Reading: Approximate Groups

Lemma 2.5.1 Let G be a arbitrary group and let $A \subset G$ b a finite subset with $|A^2| \leq K|A|$. Then $|A^{-1}A| \leq K^2|A|$ and $|AA^{-1}| \leq K^2|A|$.

This is generalization to non-abelian groups, only for $m = 1$ and $n = 1$

Theorem 2.3.1 Let G be an abelian group and let A, B be finite subsets of G.

- suppose that $|A + B| \leq K|A|$ then $|mA - nA| \leq K^{m+n}|A|$.
- if $|A + A| \leq K|A|$ then $|mA - nA| \leq K^{m+n}|A|$.

for all non-negatve integers m, n.

These looking into the axioms of group theory. There are several instances of group theory that we encounter in other branches of mathemamtics:

- permutation groups
  ABCDE $\to$ BCDEA $\to$ CDEAB $\to$ DEABC $\to$ EABCD $\to$ $[\dots]$
- groups of substutions, e.g. $x \mapsto 3x + 2y$ and $y \mapsto 4x + 3y$
- groups of transformations of physical objects (e.g. symmetries of square)

These symmetries in general were approximate since there was an enormous amount of work move and old the objects in a perfect evenly spaced circle.

Triangle inequality Let U, V, W be subsets of a group. There exists an injection:

$$\phi : U \times V^{-1}W \to UV \times UW$$

In particular if U, V, W are finite then $|U| \times |V^{-1}W| \leq |UV||UW|$.

We're left wondering why the theorem is formatted in this particular way. The proof use basic notions of algebra like "function" an "inverse" and "injection".

- $v : V^{-1}W \to V$ and $w : V^{-1}W \to W$ under then constraint that $x \in V^{-1}W$ leads to $x = v(x)^{-1}w(x)$.
- set $\phi(u, x) = (uv(x), uw(x))$.

- check that ϕ is injective
  - $(uv(x))^{-1}(uw(x)) = v(x)^{-1}w(x) = x$ so that x is **uniquely** determined by $\phi(u,x)$.
  - $(uv(x))v(x)^{-1} = u$ so that u is uniquely determined by $\phi(u,x)$ and x.

  The triangle ineqality has a logarithmic form:

$$\log \frac{|V^{-1}W|}{|V|^{1/2}|W|^{1/2}} \leq \log \frac{|U^{-1}V|}{|U|^{1/2}|V|^{1/2}} + \log \frac{|U^{-1}W|}{|U|^{1/2}|W|^{1/2}}$$

Rusza's triangle inequality was appliled with all three set's being identical $U = V = W = A$. In fact, that's the entire argument.

So are have not made any spacifications like $G = \mathbb{Z}^2$ or $G = SU(2)$ or $G = \mathsf{SL}_2(\mathbb{Z}[i])$ or $G = (\mathsf{SL}_2(\mathbb{Z})\backslash\mathsf{SL}_2(\mathbb{R})[5]$ or anything else. These were deduced abstractly from our guess on how the notion of multipicaton $\times$ or of how mirrors actually work.

Counterexample Let H be a finite group and let $G = H * \langle x \rangle$ (which is called the **free product**) of H with the infinite cyclic group (basically a copy of $\mathbb{Z}$, e.g. how many times we do something). Let $A = H \cup \langle x \rangle$ (this is called the "union"). Then

- $|A^2| \leq 3|A|$ and yet
- $HxH \subseteq A^3$ and $|HxH| = |H|^2 \asymp |A|^2$ these sets have the same number of elements without being the same set. Their definitions look similar too.

08/02 Lemma (**approximate orbit-stabilizer lemma**) Suppose a group G (not necessarily commutative) acts on a set X and let A be a K-approximate subgroup of G for some $K \geq 1$. For every integer $k \geq 2$ and $x \in X$ we have:

$$|A| \leq |A \cdot x| \; |\mathsf{Stab}(x) \cap A^k| \leq K^{k+1}|A|$$

Example Find examples of approximate groups in $\mathsf{SL}_3(\mathbb{Z}/p\mathbb{Z})$ or $G = SU(2)$. What happens when subsets don't have "perfect" multiplicative structure (e.g. *everything*) or closure properties.

Theorem (Orbit-Stabilizer) Let G be a finite group of permutations of the set S. Then for any $i \in S$ $|G| = |\mathsf{orb}(i)| \times |\mathsf{stab}(i)|$.

We have used the word **set**, we have a "set" of permutations (I usually think of them as a **box** or a **bag**. So there's varying levels of fluidity there. Usually we resort to set theory when objects or collections of objects are hard to picture or describe. We migtt try again later.

Example If I shuffle a deck of cards, I have chosen one of the $52! \approx 10^{68}$ possible arrangements of cards. There's no way we are looking through each one of those. If I stir a pot, the obects inside have been *permuted* yet this is close-but-not-quite to the mathematical definition.

References

[1] Matthew Tointon. **Approximate Groups** (London Mathematical Society Student Texts #94)

[2] Emmanuel Breuillard **A Brief Introduction to Approximate Groups** (MSRI #61)

[3] Harald Helfgott **Growth and Generation in $\mathbf{SL}_2(\mathbb{Z}/p\mathbb{Z})$** Annals of Mathematics, 2008.

[4] Terence Tao, Van Vu **Additive Combinatorics** (Cambridge Studies in Mathematics #105) Cambridge University Press, 2006. ...