7 Vorlesung. Wiederholung.

Dfn. $\hat{G} = \mathrm{Hom}(G, S^1)$

Fakt. $\hat{G} \cong G$

Orthogonalität

$$\forall r \in \hat{G} \qquad \sum_{x \in G} r(x) = \begin{cases} |G| & \text{wenn } r \text{ neutral} \\ 0 & \text{sonst} \end{cases}$$

$$\forall x \in G \qquad \sum_{r \in \hat{G}} r(x) = \begin{cases} |G| & \text{wenn } x = 0 \\ 0 & \text{sonst} \end{cases}$$

Fouriertransformation Für $f: G \longrightarrow \mathbb{C}$ ist $\hat{f}: \hat{G} \longrightarrow \mathbb{C}$ definiert durch

$$\hat{f}(r) = \sum_{x \in G} f(x) \overline{r(x)}.$$

Inversionsformel

$$f(x) = \frac{1}{|G|} \sum_{r \in \hat{G}} \hat{f}(r)\, r(x).$$

Bem 6.10. Die Fouriertransformation ist also ein Vektorraumisomorphismus von $\mathbb{C}^G$ nach $\mathbb{C}^{\hat{G}}$. Auf $\mathbb{C}^G$ hat man das Standardskalarprodukt

$$\langle f, g \rangle = \sum_{x \in G} f(x) \cdot \overline{g(x)}$$

Es transformiert sich wie folgt:

Lemma 6.11. Für je zwei Funktionen $f, g : G \longrightarrow \mathbb{C}$ gilt

$$\sum_{x \in G} f(x) \overline{g(x)} = \frac{1}{|G|} \sum_{r \in \hat{G}} \hat{f}(r) \overline{\hat{g}(r)} \quad \text{(Satz von Plancherel)}$$

Insbesondere

$$\sum_{x \in G} |f(x)|^2 = \frac{1}{|G|} \sum_{r \in \hat{G}} |\hat{f}(r)|^2 \quad \text{(Formel von Parseval)}.$$

Beweis.

$$\sum_{r \in \hat{G}} \hat{f}(r) \overline{\hat{g}(r)} = \sum_{r \in \hat{G}} \sum_{x \in G} f(x) \overline{r(x)} \cdot \sum_{y \in G} \overline{g(y)}\, r(y)$$

$$= \sum_{x,y \in G} f(x) \cdot \overline{g(y)} \underbrace{\sum_{r \in \hat{G}} r(y-x)}_{= 0 \text{ außer wenn } x=y} = |G| \sum_{x \in G} f(x) \overline{g(x)}.$$

□

Dfn 6.12. Die Faltung (Konvolution) zweier Funktionen $f, g : G \longrightarrow \mathbb{C}$ ist die Funktion

$$f * g : G \longrightarrow \mathbb{C} \qquad x \longmapsto \sum_{y+z=x} f(y)\, g(z)$$

Bem 6.13. Offenbar ist die Faltung kommutativ. Sie ist auch assoziativ, denn: Für $f, g, h : G \longrightarrow \mathbb{C}$ ist $(f * g) * h = f * (g * h)$ die Funktion

$$z \longmapsto \sum_{x=u+v+w} f(u)\, g(v)\, h(w).$$

Wir identifizieren additive Mengen $A \subseteq G$ mit ihren charakteristischen Funktionen, d.h.

$$A(x) = \begin{cases} 1 & \text{wenn } x \in A \\ 0 & \text{wenn } x \in G \setminus A \end{cases}.$$

Offenbar ist $A * B = r_{A+B}$ (siehe Dfn 1.9)

Lemma 6.14. Für je zwei Funktionen $f, g : G \longrightarrow \mathbb{C}$ gilt

$$\widehat{f * g} = \hat{f} \cdot \hat{g}$$

Beweis.

$$\widehat{f*g}(r) = \sum_{x \in G} (f*g)(x) \cdot \overline{r(x)}$$

$$= \sum_{x \in G} \sum_{y+z=x} f(y)\, g(z)\, \overline{r(y+z)}$$

$$= \sum_{y,z} f(y)\, g(z)\, \overline{r(y)}\, \overline{r(z)}$$

$$= \sum_{y} f(y)\, \overline{r(y)} \cdot \sum_{z} g(z)\, \overline{r(z)}$$

$$= \hat{f}(r) \cdot \hat{g}(r)$$

□

. . . . . .

Lemma 6.15. Sei $A \subseteq G$ eine additive Menge. Für jedes $x \in G$ ist

$$r_{2A-2A}(x) = \frac{1}{|G|} \sum_{\gamma \in \widehat{G}} |\widehat{A}(\gamma)|^4 \gamma(x)$$

Insbesondere ist

$$E(A) = \frac{1}{|G|} \sum_{\gamma \in \widehat{G}} |\widehat{A}(\gamma)|^4 .$$

Beweis. Schreibe $B = -A$ und beachte

$$\widehat{B}(\gamma) = \sum_{x \in G} B(x) \overline{\gamma(x)} = \sum_{x \in G} B(-x) \overline{\gamma(-x)}$$

$$= \sum_{x \in G} A(x) \gamma(x) = \overline{\widehat{A}(\gamma)} .$$

Somit $\widehat{r_{2A-2A}} = \widehat{r_{2A+2B}} = \widehat{A * A * B * B} = \widehat{A} \cdot \widehat{A} \cdot \widehat{B} \cdot \widehat{B} = |\widehat{A}|^4$.

Nach Lemma 6.9 folgt

$$r_{2A-2A}(x) = \frac{1}{|G|} \sum_{\gamma \in \widehat{G}} |\widehat{A}(\gamma)|^4 \gamma(x) .$$

Insbesondere ergibt sich für $x = 0$

$$E(A) = r_{2A-2A}(0) = \frac{1}{|G|} \sum_{r \in \hat{G}} |\hat{A}(r)|^4 .$$

□

Ab jetzt arbeiten wir mit $G = \mathbb{Z}/N\mathbb{Z}$. Wir identifizieren $\hat{G} = \mathbb{Z}/N\mathbb{Z}$ so, dass die Fouriertransformation

$$r(x) = e^{2\pi i \cdot rx/N}$$

ist. Für $\xi \in \mathbb{R}/\mathbb{Z}$ setzen wir

$$\|\xi\| = \min\{|\xi - z| : z \in \mathbb{Z}\}.$$

Dfn 6.16. Für $\varepsilon > 0$ und $\Gamma \subseteq \widehat{\mathbb{Z}/N\mathbb{Z}}$ heißt

$$\mathrm{Bohr}(\Gamma, \varepsilon) = \left\{ x \in \mathbb{Z}/N\mathbb{Z} : \forall r \in \Gamma \ \left\| \frac{rx}{N} \right\| < \varepsilon \right\}$$

eine Bohrmenge mit Radius ε.

Lemma 6.17. (Bogulybasov, Ruzsa). Es sei $A \subseteq \mathbb{Z}/N\mathbb{Z}$ eine additive Menge. Wenn $|A| = \delta N$, dann gibt's eine $\Gamma \subseteq \widehat{\mathbb{Z}/N\mathbb{Z}}$ der Größe $|\Gamma| \leq \delta^{-2}$ mit

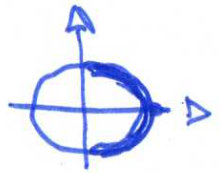
$$\mathrm{Bohr}(\Gamma, \tfrac{1}{4}) \subseteq 2A - 2A .$$

Beweis. Setze $G = \mathbb{Z}/N\mathbb{Z}$ und

$$\Gamma = \{ r \in \widehat{G} : |\hat{A}(r)| \geq \delta^{3/2} N \}.$$

Parseval's Formel lautet

$$\sum_{r \in \widehat{G}} |\hat{A}(r)|^2 = N \sum_{x \in G} |A(x)|^2 = N|A| = \delta N^2 .$$



Also ist $|\Gamma| \delta^3 N^2 \leq \delta N^2$, d.h. $|\Gamma| \leq \delta^{-2}$.

Sei nun $x \in \mathrm{Bohr}(\Gamma, \frac{1}{4})$. Für alle $r \in \Gamma$ ist $\| \frac{rx}{N} \| < \frac{1}{4}$,

also $\mathrm{Re}(e^{2\pi i rx/N}) > 0$.

Somit

$$r_{2A-2A}(x) = \sum_{r \in \hat{G}} |\hat{A}(r)|^4 \operatorname{Re}(r(x)) \qquad \text{(nach Lemma 6.16)}$$

$$= \underbrace{|\hat{A}(0)|^4}_{= \delta^4 N^4} + \underbrace{\sum_{r \in \Gamma \setminus \{0\}} |\hat{A}(r)|^4 \operatorname{Re}(r(x))}_{> 0} + \sum_{r \in \hat{G} \setminus \Gamma} |\hat{A}(r)|^4 \operatorname{Re}(r(x))$$

$$\geq \delta^4 N^4 - \sum_{r \in \hat{G} \setminus \Gamma} |\hat{A}(r)|^4$$

$$\geqslant \delta^4 N^4 - \delta^3 N^2 \cdot \sum_{r \in \hat{G} \setminus \Gamma} |\hat{A}(r)|^2$$

$$> \delta^4 N^4 - \delta^3 N^2 \cdot \delta N^2 = 0.$$

□

§ 7. Additive Geometrie.

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

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

Beispiele 7.2 $\Gamma = \{0\}$ ist das einzige Gitter vom Rang 0.

$\mathbb{Z}^d$ ist ein Gitter vom Rang d.

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

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

Beweis. Sei zunächst $k = d$. Wähle $\varepsilon > 0$ mit $B_{2\varepsilon}(0) \cap \Gamma = \{0\}$.

Beh. Sind $v_1, \dots, v_d \in \Gamma$ lin. unabh., dann ist

$$|\det(v_1, \dots, v_d)| \geq \lambda(B_\varepsilon(0)),$$

wobei λ das d-dim. Lebesgue Maß ist.

Warum? Setze

$$M = \left\{ \sum_{i=1}^{d} t_i v_i : 0 \le t_i < 1 \text{ für } i = 1, \dots, d \right\}.$$

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

Für $z = (z_1, \dots, z_k) \in \mathbb{Z}^k$ setze $M(z) = M + \sum_{i=1}^{d} z_i v_i$.

Da $v_1, \dots, v_d$ eine Basis des $\mathbb{R}^d$ ist, ist

$$\mathbb{R}^d = \dot{\bigcup_{z \in \mathbb{Z}^k}} M(z).$$

Somit ist

$$\lambda(B_\varepsilon(0)) = \sum_{z \in \mathbb{Z}^k} \lambda(B_\varepsilon(0) \cap M(z)) = \sum_{z \in \mathbb{Z}^k} \lambda(A_z),$$

wobei $A_z = (B_\varepsilon(0) \cap M(z)) - \sum_{i=1}^{d} z_i v_i \subseteq M$.

Es gilt

$$\eta \neq \zeta \Rightarrow A_\eta \cap A_\zeta = \emptyset,$$

denn: Angenommen $x \in A_\eta \cap A_\zeta$. Dann gibt's $y, z \in \Gamma$ mit $y \neq z$ und $x+y,\ x+z \in B_\varepsilon(0)$. Nun

$$\|y-z\| \leq \|x+y\| + \|x+z\| < 2\varepsilon, \text{ also}$$

$$y-z \in B_{2\varepsilon}(0) \cap \Gamma, \quad \underline{\text{Wid.}}$$

Also $\lambda(B_\varepsilon(0)) \leq \lambda(M) = |\det(v_1, \ldots, v_d)|$.

Sei nun k die kleinste ganze Zahl, für die es lin. unabh. Vektoren $v_1, \ldots, v_d \in \Gamma$ gibt mit

$$|\det(v_1, \ldots, v_d)| \leq 2^k \lambda(B_\varepsilon(0)).$$

Wir wissen $k \geq 0$, d.h. k existiert. Nun ist

$$\Gamma = \mathbb{Z} v_1 \oplus \cdots \oplus \mathbb{Z} v_d.$$

Andernfalls gäbe es

$$v \in \Gamma \setminus (\mathbb{Z} v_1 \oplus \dots \oplus \mathbb{Z} v_d).$$

Da $v_1, \dots, v_d$ Basis des $\mathbb{R}^d$ ist, gibt's $t_1, \dots, t_d \in \mathbb{R}$ mit

$v = \sum_{i=1}^{d} t_i v_i$. O.Bd.A. ist $t_1 \notin \mathbb{Z}$. Wir dürfen sogar $0 < t_1 < 1$ annehmen. Da man statt v auch $v_1 - v$ nehmen könnte dürfen wir sogar $0 < t_1 \leq \frac{1}{2}$ annehmen. Nach Minimalität von K ist

$$2^{k-1} \lambda(B_\varepsilon(0)) < |\det(v_1, v_2, \dots, v_d)| = t_1 |\det(v_1, \dots, v_d)|$$

$$\leq \frac{1}{2} \cdot 2^k \lambda(B_\varepsilon(0)), \quad \text{Widerspruch.}$$

Für den allgemeinen Fall wende man den Spezialfall $k = d$ auf den von Γ erzeugten $\mathbb{R}$-UVR von $\mathbb{R}^d$ an.

□