Asymptotic Theory of Finite Groups

Nov 17, 2015, Mexico City

$\{G_i\}_i$ infinite family of finite groups

G a group, $\varphi_i : G \to G_i$, $|G_i| < \infty$,

$\bigcap_i \operatorname{Ker} \varphi_i = (1)$

G is residually finite

Infinite Groups

Hopelessly Infinite (Geometric Group Theory)

Residually Finite (Number Theory, Combinatorics)

$\{H \triangleleft G \mid |G:H| < \infty\}$ basis of neighborhoods of 1.

The topology is complete = profinite group = inverse limit of finite groups

$\hat{G}$ = completion of G, $G \hookrightarrow \hat{G}$

In any case

$$G \to G/\cap\{H \mid |G:H|<\infty\} \to \hat{G}$$

<u>EX.</u> K/F infinite Galois extension of fields, $Gal(K/F)$ is profinite.

p a prime number, $\varphi_i : G \to G_i$, G_i are finite p-groups, $\bigcap_i \operatorname{Ker}\varphi_i = (1)$.

Then G is <u>residually-p</u>.

Complete Topology = pro-p group = inverse limit of finite p-groups.

$G_{\hat{p}}$ pro-p completion, $G \hookrightarrow G_{\hat{p}}$

In any case

$$G \to G/\cap\{H \triangleleft G \,/\, |G:H| = p^k, k \geq 0\} \to G_{\hat{p}}$$

EX. 1. F_m the free group on $x_1, \dots, x_m$; residually-p $\forall p$

$(F_m)_{\hat{p}}$ free pro-p group

EX. 2. $\mathbb{Z}_p$ p-adic integers

$$GL'(n, \mathbb{Z}_p) = I_n + p\, M_n(\mathbb{Z}_p)$$

pro-p group.

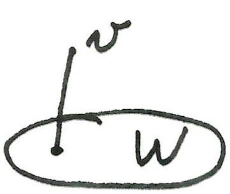
M. Lazard (1965): $\forall$ p-adic analytic group has an open subgroup which is embeddable in $GL'(n, \mathbb{Z}_p)$.

Ex. 2' R a commutative local Noetherian complete ring ($\mathbb{Z}_p$, $\mathbb{Z}_p[[x_1, \dots, x_m]]$, $GF(p^k)[[x_1, \dots, x_m]]$), $J \triangleleft R$ max ideal, $R/J \cong GF(p^k)$.

Then $GL'(n, R) = I_n + M_n(J)$ is a pro-p group (congruence subgroup).

EXPANSION.

$\Gamma = (V, E)$ finite connected graph, $\emptyset \neq W \subset V$, $\partial W = \{v \in V \,/\, v \notin W, \mathrm{dist}(v, W) = 1\}$



$W \hookrightarrow (W \cup \partial W) \to \cdots$

Def. $\varepsilon > 0$; Γ is an ε-expander

if $\forall\, \emptyset \neq W \subset V$, $|W| \leq \frac{1}{2}|V|$

$$|W \cup \partial W| \geq (1+\varepsilon)|W|$$

Wanted: infinite family of k-regular graphs $\Gamma_n = (V_n, E_n)$, which are all expanders; k, ε are fixed, $|V_n| \to \infty$.

Pinsker, 70s; Barzdin-Kolmogorov, 60s

$G = \langle X \rangle$ finite group

$\mathrm{Cay}(G, X)$ Cayley graph

$V = G$ $\quad g_1 \text{———} g_2$ if $g_2 = x^{\pm 1} g_1$, $x \in X$

Connected $|X|$-regular graph

Kazhdan (67): $\exists$ group $G = \langle X \rangle$, $|X| < \infty$ with the following property: $\exists \varepsilon > 0$ $\forall$ unitary representation $\rho : G \to U(H)$ without $\neq 0$ fixed points $\forall h \in H$ $\exists x \in X$ $\|xh - h\| \geq \varepsilon \cdot \|h\|$.

For example, $G = SL(n, \mathbb{Z})$, $n \geq 3$

Property (T)

Margulis (81): $G = \langle X \rangle$, $|X| < \infty$, residually finite & has property (T); $\varphi_i : G \to G_i$, $|G_i| < \infty$, $X \to X_i$, $G_i = \langle X_i \rangle$. Then $\{ Cay(G_i, X_i) \}_i$ is an expander family.

Ershov - Jaikin, (2010) R finitely generated associative ring, $E(n,R) = gp\langle I_n + e_{ij}(a) \mid 1 \le i \ne j \le n, a \in R\rangle$ has (T) for $n \ge 3$.

Ershov-Kassabov-Jaikin (recently): all Chevalley and Steinberg groups (rank ≥ 2) over commutative rings.

Even over nonassociative rings ($n = 3$, Z. Zhang).

Kassabov, (2003): $A_n = \langle X_n \rangle$, $|X_n| \le$ const, $\{Cay(A_n, X_n)\}$ expander family.

Idea: He first did it for $SL(3n, \mathbb{Z}/p\mathbb{Z}) = E_3(3, M_n(\mathbb{Z}/p\mathbb{Z}))$.

Lubotzky - Kassabov : all infinite families of finite simple groups except Suzuki groups.

Breuillard - Green - Tao : also Suzuki groups.

Approximate Groups.

G a group, $A \subset G$ a subset (symmetric: $A = A^{-1}$), $K \geq 1$.

The properties:

(1) for $x, y \in A$ $xy^{-1} \in A$ with probability $\geq \frac{1}{K}$;

(2) $|A^2| \leq K|A|$

(3) A^2 is covered by K right translates of A, $A^2 \subseteq \bigcup_{i=1}^{K} A g_i$.

$\rightsquigarrow$ to the same theories.

A is a K-approximate group.

EX. $A = \{ g^n \mid -N \leq n \leq N \}$, $g \in G$, is a 2-approximate group

EX. d-dimensional arithmetic progression $A = \{ n_1 x_1 + \dots + n_d x_d \mid |n_i| \leq N_i \} \subset \mathbb{Z}$, is a 2^d-approximate group.

- No fast expansion $\rightsquigarrow$ approximate subgroups
- Polynomial growth (Gromov Thm)

$\rightsquigarrow$ balls of radius n are nice approximate subgroups.

Freiman - Rusza : $A \subseteq \mathbb{Z}$ a K-approximate subgroup $\Rightarrow A \subseteq P = \{ n_1 x_1 + \dots + n_d x_d \mid |n_i| \leq N_i \}, d \leq K,$

$$\frac{|P|}{|A|} \leq f(K).$$

Helfgott, Gamburd-Bourgain-Sarnak, Hrushovski, Breuillard-Green-Tao, Pyber-Szabo ... $\Rightarrow$ a noncommutative version.

Side effects : better understanding (efficient version) of Gromov's theorem on groups of polynomial growth; a new approach to Hilbert's 5th Problem.

The strongest recent result on linear groups (the "superstrong approximation"):

Salehi-Golsefidy-Sarnak.

$\Gamma = \langle X \rangle \leq SL(n, \mathbb{Z})$, $\overline{\Gamma}$ Zariski closure, $\overline{\Gamma} = [\cancel{k}\overline{\Gamma}, \overline{\Gamma}]$

$SL(n, \mathbb{Z}) \to SL(n, \mathbb{Z}/(m))$

$\Gamma \to \Gamma/(m)$, $X \to X_m$

m square free $\Rightarrow$

$\{Cay(\Gamma/(m), X_m)\}$ expander family.

Linearity of free pro-p groups and pro-p identities.

Recall the examples 1, 2, 2'

Problem: $(F_m)_{\hat{p}} \overset{?}{\hookrightarrow} GL'(n, R)$

for some n

Zubkov (89): NO if $n=2$, $p>2$

Pink (98), Barnea-Larsen (99):

NO if $R = GF(p^k)[[t]]$.

The question is related to identities.

$$S_n(x_1, \dots, x_n) = \sum_{\sigma \in P_n} (-1)^{|\sigma|} x_{\sigma(1)} \cdots x_{\sigma(n)}$$

Amitsur-Levitzki (51):

$\forall$ commutative ring R

$S_{2n}(x_1, \ldots, x_{2n}) = 0$ holds identically

on $M_n(R)$.

Theorem Let $p > n$. Then

$\exists\ 1 \neq w(x_1, x_2) \in (F_2)_{\hat{p}}$: $\forall$ ring R

$w(x_1, x_2) = 1$ holds identically on

the pro-p group $GL'(n, R)$.

Remark. It is sufficient for $w = 1$

to hold identically on $GL'(n, \mathbb{Z}_p)$.

Corollary. For $p > n$ $(F_2)_{\hat{p}}$ is not

embeddable in $GL'(n, R)$.

In fact, Thm $\iff$ Corollary.

Let $R = \mathbb{Z}_p[[x_{ij}^{(k)}]]$; $1 \le i,j \le n$,

$k = 1, \dots, m$

Maximal ideal $J = (p, x_{ij}^{(k)})$

Generic Matrices :

$$X_k = (x_{ij}^{(k)})_{1 \le i,j \le n}, \quad k = 1, \dots, m$$

Procesi (66) : $D = \langle X_1, \dots, X_m \rangle$ is a domain

Amitsur (72) $(Z(D) \setminus \{0\})^{-1} D$ is a finite dimensional division algebra, which is not a crossed product.

$$G_{m,n} = gp\langle 1+X_1, \dots, 1+X_m\rangle$$

the <u>universal n-linear pro-p group.</u>

$$\begin{tikzcd} & G_{m,n} \arrow[d] & & \langle X_1, \dots, X_m\rangle \arrow[d] \\ (F_m)\hat{_p} \arrow[ur] \arrow[r] & GL'(n,R) & & M_n(R) \end{tikzcd}$$

<u>Question:</u> is $G_{m,n}$ a free pro-p group?

If YES then we have an embedding.

If NO then $\exists\, 1 \neq w(x_1, \dots, x_m) \in (F_m)\hat{_p}$:

$w(1+X_1, \dots, 1+X_m) = 1$.

Then $w = 1$ holds identically on all $GL'(n,R)$.

Golod-Shafarevich Groups.

Let $Y \subseteq (F_m)_{\hat{p}}$, $N(Y)$ = closed normal subgroup of $(F_m)_{\hat{p}}$ generated by Y.

$\langle x_1, \dots, x_m \mid Y = 1 \rangle = (F_m)_{\hat{p}} / N(Y)$

If $\langle X \mid Y = 1 \rangle$ is a discrete presentation then

$$\langle X \mid Y = 1 \rangle_{\hat{p}} = \langle X \mid Y = 1 \rangle$$

in the category of pro-p groups.

$G = \langle x_1, \dots, x_m \mid r_1 = 1, \dots, r_s = 1 \rangle$,

$r_i \in F^p[F, F]$, $F = (F_m)_{\hat{p}}$, and

$s < m^2/4$.

<u>Golod</u> - <u>Shafarevich</u> (64) : G is infinite.

Golod-Shafarevich group (GS).

<u>EX. 1.</u> X a compact hyperbolic 3-manifold, $\Gamma = \pi_1(X)$. Then for almost all p $\Gamma_{\hat{p}}$ is GS.

(Lubotzky, 83)

<u>EX. 2.</u> S finite set of primes, $p \notin S$, $|S| = m > 4$; $K/\mathbb{Q}$ = max pro-p extension unramified outside of S. Then

$Gal(K/\mathbb{Q}) = \langle x_1, \ldots, x_m \mid x_i^{p^{k_i}} = [x_i, a_i],$

$1 \leq i \leq m \rangle$ is a GS-group since $m < m^2/4$ (Shafarevich, 63).

E. Z. (2000) : $\forall$ GS-group contains

$(F_2)_{\hat{p}}$.

Fontaine-Mazur Conjecture:

$\forall\, \rho : Gal(K/\mathbb{Q}) \to GL'(n, R)$

the image of ρ is finite.

It is not known even if $Gal(K/\mathbb{Q})$

is not linear.

Thm $Gal(K/\mathbb{Q})$ is not ~~linear~~

n-linear if $p \gg n$.

Question (a dream...): a theory of

pro-p groups that satisfy a nontrivial

identity (somewhat parallel to the

theory of PI-algebras).

Conjecture Let G be a just infinite pro-p group, that satisfies a pro-p identity. Then it is analytic over $\mathbb{Z}_p$ or over $GF(p^k)[[t]]$.

Thm For $p >> n$ all identities of $GL'(n, \mathbb{Z}_p)$ follow from finitely many.