1, \dots, x_n)^2 + \dots + z_n(x_1, \dots, x_n)^2,$$

where $z_i : \mathbb{R}^n \to \mathbb{R}$ are linear in the x_i.

Define a new scalar product on $\mathbb{R}^n$ with quadratic form

$$q := \sum_{i=1}^{n} \frac{1}{\lambda_i(\Lambda)^2} z_i^2$$

so,
$$\|x\|_q^2 = q(x) = \sum_{i=1}^{n} \frac{1}{\lambda_i(\Lambda)^2} z_i(x_1, \dots, x_n)^2$$

The Gram matrix Q_q of this form satisfies

$$\det Q_q = \prod_{i=1}^{n} \frac{1}{\lambda_i(\Lambda)^2} \det Q \Rightarrow \prod_{i=1}^{n} \lambda_i(\Lambda) = \frac{\sqrt{\det Q}}{\sqrt{\det Q_q}}$$

Let Λ_q be the lattice associated to Q_q. Then by §6.6:

$$\frac{\lambda_1(\Lambda_q)^n}{\sqrt{\det Q_q}} = \frac{\lambda_1(\Lambda_q)^n}{d(\Lambda_q)} \leq \sqrt{\gamma_n}^{\,n}$$

If we can show that $\lambda_1(\Lambda_q) \geq 1$, then it follows that

$$\prod_{i=1}^{n} \lambda_i(\Lambda) = \frac{\sqrt{\det Q}}{\sqrt{\det Q_q}} \leq \lambda_1(\Lambda_q)^n \cdot \frac{\sqrt{\det Q}}{\sqrt{\det Q_q}} \leq \sqrt{\gamma_n}^{\,n} \cdot \sqrt{\det Q} = \sqrt{\gamma_n}^{\,n}\, d(\Lambda)$$

proving the claim.

For $x = \sum x_i v_i \in \Lambda$ let $r = \max\{i \mid x_i \neq 0\}$.

We have
$$\|x\|_q^2 = \sum_{i=1}^{n} \frac{1}{\lambda_i^2(\Lambda)} z_i(x_1, \dots, x_n)^2 \geq \sum_{i=1}^{r} \frac{1}{\lambda_i^2(\Lambda)} z_i(x_1, \dots, x_n)^2 \underset{\lambda_r(\Lambda) \geq \lambda_i(\Lambda)}{\geq} \frac{1}{\lambda_r^2(\Lambda)} \sum_{i=1}^{r} z_i(x_1, \dots, x_n)^2$$

$$= \frac{1}{\lambda_r^2(\Lambda)} \|x\|^2$$ (all terms for $i > r$ in the quadratic supplement vanish)

On the other hand, we know from Lemma 6.20 that $\|x\|^2 \geq \lambda_r^2(\Lambda)$

$\Rightarrow \|x\|_q^2 \geq 1 \Rightarrow \lambda_1(\Lambda_q) \geq 1$. □

6.8 Lattice reduction

We would like to find a basis of Λ consisting of short vectors.

The (hypothetical) shortest basis $b_1, \dots, b_n$ would satisfy $\|b_i\| = \lambda_i(\Lambda)$ $\forall i = 1, \dots, n$.

However, such a basis does not exist in general (see Exercise 7.3).

The shortest possible bases that do exist are <u>Minkowski reduced</u> bases, which are minima of the set $\mathcal{B}_\Lambda$ of all bases wrt

$$(b_1, \dots, b_n) < (b_1', \dots, b_n') \text{ if } \|b_i\| = \|b_i'\| \ \forall i < j \text{ and } \|b_j\| < \|b_j'\|$$

Such bases are computable but not efficiently.

Here is what we can do more practically.

Lemma 6.22

If $x \in \Lambda$ with $\|x\| = \lambda_1(\Lambda)$, then there is a basis $x = b_1, b_2, \dots, b_n$ of Λ.

For the proof, we will use a general lemma about supplementing vectors to a basis, and for this, we first need another general lemma.

Lemma 6.23

For any $a_1, \dots, a_n \in \mathbb{Z}$ there is $T \in GL_n(\mathbb{Z})$ such that

$$(a_1, \dots, a_n) \cdot T = (g, 0, \dots, 0) \text{ where } g = \gcd(a_1, \dots, a_n).$$

<u>Proof:</u>

By induction on n.

$n=1$: is obvious.

$n=2$: this comes from extended euclidean algorithm. Namely, set $x_0 := a_1$, $x_1 := a_2$.

In each step of the algorithm we compute $x_{i-1} = q_i x_i + r_i$.

Set $U_i := \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$, $A_1 := (x_0, x_1)$, $A_{i+1} = A_i T_i = (x_i, x_{i-1} - q_i a_i)$

Then we arrive eventually at $(g, 0)$.

$n > 2$: Assume there is $U \in GL_n(\mathbb{Z})$ with $(a_1, .., a_n) \cdot U = (g, 0, .., 0)$, $g = \gcd(a_1, .., a_n)$. Let

$$\tilde{U} := \left(\begin{array}{c|c} U & 0 \\ \hline 0 & 1 \end{array}\right) \in GL_{n+1}(\mathbb{Z})$$

Then

$$(a_1, .., a_n, a_{n+1}) \tilde{U} = (g, 0, .., 0, a_{n+1})$$

By the $n=2$ case there is $\begin{pmatrix} u & x \\ v & y \end{pmatrix} \in GL_2(\mathbb{Z})$ with

$$(g, a_{n+1}) \cdot \begin{pmatrix} u & x \\ v & y \end{pmatrix} = (\tilde{g}, 0),$$

where

$$\tilde{g} = \gcd(g, a_{n+1}) = \gcd(a_1, .., a_{n+1})$$

Hence with

$$T := \tilde{U} \cdot \begin{pmatrix} u & 0 & \cdots & 0 & x \\ 0 & & & & 0 \\ \vdots & & 0 & & \vdots \\ 0 & & & & 0 \\ v & 0 & \cdots & 0 & y \end{pmatrix}$$

the claim holds. $\square$