Tutorial : Ping-Pong Lemma

Half of these projects start by a conjectured relationship between two theorems. And it's not always correct. Today's pair is:

- Ping-Pong Lemma
- Sum-Product Theorem

I *think* that's correct. Let's state these results and being the long journey of connecting these thing to "real life".

#1 Ping-Pong Lemma I was able to find two examples of Ping-Pong Lemma having to with group matrices over the integers $\mathbb{Z}$ we can have

- Banach-Tarski paradox
- Establishing free groups

Here's a proposition:

> This is a Free group on two generators (no relations)
>
> $$\left\langle \left(\begin{array}{cc} 1 & 2 \\ 0 & 1 \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 2 & 1 \end{array} \right) \right\rangle \subseteq SL_2(\mathbb{Z})$$
>
> Proof: use the ping-pong Lemma. Another example I found from Sarnak[1]
>
> $$\left\langle \left(\begin{array}{cccc} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{array} \right), \left(\begin{array}{cccc} 1 & 0 & 0 & -5 \\ 0 & 1 & 0 & -5 \\ 0 & 0 & 1 & -5 \\ 0 & 0 & 0 & -5 \end{array} \right) \right\rangle \subseteq SL_4(\mathbb{Z})$$
>
> and these play generalized Ping-Pong. The reason we like the free group F_2 is becuase it's one of the few discrete groups we can understand. And I don't even think that's true, because if $A, B \in SO(3)$ that group is compact and we can measure:
>
> $$\phi : \langle A, B \rangle \to SO(3)$$
>
> we'd have that $\overline{\langle A, B \rangle} \subseteq SO(3)$ is a **dense** subgroup, so we can try to quantify (by whatever means we have availble) how quickly this is mixing.

In another direction we have the Banach-Tarski paradox. The groups used to contruct the paradox seem related to the Pythagorean theorem[2] He will use:

---

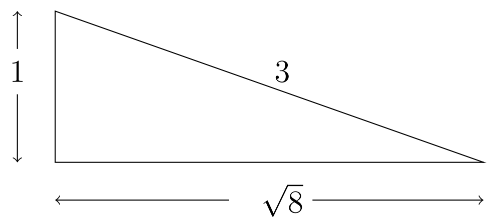
[1] `http://web.math.princeton.edu/sarnak/NotesOnThinGroups.pdf`

[2] https://stanford.box.com/shared/static/wesg27648yqomf4ar3mkmfwf89ptzqj4.pdf

This group is free:

$$\left\langle \begin{pmatrix} \frac{1}{3} & +\frac{2\sqrt{3}}{3} & 0 \\ -\frac{2\sqrt{3}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & +\frac{\sqrt{8}}{3} \\ 0 & -\frac{\sqrt{8}}{3} & \frac{1}{3} \end{pmatrix} \right\rangle \subseteq SO_3(\mathbb{R})$$

This group is related to the right triangle with side lengths 1 and $\sqrt{8}$



This tringle is oriented in various ways in three dimensional space.

Therefore... without stating the ping-pong Lemma we can imagine such a thing could be useful! Now for the statement:

Ping-Ping Lemma Let G be a group acting on a set X. Let H_1, H_2 be sub-groups and suppose we can find subsets $X_1, X_2 \subseteq X$ subset that we observe

$$\big[g \in H_1 \to g(X_2) \subseteq X_1 \big] \text{ and } \big[g \in H_2 \to g(X_1) \subseteq X_2 \big]$$

then our subgroup is free, $\langle H_1, H_2 \rangle = H_1 * H_2 \simeq F_2$.

One thing we notice is that ping-pong "works" (i.e. produces free groups or expander graphs?) only for 3×3 and not for 2×2. Another possiblity is that the group we are studying isn't free (there are relations). This is not a bad thing, $SL(2, \mathbb{Z})$ is not free, there's a relation:

$$SL_2(\mathbb{Z}) \simeq \big\langle S, T : S^2 = (ST)^3 = 1 \big\rangle \simeq \big(\mathbb{Z}/2\mathbb{Z}\big) * \big(\mathbb{Z}/3\mathbb{Z}\big)$$

and for a general number field, F, $SL_2(\mathcal{O}_F)$ for the ring of integers $\mathcal{O}_F$ can be an open problem. Therefore, we conclude, $SL(2, \mathbb{Z})$ can house rather complicated objects.

I should remark this is a case of the **Tits alternative**.

Veresion #2 $SO(3)$ contains a copy of the free group on two generators.

Our candidate free group will be the the standard 3-4-5 triangle. Since $3^2 + 4^2 = 5^2$ we have

$$\left\langle \begin{pmatrix} \frac{3}{5} & -\frac{4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{3}{5} & -\frac{4}{5} \\ 0 & \frac{4}{5} & \frac{3}{5} \end{pmatrix} \right\rangle \subseteq SO_3(\mathbb{Q})$$

and we resort to 5-adic numbers to choose our ping-pong sets:

- $A_\pm = 5^{\mathbb{Z}} \cdot \{(x, y, z) \in \mathbb{Z}^3, x \pm 3y \in 5\mathbb{Z}, z \in 5\mathbb{Z}\}$
- $B_\pm = 5^{\mathbb{Z}} \cdot \{(x, y, z) \in \mathbb{Z}^3, z \pm 3y \in 5\mathbb{Z}, z \in 5\mathbb{Z}\}$

and our set is $X = A_- \cup A_+ \cup B_- \cup B_+ \cup \{(0, 1, 0)\}$ and this is our **ping-pong** set!

So our ping-pong style proofs involve finding a "tennis court" and playing a game!

#2 Sum-Product Theorem This is the dumbest-sounding theorem I have ever heard of.

Emmanuel Breuillard put the origin of approximate groups with the Sum-Product Theorem:

> Thm Let $\mathbb{F}_p$ be a finite field with p elements (where p is prime). They for every $\delta > 0$ there is an $\epsilon > 0$ (which does not depend on p) such that:
>
> $$|S \times S| + |S + S| \geq |S|^{1+\epsilon}$$
>
> for every subset $|S| \subset \mathbb{F}_p$ such that $p^\delta < |S| < p^{1-\delta}$.

For me it is not so easy to picture what this set S could look like. In a sense, we'll never be told what numbers δ or ϵ should be. It just says

> Give me $\epsilon \to$ find δ such that $S+S$ or $S \times S$ is growing. And this is only for sets which that do not have just a few elements or all of $\mathbb{F}_p$.

and approximate group will start here. I can't even turn this statement into a hypothesis to test. I can't connect it to other number theory facts I have learned. Very basic but I don't know what it means. Here's another, due to Helfgott:

> For every ϵ we can find a δ such that $|S \times S \times S| \geq |S|^{1+\epsilon}$ for every generating set S of $SL_2(\mathbb{Z}/p\mathbb{Z})$ such that $|S| < |SL_2(\mathbb{Z}/p\mathbb{Z})|^{1-\delta}$

Commendible. What do you mean this was only discovered in 2008? I said to myself the following: consider the expansion of sine:

$$\sin x \approx x - \frac{x^3}{3!} + \frac{x^3}{5!} = x - \frac{x \times x \times x}{1 \times 2 \times 3} + \frac{x \times x \times x \times x \times x}{1 \times 2 \times 3 \times 4 \times 5}$$

How many instances of $+$ and $\times$ and $\div$ have we done? And if we are using floating-point arithmetic, we are losing accuracy every step of the way. What happens if we use a million of these?

That error will be pseudo-random, but maybe the result will be in tact.

I don't know if I could have articulated the result as nicely as Helfgott or Tao or Bourgain, but if definitely know if I had proposed such a thing I'd be laughed out of the room.[3] **#2 Approximate Groups** ...

#3 Do these two overlap? I guess not.

References

(1) Emmanuel Breulliard **A brief introduction to approximate groups** from: "Thin Groups and Superstrong Approximation" (MSRI Publications, **61**) 2013.

[3] In fact, yes.