§5. Freiman-Homomorphismen.

Dfn 5.1. Es seien A, B additive Mengen in eventuell verschiedenen umgebenden Gruppen und $r \geq 2$. Eine Abb. $\varphi: A \longrightarrow B$ heißt **Freiman-Homomorphismus der Ordnung r** (F_r-Homomorphismus) wenn für alle $a_1, \ldots, a_r, a_1', \ldots, a_r' \in A$ mit

$$a_1 + \ldots + a_r = a_1' + \ldots + a_r'$$

auch $\varphi(a_1) + \ldots + \varphi(a_r) = \varphi(a_1') + \ldots + \varphi(a_r')$ gilt.

Man nennt φ einen **F_r-Isomorphismus**, wenn φ bijektiv ist und φ, φ^{-1} F_r-Homom. sind.

Bem 5.2 (1) Additive Mengen und F_r-Homom. bilden eine Kategorie.

(2) "F_r-isomorph sein" ist Äqu.relation

(3) Für $r \geq r' \geq 2$ sind alle F_r-Homom. auch $F_{r'}$-Homom.

Beispiele 5.3. (1) Gruppenhomomorphismen sind F_r-Homom. f. alle $r \geq 2$

(2) Verschiebungen $x \longmapsto x + t$ sind F_r-Isom. für alle $r \geq 2$.

(3) Sein $m, n \in \mathbb{N}$ und $r \geq 2$.

Dann ist $i \longmapsto i + m\mathbb{Z}$ ein F_r-Homom von $[n] (\subseteq \mathbb{Z})$ nach $\{ i \in m\mathbb{Z} : i \in [n] \} \subseteq (\mathbb{Z}/m\mathbb{Z})$. Falls $m \geq r \cdot n$ ist dies sogar ein F_r-Isomorphismus.

(4) Sein $M, d \geq 1$, $r \geq 2$ und $N \geq Mr$. Dann definiert

$$\varphi(m_1, \ldots, m_d) = \sum_{i=1}^{d} m_i N^{i-1}$$

$[M]^d$

einen F_r-Isom. zwischen $[M]^d$ und einer Teilmenge von $\mathbb{Z}$.

Lemma 5.4. Es seien P eine GAP und $\varphi : P \longrightarrow B$ ein F_2-Homomorphismus. Dann ist $\varphi[P]$ eine GAP mit gleichem Rang und gleicher Länge wie P. Wenn φ ein F_2-Isom ist und P echt, dann ist auch $\varphi[P]$ echt.

Beweis. ~~Setze~~ Schreibe

$$P = \{a + k_1 d_1 + \dots + k_r d_r : 0 \le k_i < m_i \text{ für } i \in [r]\}.$$

Setze $\varphi(a) = a'$ und $d_i' = \varphi(a + d_i) - \varphi(a)$ für alle $i \in [r]$.

Dann gilt

$$\varphi(a + k_1 d_1 + \dots + k_r d_r) = a' + k_1 d_1' + \dots + k_r d_r'$$

für alle $k_1, \dots, k_r \in \mathbb{N}_0$.

[Warum? Induktion nach $k = k_1 + \dots + k_r$. Der Fall $k = 0$ ist klar. Sei nun $k \ge 1$. Wähle $j \in [r]$ mit $k_j \ge 1$.

Sehe $z = a + k_1 d_1 + \dots + k_r d_r$ und $z' = a' + \overset{k_i}{d_i'} + \dots + k_r d_r'$.

Wegen

$$a + z = (a + d_j) + (z - d_j)$$

ist

$$\varphi(a) + \varphi(z) = \varphi(a + d_j) + \varphi(z - d_j).$$

Nach Ind. Ann ist $\varphi(z - d_j) = z' - d_j'$. Also

$$\varphi(z) = \underbrace{\left(\varphi(a + d_j) - \varphi(a)\right)}_{= d_j'} + \left(z' - d_j'\right) = z'. \quad]$$

Somit

$$\varphi[P] = \left\{ a' + k_1 d_1' + \dots + k_r d_r' : 0 \le k_i < m_i \text{ für } i \in [r] \right\}.$$

Dies ist eine GAP vom Rang r mit Länge $(m_1, \dots, m_d)$.

Wenn P echt ist und φ ein F_2-Isom., dann ist φ bijektiv,

also $|\varphi[P]| = |P|$, d.h. $\varphi[P]$ ist auch echt. □

Lemma 5.5. Sei $\varphi : A \to B$ ein surjektiver F_r-Homomorphismus.

Dann gilt

$$|\varepsilon_1 \varphi[A_1] + \dots + \varepsilon_r \varphi[A_r]| \leq |\varepsilon_1 A_1 + \dots + \varepsilon_r A_r|$$

für alle nicht-leeren $A_1, \dots, A_r$ und $\varepsilon_1, \dots, \varepsilon_r \in \{+1, -1\}$

Insbesondere

$$|mB - nB| \leq |mA - nA|$$

für alle m, n mit $m+n \leq r$.

Beweis. Definiere äqu. Rel. $\equiv$ auf $A_1 \times \dots \times A_r$ durch

$$(a_1, \dots, a_r) \equiv (a_1', \dots, a_r') \iff \varepsilon_1 a_1 + \dots + \varepsilon_r a_r = \varepsilon_1 a_1' + \dots + \varepsilon_r a_r'.$$

Dann ist $|\varepsilon_1 A_1 + \dots + \varepsilon_r A_r| = |A_1 \times \dots \times A_r / \equiv|$.

Es genügt z.z. dass aus

$(a_1, \dots, a_r) \equiv (a_1', \dots, a_r')$ stets $\sum_i \varepsilon_i \varphi(a_i) = \sum \varepsilon_i \varphi(a_i')$

folgt.

Sehe dann $X = \{i \in [r] : \varepsilon_i = +1\}$ und $Y = [r] \setminus X$.

Nun

$$(a_1, \dots, a_r) \equiv (a_1', \dots, a_r')$$

$$\Rightarrow \sum_{i \in X} a_i - \sum_{i \in Y} a_i = \sum_{i \in X} a_i' - \sum_{i \in Y} a_i'$$

$$\Rightarrow \sum_{i \in X} a_i + \sum_{i \in Y} a_i' = \sum_{i \in X} a_i' + \sum_{i \in Y} a_i$$

φ ist F_r-Homom

$$\Rightarrow \sum_{i \in X} \varphi(a_i) + \sum_{i \in Y} \varphi(a_i') = \sum_{i \in X} a_i' + \sum_{i \in Y} \varphi(a_i)$$

$$\Rightarrow \sum_{i \in [r]} \varepsilon_i \varphi(a_i) = \sum_{i \in [r]} \varepsilon_i \varphi(a_i')$$

□

Lemma 5.6. Seien $m, n \geq 1$, $r \geq 2$ natürliche Zahlen und A, B zwei $F_{r(m+n)}$-isomorphe Mengen. Dann sind $mA - nA$, $mB - nB$ F_r-isomorph.

Beweis. Sei $\varphi : A \longrightarrow B$ ein $F_{\tau(m+n)}$ - Isomorphismus.

Definiere $\psi : mA - nA \longrightarrow mB - nB$ folgendermaßen.

Ist $z \in mA - nA$ gegeben, so schreibe $z = a_1 + \dots + a_m - a_{m+1} - \dots - a_{m+n}$

und setze $\psi(z) = \varphi(a_1) + \dots + \varphi(a_m) - \varphi(a_{m+1}) - \dots - \varphi(a_{m+n})$

Dies ist wohldefiniert, denn:

$$a_1 + \dots + a_m - a_{m+1} - \dots - a_{m+n} = a_1' + \dots + a_m' - a_{m+1}' - \dots - a_{m+n}'$$

$$\Rightarrow a_1 + \dots + a_m + a_{m+1}' + \dots + a_{m+n}' = a_1' + \dots + a_m' + a_{m+1} + \dots + a_{m+n}$$

φ ist F_{m+n}-Isom.

$$\Rightarrow \varphi(a_1) + \dots + \varphi(a_m) + \varphi(a_{m+1}') + \dots + \varphi(a_{m+n}')$$

$$= \varphi(a_1') + \dots + \varphi(a_m') + \varphi(a_{m+1}) + \dots + \varphi(a_{m+n})$$

$$\Rightarrow \varphi(a_1) + \dots + \varphi(a_m) - \varphi(a_{m+1}) - \dots - \varphi(a_{m+n})$$

$$= \varphi(a_1') + \dots + \varphi(a_m') - \varphi(a_{m+1}') - \dots - \varphi(a_{m+n}').$$

Da man analog eine Umkehrabb. von φ definieren kann, genügt z.z. dass φ ein F_r-Homom. ist.

Seien dann $x_1, \dots, x_r, x_1', \dots, x_r' \in mA - nA$.

Schreibe $x_i = \sum_j a_{ij} - \sum_k a_{ik}$, $x_i' = \sum_j a_{ij}' - \sum_k a_{ik}'$,

wobei j immer $[m]$ und k immer $[m+1, m+n]$ durchläuft.

Nun $$\sum_{ij} a_{ij} - \sum_{ik} a_{ik} = \sum_{ij} a_{ij}' - \sum_{ik} a_{ik}'.$$

Also $$\sum_{ij} \varphi(a_{ij}) - \sum_{ik} \varphi(a_{ik}) = \sum_{ij} \varphi(a_{ij}') - \sum_{ik} \varphi(a_{ik}'),$$

d.h. $$\sum_i \varphi(x_i) = \sum \varphi(x_i').$$

□

Proposition 5.7 (Ruzsa). Es sei p eine Primzahl, $r \geq 2$ und $A \subseteq \mathbb{Z}/p\mathbb{Z}$ eine additive Menge. Für jede nat. Zahl N mit

$$2r\,|rA - rA| < N < p$$

existiert eine Teilmenge $A' \subseteq A$ mit $|A'| \geq |A|/r$, die F_r-isomorph zu einer Teilmenge von $\mathbb{Z}/N\mathbb{Z}$ ist.

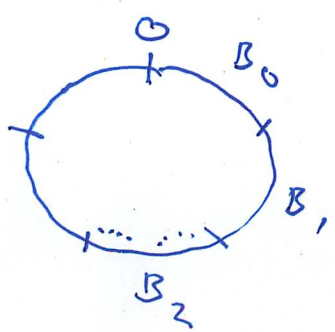
Beweis. Definiere $\pi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$ durch

$$\pi(i + p\mathbb{Z}) = i + N\mathbb{Z} \quad \text{für } i = 0, 1, \ldots, p-1.$$

Partitioniere $\mathbb{Z}/p\mathbb{Z} = B_0 \dot\cup \ldots \dot\cup B_{r-1}$,

$$B_s = \left\{ i + p\mathbb{Z} : \frac{sp}{r} \leq i < \frac{(s+1)p}{r} \right\} \quad \text{für } 0 \leq s \leq r-1$$

Die Einschränkungen von π auf $B_0, \ldots, B_{r-1}$ sind F_r-Homomorphismen.



[Warum? Sei $s \in [0, r-1]$. Betrachte $i_1, \ldots, i_r, i_1', \ldots, i_r' \in \left[\frac{sp}{r}, \frac{(s+1)p}{r}\right)$

deren Restklassen B_s angehören, und die

$$i_1 + \ldots + i_r \equiv i_1' + \ldots + i_r' \pmod{p}$$

erfüllen. Wegen

$$sp \leq i_1 + \ldots + i_r,\ i_1' + \ldots + i_r' < (s+1)p$$

gilt sogar

$$i_1 + \ldots + i_r = i_1' + \ldots + i_r'.$$

Folglich

$$\pi(i_1 + p\mathbb{Z}) + \ldots + \pi(i_r + p\mathbb{Z})$$

$$= (i_1 + \ldots + i_r) + N\mathbb{Z}$$

$$= (i_1' + \ldots + i_r') + N\mathbb{Z}$$

$$= \pi(i_1' + p\mathbb{Z}) + \ldots + \pi(i_r' + p\mathbb{Z}). \quad]$$

Ist nun $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$, so gibt es $s \in [0, r-1)$ mit $|\lambda A \cap B_s| \geq \frac{|A|}{r}$.

Die Menge $A' = A \cap \lambda^{-1} B_s$ erfüllt dann $|A'| \geq \frac{|A|}{r}$ und

$\varphi : A' \longrightarrow \mathbb{Z}/N\mathbb{Z}$, $a \longmapsto \pi(\lambda a)$ ist F_r-Homomorphismus.

Wir zeigen, dass es $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$ gibt, so dass φ ein F_r-Isom. ist.

Dies kann nur so schiefgehen, dass es $a_1, \dots, a_r' \in [0, p)$

mit $a_1 + p\mathbb{Z}, \dots, a_r' + p\mathbb{Z} \in \lambda A'$,

$$a_1 + \dots + a_r \equiv a_1' + \dots + a_r' \pmod{N}$$

aber

$$a_1 + \dots + a_r \not\equiv a_1' + \dots + a_r' \pmod{p}$$

Die ganze Zahl $k = \dfrac{(a_1 + \dots + a_r) - (a_1' + \dots + a_r')}{N}$ hat die

Eigenschaften $k \neq 0$, $|k| \leq \frac{r(p-1)}{N}$. Ferner ist

$\lambda^{-1}(kN + p\mathbb{Z})$ ein Element von $rA - rA$, d.h.

$\lambda^{-1} \in (kN + p\mathbb{Z})^{-1} \cdot (rA - rA)$.

Da $\left| \bigcup_{k \neq 0,\ |k| \leq \frac{r(p-1)}{N}} (kN + p\mathbb{Z})^{-1} (rA - rA) \right|$

$$\leq 2 \cdot \frac{r(p-1)}{N} \cdot |rA - rA| < p - 1$$

gibt es ein $\lambda \in (\mathbb{Z}/p\mathbb{Z})^*$ mit

$$\lambda^{-1} \notin (kN + p\mathbb{Z})^{-1} (rA - rA)$$

f. alle $k \neq 0$ mit $|k| \leq \frac{r(p-1)}{N}$.

Für dieses λ ist φ dann ein F_r-Isomorphismus. □