Are p-adic Lie groups useful beyond Number Theory ?

Yves Benoist

CNRS - Paris-Saclay University

June 2021

NUS Colloquium

www.math.u-psud.fr/~benoist/conference

Introduction

Let G be a compact simple Lie group, $\Gamma \subset G$ a dense subgroup.

Example: $G = \mathrm{SO}(n,\mathbb{R})$ or $G = \mathrm{SU}(n,\mathbb{R})$.

We will discuss three independent naive questions:

Question 1 Does Γ contain a non-abelian free subgroup ?

Question 2 Does Γ contain a g with $\overline{g^{\mathbb{Z}}}$ maximal abelian ?

Let $S = S^{-1}$ be a finite subset generating Γ
P be the operator on $L^2(G)$: $P\varphi(g) = \frac{1}{|S|}\sum_{s\in S}\varphi(sg)$,
and $L^2_0(G) = \{\varphi \in L^2(G) \mid \int_G \varphi = 0\}$.

Question 3 Does one have $\sup_{\varphi \in L^2_0(G)} \frac{\|P\varphi\|_{L^2}}{\|\varphi\|_{L^2}} < 1$?

What do these three questions have in common?

⋆ They deal with dense subgroups of compact groups.

⋆ You can generalize them to Zariski-dense subgroups Γ of simple Lie groups $G \subset \mathrm{GL}(n,\mathbb{R})$.

⋆ The case when G is compact is most difficult.

⋆ You need p-adic Lie groups to solve them.

What shall we see in this talk? Three independent parts!

Part 1 Free subgroup question (Tits).

Part 2 Hyper-regular element question (Prasad-Rapinchuk).

Part 3 Spectral gap question (Sarnak, Benoist-DeSaxcé).

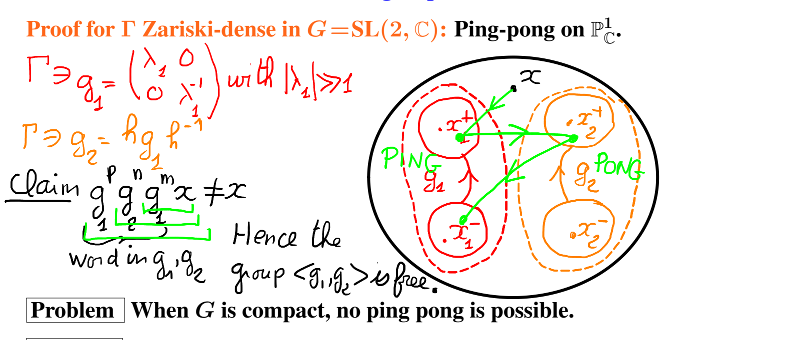
We will see why $\mathbb{Q}_p$ is better than $\mathbb{R}$ for each of these questions.

Part 1. Tits alternative. A linear group $\Gamma \subset \mathrm{GL}(n,\mathbb{R})$ either has a finite index solvable subgroup or contain non-abelian free subgroups.

Reformulation: Let $G \subset \mathrm{GL}(n,\mathbb{R})$ be a simple Lie group.

Theorem 1 (Tits, 1970) All Zariski-dense subgroups $\Gamma \subset G$ contain non-abelian free subgroups.

Proof for Γ Zariski-dense in $G = \mathrm{SL}(2,\mathbb{C})$: Ping-pong on $\mathbb{P}^1_{\mathbb{C}}$.



Problem When G is compact, no ping pong is possible.

Solution Use p-adic Lie groups.

Definition For p prime, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ for the absolute value $|p^n\frac{a}{b}|_p = p^{-n}$ for a, b prime to p.
A p-adic field K is a finite extension of $\mathbb{Q}_p$.
The absolute value $|.|_p$ extends as an absolute value $|.|_K$ on K.

Concretely : $\mathbb{Q}_p = \{p^{k_0}\sum_{k\geq 0} a_k p^k \mid 0 \leq a_k < p,\ k_0 \in \mathbb{Z}\}$,
$K = \mathbb{Q}_p[\sqrt{p}] = \{p^{k_0/2}\sum_{k\geq 0} a_k p^{k/2} \mid 0 \leq a_k < p,\ k_0 \in \mathbb{Z}\}$.

Fact 1 Let $k \subset \mathbb{C}$ be a finitely generated field and $\lambda \in k$ with $\lambda^n \neq 1\ \forall n \geq 1$. Then there exists an embedding $k \hookrightarrow K$ in $\mathbb{C}$ or in a p-adic field such that $|\lambda|_K > 1$.

Example : for $\lambda = (3+4\sqrt{-1})/5$, one needs $K = \mathbb{Q}_5$ and $\lambda \mapsto (3+4i)/5$ where $i = 2+5+2.5^2+5^3+\dots$ has square -1.

Proof for Γ dense in $G = \mathrm{SU}(n,\mathbb{C})$.

⋆ Step 1. Replace Γ by a finitely generated subgroup so that $\Gamma \subset \mathrm{SL}(n,k)$ where k is a finitely generated field.

⋆ Step 2. By Fact 1, one has an embedding $\Gamma \subset \mathrm{SL}(n,K)$ with K p-adic and $g \in \Gamma$ with a jump among its eigenvalues: $|\lambda_1|_K \geq \dots \geq |\lambda_\ell|_K > |\lambda_{\ell+1}|_K \geq \dots \geq |\lambda_n|_K$.

⋆ Step 3. Use g to play ping-pong on $\{\ell\text{-planes in } K^n\}$.

Part 2. Prasad-Rapinchuk hyper-regularity.

Let $G \subset \mathrm{GL}(n,\mathbb{R})$ be a simple Lie group.

Theorem 2 (Prasad-Rapinchuk, 2000) All Zariski-dense subgroups $\Gamma \subset G$ contain hyper-regular elements g.

i.e. g is semisimple and the Zariski-closed subgroup generated by g is maximal abelian in G.

We will assume $G = \mathrm{SL}(n,\mathbb{R})$ or $G = \mathrm{SU}(n,\mathbb{C})$.

In this case, we are asking that there are no relations $\lambda_1^{k_1}\cdots\lambda_n^{k_n} = 1$ among the eigenvalues λ_i of g except when $k_1 = \dots = k_n$.

Starting the proof of Theorem 2. Since Γ is Zariski dense, we can find $g \in \Gamma$ with distinct eigenvalues. This element g belongs to a unique maximal $\mathbb{R}$-torus $T \subset G$.

We want that no g^k, $k \geq 1$ belong to smaller $\mathbb{R}$-subtori S.

Definition A $\mathbb{R}$-torus $T \subset G$ is an abelian, Zariski-connected and Zariski-closed subgroup whose elements are semisimple.

Example : $T_0 := \left\{ g = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x^2+y^2 = 1 \right\}$.

Problem A $\mathbb{R}$-torus T with $\dim T \geq 3$ always contains infinitely many $\mathbb{R}$-subtori S.

Example: $T = T_0^3$, take $S = \{t \in T_0^3 \mid t_1^{k_1}t_2^{k_2}t_3^{k_3} = 1\}$.

Solution Use p-adic Lie groups.

Fact 2A Let $R \subset \mathbb{C}$ be a finitely generated ring. Then, there exists a ring embedding $j : R \hookrightarrow \mathbb{Z}_p$.

$\mathbb{Z}_p = \{\sum_{k\geq 0} a_k p^k \mid 0 \leq a_k < p\} = \{\lambda \in \mathbb{Q}_p \mid |\lambda|_p \leq 1\}$ is the ring of integers of $\mathbb{Q}_p$.

Fact 2B The group $G_p = \mathrm{SL}(n,\mathbb{Q}_p)$ contains a maximal $\mathbb{Q}_p$-torus T_p with only finitely many $\mathbb{Q}_p$-subtori S_p.

Example: $T_p = \{x \in K \mid N_{K/\mathbb{Q}_p}(x) = 1\}$ where K is an abelian extension of degree n of $\mathbb{Q}_p$.

⋆ Step 1. Replace Γ by a finitely generated subgroup so that $\Gamma \subset \mathrm{SL}(n,R)$ where R is a finitely generated ring.

⋆ Step 2. By Fact 2A one has an embedding $\Gamma \subset \mathrm{SL}(n,\mathbb{Z}_p)$. Then the closure $\overline{\Gamma}$ is an open subgroup of $G_p = \mathrm{SL}(n,\mathbb{Q}_p)$.

⋆ Step 3. Use the maximal $\mathbb{Q}_p$-torus $T_p \subset G_p$ from Fact 2B. The set $T'_p := T_p \smallsetminus \cup(\mathbb{Q}_p\text{-subtori})$ is open in T_p.

The union of G_p-conjugates of T'_p is open in G_p, hence meets $\overline{\Gamma}$ and contains an element $g \in \Gamma$. Such a g is hyper-regular.

Part 3. Spectral gap.

Let $G \subset \mathrm{GL}(n,\mathbb{R})$ be a simple Lie group,
Γ be a Zariski-dense subgroup of G,
$S = S^{-1} \subset \Gamma$ be a finite symmetric generating subset.
Set $P\varphi(g) = \frac{1}{|S|}\sum_{s\in S}\varphi(sg)$, for $\varphi \in L^2(G)$.
P is the averaging operator for $\mu := \frac{1}{|S|}\sum_{s\in S}\delta_s$.

Sarnak conjecture For G compact, there exists $C < 1$ such that $\|P\varphi\|_{L^2} \leq C\|\varphi\|_{L^2}$ for all $\varphi \in L^2(G)$ with $\int_G \varphi = 0$.

Theorem 3 (Benoist-DeSaxcé, 2015) Sarnak conjecture is true when $S \subset \mathrm{GL}(n,\overline{\mathbb{Q}})$.

Here $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.

This was due to Bourgain-Gamburd for $G = \mathrm{SU}(n,\mathbb{C})$.

Key Proposition There exists $c > 0$ such that, for $n \geq 1$ and Zariski-closed subgroup $H \subsetneq G$, one has $\mu^{*n}(H) \leq e^{-cn}$.

Here $\mu^{*n} = \mu * \dots * \mu = n^{th}$-convolution power of μ.

No time to explain why Key Proposition implies Theorem 3...

Proof of Key Proposition when $G/H = Gv$ with $v \in \mathbb{R}^n$.

The behavior of $\|gv\|$ is controlled by the first Lyapunov exponent $\lambda_1 := \lim_{n\to\infty}\frac{1}{n}\int_\Gamma \log\|gv\|\, d\mu^{*n}(g)$.

Most often, by Furstenberg's theorem, one has $\lambda_1 > 0$.

Then, the large deviation estimates tell us that $\mu^{*n}(\{g \in \Gamma \mid \|g.v\| \leq \|v\|\}) = O(e^{-cn})$.

Problem This method works only when G is non compact.

Solution Use p-adic Lie groups.

Fact 3 For random walks on p-adic Lie groups, one still has large deviation estimates.

⋆ Step 1. As in Tits alternative, replace Γ by an unbounded Zariski-dense subgroup of a p-adic Lie group $\mathrm{SL}(n,K)$.

⋆ Step 2. Apply the large deviation estimates of Fact 3.

For more: see Inv. Math. 205 (2016) p.337-361

FINAL CHALLENGE
For these 3 questions, find a proof that does not use p-adic numbers.