Asymptotic Theory of Groups

E. Zelmanov

Introduction

Assume known: the concept of a GROUP.

G a group, $\varphi_i : G \to G_i$, $|G_i| < \infty$ homomorphisms,
$\bigcap\limits_i \ker \varphi_i = (1)$.

G is residually finite

Ex.1 A finitely generated group of matrices;

Ex.2 F_m the free group on m free generators $x_1, \dots, x_m$;

Ex.3 K/F an infinite Galois extension, $\mathrm{Gal}(K/F)$.

Introduction

Infinite Groups

Hopelessly Infinite
(Geometric Group Theory)

Residually Finite
(Number Theory, Combinatorics)

These classes behave differently.

The Burnside Problem (1902)

$$G = \langle a_1, \dots, a_m \rangle, \ \exists n : \ \forall g \in G \ \ g^n = 1 \ \ \overset{?}{\Longrightarrow} \ |G| < \infty.$$

More generally, what makes a group finite?

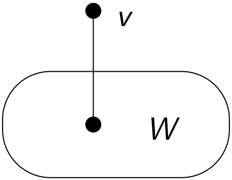
No (Novikov-Adian, 1968)

For Residually Finite Groups: YES (E.Z., 1991)

Expanders.

$\Gamma = (V, E)$ finite connected graph, $\emptyset \neq W \subset V$,

$\partial W = \{v \in V \mid v \notin W,\ \operatorname{dist}(v, W) = 1\}$



$$W \hookrightarrow (W \cup \partial W) \hookrightarrow \dots$$

Definition. $\epsilon > 0$; Γ is an ϵ-expander if $\forall \emptyset \neq W \subset V$ such that $|W| \leq \frac{1}{2}|V|$

$$|W \cup \partial W| \geq (1 + \epsilon)|W|.$$

Expanders

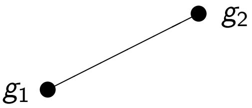
Wanted: infinite family of k-regular graphs $\Gamma_n = (V_n, E_n)$ that are all ϵ-expanders; k, ϵ are fixed, $|V_n| \to \infty$.

Pinsker, 70s; Barzdin-Kolmogorov, 60s

$G = \langle X \rangle$ finite group

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

$V = G$



if $g_2 = x^{\pm 1} g_1,\ x \in X$.

Connected $2|X|$-regular graph.

Expanders

Kazhdan (1967): $\exists$ groups $G = \langle X \rangle$, $|X| < \infty$, with the following property:

Property (T)

$\exists \epsilon > 0$ $\forall$unitary representation $\rho : G \to U(H)$ without $\neq 0$ fixed points: $\quad \forall h \in H \;\; \exists x \in X \;\; ||xh - h|| \geq \epsilon ||h||$.

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

G. Margulis (1981): $G = \langle X \rangle$, $|X| < \infty$, residually finite & has property (T); $\varphi : G \to G_i$, $|G_i| < \infty$, $X \to X_i$, $G_i = \langle X_i \rangle$. Then $\{\mathrm{Cay}(G_i, X_i)\}_i$ is an expander family.

Kassabov, Lubotzky, Breuillard, Green, Tao: any infinite family of finite simple groups $\rightsquigarrow$ expander family.

Growth of Groups.

G a group, $G = \langle x_1, \ldots, x_m \rangle$

$B(n) = \left\{ x_{i_1}^{\pm 1} \cdots x_{i_k}^{\pm 1},\ k \le n \right\}$

$\bigcup\limits_{n \ge 1} B(n) = G.$

$B(n) =$ ball of radius n with the center at 1 in $\mathrm{Cay}(G, X)$.

$g(X, n) = |B(n)| < \infty$

$g(1) \le g(2) \le \ldots$ growth function

Unfortunately, $g(X, n)$ depends on X.

Growth of Groups

$$\mathbb{N} = \{1, 2, \ldots\}$$

$$f, g : \mathbb{N} \to [1, \infty)$$

Definition. $f \leq g$ asymptotically less than or equal to g if $\exists c \geq 1$:

$$f(n) \leq c\, g(cn) \quad \text{for all } n.$$

If $f \leq g,\ g \leq f$ then $f \sim g$ asymptotically equivalent.

If $G = \langle X \rangle = \langle Y \rangle,\ |X| < \infty,\ |Y| < \infty$ then

$$g(X, n) \sim g(Y, n).$$

Growth of G = class of equivalence.

J. Milnor (1968):

(1) is it true that the growth of a group is polynomially bounded iff $G \rhd H$, $|G : H| < \infty$, H is nilpotent?

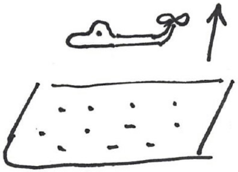
(2) Do there exist groups of intermediate growth?

Both problems were solved at about the same time in 1980-1982.

Growth of Groups

Gromov: groups of polynomial growth.

$G \rightsquigarrow \text{Cay}(G)$ metric space
G acts on $\text{Cay}(G)$ by isometries $g : x \to xg,\ x \in G$

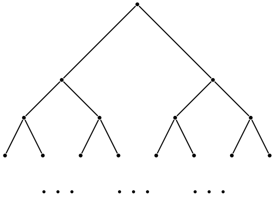


$\text{Cay}(G) \rightsquigarrow R^n.$

G acts on R^n, $G \to \text{GL}(n, R)$ linear group.

Growth of Groups

Grigorchuk: groups of intermediate growth.

$T =$  $G \leq \mathrm{Aut}(T)$

Now Branch Groups or Fractal Groups

$\rightsquigarrow$ Dynamical Systems, Number Theory, etc. etc.

Growth of Algebras

Algebras: F a field, $A = F$-algebra generated by a finite dimensional subspace V.

$$V^n = \sum \underbrace{V \cdots V}_{k},\ k \leq n,$$

$$V^1 \subseteq V^2 \subseteq \ldots, \quad \bigcup V^n = A,$$

$$g(V, n) = \dim_F(V^n).$$

If $g(V, n) \leq n^d$ (polynomially bounded) then the minimal such d = Gelfand-Kirillov dimension of A.

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 $\geq \dfrac{1}{k}$;

(2) $|A^2| \leq k|A|$;

(3) A^2 is covered by k right translates of A, $\; A^2 \subseteq \bigcup_{i=1}^{k} Ag_i$,

$\rightsquigarrow$ to the same theories.

A is a k-approximate group.

Approximate Groups

Examples.

(i) $A = \{n \mid -N \leq n \leq N\}$ is a 2-approximate group in $\mathbb{Z}$.

(ii) d-dimensional arithmetic progression

$$A = \{n_1 x_1 + \ldots + n_d x_d \mid |n_i| \leq N_i\} \subset \mathbb{Z}$$

is a 2^d-approximate subgroup

- No fast expansion $\rightsquigarrow$ approximate subgroups
- Polynomial growth (Gromov's Theorem) $\rightsquigarrow$ balls of radius n are nice approximate subgroups.

Approximate Groups

Freiman-Ruzsa: $A \subseteq \mathbb{Z}$ a k-approximate subgroup

$$\Rightarrow A \subseteq P = \{n_1 x_1 + \ldots + n_d x_d \mid |n_i| \leq N_i\}, \;\; d \leq k, \;\; \frac{|P|}{|A|} \leq f(k).$$

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

Side Effects: better understanding (efficient version) of Gromov's theorem, a new approach to Hilbert's 5th Problem.

Profinite and Pro-p Groups.

G residually finite

$\bigcap\{H \lhd G \mid |G : H| < \infty\} = (1)$.

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

$$G \longrightarrow G/\bigcap\{H \lhd G \mid |G : H| < \infty\} \longrightarrow \hat{G}$$

Profinite and Pro-p Groups

Example. K/F infinite Galois extension of fields, $\mathrm{Gal}(K/F)$ is profinite.

p a prime number, $\varphi_i : G \to G_i$, G_i are finite p-groups, $\bigcap_i \ker \varphi_i = (1)$. Then G is residually-p.

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

$$G \longrightarrow G/\bigcap\left\{H \lhd G \,\middle|\, |G:H| = p^k,\ k \geq 0\right\} \longrightarrow G_{\hat{p}}$$

Profinite and Pro-p Groups

Ex.1 F_m the free group on $x_1, \ldots, x_m$; $\forall p$ residually-p,
$(F_m)_{\hat{p}}$ free pro-p group.

Ex.2 $\mathbb{Z}_p$ p-adic integers, $\mathrm{GL}^1(n, \mathbb{Z}_p) = 1_n + pM_n(\mathbb{Z}_p)$ pro-p group.

M. Lazard (1965): $\forall p$-adic Lie group has an open subgroup that is $\hookrightarrow \mathrm{GL}^1(n, \mathbb{Z}_p)$.

Ex.2' $\mathrm{GL}^1(n, R)$, R more general commutative rings.

Polynomial identity: $1 \neq w(x_1, \ldots, x_m) \in (F_m)_{\hat{p}}$

$$\forall g_1, \ldots, g_m \in G \quad w(g_1, \ldots, g_m) = 1.$$

(p-adic Lie groups) $\subset$ (PI-groups)

Possible application

Fontaine-Mazur Conjecture:

$\forall \rho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}^1(n, R)$ the image of ρ is finite.