

Simple Groups, Buildings and Applications

Oslo, May 2008

Abel Prize to (J. T.)²: J. Thompson & J. Tits

Alex Lubotzky
Hebrew University
Jerusalem, ISRAEL

Every finite group is built out of the Finite Simple Groups ("the atoms")

CFSG Thm If G is a finite simple group (i.e. $N \triangleleft G \Rightarrow N = \{1\}$ or $N = G$) then G is one of the following:

- 1) A cyclic group of prime order.
- 2) $G \cong \text{Alt}(n)$ ($n \geq 5$) - the group of even permutations on n letters.
- 3) A group of Lie type (e.g. $\text{PSL}_n(\mathbb{F}_q)$, $\text{PSp}(2n, \mathbb{F}_q)$ etc.).
- 4) One of a list of 26 sporadic groups.

Outcome of work of many people & thousands of journal pages. But the one who enabled all this to happen is

John Thompson.



Choose elements by name, by atomic number, by symbol, by mass

I	II	III	IV	V	VI	VII	VIII
H ₁	Be ₄	B ₃	C ₆	N ₇	O ₈	F ₉	Ne ₁₀
Li ₃	Mg ₁₂	Sc ₂₁	Ti ₂₃	Al ₁₃	Si ₁₄	Cl ₁₇	Ar ₁₈
Na ₁₁		Y ₂₁	Cr ₂₄	Zn ₃₀	Ga ₃₁	As ₃₃	
K ₁₉	Ca ₂₀	Mn ₂₅	Fe ₂₆	Cu ₂₉	Ge ₃₂	Se ₃₄	
Rb ₃₇	Sr ₃₈	Zr ₄₀	Tc ₄₃	Pd ₄₆	Ag ₄₇	Te ₅₂	
Cs ₅₅	Ba ₅₆	Nb ₄₁	Mo ₄₂	Ru ₄₄	Rh ₄₅	Br ₃₅	
Fr ₈₇	Ra ₈₈	Hf ₇₂	Ta ₇₃	Os ₇₆	Ir ₇₇	Kr ₃₆	
	Ac ₈₉	Rf ₉₁	Df ₉₂	Pa ₉₃	U ₉₅	Xe ₅₄	
		105	106	107	108	109	110
		104				111	112
						113	114
						115	116

Click here for the history of the periodic table.

Ce ₅₈	Pr ₅₉	Nd ₆₀	Pm ₆₁	Sm ₆₂	Eu ₆₃	Gd ₆₄	Tb ₆₅	Dy ₆₆	Ho ₆₇	Er ₆₈	Tm ₆₉	Yb ₇₀	Lu ₇₁
Th ₉₀	Pa ₉₁	U ₉₂	Nd ₉₃	Pu ₉₄	Am ₉₅	Cm ₉₆	Bk ₉₇	Cf ₉₈	Ef ₉₉	Fm ₁₀₀	Md ₁₀₁	No ₁₀₂	Lr ₁₀₃

Thompson's main works:

1) Odd Order Theorem (with Walter Feit):

Every finite group of odd order is solvable (equ. every finite simple group of odd order is cyclic of order p).

2) N -group Theorem: A classification of the gps G in which $N_G(A)$ ($= \{g \in G \mid g^{-1}Ag = A\}$) is solvable for every $1 \neq A$ abelian subgroup of G .

(In particular: classification of the minimal simple group - those with every proper subgp is solvable).

Results & methods influences CFSG.

Tits main work :

(1) Buildings : The inventor!

$\rightsquigarrow G(k)$; simple gp over field k
 $\therefore k$ finite \rightsquigarrow FSG

For p -adic fields k - an additional:

"Bruhat-Tits buildings" - affine buildings

Analogous to Symmetric Spaces of
 simple Lie gps over \mathbb{R}

(2) Classifications of:

(a) spherical (resp. affine) buildings
 of rank ≥ 3 (resp. ≥ 4).

(b) simple alg. gps over k (p -adic....)

\therefore Buildings "≡" Groups (Klein
 Erlangen Program)

Related to CFSG by Aschbacher
 via Shult graphs.

More on affine building

$G = \text{Simple (non-comp.)}$

Lie group over \mathbb{R}

e.g. $G = SL_n(\mathbb{R})$

$K = \text{max. comp. subgroup}$

$G/K = \text{Symmetric Space}$

- a Riemannian manifold
- contractible

Ex: $G = SL_2(\mathbb{R})$

$K = SO_2(\mathbb{R})$

$G/K \cong U = \{x+iy \mid \begin{matrix} x \in \mathbb{R} \\ y \in \mathbb{R}_+ \end{matrix}\}$

$g \in G$ acts $(\begin{pmatrix} a & b \\ c & d \end{pmatrix})(z) = \frac{az+b}{cz+d}$

preserving the Hyperbolic structure of U .

$G = \text{Simple (non-comp.)}$

Lie group over \mathbb{Q}_p

e.g. $G = SL_n(\mathbb{Q}_p)$

$K = \text{max. comp. subgp}$

$G/K = \text{An affine building}$

- A CW-complex
- contractible

Ex: $G = SL_2(\mathbb{Q}_p)$

$K = SL_2(\hat{\mathbb{Z}}_p)$

$G/K \cong T_{p+1} = \text{the}$

$(p+1)$ - regular tree

"hyperbolic discrete".

G acts as auto
gps of T .

APPLICATIONS of CFSG

(A) Finite Groups

(1) Dixon, Kantor -L., Liebeck-Shalev:

2 random elements of a FSG generate it with Prob. $\rightarrow 1$ as $|G| \rightarrow \infty$.

- Full CFSG is needed even for $PSL_n(q)$!
- without CFSG even 2-generators not known.
- via maximal subgps - need CFSG again.

(2) Aschbacher - Guralnick: Every finite G is generated by 2 conjugate solvable subgps.

not true for infinite gps - e.g. F_n - free gbs.

(3) Pyber: The number of finite groups of order $\leq n$ is $N^{\frac{2}{27}(\log n)^2 + o(1)}$

(B) Permutation Groups, Graphs

(1) Full classification of
2-transitive subgps of $\text{Sym}(n)$

cor: 6-transitive is $\text{Alt}(n)$ or $\text{Sym}(n)$

→ many app's outside gp theory -
e.g. logic & model theory

(2) Computational group theory

Kantor: There is a polynomial time algorithm for finding a p -Sylow subgp of a subgp of $\text{Sym}(n)$.

(3) Cameron, Praeger, Saxl, Seitz

For $k \in \mathbb{N}$, there are only finitely many distance-transitive k -regular graphs.

(C) Infinite Groups

(1) "Theory of Finiteness Properties" failed!

e.g. Burnside Problem.

Counter example: Tarski Monster (Olshanski/Rips)

But: Theorem (Zelmanov) For $m, n \in \mathbb{N}$:

If G is generated by m elements and

$g^n = 1 \quad \forall g \in G$ and G is residually finite

(i.e. $\cap \{N \triangleleft G \mid [G:N] < \infty\} = \{1\}$)

Then G is finite.

Used CFSG via Hall-Higman

(2) Asymptotic Group Theory

Thm (L.-Mann-Segal) G finitely generated, residually finite and of polynomial subgroup growth

(i.e. $S_n(G) = \#\{H \leq G \mid [G:H] \leq n\} = n^{O(1)}$)

$\therefore G$ is virtually solvable

(B) Number theory / Central simple algs,

k - number field, $[k:\mathbb{Q}] < \infty$

D k -division alg, $Z(D) = k$, $\dim_k D < \infty$

$D \otimes_{\mathbb{K}} \mathbb{C} = M_n(\mathbb{C})$ "splits".

Thm (Fein, Kantor, Schacher) $Q \leq k \leq K$

number fields. Then $\exists \infty$ -many k -division alg's which splits over K . (i.e. $|B_2(K/k)| = \infty$)

This Thm is equivalent to:

Thm' G transitive group on X , $|X| > 1$.

Then $\exists p$ and $\exists g \in G$ of order p -power which fixes no element of X .

Thm' need CFSG!

(E) Finite Fields

- 11 -

(1) Thm (Guralnick-Wan) $\mathbb{F} = \mathbb{F}_q$, $f(x) \in \mathbb{F}[x]$

of degree n and $f: \mathbb{F}_{q^e} \rightarrow \mathbb{F}_{q^e}$.

Then either f is bijective or:

$$|f(\mathbb{F}_{q^e})| \leq \frac{5}{6} q^e + O_n(q^{e/2})$$

(2) Thm (Guralnick-Zierer) $\mathbb{F} = \mathbb{F}_q = \mathbb{F}_{p^e}$,

$f \in \mathbb{F}[x]$ of degree n , $n \neq p^\alpha$, an indecomposable poly (i.e. not a composition of poly's each of degree > 1). Then

if f become indecomposable over some finite ext. then $p=11$ and $n=55$ or $p=7$ and $n=21$.

Part of a general theory on curves, varieties etc.

Applications of Buildings

The building for $G(\mathbb{Q}_p)$ is what
the Symmetric space for $G(\mathbb{R})$.

It is THE basic tool for doing

Harmonic analysis, Representation theory,
discrete subgroups, cohomology,-----

e.g. $\Gamma \leq G(\mathbb{Q}_p) = \mathrm{SL}_n(\mathbb{Q}_p)$ a cocompact
lattice. Very little can be said without
 B - the building of $\mathrm{SL}_n(\mathbb{Q}_p)$. But with B ,
we know, e.g.

$$\mathrm{vcd}(\Gamma) = \dim B = \mathrm{rank}_{\mathbb{Q}_p}(G) = n-1$$

Garland's "p-adic curvature" gives
various vanishing results on $H^i(\Gamma; -)$
etc. etc.

This is relevant also to less abstract groups, e.g. $\Gamma = SL_n(\mathbb{Z}[\frac{1}{p}]) \leq SL_n(\mathbb{R}) \times SL_n(\mathbb{Q}_p)$ an S-arithmetic gp. It is studied via products of sym. space & building.

Then (a) (Serre) Γ - a f.g. subgp of $GL_n(\tilde{\mathbb{Q}})$. Then $vcd(\Gamma) < \infty$.

(b) (Alperin-Shalen) Γ f.g. $\leq GL_n(\mathbb{C})$.
 $vcd(\Gamma) < \infty \iff \exists$ a bound on the rank of abelian subgps of Γ .

-14-

Application "to Computer Science

Recall $G = SL_2(\mathbb{R})$, $K = SO(2)$, $G/K \simeq \mathbb{H}^2$

$\Gamma \leq G$ torsion-free, discrete, co-compact

$\therefore \Gamma \backslash G/K = \text{a Riemann Surface}$

Theorem (Selberg  \otimes Jacquet-Langlands)

If Γ is an arithmetic lattice, then

$$\lambda_1(\Gamma(n) \backslash G/K) \geq \frac{3}{16}$$

for every congruence subgroup $\Gamma(n)$.

λ_1 = smallest positive eigen-value of the Laplacian.

More to p -adic

$G = SL_2(\mathbb{Q}_p)$, $K = SL_2(\hat{\mathbb{Z}}_p)$, $G/K = T_{p+1}$

$\Gamma \leq G$ torsion-free,

$\Gamma \backslash G/K = "p\text{-adic Riemann Surface"} = \text{finite } (p+1)\text{-regular graph}$

Theorem (Lubotzky-Phillips-Sarnak / Margalit)
based on: Hecke, Deligne, T-L.

$\Gamma \leq SL_2(\mathbb{Q}_p)$ arithmetic

$$|\lambda_{\Gamma(m)\backslash G/K}| \leq 2\sqrt{p}$$

λ - non-trivial eigen-val's of
the adjacency matrix of the $(p+1)$ -regular
graph $X = \Gamma(m)\backslash G/K$

i.e. X is a finite Ramanujan
GRAPH!

Ramanujan graphs are
"optimal EXPANDERS"

Expander graphs are basic building blocks in CS: networks, algorithms, etc. etc.

$\Gamma^{(m)} \backslash G / K$ give explicit constructions

\approx Cayley Graphs $\text{Cay}(PSL_2(p); S)$

S - a well chosen set of generators

" $PSL_2(p)$ - The simple groups of Galois!"

Current challenges:

The combinatorics of $\Gamma^{(m)}$ for the general Bruhat-Tits buildings.