9. Vorlesung.

Es sei nun $A \subseteq B$ offen und $A' = \Phi[A]$.

Da f stetig ist, ist A' offen (!) Außerdem ist

$$\lambda(A') = \vartheta^k \lambda(A),$$

denn: Schreibe $\lambda(A) = \int_{\mathbb{R}^{d-k}} \lambda(A_y)\, dy$, wobei $A_y = \{x \in \mathbb{R}^k : (x,y) \in A\}$,

und analog für A'. Da

$$A'_y = \vartheta A_y + (1-\vartheta) f(y)$$

gilt $\lambda(A'_y) = \vartheta^k \lambda(A_y)$ für alle $y \in \mathbb{R}^{d-k}$, also in der Tat

$$\lambda(A') = \int_{\mathbb{R}^{d-k}} \lambda(A'_y)\, dy = \vartheta^k \int_{\mathbb{R}^{d-k}} \lambda(A_y)\, dy = \vartheta^k \lambda(A).$$

Außerdem ist

$$(A' - A') \cap V = \{ [\vartheta x_1 + (1-\vartheta) f(y_1)] - [\vartheta x_2 + (1-\vartheta) f(y_2)] : (x_1,y_1), (x_2,y_2) \in A \text{ und } y_1 = y_2 \}$$

$$= \{ \vartheta (x_1 - x_2) : (x_1,y_1), (x_2,y_2) \in A \ \& \ y_1 = y_2 \}$$

$$= \vartheta (A - A) \cap V. \qquad \square$$

Beweis von Satz 7.9. Definiere linear unabhängige $v_1, \ldots, v_d \in \Gamma$ folgendermaßen: Wenn $1 \leq i \leq d$ und $v_1, \ldots, v_{i-1}$ schon gewählt sind, dann wähle $v_i \in \overline{\lambda_i B} \cap \Gamma$ von $v_1, \ldots, v_{i-1}$ lin. unabh.

[Warum geht das? Für alle $n \in \mathbb{N}$ gibt's Kandidaten

$$v_i^n \in \left(\lambda_i + \tfrac{1}{n}\right) B \cap \Gamma .$$

Da B beschränkt ist und Γ diskret ist, ist $\{v_i^n : n \in \mathbb{N}\}$ endlich. Also gibt's $v \in \Gamma$ derart, dass $\{n \in \mathbb{N} : v_i^n = v\}$ unendlich ist. Nun tut's $v_i = v$.]

Der von $v_1, \ldots, v_i$ erzeugte UVR von $\mathbb{R}^d$ heiße V_i. Es gilt $\lambda_i B \cap V_{i+1} \subseteq V_i$ für alle $i \in [d-1]$. Setze

$$A_0 = \frac{\lambda_d}{2} B$$

und konstruiere offene Mengen $A_1, \dots, A_{d-1} \subseteq A_0$ rekursiv folgendermaßen. Wenn A_{i-1} für $i \in [d-1]$ bereits konstruiert ist, wende Fakt 3.10 auf

$$A_{i-1}, \quad A_0, \quad \lambda_i / \lambda_{i+1}, \quad V_i$$

statt

$$A, \quad B, \quad \vartheta, \quad V$$

an. Dies liefert $A_i \subseteq A_0$ mit

$$\lambda(A_i) = \left(\frac{\lambda_i}{\lambda_{i+1}}\right)^i \lambda(A_{i-1}) \quad \text{und} \quad (A_i - A_i) \cap V_i = \frac{\lambda_i}{\lambda_{i+1}} (A_{i-1} \cap A_{i-1}) \cap V_i.$$

Nun ist

$$\lambda(A_{d-1}) = \lambda(A_0) \prod_{i=1}^{d-1} \frac{\lambda(A_i)}{\lambda(A_{i-1})} = \left(\frac{\lambda_d}{2}\right)^d \lambda(B) \prod_{i=1}^{d-1} \left(\frac{\lambda_i}{\lambda_{i+1}}\right)^i$$

$$= \frac{\lambda_1 \cdot \ldots \cdot \lambda_d \cdot \lambda(B)}{2^d}.$$

Wir müssen also $\lambda(A_{d-1}) \leq \lambda(\mathbb{R}^d / \Gamma)$ zeigen. Andernfalls gäbe es nach Lemma von Blichfeldt verschiedene $x, y \in A_{d-1}$ mit $x - y \in \Gamma$.

Wähle i minimal mit

$$(A_{d-1} - A_{d-1}) \cap V_i \cap \Gamma \neq \{0\}.$$

Nun

$$\begin{aligned}(A_{d-1} - A_{d-1}) \cap V_i &= \frac{\lambda_{d-1}}{\lambda_d} (A_{d-2} - A_{d-2}) \cap V_i \\ &= \frac{\lambda_{d-2}}{\lambda_d} (A_{d-3} - A_{d-3}) \cap V_i \\ &= \ldots = \frac{\lambda_i}{\lambda_d} (A_{i-1} - A_{i-1}) \cap V_i \\ &\subseteq \frac{\lambda_i}{\lambda_d} (A_0 - A_0) \cap V_i = \lambda_i B \cap V_i \subseteq V_{i-1},\end{aligned}$$

im Widerspruch zur Minimalität von i. $\square$

Satz 7.11. (Ruzsa) Es sei N eine Primzahl und $\Gamma \subseteq \widehat{\mathbb{Z}/N\mathbb{Z}} \setminus \{0\}$ sei nicht leer. Ist $\varepsilon \in (0, \frac{1}{2})$, so gibt's eine echte GAP $P \subseteq \mathrm{Bohr}(\Gamma, \varepsilon)$ mit $|P| \geq \left(\frac{\varepsilon}{|\Gamma|}\right)^{|\Gamma|} N$.

Beweis. Wir identifizieren $\widehat{\mathbb{Z}/N\mathbb{Z}}$ in der üblichen Weise mit $\mathbb{Z}/N\mathbb{Z}$. Schreibe $\Gamma = \{u_1, \dots, u_k\}$, wobei $k = |\Gamma|$. Es sei $\Lambda \subseteq \mathbb{R}^k$ das von $\mathbb{Z}^k$ und $\frac{1}{N}(u_1, \dots, u_k)$ erzeugte Gitter. Da $[\Lambda : \mathbb{Z}^k] = N$ ist nach Satz 7.5

$$\lambda(\mathbb{R}^k / \Lambda) = \frac{1}{N}.$$

Es seien $\lambda_1, \dots, \lambda_k$ die sukzessiven Minima von $B = (-1, +1)^k$ bzgl. Λ.

Minkowskis zweiter Satz impliziert

$$\lambda_1 \cdot \ldots \cdot \lambda_k \leq \frac{2^k \lambda(\mathbb{R}^k / \Lambda)}{\lambda(B)} = \lambda(\mathbb{R}^k / \Lambda) = \frac{1}{N}.$$

Wie im Beweis von Satz 7.9 gibt's lin. unabh. $v_1, \dots, v_k \in \Gamma$ mit $v_i \in \overline{\lambda_i B}$, d.h. $\|v_i\|_\infty \le \lambda_i$. Für alle $i \in [k]$ sei d_i eine ganze Zahl mit

$$v_i \in \frac{d_i}{N}(u_1, \dots, u_k) + \mathbb{Z}^k$$

und

$$l_i = \left\lceil \frac{\varepsilon}{k\lambda_i} \right\rceil - 1.$$

Wir zeigen, dass die GAP

$$P = \{ d_1 x_1 + \dots + d_k x_k : |x_i| \le l_i \text{ für alle } i \in [k] \}$$

wie gewünscht ist.

Warum $P \subseteq \mathrm{Bohr}(\Gamma, \varepsilon)$? Seien $x = \sum_{i=1}^{k} d_i x_i$ und $u_j \in \Gamma$ beliebig.

Zu zeigen ist $\left\| \frac{x u_j}{N} \right\| < \varepsilon$. In der j-ten Koordinate von $\|v_i\|_\infty \le \lambda_i$ steht $\left\| \frac{d_i u_j}{N} \right\| \le \lambda_i$. Also

$$\left\| \frac{x u_j}{N} \right\| \le \sum_{i=1}^{k} \left\| \frac{d_i x_i u_j}{N} \right\| \le \sum_{i=1}^{k} |x_i| \left\| \frac{d_i u_j}{N} \right\| \le \sum_{i=1}^{k} l_i \lambda_i < k \cdot \frac{\varepsilon}{k} = \varepsilon.$$

Warum ist P echt? Es sei $\sum_{i=1}^{k} d_i x_i = \sum_{i=1}^{k} d_i y_i$ mit $|x_i|, |y_i| \leq \ell_i$.

Setze $z_i = x_i - y_i$. Dann $\sum_{i=1}^{k} d_i z_i = 0$ und $|z_i| \leq 2\ell_i$ für alle $i \in [k]$.

Setze $v = \sum_{i=1}^{k} z_i v_i$. Nach Definition der d_i ist

$$v \in \left(\sum_{i=1}^{k} \frac{z_i d_i}{N} \right) (u_1, \dots, u_k) + \mathbb{Z}^k = \mathbb{Z}^k .$$

Andererseits ist

$$\|v\|_\infty \leq \sum_{i=1}^{k} |z_i| \|v_i\|_\infty \leq \sum_{i=1}^{k} 2 \ell_i \lambda_i < 2\varepsilon < 1 .$$

Also $v = 0$ und da $v_1, \dots, v_k$ lin. unabh. sind folgt $z_1 = \dots = z_k = 0$, wie gewünscht.

Schließlich $|P| = \prod_{i=1}^{k} (2\ell_i + 1) = \prod_{i=1}^{k} \left(2 \left\lceil \frac{\varepsilon}{k\lambda_i} \right\rceil - 1 \right) \geq \prod_{i=1}^{k} \frac{\varepsilon}{k\lambda_i}$

$$\geq \left(\frac{\varepsilon}{k}\right)^k N .$$

$\square$