Ruzsa's embedding lemma

Plünnecke's theorm

Lemma (Gixgis) If $|B+A| \le K|B|$ then

$$\exists B_0 \subseteq B, \exists K_0 \le K \text{ s.t. } \forall h \in \mathbb{N}: |B_0 + hA| \le K_0^h |B_0|$$

Proof $\forall B' \subseteq B$, $\frac{|B'+A|}{|B'|}$ and choose B_0 to minimaze this ration

so $|B_0+A| = K_0|B_0|$ but $\forall Z \subseteq B_0 : |Z+A| \ge K_0|Z|$

By induction on h it is enough to prove that $\forall C$

$$|B_0+A+C| \le K_0 |B_0+C|$$

If $|C|=1$: $|B_0+A| \le K_0 |B_0|$

If $C' = C \cup \{x\}$

$$B_0+A+C' = (B_0+A+C) \cup (B_0+A+x) = (B_0+A+C) \cup ((B_0+A+x) \setminus (Z+A+x))$$

where $Z = \{b \in B_0 \mid b_0+A+x \subseteq B_0+A+C\}$

$$|B_0+A+C'| \le |B_0+A+C| + |B_0+A| - |Z+A|$$
$$\le K_0(|B_0+C| + |B_0| - |Z|) \overset{?}{\le} K_0|B_0+C'|$$

enough to prove : $|B_0+C| + |B_0| - |Z| \le |B_0+C'|$

$$B_0+C' = (B_0+C) \cup (B_0+X) = (B_0+C) \cup ((B_0+X) \setminus (W+X))$$

where $W = \{b \in B_0 ; b_0 + x \in B_0 + C$

$$|B_0+C'| = |B_0+C| + |B_0| - |W|$$

If $b \in W \Rightarrow b_0 + x \in B_0 + C \Rightarrow b_0 + A + x \subseteq B_0 + A + C$

So $W \subseteq Z \Rightarrow |W| \leq |Z| \Rightarrow$

$$|B_0+C| + |B_0| - |Z| \leq |B_0+C| + |B_0| + |W| .$$

$\square$

Lemma (Ruzsa's Δ-ineq.) U, V, W

$$|U| \cdot |V-W| \leq |U+V| \cdot |U+W|$$

Proof For any $y \in V-W$, let $(v(y), w(y)) \in V \times W$ s.t. $v(y) - w(y) = y$

$\phi : U \times (V-W) \longmapsto (U+V) \times (U+W)$

$(x, y) \longrightarrow \phi(x,y) = (x+v(y), x+w(y)) \in$

$x' + v(y')$ $x' + w(y')$

Suppose $\phi(x,y) = \phi(x',y') \Rightarrow w(y) - v(y) = w(y') - v(y')$

$\Rightarrow y = y' \Rightarrow v(y) = v(y')$

& $x + v(y) = x + v(y') \Rightarrow x = x'$

$\Rightarrow \phi$ is one-one $\Rightarrow$ $\square$

Note • An additive group G has torsion $r \in \mathbb{N}$ if

$\underbrace{a + \dots + a}_{r} = ra = 0 \quad \forall a \ G.$

• $H \leq G$ generated by $a_1, \dots, a_d$, then

$H = \{ a_1 m_1 + \dots + a_d m_d ; \ 0 \leq m_i < r \}$ ($\Longleftrightarrow$ GAP)

Thm (Freiman, for torsion groups).

Let G be an additive group of torsion r, and let $A \subseteq G$ s.t. $|A+A| \leq C|A|$. Then $\exists H \leq G$ such that $A \subseteq H$ and $|H| \leq C^4 \cdot r^{C^4} |A|$

~~and H is generated by ≤ , elements~~.

Proof Assume, first that $A = -A$.

the group gen. by A: $\langle A \rangle = \bigcup_{j \geq 0} jA$, $jA = \underbrace{A + \cdots + A}_{j}$

Let $X \subseteq 3A$ be maximal, such that the sets $A + x$ are disjoint for all $x \in X$.

$$|A|\,|X| \leq 4|A| \leq C^4|A| \Rightarrow |X| \leq C^4$$

For any $y \in 3A$ $\exists x \in X$: $(A+y) \cap (A+x) \neq \emptyset$

$$\exists a_1, a_2 \in A : a_1 + y = a_2 + x \Rightarrow$$

$$\Rightarrow y = a_2 - a_1 + X \in A - A + X$$

$$\Rightarrow 3A \subseteq A - A + X = 2A + X$$

$$\Rightarrow 4A = A + 3A \subseteq 3A + X \subseteq 2A + 2X$$

$$\Rightarrow jA \subseteq 2A + (j-2)X$$

$$\Rightarrow \langle A \rangle \leq 2A + \langle X \rangle$$

$$\Rightarrow |\langle A \rangle| \leq |2A|\,|\langle X \rangle| \leq C|A|\, r^{C^4}$$

$$(= C_r |A|)$$

In general let $X \subseteq 2A - A$ be maximal, s.t. the sets $A + x$ are disjoint for $x \in X$

$\Rightarrow \quad |X| \le C^4$ and $2A - A \subseteq A - A + X$.

$$jA - A \subseteq A - A + \langle X \rangle$$

$$\Rightarrow \langle A \rangle \subseteq A - A + \langle X \rangle$$

$\square$

Def Let G, H be additive groups, $k \in \mathbb{N}$, $A \subseteq G$, $B \subseteq H$. Then $\phi : A \to B$ is a Freiman k-homomorphism ("hom.") if

$$a_1 + \dots + a_k = c_1 + \dots + c_k; \; a_i, c_i \in A \implies \phi(a_1) + \dots + \phi(a_k) = \phi(c_1) + \dots + \phi(c_k)$$

k-isom. is when $\phi : A \to B$ is bijective and

$$a_1 + \dots + a_k = b_1 + \dots + b_k \iff \phi(a_1) + \dots + \phi(a_k) = \phi(b_1) + \dots + \phi(b_k)$$

Note

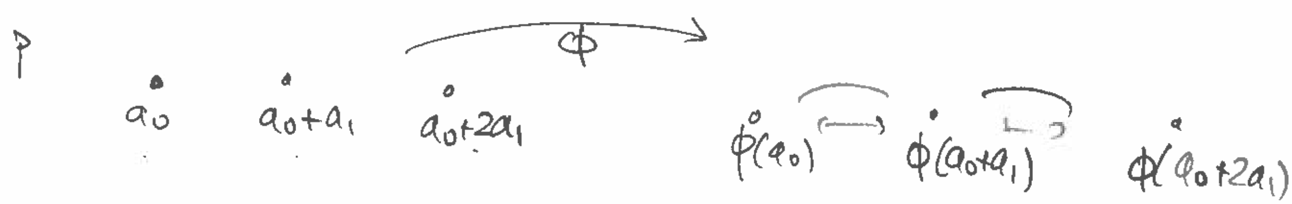
- If $\phi : A \to B$ is a k-hom., it extends to $\phi_k : kA \to kB$ def. by. $\phi(a_1 + \dots + a_k) := \phi(a_1) + \dots + \phi(a_k)$

  If $\phi : A \to B$ is a k-isom, then ϕ_k is a bij. $\Rightarrow$

  $\Rightarrow |kA| = |kB|$.

- If ϕ is a 2-hom. and $P = \{a_0 + a_1 m \; ; \; 0 \le m < n\}$ (n-term AP)

  then $\phi(P) = \{\phi(a_0) + (\phi(a_0 + a_1) - \phi(a_0)) m \; ; \; 0 \le m < n\}$



$X_0 = a_0, \quad X_1 = a_0 + a_1, \quad X_2 = a_0 + 2a_1;$

$$X_1 - X_0 = X_2 - X_1 \iff X_1 + X_1 = X_0 + X_2 \Rightarrow \phi(X_1) + \phi(X_1) = \phi(X_0) + \phi(X_2)$$

$$\Rightarrow \underbrace{\phi(X_1) - \phi(X_0)}_{} = \underbrace{\phi(X_2) - \phi(X_1)}_{}$$

Similarly if $P = \{a_0 + \sum_{i=1}^{d} a_i m_i ; \ 0 \le m_i < n_i\} \Rightarrow$

$$\Rightarrow \phi(P) = \{\phi(a_0) + \sum_{i=1}^{d} (\phi(a_0 + a_i) - \phi(a_0)) m_i ; \ 0 \le m_i < n_i\}$$

$\square$

<u>Ex 1</u> $A \subseteq \mathbb{Z}$, $N \in \mathbb{N}$. Let $\phi : A \mapsto \mathbb{Z}/N$ simply

$$\phi(a) = a \pmod N \in \mathbb{Z}/N.$$

- If $A \subseteq I$ (interval) and $N > |I|$ then ϕ is one-one ($\exists \phi^{-1} : \phi(A) \to A$)
- If $A \subseteq I$, $N > k|I|$ then $\phi : A \to \phi(A) \subseteq \mathbb{Z}/N$ is a k-isom. Indeed,

Suppose $\phi(a_1) + \dots + \phi(a_k) = \phi(b_1) + \dots + \phi(b_k)$, $a_i, b_i \in A$

$$\Rightarrow a_1 + \dots + a_k - (b_1 + \dots + b_k) \equiv 0 \pmod N$$

$$\Rightarrow |a_1 - b_1| + \dots + |a_k - b_k| \le k|I| < N$$

$$\Rightarrow a_1 + \dots + a_k = b_1 + \dots + b_k$$