8. Vorlesung

Wo sind wir ?

Ziel: Satz von Freiman. Sei $A \subseteq \mathbb{Z}$ additive Menge mit $|A+A| \leq K|A|$.
Dann gibt's GAP $P \supseteq A$ mit Rang $\leq d(K)$ und $|P| \leq s(K)|A|$.

Folg. 5.9. Für jede additive Menge $A \subseteq \mathbb{Z}$ gibt's Primzahl $N \leq 32|8A-8A|$ und $A' \subseteq A$, $B \subseteq \mathbb{Z}/N\mathbb{Z}$ mit $|A'| = |B| \geq \frac{1}{8}|A|$, für die $2A'-2A'$, $2B-2B$ F_2-isomorph sind.

Lemma 6.17. Sei $A \subseteq \mathbb{Z}/N\mathbb{Z}$ additive Menge mit $|A| = \delta N$. Dann gibt's $\Gamma \subseteq \widehat{\mathbb{Z}/N\mathbb{Z}}$ mit $|\Gamma| \leq \delta^{-2}$ und $\mathrm{Bohr}(\Gamma, \frac{1}{4}) \subseteq 2A-2A$, wobei

$$\mathrm{Bohr}(\Gamma, \tfrac{1}{4}) = \left\{ x \in \mathbb{Z}/N\mathbb{Z} : \forall \gamma \in \Gamma \quad \left\| \frac{\gamma x}{N} \right\| < \frac{1}{4} \right\}.$$

Plan: Finde "große" GAP $Q \subseteq \mathrm{Bohr}(\Gamma, \frac{1}{4})$ von "kleinem" Rang.
Danach braucht man ein Überdeckungsargument.

Wiederholung zu §7.

Dfn 7.1. Ein Gitter ist eine diskrete Untergruppe $\Gamma \subseteq \mathbb{R}^d$.

Der Rang von Γ ist die Dimension des von Γ erzeugten UVRs von $\mathbb{R}^d$.

Satz 7.3. Für jedes Gitter $\Gamma \subseteq \mathbb{R}^d$ vom Rang k existieren lin. unabh. Vektoren $v_1, \dots, v_k$ mit $\Gamma = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_k$.

Insbesondere ist $\Gamma \cong \mathbb{Z}^k$.

Bem 7.4. In der Algebra lernt man, dass jede endlich erzeugte torsionsfreie abelsche Gruppe zu einem $\mathbb{Z}^k$ isomorph ist. Satz 7.3 folgt also auch daraus, dass Gitter endlich erzeugt sind.

Betrachte Gitter $\Gamma \subseteq \mathbb{R}^d$ vom Rang d. Wird Γ als Gruppe von $v_1, \dots, v_d$ erzeugt, so heißt

$$M = \{ t_1 v_1 + \dots + t_d v_d : 0 \le t_i < 1 \text{ für } i = 1, \dots, d \}$$

eine Fundamentalmasche von Γ. Es gilt dann

$$\lambda(M) = |\det(v_1, \dots, v_d)|$$

und M ist ein Repräsentantensystem von $\mathbb{R}^d / \Gamma$, d.h. $\mathbb{R}^d = \dot{\bigcup}_{v \in \Gamma} M + v$.

Sind nun $w_1, \dots, w_d \in \Gamma$ bel., so ist

$$a = \frac{\det(w_1, \dots, w_d)}{\det(v_1, \dots, v_d)}$$

eine ganze Zahl. Wenn nun $w_1, \dots, w_d$ ein Erzeugendensystem von Γ

mit Fundamentalmasche M' bilden, dann ist auch

$$b = \frac{\det(v_1, \ldots, v_d)}{\det(w_1, \ldots, w_d)} \in \mathbb{Z}.$$

Da $ab = 1$ folgt $a = b = \pm 1$. Folglich

$$\lambda(M') = |\det(w_1, \ldots, w_d)| = |\det(v_1, \ldots, v_d)| = \lambda(M).$$

Also ist es wohldefiniert

$$\lambda(\mathbb{R}^d / \Gamma) = \lambda(M)$$

zu setzen.

<u>Satz 7.5.</u> Sind $\Gamma \subseteq \Gamma' \subseteq \mathbb{R}^d$ Gitter vom Rang d, so gilt

$$\frac{\lambda(\mathbb{R}^d / \Gamma)}{\lambda(\mathbb{R}^d / \Gamma')} = [\Gamma' : \Gamma].$$

Beweis. Induktion nach $[\Gamma' : \Gamma]$.

Anfang. Wenn $[\Gamma' : \Gamma] = 1$ ist $\Gamma' = \Gamma$. Klar.

Schritt. Wenn es ein Gitter Λ mit $\Gamma \subsetneq \Lambda \subsetneq \Gamma'$ gibt folgt aus der Ind. Ann.

$$\frac{\lambda(\mathbb{R}^d/\Gamma)}{\lambda(\mathbb{R}^d/\Gamma')} = \frac{\lambda(\mathbb{R}^d/\Lambda)}{\lambda(\mathbb{R}^d/\Gamma')} \cdot \frac{\lambda(\mathbb{R}^d/\Gamma)}{\lambda(\mathbb{R}^d/\Lambda)} = [\Gamma' : \Lambda] \cdot [\Lambda : \Gamma]$$

$$= [\Gamma' : \Gamma].$$

Ab jetzt gebe es kein solches Gitter Λ. OBdA sei $\Gamma = \mathbb{Z}^d$.

Sei $a \in \Gamma' \setminus \mathbb{Z}^d$. Schreibe $a = (a_1, \dots, a_d)$.

Ann $a \notin \mathbb{Q}^d$.

Sei OBdA $a_1 \notin \mathbb{Q}$. Für $n \in \mathbb{Z}$ sei $\alpha_n \in [0,1]$ die Zahl mit $n a_1 - \alpha_n \in \mathbb{Z}$. Nun ist $\{\alpha_n : n \in \mathbb{Z}\}$ unendlich. Wähle $m, n \in \mathbb{Z}$ mit $m \neq n$ $|\alpha_m - \alpha_n| < \lambda(\mathbb{R}^d/\Gamma')$.

Setze $k = a_1(m-n) - (\alpha_m - \alpha_n) \in \mathbb{Z}$

Nun $\left|\det\left(a(m-n) - ke_1, e_2, \dots, e_d\right)\right| = a_1(m-n) - k = \alpha_m - \alpha_n$

$< \lambda(\mathbb{R}^d / \Gamma')$. Wid.

Sei nun $p \in \mathbb{N}$ minimal mit $p \cdot a \in \mathbb{Z}^d$.

Ann: p nicht prim.

Schreibe $p = r \cdot s$ mit $r, s \geq 2$. Sei Λ das von $\mathbb{Z}^d$, ra erzeugte Gitter. Nun $\Gamma \subseteq \Lambda \subseteq \Gamma'$. Nach Minimalität von p ist $\Gamma \neq \Lambda$.

Also $\Lambda = \Gamma'$, d.h. es gibt $m \in \mathbb{Z}$ mit $a \in m \cdot ra + \mathbb{Z}^d$.

Nun $(mr-1) \cdot a,\ rs \cdot a \in \mathbb{Z}^d$. Da $s = m \cdot rs - s(mr-1)$

folgt $s \cdot a \in \mathbb{Z}^d$ Wid. (zur Minimalität von p).

Nun ist

$$\Gamma' = \{ z + i \cdot a : z \in \mathbb{Z}^d \text{ und } 0 \le i \le p-1 \}$$

das von $\mathbb{Z}^d$, a erzeugte Gitter und $[\Gamma' : \Gamma] = p$.

Es bleibt $\lambda(\mathbb{R}^d / \Gamma') = \frac{1}{p}$ zu zeigen.

O.Bd.A. sei $a_1 \notin \mathbb{Z}$. Schreibe $a_1 = \frac{r}{p}$ mit $r \in \mathbb{Z}$. Wegen $p \nmid r$ gibt's $s, k \in \mathbb{Z}$ mit $rs + pk = 1$. Nun

$$\left| \det \left(\underbrace{s \cdot a + k e_1}_{\in \Gamma'}, e_2, \dots, e_d \right) \right| = \left| \frac{rs}{p} + k \right| = \frac{1}{p}$$

Also genügt z.z. dass Γ' das von $s \cdot a + k e_1, e_2, \dots, e_d$ erzeugte Gitter Δ ist. Nun ist $p(sa + ke_1) \in \Delta \cap \mathbb{Z}^d$ und die erste Koordinate von $p(sa + ke_1)$ ist ± 1. Also $e_1 \in \Delta$, d.h. $\Gamma \subseteq \Delta \subseteq \Gamma'$.

Wegen $s \cdot a \notin \Gamma$ folgt $\Delta = \Gamma'$.

□

Lemma 7.6 (Blichfeldt) Es sei $\Gamma \subseteq \mathbb{R}^d$ ein Gitter vom Rang d und $\mathcal{U} \subseteq \mathbb{R}^d$ eine offene Menge mit $\lambda(\mathcal{U}) > \lambda(\mathbb{R}^d / \Gamma)$. Dann gibt's verschiedene $x, y \in \mathcal{U}$ mit $x - y \in \Gamma$.

Beweis. OBdA $\Gamma = \mathbb{Z}^d$. Da $\lim_{n \to \infty} \lambda(B_n(0) \cap \mathcal{U}) = \lambda(\mathcal{U})$ dürfen wir annehmen, dass $\mathcal{U}$ beschränkt ist. Wähle $R > 0$ mit $\mathcal{U} \subseteq [-R, R]^d$. Sei $N \in \mathbb{N}$. Es gilt

$$\{1, \dots, N\}^d + \mathcal{U} \subseteq [1 - R, N + R]^d.$$

Wenn die Mengen der Form $a + \mathcal{U}$ mit $a \in \{1, \dots, N\}^d$ paarweise disjunkt sind, folgt $N^d \lambda(\mathcal{U}) \leq (N + 2R - 1)^d$, d.h. $\lambda(\mathcal{U}) \leq \left(1 + \frac{2R-1}{N}\right)^d$. Da $\lambda(\mathcal{U}) > 1$ ist dies für große N falsch. Es gibt also $a, b \in \mathbb{Z}^d$ mit $a \neq b$ und $(a + \mathcal{U}) \cap (b + \mathcal{U}) \neq \emptyset$. Wähle $x, y \in \mathcal{U}$ mit $a + x = b + y$. Nun $x - y = b - a \in \mathbb{Z}^d$. $\square$

Satz 7.7. (Minkowskis erster Satz). Es sei $\Gamma \subseteq \mathbb{R}^d$ ein Gitter vom Rang d. Außerdem sei $B \subseteq \mathbb{R}^d$ eine offene konvexe Menge, die bzgl. des Ursprungs symmetrisch ist (d.h. $-B = B$). Wenn $\lambda(B) > 2^d \lambda(\mathbb{R}^d / \Gamma)$, dann gibt's $v \in B \cap \Gamma$ mit $v \neq 0$.

Beweis. Wegen $\lambda(\frac{B}{2}) = \frac{1}{2^d} \lambda(B) > \lambda(\mathbb{R}^d / \Gamma)$ gibt's verschiedene $x, y \in \frac{B}{2}$ mit $x - y \in \Gamma$. Nun $2x, 2y \in B$.

Wegen $-B = B$ ist $-2y \in B$. Da B konvex ist, folgt

$$x - y = \frac{2x + (-2y)}{2} \in B.$$

Also tut's $v = x - y$. □

Dfn 7.8. Sein $\Gamma \subseteq \mathbb{R}^d$ ein Gitter vom Rang k und $U \subseteq \mathbb{R}^d$ eine offene Umgebung von 0. Die Zahlen $\lambda_1 \leq \ldots \leq \lambda_k$ definiert durch

$$\lambda_i = \inf\{\lambda > 0 : \lambda U \text{ enthält } i \text{ lin. unabh. Elemente von } \Gamma\}$$

heißen sukzessiven Minima von U bzgl. Γ.

Satz 7.9 (Minkowskis zweiter Satz)

Es seien $\Gamma \leq \mathbb{R}^d$ ein Gitter vom Rang d, $B \subseteq \mathbb{R}^d$ eine nichtleere, offene, konvexe, symmetrische Menge und $\lambda_1 \leq \dots \leq \lambda_d$ die sukzessiven Minima von B bzgl. Γ.

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

Beobachtung: Wenn $\lambda = \lambda_1 \cdot \dots \cdot \lambda_d$ ist ~~$\left(\frac{\lambda}{2}\right)^d \cdot \lambda(B) < \dots$~~

, ~~λ B~~) $\lambda(\lambda B) \leq 2^d \lambda(\mathbb{R}^d / \Gamma)$ zu zeigen.

Wäre das falsch, gäbe es nach Minkowskis erstem Satz einen Punkt $v \in \lambda B \cap \Gamma$ mit $v \neq 0$. Wid. zur Wahl von λ_1.

Fakt 7.10 Es seien $B \overset{\subseteq \mathbb{R}^d}{\text{eine}}$ konvexe offene Menge, $V \subseteq \mathbb{R}^d$ ein k-dim. UVR und $\vartheta \in (0,1]$. Dann gibt's zu jeder offenen Menge $A \subseteq B$ eine offene Menge $A' \subseteq B$ mit $\lambda(A') = \vartheta^k \lambda(A)$ und

$$(A'-A')\cap V = r(A-A)\cap V.$$

Beweis. OBdA $V = \mathbb{R}^k \times \{0\}$. Sei $\pi: \mathbb{R}^d \to \mathbb{R}^{d-k}$ die Projektion auf die letzten $d-k$ Koordinaten.

Wähle eine stetige Abb. $f: \pi[B] \to \mathbb{R}^k$ mit

$(f(y), y) \in B$ für alle $y \in \pi[B]$.

[Warum gibt es f? Z.B. könnte $f(y)$ der Schwerpunkt von $\{x \in \mathbb{R}^k : (x,y) \in B\}$ sein.]

Sei $\Phi: B \to \mathbb{R}^d$ die Abb. $(x,y) \mapsto (rx + (1-r)f(y), y)$.

Wegen $\Phi(x,y) = r\cdot\underbrace{(x,y)}_{B} + (1-r)\underbrace{(f(y),y)}_{\in B}$ ist $\Phi[B] \subseteq B$.

Ist nun eine offene Menge $A \subseteq B$ gegeben, so setzen wir $A' = \Phi[A]$.