

## 11. Vorlesung

Ziel:

Satz 8.5. Für jede GAP  $P \subseteq \mathbb{Z}$  vom Rang  $d$  existiert eine echte GAP  $Q \supsetneq P$  vom Rang  $\leq d$  mit  $|Q| \leq d^{4d^3} |P|$ .

Proposition 8.6. Jedes Gitter  $\Gamma \subseteq \mathbb{R}^d$  vom Rang  $d$  hat eine Basis

$w_1, \dots, w_d \in \Gamma$  mit

$$\|w_1\| \cdot \dots \cdot \|w_d\| \leq d^{3d/2} \lambda(\mathbb{R}^d / \Gamma),$$

Beweis. Der Fall  $d=1$  ist klar. Ab jetzt gelte  $d \geq 2$ . Es seien  $\lambda_1 \leq \dots \leq \lambda_d$  die sukzessiven Minima von  $B = B_1(0)$  bezüglich  $\Gamma$ .

Da  $\lambda(B) = \frac{\pi^{d/2}}{\Gamma(\frac{d}{2}+1)} \geq d^{-d/2}$  folgt aus Minkowski's zweitem

Satz  $\lambda_1 \cdot \dots \cdot \lambda_d \leq \frac{2^d \lambda(\mathbb{R}^d / \Gamma)}{\lambda(B)} \leq 2^d \cdot d^{d/2} \lambda(\mathbb{R}^d / \Gamma)$ ,

Wie im Beweis von Minkowski's zweitem Satz gibt's lin. unabh.

$v_1, \dots, v_d \in \Gamma$  mit  $v_i \in \overline{\lambda_i B}$ , d.h.  $\|v_i\| \leq \lambda_i$  für alle  $i \in [d]$ .

Für  $i \in [d]$  sei  $V_i$  die von  $v_1, \dots, v_i$  erzeugte UVR von  $\mathbb{R}^d$ .

Wir wollen  $w_1, \dots, w_d \in \Gamma$  rekursiv so wählen, dass

(a)  $i \in [d] \Rightarrow w_1, \dots, w_i$  ist Basis von  $V_i \cap \Gamma$

(b)  $\|w_1\| \leq \lambda_1$

(c)  $i \in [2, d] \Rightarrow \|w_i\| \leq \frac{i \lambda_i}{2}$ .

Wenn dies gelingt ist  $w_1, \dots, w_d$  Basis  $\Gamma$  (nach (a) für  $i = d$ )

$$\text{und} \quad \|w_1\| \cdot \dots \cdot \|w_d\| \leq \frac{d!}{2^{d-1}} \cdot \lambda_1 \cdot \dots \cdot \lambda_d \leq 2d! \cdot d^{d/2} \lambda(\mathbb{R}^d | \Gamma) \\ \leq d^{3d/2} \lambda(\mathbb{R}^d | \Gamma).$$

Zur Konstruktion: Sei  $w_1$  Basis von  $V_1 \cap \Gamma \neq \emptyset \ni \mathbb{Z}v_1$ . Dann

$$w_1 = \frac{v_1}{n} \quad \text{für ein } n \in \mathbb{N}, \text{ also } \|w_1\| \leq \|v_1\| \leq \lambda_1.$$

3

Sei nun  $i \in [2, d]$  und  $w_1, \dots, w_{i-1}$  frñm schon gewählt.

Da  $v_1, \dots, v_i$  Basis von  $V_i$  ist und  $v_i \in (V_i \setminus V_{i-1}) \cap \Gamma$

gibt's Vektoren  $w \in (V_i \setminus V_{i-1}) \cap \Gamma$ , die man in der Form

$$w = t_1 v_1 + \dots + t_{i-1} v_{i-1} + t_i v_i \quad \text{mit } |t_j| \leq \frac{1}{2} \text{ für } j \in [i-1] \\ |t_i| \leq 1, t_i \neq 0,$$

schreiben kann. Da  $\Gamma$  diskret ist, gibt's nur endlich viele solche.

Es sei  $w_i$  einer von ihnen, bei demen  $|t_i|$  minimal ist.

Dann ist  $|t_i| = \frac{1}{n}$  für ein  $n \in \mathbb{N}$  und  $w_1, \dots, w_i$  ist Basis von  $V_i \cap \Gamma$ .

Wenn  $n=1$  hätte man man  $w_i = v_i$  nehmen können, da  $\|v_i\| \leq \lambda_i \leq \frac{i\lambda_i}{2}$ .

Wenn  $n \geq 2$  ist

$$\|w_i\| \leq \frac{1}{2} (\|v_1\| + \dots + \|v_i\|) \quad (\text{nach Dreiecksungl.})$$

$$\leq \frac{1}{2} (\lambda_1 + \dots + \lambda_i) \leq \frac{i\lambda_i}{2}$$

□

(4)

Proposition 8.7. Für jedes Gitter  $\Gamma \subseteq \mathbb{R}^d$  vom Rang  $r$  gibt's  $w_1, \dots, w_r \in \Gamma$  und  $n_1, \dots, n_r \in \mathbb{N}$  mit

$$\left\{ \sum_{i=1}^r k_i w_i : |k_i| < n_i, \text{ für alle } i \in [d] \right\} \subseteq B_1(0) \cap \Gamma$$

und

$$B_R(0) \cap \Gamma \subseteq \left\{ \sum_{i=1}^r k_i w_i : |k_i| < R^{3r/2+1} n_i, \text{ für alle } i \in [r] \right\}$$

für alle  $R > 0$ .

Beweis. O.B.d.A. ist  $d=r$ . Nach Prop. 8.6 hat  $\Gamma$  eine Basis  $w_1, \dots, w_d$

mit  $\prod_{i=1}^d \|w_i\| \leq d^{3d/2} \lambda(\mathbb{R}^d / \Gamma)$ . Setze  $n_i = \left\lceil \frac{1}{d \|w_i\|} \right\rceil$  für alle  $i \in [d]$ .

Diese Vektoren und Zahlen tun's, denn:

$$\begin{aligned} \text{Sei } |k_i| < n_i \text{ für alle } i \in [d]. \text{ Dann } \left\| \sum_{i=1}^d k_i w_i \right\| &\leq \sum_{i=1}^d |k_i| \cdot \|w_i\| \\ &< \sum_{i=1}^d n_i \cdot \|w_i\| \leq \sum_{i=1}^d \frac{\|w_i\|}{d \|w_i\|} = \frac{d}{d} = 1, \text{ d.h.} \end{aligned}$$

$$\sum_{i=1}^d k_i w_i \in B_1(0) \cap \Gamma.$$

Sei nun  $R > 0$  und  $x \in B_R(0) \cap \Gamma$ . Schreibe  $x = \sum_{i=1}^d k_i w_i$   
mit  $k_1, \dots, k_d \in \mathbb{Z}$ . Für alle  $i \in [d]$  ist

$$|k_i| = \left| \frac{\det(x, w_1, \dots, w_{i-1}, w_{i+1}, \dots, w_d)}{\det(w_1, \dots, w_d)} \right| \leq \frac{\|x\| \cdot \|w_1\| \cdot \dots \cdot \|w_d\|}{\|w_1\| \lambda(\mathbb{R}^d | \Gamma)}$$

$$< \frac{R}{\|w_1\|} \cdot 3 d^{3d/2} \leq R n_i d^{3d/2+1}$$

□

Folgerung 8.8. Es sein  $\Gamma \subseteq \mathbb{R}^d$  ein Gitter vom Rang  $d$  und  $B = \prod_{i=1}^d (-a_i, a_i)$   
ein symmetrischer offener Quader. Dann gibt's  $w_1, \dots, w_d \in \Gamma$  und  
 $n_1, \dots, n_d \in \mathbb{N}$  mit

$$\left\{ \sum_{i=1}^d k_i w_i : |k_i| < n_i \right\} \subseteq B \cap \Gamma \subseteq \left\{ \sum_{i=1}^d k_i w_i : |k_i| < d^{\frac{3}{2}(d+1)} n_i \right\}.$$

Beweis. O.B.d.A. sei  $B = (-1, +1)^d$  (sonst benutze eine affine Abb.).

Nach Prop 8.7 gibt's  $w_1, \dots, w_d \in \Gamma$  und  $n_1, \dots, n_d \in \mathbb{N}$  mit

$$\left\{ \sum_{i=1}^d k_i w_i : |k_i| < n_i \right\} \subseteq B_1(0) \cap \Gamma$$

und

$$B_{\sqrt{d}}(0) \cap \Gamma \subseteq \left\{ \sum_{i=1}^d k_i w_i : |k_i| < d^{\frac{3}{2}(d+1)} n_i \right\}.$$

Da  $B_1(0) \subseteq B \subseteq B_{\sqrt{d}}(0)$  sind wir fertig.  $\square$

Prop 8.9. Es sein  $d \geq 2$  und  $P \subseteq \mathbb{Z}^d$  eine GAP, die nicht echt ist.

Dann gibt's GAP  $Q \supseteq P$  vom Rang  $d-1$  mit  $|Q| \leq d^{4d^2+d} |P|$ .

Beweis. O.B.d.A. sei

$$P = \left\{ \sum_{i=1}^d k_i t_i : 0 \leq k_i < N_i \right\}, \text{ wobei } t_1, \dots, t_d \geq 1 \text{ die}$$

Schrittwerte sind und  $N_1, \dots, N_d \geq 2$ . Da  $P$  nicht echt ist, gibt's

$(m_1, \dots, m_d) \in \underbrace{\mathbb{Z}^d}_{\setminus \{0\}}$  mit  $m_1 t_1 + \dots + m_d t_d = 0$  und  $|m_i| < N_i$  für  $i \in [d]$ .

O B d A

- seien  $m_1, \dots, m_d$  teilerfremd
- gelte  $\frac{|m_d|}{N_d} \geq \frac{|m_i|}{n_i}$  für alle  $i \in [d]$
- und sei  $m_d > 0$ .

Setze

$$q = \left( -\frac{m_1}{m_d}, \dots, -\frac{m_{d-1}}{m_d} \right) \in \mathbb{R}^{d-1} \quad \text{und} \quad \Gamma = \mathbb{Z}^{d-1} + q \cdot \mathbb{Z}.$$

Nun ist  $\Gamma$  ein Gitter vom Rang  $d-1$  und

$$f: \Gamma \longrightarrow \mathbb{Z} \quad (n_1, \dots, n_{d-1}) + n_d q \longmapsto \sum_{i=1}^d n_i t_i$$

ist wohldefiniert, denn: Wenn  $(n_1, \dots, n_{d-1}) + n_d q = (n'_1, \dots, n'_{d-1}) + n'_d q$ ,

dann  $n_i - \frac{m_i}{m_d} n_d = n'_i - \frac{m_i}{m_d} n'_d$  für alle  $i \in [d-1]$ , d.h.

$$\sum_{i=1}^{d-1} (n_i - n'_i) t_i = \sum_{i=1}^{d-1} \frac{m_i}{m_d} (n_d - n'_d) t_i = \frac{n_d - n'_d}{m_d} \sum_{i=1}^{d-1} m_i t_i$$

$$= -(n_d - n'_d) t_d.$$

Für den Quader  $B = \prod_{i=1}^{d-1} (-2N_i, 2N_i)$  gilt

$$P \subseteq f[B \cap \Gamma] \subseteq 3P - 3P, \quad (*)$$

denn: Sei  $x \in P$ . Dann schreibe  $x = \sum_{i=1}^d k_i e_i$  mit  $|k_i| < n_i$ .

Nun  $x = f(y)$  für  $y = (k_1, \dots, k_{d-1}) + k_d q \in \Gamma$ .

Für  $i \in [d-1]$  ist die  $i$ -te Koordinate von  $y$  die Zahl

$$k_i - \frac{m_i}{m_d} k_d. \quad \text{Da} \quad \left| k_i - \frac{m_i}{m_d} k_d \right| \leq |k_i| + \left| \frac{m_i k_d}{m_d} \right|$$

$$< N_i + \frac{|m_i|}{m_d |N_d|} \leq N_i + \frac{|m_i|}{|m_i| N_i} = 2N_i$$

ist  $y \in B$ , also  $x \in f[B \cap \Gamma]$ .

Nun sei  $y = (n_1, \dots, n_{d-1}) + n_d q \in B \cap \Gamma$  beliebig.

Wir wollen  $f(y) \in 3P - 3P$  zeigen. O.B.d.A.  $|n_d| \leq \frac{|m_d|}{2} \leq \frac{N_d}{2}$

Für  $i \in [d-1]$  ist nun  $\left| n_i - \frac{m_i}{m_d} n_d \right| < 2N_i$  (nach Dfn von  $B$ )

also  $|k_i| < 2N_i + \left| \frac{m_i}{m_d} n_d \right| \leq 2N_i + \frac{|m_i|}{m_d |N_d|} \leq 2N_i + \frac{|m_i|}{|m_i| N_i} \leq 3N_i.$

Damit ist (\*) gezeigt. Nach Folg. 8.8 gibt's  $w_1, \dots, w_{d-1} \in \Gamma$  und

$M_1, \dots, M_{d-1} \in \mathbb{N}$  mit

$$\left\{ \sum_{i=1}^{d-1} k_i w_i : |k_i| < M_i \right\} \subseteq B \cap \Gamma \subseteq \left\{ \sum_{i=1}^{d-1} k_i w_i : |k_i| < d^{3(d+1)/2} M_i \right\}$$

Folglich

$$\left\{ \sum k_i f(w_i) : |k_i| < M_i \right\} \subseteq f[B \cap \Gamma] \subseteq \left\{ \sum k_i f(w_i) : |k_i| < d^{3(d+1)/2} M_i \right\}$$

Setze  $Q = \left\{ \sum_{i=1}^{d-1} k_i f(w_i) : |k_i| < d^{3(d+1)/2} \right\}$ . Offensiv hat  $Q \subseteq \mathbb{Z}$

Rang  $d-1$  und  $P \subseteq f[B \cap \Gamma] \subseteq Q$ . Zudem

$$|Q| \leq (2 d^{3(d+1)/2})^{d-1} |f[B \cap \Gamma]|$$

$$\leq (2 d^{3(d+1)/2})^{d-1} |3P - 3P|$$

$$\leq 6^d (2 d^{3(d+1)/2})^{d-1} |P|$$

$$\leq d^{4d^2+d} |P|.$$

9

