Linear methods in the study of automorphisms

Khukhro, E. I.

2012

MIMS EPrint: **2012.104**

ISSN 1749-9097

Linear methods in the study of automorphisms

Evgeny KHUKHRO

Overview

Mainly about automorphisms of finite groups, but also some infinite (especially nilpotent).

1. Survey
   - Results on fixed-point-free and almost fixed-point-free automorphisms
   - Open problems
2. Some methods of representation theory
   - Automorphisms as linear transformations
   - Clifford's theorem
   - Hall–Higman–type theorems
   - Automorphism of prime order with fixed-point subgroup of given rank
3. Lie ring methods
   - Automorphisms of Lie rings
   - Associated Lie rings
   - Method of graded centralizers
   - Automorphism of order p acting on a finite p-group
   - Frobenius groups of automorphisms with fixed-point-free kernel
   - Lazard Lie algebra
4. Baker–Campbell–Hausdorff formula
   - Mal'cev correspondence
   - Lazard correspondence
   - Automorphism of order p^n acting on a finite p-group
5. Elimination of operators by nilpotency

Philosophical remark:

Results modulo other parts of mathematics:

- simple or non-soluble groups are often studied modulo soluble groups: for example,
  determine simple composition factors,
  or the quotient $G/S(G)$ by the soluble radical;
- soluble modulo nilpotent: for example,
  bounding the Fitting height, or p-length;
- nilpotent modulo abelian or "centrality": typically,
  bounding the nilpotency class or derived length;
- ...finite abelian modulo number theory?

Example: Restricted Burnside Problem

If a finite group G is d-generated and has exponent n, then $|G| \leqslant f(d, n)$.

Classification $\Rightarrow$ reduction to soluble.

Hall–Higman paper $\Rightarrow$ reduction to p-groups.

Zel'manov's reduction for p-groups to Lie algebras.

Zel'manov's theorem on Engel Lie algebras.

Part 1. Survey on fixed-point-free and almost fixed-point-free automorphisms

Some definitions and notation:

$C_G(\varphi) = \{g \in G \mid \varphi(g) = g\}$ fixed-point subgroup (or subring)

Fixed-point-free: $C_G(\varphi) = 1$ (for Lie rings: $C_L(\varphi) = 0$).

Fitting series: $F_1(G) := F(G)$ Fitting subgroup
(largest normal nilpotent subgroup),

$F_{i+1}(G)$ full inverse image of $F(G/F_i(G))$ in G.

Fitting height (=nilpotent length) is the least l such that $F_l(G) = G$ in a soluble finite group G.

$\alpha(n) =$ the number of (not necessarily distinct) primes whose product is n: $\alpha(n) = \sum k_i$ if $n = \prod p_i^{k_i}$. For brevity, $\alpha(A) = \alpha(|A|)$.

G has rank $\leqslant r$ if every subgroup can be generated by r elements.

$(a, b, \dots)$-bounded means bounded above in terms of $a, b, \dots$

Fixed-point-free and almost fixed-point-free automorphisms

If a finite group (or a Lie ring) admits a fixed-point-free automorphism, then often the group (Lie ring) must be soluble or nilpotent, sometimes with bounds for the derived length or nilpotency class, or of bounded Fitting height.

Studying an *almost fixed-point-free* automorphism $\varphi \in \mathrm{Aut}\, G$ means obtaining restrictions on G depending on the fixed-point subgroup $C_G(\varphi)$ and the order of φ.

It is natural to expect that if $C_G(\varphi)$ is "small", then properties of G are correspondingly close to the case where φ is fixed-point-free: "almost" soluble, or nilpotent, or of bounded Fitting height.

Many results are also valid for non-cyclic (almost) fixed-point-free groups of automorphisms $A \leqslant \mathrm{Aut}\, G$.

Example: fixed-point-free automorphism of prime order

φ / $C_G(\varphi)$ / G	$\lvert\varphi\rvert = p$ prime, $C_G(\varphi) = 1$	$\lvert\varphi\rvert = p$ prime, $\lvert C_G(\varphi)\rvert = m$	$\lvert\varphi\rvert = p$ prime, $p \nmid \lvert G\rvert$ for insol. G, $\mathbf{r}(C_G(\varphi)) = r$ of given rank
finite	nilpotent Thompson, 59	$\lvert G/S(G)\rvert \leqslant f(p,m)$ Fong+CFSG, 76	$\mathbf{r}(G/S(G)) \leqslant f(p,r)$ EKh+Maz+CFSG, 06
+soluble	nilpotent Clifford, 30s	$\lvert G/F(G)\rvert \leqslant f(p,m)$ Hartley+Meixner, Pettet, 81	$G \geqslant N \geqslant R \geqslant 1$, $\mathbf{r}(G/N)$, $\mathbf{r}(R) \leqslant f(p,r)$, N/R nilpotent EKh+Maz, 06
+nilpotent	class $\leqslant h(p)$ Higman, 57 Kostrikin–Kreknin, 63	$G \geqslant H$, $\lvert G : H\rvert \leqslant f(p,m)$, H nilp. class $\leqslant g(p)$ EKh, 90	$G \geqslant N$, $\mathbf{r}(G/N) \leqslant f(p,r)$, N nilp. class $\leqslant g(p)$ EKh, 08
Lie ring	same, by same	same, EKh, 90 ideal, Mak. 2006	same

Automorphisms of arbitrary (composite) coprime order

φ $C_G(\varphi)$ G	$\|\varphi\| = n$ coprime $C_G(\varphi) = 1$	$\|\varphi\| = n$ coprime $\|C_G(\varphi)\| = m$	$\|\varphi\| = n$ coprime $\mathbf{r}(C_G(\varphi)) = r$
finite	soluble CFSG	$\|G/S(G)\| \leqslant f(n,m)$ Hartley, 92 +CFSG	$\mathbf{r}(G/S(G)) \leqslant f(n,r)$ EKh+Maz+CFSG, 06
+soluble	Fitting height $\leqslant \alpha(n)$ Shult, Gross, Berger	$\|G/F_{2\alpha(n)+1}(G)\|$ $\leqslant f(n,m)$ Turull+ Hartley+Isaacs	$\mathbf{r}(G/F_{4^{\alpha(n)}}(G)) \leqslant f(n,r)$ (Thompson+) EKh+Maz, 06
+nilpotent	*der. length bounded??* only $\|\varphi\| = 4$ Kovács, 61	*??????* only $\|\varphi\| = 4$ EKh+Mak, 96, 06	*??????*
Lie algebra	soluble of d.l.$\leqslant k(n)$ Kreknin, 63	$L \geqslant N$ ideal codim $N \leqslant f(n,m)$ N sol. d.l. $\leqslant g(n)$ EKh+Mak, 04	same as $\leftarrow$

Automorphisms of arbitrary (composite) non-coprime order

φ	$\|\varphi\| = n$ **non-coprime**		
G	$C_G(\varphi) = 1$	$\|C_G(\varphi)\| = m$	$\mathbf{r}(C_G(\varphi)) = r$
finite	soluble Rowley, 95 +CFSG	$\|G/S(G)\| \leqslant f(n,m)$ Hartley, 92 +CFSG	$\mathbf{r}(G/S(G)) \to \infty$ even n prime
+soluble	Fitting height $\leqslant 10 \cdot 2^{\alpha(n)}$ Dade, 69 $\leqslant \alpha(n)$*??* (proved in some cases, Ercan, Güloğlu) *polynom. in $\alpha(n)$??* *linear in $\alpha(n)$??*	Is $\|G/F_{f(\alpha(n))}(G)\|$ $\leqslant f(n,m)$*??* (proved for $\|\varphi\| = p^k$ Hartley+Turau, 87) *(open even for $\|\varphi\| = 6$)* *At least, is Fitting height $\leqslant f(n,m)$??*	Bell-Hartley examples for A non-nilp. *for A non-cyclic nilp.???*
+nilpotent	Is *der. length bounded??*	same *??* (only $\|\varphi\| = 4$ EKh+Makar. 96, 06)	*??*
Lie algebra	soluble der. length $\leqslant k(n)$ Kreknin, 63	ideal codim $\leqslant f(n,m)$ solub. d.l. $\leqslant g(n)$ EKh+Makar. 04	same as $\leftarrow$

"Modular situation"

... is when a finite p-group P admits an automorphism φ of order p^n
(which cannot be fixed-point-free);

aim: restrictions on P in terms of $|\varphi|$ and $|C_G(\varphi)|$.

(As we shall see, rank of P is easily bounded in terms of $|\varphi|$ and rank of $C_G(\varphi)$.)

Various Lie ring methods and Higman–Kreknin–Kostrikin theorems were very successfully applied (also to pro-p-groups of given coclass) in the papers of Alperin, Jaikin-Zapirain, Khukhro, Medvedev, Shalev, Shalev–Zel'manov.

(Some of these later.)

Frobenius groups of automorphisms

Frobenius group FH with kernel F and complement H
$FH \leqslant \mathrm{Aut}\, G$ with fixed-point-free kernel: $C_G(F) = 1$.

$C_G(F) = 1$ already $\Rightarrow$ G soluble by Belyaev–Hartley using CFSG.

and Fitting height of G bounded in terms of $\alpha(|F|)$
(Thompson, Shult, Gross, Berger, ... , Kurweil, Turull).

New approach: bounding G in terms of $C_G(H)$ and H
(recent results by EKh–Makarenko–Shumyatsky):

Order and rank of G — easy.

Fitting height of G = Fitting height of $C_G(H)$

If $C_G(H)$ is nilpotent and F cyclic, then G is nilpotent of class bounded in terms of the class of $C_G(H)$ and $|H|$

(not true if F is not cyclic).

When F is cyclic, the exponent of G is bounded in terms of exponent of $C_G(H)$ and $|FH|$.

Open problems

In accordance with our philosophy, problems in "layers":

Modulo CFSG many problems nowadays are reduced to soluble groups.

For soluble groups modulo nilpotent, problems are to bound the Fitting height, or p-length, even if the question is on exponent, say. Requires methods of representation theory.

For nilpotent groups further problems of bounding derived length, nilpotency class, exponent, etc.

Similar problems for Lie rings (algebras) – often easier, but some still open, too.

Open problems for soluble modulo nilpotent

For (almost) f-p-f automorphisms of coprime order a lot is already known. Further questions remain for non-slouble groups of autom., though. Some progress by Turull, Kurzweil.

But some major important problems remain open in the non-coprime case.

Open problems: centralizer of an element

Kourovka 13.8(a), Hartley's problem, included by Belyaev:

Almost fixed-point-free automorphism of non-coprime order

Suppose that φ is an automorphism of a soluble group G. Is the Fitting height of G bounded in terms of $|\varphi|$ and $|C_G(\varphi)|$?

Equivalent: element $g \in G$, Fitting height in terms of $|C_G(g)|$?

Bounds (and nice) are known for $|\varphi| = p^k$ being a prime-power (Hartley–Turau), basically because of easy reduction to coprime case.

But even the case $|\varphi| = 6$ is open.

Open problems: non-coprime

Recall

Dade's theorem

Suppose that A is a Carter (nilpotent self-normalizing) subgroup of a finite soluble group G. Let $|A|$ be the product of $\alpha(A)$ primes (not necessarily different). Then Fitting height of G is bounded by a function of $\alpha(A)$.

In Dade's paper the function is exponential.

Better bounds in Dade's theorem

Find a polynomial function of $\alpha(A)$ bounding the Fitting height of G.

Find a linear function of $\alpha(A)$ bounding the Fitting height of G.

Open problems: non-coprime

Special case of better bounds in Dade's theorem for fixed-point-free group of automorphisms

Suppose that a soluble group G admits a nilpotent fixed-point-free group of automorphisms A. Find a polynomial function of $\alpha(A)$ bounding the Fitting height of G.

Find a linear function of $\alpha(A)$ bounding the Fitting height of G.

Known only for some special cases, for example, A abelian of square-free odd order (where Turull's bound $5\alpha(A)$ was improved by Ercan and Güloğlu to best-possible $\alpha(A)$).

But all is known for coprime $(|A|, |G|) = 1$, even for A soluble group of automorphisms (Thompson–...–Kurzweil–...–Turull).

Examples of Bell–Hartley: any non-nilpotent soluble group can act fixed-point freely on groups of unbounded Fitting height.

Open problems: non-coprime cyclic

Special case of Dade's th'm for a fixed-point-free automorphism
Suppose that a soluble group G admits a fixed-point-free automorphism φ. Find a polynomial function of $\alpha(\varphi)$ bounding the Fitting height of G.

Find a linear function of $\alpha(\varphi)$ bounding the Fitting height of G.

Known only in some special cases (Ercan, Güloğlu, even with best-possible bound $\alpha(\varphi)$).

Open problems: rank, non-coprime

Suppose a finite soluble group G admits a nilpotent group of automorphisms A (of non-coprime order).

Rank analogue
Is there a function $f(\alpha(A))$ such that the rank of $G/F_{f(\alpha(A))}$ is bounded in terms of $|A|$ and the rank of $C_G(A)$?

The same question for A cyclic.

(Recall, Bell–Hartley examples for A non-nilpotent non-coprime...)

Open problems: for coprime with rank

Theorem (Khukhro–Mazurov, 06)**.** *Suppose a finite group G admits a soluble group of automorphisms A of coprime order. Then*

(a) *the rank of $G/F_{4^{\alpha(A)}-1}(G)$ and*

(b) *the order of $G/F_{5\cdot(4^{\alpha(A)}-1)/3}(G)$*

are bounded in terms of $|A|$ and the rank of $C_G(A)$.

Better bounds
Can exponential functions $4^{\alpha(A)}$ here be replaced by
linear functions of $\alpha(A)$?

(as in best possible results in terms of $|C_G(A)|$).

Better bounds
The same question for A cyclic.

Some other Hall–Higman–type problems

Wilson's problem 9.68 in Kourovka
Let $\mathfrak{V}$ be a proper variety of groups. Is there a bound on the p-lengths of the finite p-soluble groups whose Sylow p-subgroups are in $\mathfrak{V}$?

So far, Hall–Higman paper: for $\mathfrak{V}$ being varieties of soluble groups of given derived length, of nilpotent groups of given class, of groups of given exponent. Apparently, also n-Engel groups.

One of simplest open cases: $\mathfrak{V}$ given by law $[x,y]^{p^n}=1$.

Just recently some progress for $[x,y]^p=1$.

Some other Hall–Higman–type problems

Shumyatsky's problem 17.126 in Kourovka
Let G be a finite soluble group satisfying the identity $[x,y]^n=1$; is the Fitting height of G bounded in terms of n?

Shumyatsky proved this in the case $n=p^k$ (actually, then even $[G,G]$ is a p-group).

Would provide reduction to nilpotent p-groups for Shumyatsky's problem: if $[x,y]^n=1$ in a residually finite group, then $[G,G]$ is locally finite.

For nilpotent groups Shumyatsky developed technique based on RBP and Lie ring methods. For a change, it is reduction to nilpotent case that is still missing.

More Hall–Higman–type problems

Grishkov's problem on groups with triality
??

Important for finishing solution of Restricted Burnside Problems for Moufang loops??.

Again, here it is reduction to nilpotent case that is still missing, while Grishkov and Zel'manov already have results for "nilpotent case".

Recall Kreknin's theorem for Lie rings

Kreknin's theorem
Suppose that a Lie ring L admits a fixed-point-free automorphism $\varphi \in \mathsf{Aut}\, L$ of finite order n: $C_L(\varphi) = 0$. Then L is soluble of n-bounded derived length (actually $\leqslant 2^n - 2$).

Method of proof discussed later.

Open problems for nilpotent groups

Analogue of Kreknin's theorem for (nilpotent) groups
Suppose that $\varphi \in \mathsf{Aut}\, G$ is fixed-point-free: $C_G(\varphi) = 1$.
Is the derived length of G bounded in terms of $|\varphi|$?

... if in addition $(|G|, |\varphi|) = 1$?

Already reduced to G nilpotent. Only known for $|\varphi| = 4$ or a prime.

Associated Lie ring method, $L(G) = \bigoplus \gamma_i/\gamma_{i+1}$, does not work here (as it does for nilpotency in Higman's theorem), because the derived length is not preserved.

(Other Lie ring methods do work in special situations: for example, for locally nilpotent torsion-free groups, or polycyclic groups. Plus, Kreknin's theorem successfully applied for finite p-groups with automorphisms of order p^n.)

Open problems for nilpotent groups
Proving (or refuting??!!) an analogue of Kreknin's theorem obviously takes precedence before other open problems for nilpotent groups with almost fixed-point-free automorphisms, coprime or not.

Frobenius groups of automorphisms
Frobenius group FH with kernel F and complement H
$FH \leqslant \mathsf{Aut}\, G$ with fixed-point-free kernel: $C_G(F) = 1$.

Recall: G is soluble, bounds in terms of F....

New approach: bounding G in terms of $C_G(H)$ and H.

Fitting height of G = Fitting height of $C_G(H)$, so now about nilpotent.

Theorem (EKh–Makarenko–Shumyatsky, 10). *If FH is metacyclic, $C_G(F) = 1$, and $C_G(H)$ is nilpotent, then the nilpotency class of G is bounded in terms of $|H|$ and the nilpotency class of $C_G(H)$.*

Question
Is the dependence on $|H|$ necessary?

So far, only examples (Antonov–Chekanov) with class of G greater than that of $C_G(H)$.

Frobenius group of automorphisms: exponent

Theorem (Khukhro–Makarenko–Shumyatsky, 10). *Suppose that a finite group G admits a metacyclic Frobenius group FH of automorphisms with kernel F and complement H such that $C_G(F) = 1$. Then the exponent of G is bounded in terms of $|FH|$ and the exponent of $C_G(H)$.*

Question
Is the dependence on $|F|$ or $|H|$ necessary?

Mazurov's problem 17.72(b) in Kourovka Notebook:
If GFH is a double Frobenius group, is the exponent of G bounded in terms of $|H|$ and the exponent of $C_G(H)$?

Examples (Antonov–Chekanov) show that exponent of G may be greater than that of $C_G(H)$.

Exponent, continued

Question
Is metacyclic condition necessary in the above exponent theorem?

Only for $FH \cong A_4$ a similar result was proved by Shumyatsky, 2011.

Frobenius group of automorphisms: derived length

Metacyclic Frobenius group FH with kernel F and complement H
$FH \leqslant \mathsf{Aut}\, G$ with fixed-point-free kernel: $C_G(F) = 1$.

Problem on derived length:
Is the derived length of G bounded in terms of $|H|$ and the derived length of $C_G(H)$?

Already reduced to case of G nilpotent. Examples show "metacyclic" essential.

This question is open even if GFH is a 2-Frobenius group.

(For the derived length, it is unclear how to reduce to Lie rings, since the associated Lie ring may have smaller derived length than G.)

The same question on derived length is open even for Lie rings.

Similar questions can be asked for other properties and parameters of a finite group G with a Frobenius group of automorphisms FH such that $C_G(F) = 1$: if $C_G(H)$ is supersoluble? satisfies other laws, like Engel?

Open problems for Lie rings and algebras

Definition. Let $k(n)$ be Kreknin's function bounding the derived length of a Lie ring with a fixed-point-free automorphism of order n.

Kreknin's bound: $k(n) \leqslant 2^n - 2$.

Better bounds for Kreknin's function
Find a polynomial bound for $k(n)$.

Is there a linear function of n bounding $k(n)$?

Open problems: Higman function

Definition. Let $h(p)$ be Higman's function bounding the nilpotency class of a Lie ring with a fixed-point-free automorphism of prime order p.

Kreknin+Kostrikin bound: $h(p) \leqslant \dfrac{(p-1)^{k(p)} - 1}{p-2} \approx p^{2^p}$

Better bounds for Higman's functions

Find a polynomial function of p bounding above $h(p)$.

Is $h(p) = (p^2 - 1)/4$?

Higman's examples show $h(p) \geqslant (p^2 - 1)/4$.

Conjecture $h(p) = (p^2 - 1)/4$ confirmed for $p = 3, 5, 7, 11$.

Frobenius group of automorphisms

Lie ring L admits a metacyclic Frobenius group $FH \leqslant \mathsf{Aut}\, L$ with kernel F and complement H, with fixed-point-free kernel: $C_L(F) = 0$.

Problem on derived length:
Is the derived length of L bounded in terms of $|H|$ and the derived length of $C_L(H)$?

Examples show that metacyclic is essential.

2. Some methods of representation theory

Group language $\leftrightarrow$ linear transformations

Let V be an elementary abelian p-group. Then V can be regarded as a vector space over $\mathbb{F}_p$: addition $a + b := ab$, scalar multiplication by $k \in \{0, 1, \dots, p-1\}$ is $ka := a^k$.

Let this $V = N/M$ be a normal section of a group G (i.e. both N, M are normal). Then any element $g \in G$ induces by conjugation a linear transformation $\bar{g} \in \mathsf{Hom}_{\mathbb{F}_p}(V)$, which we denote by right operators: $v\bar{g} := v^g$ (often bar is omitted $= vg$).

If in addition V is also φ-invariant for $\varphi \in \mathsf{Aut}\, G$, then also $\varphi \in \mathsf{Hom}_{\mathbb{F}_p}(V)$.

Representation theory applies. One of advantages: extending the ground field, eigenvectors, etc.

Group language $\leftrightarrow$ linear transformations

For example, $[v, g] = v^{-1}v^g = -v + v\bar{g} = v(\bar{g} - 1)$;
then $[[v, g], g] = v(\bar{g} - 1)^2$, etc.

Let $|\varphi| = n$. Free $k\langle\varphi\rangle$-module: $V = V_1 \oplus \cdots \oplus V_n$
with $V_i\varphi = V_{i+1}$ and $V_n\varphi = V_1$.
Clearly, then $C_V(\varphi) \neq 0$ ($=$ "diagonal").

(Free modules imply other nice properties – later.)

Recall Maschke's theorem: if $(|G|, |V|) = 1$, then every G-invariant subspace U has G-invariant complement W s.t. $V = U \oplus W$.

Irreducible nilpotent linear group has cyclic centre: if V is minimal G-invariant for G nilpotent, then $Z(G/C_G(V))$ is cyclic.

If in addition over splitting field for G, then $Z(G/C_G(V))$ is represented by scalar transformations, so $Z(G/C_G(V)) \leqslant Z(GL(V))$.

p-element in characteristic p

Let $g \in GL(V)$ in char. p such that $|g| = p^n$.

$g^{p^n} = 1 \Rightarrow g^{p^n} - 1 = 0 \Rightarrow g$ is a root of $X^{p^n} - 1$.

But in char. p we have $X^{p^n} - 1 = (X - 1)^{p^n}$.
So all eigenvalues of g are 1.
So no need to extend ground field — there is a Jordan basis (even over $\mathbb{F}_p$), where matrix of g is block-diagonal with blocks

$$J = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}$$

Powers are easily computed:

$$J^k = \begin{pmatrix} 1 & \binom{k}{1} & \binom{k}{2} & & \\ & 1 & \binom{k}{1} & \ddots & \\ & & \ddots & \ddots & \\ & & & 1 & \binom{k}{1} \\ & & & & 1 \end{pmatrix}$$

To have $|g| = p^n$, by divisibility argument,
all sizes must be $\leqslant p^n \times p^n$, with at least one $> p^{n-1} \times p^{n-1}$.

Clearly, each block contributes exactly 1 to $\dim C_V(g)$.
As a result, $\dim V \leqslant p^n \cdot \dim C_V(g)$.

Corollary. *If φ is an automorphism of order p^n of a finite p-group P, then the rank of P is bounded in terms of p^n and the rank of $C_V(g)$.*

Choose maximal abelian normal $A \leqslant P\langle\varphi\rangle$,
then $V = \Omega_1(A)$ same rank as A.

Rank of $V = \dim V$ is bounded as we saw above.

Hall–Merzlyakov–Gorchakov lemma: the rank of a p-group of automorphisms of an abelian p-group of rank r is bounded in terms of r. Apply to $P/(A \cap P)$ acting faithfully on A.

Clifford's theorem

Theorem (Clifford, 1937)**.** *Let V be an irreducible kG-module, and N a normal subgroup of G. Then $V = W_1 \oplus \cdots \oplus W_n$, where each W_i is the sum of all isomorphic irreducible kN-submodules of a given type, called Wedderburn homogeneous components, which are transitively permuted by G.*

Example of application of Clifford's theorem

Theorem (Folklore)**.** *If a finite soluble group G admits a fixed-point-free automorphism φ of prime order q, then G is nilpotent.*

Clearly, $(q, |G|) = 1$ (otherwise φ would have nontrivial fixed point in Sylow q-subgroup of G, which could be chosen φ-invariant: include φ in a Sylow q-subgroup of $G\langle\varphi\rangle$ and intersect with normal subgroup G).

Hence φ is f-p-f on all invariant sections by well-known properties of coprime action.

Sufficient: $G = O_{p',p}(G)$ for every prime p.
Suppose $G \neq O_{p',p}(G)$. Known: $\bar{G} := G/O_{p',p}(G)$ faithful on $V := O_{p',p}(G)/\Phi$ (where Φ is preimage of Frattini of $O_{p',p}/O_{p'}$).

Since $O_p(\bar{G}) = 1$, a minimal φ-invariant abelian $R \leqslant \bar{G}$ is elementary abelian r-group for $r \neq p$.
Consider the linear action of $R\langle\varphi\rangle$ on V regarded as a vector space. Aim: contradiction with $C_G(\varphi) = 1$. Extend the ground field to algebraically closed k. Choose an irreducible $R\langle\varphi\rangle$ submodule W where R is nontrivial.

Apply Clifford's theorem with respect to R:
$W = W_1 \oplus \cdots \oplus W_n$.

Since φ permutes the W_i transitively, either $n = 1$ or $n = q$.

If $n = 1$, then W is a homogeneous kR-module, but R abelian $\Rightarrow$ acts scalarly $\Rightarrow$ φ centralizes $R/C_R(W) \Rightarrow$ φ has a fixed point in R
since action is coprime $\Rightarrow$ φ has a fixed point also in G.

If $n = q$, then W is a free $\langle\varphi\rangle$-module and we get a "diagonal" fixed point in W (recall: for $0 \neq w \in W_1$ the sum over orbit: $0 \neq w + w\varphi + w\varphi^2 + \cdots + w\varphi^{q-1} \in C_W(\varphi)$). Fixed point independent of the field $\Rightarrow C_V(\varphi) \neq 0$ $\Rightarrow$ φ has fixed point in G, contradiction.

Frobenius group of automorphisms with f-p-f kernel

Lemma. *Suppose that V is a vector space over any field k admitting a finite Frobenius group of linear transformations FH with kernel F and complement H such that $C_V(F) = 0$. Then V is a free kH-module.*

Reduction to $|F|$ coprime to characteristic p:
$F = F_p \times F_{p'}$. Must have $C_V(F_{p'}) = 0$ — otherwise F_p has nontrivial fixed points on $C_V(F_{p'})$ (which is F_p-invariant); then $0 \neq C_{C_V(F_{p'})}(F_p) = C_V(F)$.

May assume ground field k algebraically closed (condition $C_V(F) = 0$ is preserved, and it suffices to prove that V is a free H-module over larger field: by Deuring–Noether theorem, as being free module means having basis permuted by H regularly).

$$\overline{V} = U_1 > U_2 > \cdots > U_l > U_{l+1} = 0,$$

where each factor U_i/U_{i+1} is an irreducible kFH-module.
It is sufficient to prove that each factor $U = U_i/U_{i+1}$ is a free kH-module.

Since action of F is coprime, we also have $C_U(F) = 0$.

Clifford's theorem with respect to F:

$$U = W_1 \oplus \cdots \oplus W_t.$$

Wedderburn components W_i transitively permuted by H.
Let H_1 be the stabilizer of W_1 in H acting on $\{W_1, \dots, W_t\}$.

If $H_1 = 1$, then U is a free kH-module.

But if $H_1 \neq 1$, then H_1 centralizes the centre $Z(F/C_F(W_1))$ represented on W_1 by scalar linear transformations.
This centre is nontrivial, as $F/C_F(W_1)$ is nilpotent.
Then we obtain nontrivial fixed points of H_1 on F — impossible in Frobenius group FH.

Frobenius groups of automorphisms
Finite group G admitting a Frobenius group of automorphisms $FH \leqslant \mathrm{Aut}\, G$ with kernel F and complement H,
such that $C_G(F) = 1$. (by Belyaev–Hartley + CFSG, G is soluble)

Easy corollaries of "freedom lemma" for order and rank:

As we saw, all FH-invariant normal elementary abelian sections
are free H-modules $\Rightarrow |G| = |C_G(H)|^{|H|}$;

and just a bit more work: rank of G is bounded in terms of rank of $C_G(H)$ and $|H|$.

Other results EKh–Makarenko–Shumyatsky are more difficult: the Fitting height, nilpotency class, exponent.

Bounding nilpotency class and exponent are by various Lie ring methods, including similar results for Lie rings with such Frobenius groups of automorphisms — later.

Hall–Higman type theorems

Example: bounding Fitting height of a finite soluble group G with a fixed-point-free automorphism φ of prime-power order q^n.

Again, $(q, |G|) = 1$; so φ is f-p-f on all invariant sections.

Idea: if φ is not faithful on $G/F(G)$, then induction on $|\varphi|$ applies to $G/F(G)$.

In most cases, *if φ is faithful on $G/F(G)$, then $C_{F(G)}(\varphi) \neq 1$.* "Most cases" have exceptions, but these are quite constrained and can be controlled by Hall–Higman–type theorems.

Since $F(G) = \bigcap O_{p',p}(G)$, we can assume φ is faithful on one of $\bar{G} = G/O_{p',p}(G)$ (for if $[\varphi^{q^{n-1}}, G] \leqslant O_{p',p}(G)$ for all p, then $[\varphi^{q^{n-1}}, G] \leqslant \bigcap O_{p',p}(G) = F(G)$).

Linear action of $\bar{G}\langle\varphi\rangle$ on elementary abelian p-group $V = O_{p',p}(G)/\Phi$,
extend ground field; aim: $C_V(\varphi) \neq 0$, which would be a contradiction.

Application of Clifford's theorem

Minimal normal φ-invariant R of $\bar{G}$, where $\varphi^{q^{n-1}} \neq 1$. Known: R is a special r-group for some prime r: either elementary abelian,
or nilpotent of class 2 with $Z(R) = [R, R] = \Phi(R)$.

If R is abelian, then $R\langle\varphi\rangle$ is Frobenius and as before we arrive at free $\langle\varphi\rangle$-submodule $\Rightarrow$ a fixed point of φ.

Hall–Higman–type theorems for class 2 case: basically, a free $\langle\varphi\rangle$-submodule still exists with a few very constrained exceptions.

First apply Clifford's theorem — induction reduces to the case of one $W = W_1$. Then R an extra-special r-group.

Lemma ("non-modular Hall-Higman"). *Let G be a group of linear transformations acting irreducibly on a vector space V over an algebraically closed field k of characteristic prime to $|G|$. Assume $G = RQ$, where $R \lhd G$, R is extra-special of order r^{2t+1}, $Q = \langle g\rangle$ is cyclic of order q^n, and Q acts faithfully and irreducibly on R/R' and trivially on R'. Then either*

(a) the minimal polynomial of g on V is $X^{q^n} - 1$
(means there is a free $k\langle g\rangle$-submodule $\Rightarrow$ fixed point)

or

(b) minimal polynomial of g on V is $(X^{q^n} - l)/(X - 1)$ and $r^t = q^n - 1$.

(b) is called exceptional case.

For example, if $|G|$ and q are odd, only (a) possible.

Rank analogue of Hartley–Meixner–Pettet theorem

Theorem (Khukhro–Mazurov, 06). *If a finite soluble group G has an automorphism φ of prime order q with $C_G(\varphi)$ of rank r, then G has characteristic subgroups $G \geqslant N \geqslant R$ such that N/R is nilpotent and both G/N and R have (q, r)-bounded rank.*

"Soluble" can be dropped if $(q, |G|) = 1$ (using CFSG), but there are examples with non-coprime with $|G/S(G)| \to \infty$.

Later: also nilpotency class of N/R is q-bounded.

Induction plus Thompson-64 give consequences for soluble $A \leqslant \operatorname{Aut} G$ of coprime order with given rank of $C_G(A)$.

In contrast to Hartley–Meixner–Pettet
(where $|G/F(G)| \leqslant f(q, |C_G(\varphi)|)$),
examples show that here R is unavoidable.

R unavoidable in our theorem: $C_G(\varphi)$ of rank r $\Rightarrow G \overset{b.r.}{\geqslant} N \overset{nilp}{\geqslant} R \overset{b.r.}{\geqslant} 1$

Example. Let $p_1, p_2, \ldots, p_n$ be distinct primes > 7.
For each i, let E_i be elementary abelian group of order p_i^6

$\operatorname{Aut} E_i$ contains Frobenius group F_i with kernel A_i of order 7 and cyclic complement $\langle B_i\rangle$ of order 6 such that A_i is fixed-point-free on E_i.

Consider $(E_1 \rtimes F_1) \times \cdots \times (E_n \rtimes F_n)$.
Let $b = b_1 \cdots b_n$ and $G = \langle b^2,\ E_i,\ A_i \mid i = 1, \ldots n\rangle$.

b^3 induces automorphism φ of G of order $q = 2$.
Then $C_G(\varphi)$ has rank 3.

But both the rank of $G/F(G)$ and the rank of any normal subgroup with nilpotent quotient is equal to n.

Initial reductions in the proof

We deal only with soluble case
(by CFSG, if $(|\varphi|, |G|) = 1$, then $G/S(G)$ is of bounded rank).

Theorem (Khukhro–Mazurov, 06). *If a finite soluble group G has an automorphism φ of prime order q with $C_G(\varphi)$ of rank r, then G has characteristic subgroups $G \geqslant N \geqslant R$ such that N/R is nilpotent and both G/N and R have (q, r)-bounded rank.*

Easy reduction to G of coprime order.
So we assume from the outset that $(|G|, q) = 1$.

Non-modular Hall–Higman–type theorem

Recall "non-modular" Hall–Higman–type lemma in our case:

Lemma ("H-H-Lemma"). *Let $T \rtimes \langle\varphi\rangle$, where T is a t-subgroup and $|\varphi| = q$ is a prime $\neq t$. Suppose that $T = [T, \varphi] \neq 1$, and $T/Z(T)$ is abelian of exponent t. If $T \rtimes \langle\varphi\rangle$ acts faithfully and irreducibly on a vector space V over a splitting field of characteristic $\neq t, q$, then either*

(a) *$C_V(\varphi) \neq 0$ and $\dim V = q \cdot \dim C_V(\varphi)$ or*

(b) *$C_V(\varphi) = 0$, the group T is extraspecial, $[Z(T), \varphi] = 1$, the order $|T|$ is bounded in terms of q, $t = 2$, and $q = t^m + 1$ for some positive integer m.*

Part (b) — "exceptional case".

"Weak" bound for Fitting height, in terms of q and r

Proposition. *The Fitting height of G is (q, r)-bounded.*

Proved by using H–H–type lemma and standard tools, like Kolchin–Mal'cev theorem.

aim: STRONG (bounded rank)–nilp–(bounded rank)

Already have: Fitting height of G is (q, r)-bounded.

So we can use induction on the Fitting height.

Characteristic from normal

In our induction on the Fitting height,

great help: "turning" normal subgroups into characteristic ones:

Theorem (Khukhro–Mazurov, 06). *If a finite soluble group G has normal subgroups $G \geqslant N \geqslant R$ such that N/R is nilpotent and both G/N and R have rank $\leqslant r$, then G has characteristic subgroups $G \geqslant N_1 \geqslant R_1$ such that N_1/R_1 is nilpotent and both G/N_1 and R_1 have r-bounded rank.*

This theorem makes it possible to reduce our induction on the Fitting height just to the case $G = F_2(G)$ (in a typical case).

Hall–Higman–type theorems combined with powerful p-groups

We shall see in detail a special but typical non-exceptional case, to see how Hall–Higman–Lemma is combined with powerful p-groups.

Powerful p-groups

Definition. A finite p-group P is *powerful* if $[P, P] \leqslant P^p$ for $p \neq 2$,
or $[P, P] \leqslant P^4$ for $p = 2$.

Theorem (Lubotzky–Mann, 87). (a) *If a powerful p-group P is generated by d elements, then the rank of P is at most d and P is a product of d cyclic subgroups.*

(b) *Any finite p-group of rank r contains a characteristic powerful subgroup of index at most $p^{r(\log_2 r+2)}$.*

Corollary. *If a finite p-group has rank r and exponent e, then its order is at most $e^{f(r)}$ for some r-bounded number $f(r)$.*

Proof: By part (b), the group can be assumed to be a powerful p-group; part (a) completes the proof.

Typical non-exceptional case
$\gamma_i(X)$ lower central series; $\gamma_\infty(G) = \bigcap_i \gamma_i(X)$ nilpotent coradical.

Proposition. *Suppose that a finite soluble q'-group G admits an automorphism φ of prime order q such that $C_G(\varphi)$ has rank r. Suppose that $G = PT$, where $P = F(G)$ is a p-subgroup and $T = [T,\varphi]$ is a t-subgroup, where p, q, t are distinct primes and $q \neq 2 \neq t$. Then $\gamma_\infty(G)$ has (q,r)-bounded rank.*

In the theorem, $R = \gamma_\infty(G)$

Remark: may look as if even $G > R > 1$ with R of bounded rank and G/R nilpotent – but in general need reductions from G to $[G,\varphi]$, and from G to $O_{q'}$, so a bit of bounded rank on top appears (and also due to other reasons).

P is (q,r)-boundedly generated
$\gamma_\infty(G) = [P,T] = [P,T,T] = \cdots$, so may assume $P = [P,T]$.

Lemma. *P is generated by (q,r)-boundedly many elements,*
that is, rank (= dim) of $V = P/\Phi(P)$ is (q,r)-bounded.

Proof: $V = V_1 \supset V_2 \supset \cdots \supset 0$, with $\mathbb{F}_p T\,\langle\varphi\rangle$-irreducible $U_i = V_i/V_{i+1}$.

By Maschke's theorem, $[U_i,T] = U_i$ for each i. In particular, T acts non-trivially on U_i.

Since $[T,\varphi] = T$, by non-exceptional H-H-Lemma $\dim U_i \leqslant q \cdot \dim C_{U_i}(\varphi)$.

Since $\sum_i \dim C_{U_i}(\varphi) = \dim C_V(\varphi) \leqslant r$, as a result we have

$$\dim V = \sum_i \dim U_i \leqslant q \dim C_V(\varphi) \leqslant qr,$$

so P is (q,r)-boundedly generated.

Powerful subgroup
The crucial step is to show that P has a powerful p-subgroup of bounded rank and 'co-rank'. The construction of a powerful subgroup is similar to a part of Shumyatsky-98 proof for $q = 2$.

Let M be some normal $T\langle\varphi\rangle$-invariant subgroup of P
(which we shall choose later).

Consider the quotient $\overline{P} = P/M^p$ (or P/M^4 if $p = 2$); let the bar denote the images.

Since $\overline{M} = M/M^p$ (or M/M^4) has exponent p (or 4), the <u>order</u> of the centralizer of φ in this group is at most p^f for some r-bounded number $f = f(r)$.

Recall: $\overline{P} = P/M^p$ (or P/M^4) and $|C_{\overline{M}}(\varphi)| \leqslant p^f$
We denote by $\zeta_i(X)$ the upper central series.

Lemma. $\overline{M} \leqslant \zeta_{2f+1}(\overline{P})$.

Proof: Consider the following central series of $\overline{P}$:
$M_1 = \overline{M} > M_2 > M_3 > \cdots > 1$, where $M_i = [\overline{M}, \overline{P}, \ldots, \overline{P}]$ (i times;
we can simply write P instead of $\overline{P}$).

All the M_i are normal and $T\langle\varphi\rangle$-invariant.

Let $V_i = M_i/M_{i+1}$. These are elementary abelian p-groups, regarded as $\mathbb{F}_p T\,\langle\varphi\rangle$-modules.

Whenever $[V_i,T] \neq 0$ we have $C_{V_i}(\varphi) \neq 0$ by non-exceptional H-H-Lemma.

Since $|C_{\overline{M}}(\varphi)| \leqslant p^f$, there can be at most f factors V_i with $[V_i,T] \neq 0$.

Proving $\overline{M} \leqslant \zeta_{2f+1}(\overline{P})$
Therefore for some $k \leqslant 2f+1$ we must have

both $[V_k,T] = 0$ and $[V_{k+1},T] = 0$. In other words, we have

$[[T,M_k],P] \leqslant [M_{k+1},P] = M_{k+2}$ and

$[[M_k,P],T] = [M_{k+1},T] \leqslant M_{k+2}$.

By Three Subgroup Lemma:

$[[P,T],M_k] = [P,M_k] = M_{k+1} \leqslant M_{k+2}$.

Then, of course, $M_{k+1} = 1$, since P is nilpotent: $M_{k+1} \leqslant M_{k+2} \Rightarrow [M_{k+1},P] \leqslant [M_{k+2},P]$, that is, $M_{k+2} \leqslant M_{k+3}$, and so on, $= 1$ in the end.

This means precisely that $\overline{M} \leqslant \zeta_k(\overline{P}) \leqslant \zeta_{2f+1}(\overline{P})$.

Recall: $\overline{M} \leqslant \zeta_{2f+1}(\bar{P})$. **Bounding rank of** P

We now put $M = \gamma_{2f+1}(P)$ ($= \gamma_{2f+1}$ for brevity).

Then $[\overline{M}, \overline{M}] \leqslant [\gamma_{2f+1}(\bar{P}), \zeta_{2f+1}(\bar{P})] = 1$, that is, $[M, M] \leqslant M^p$ (or $[M, M] \leqslant M^4$). Thus, $M = \gamma_{2f+1}(P)$ is a powerful p-subgroup of P.

The quotient P/γ_{2f+1}^p is then nilpotent of class $4f + 1$ (since $\gamma_{2f+1}/\gamma_{2f+1}^p \leqslant \zeta_{2f+1}(P/\gamma_{2f+1}^p)$ by above).

Since P is (q, r)-boundedly generated and P/γ_{2f+1}^p is nilpotent of class $4f + 1$, the rank of P/γ_{2f+1}^p is (q, r)-bounded.

In particular, rank of $\gamma_{2f+1}/\gamma_{2f+1}^p$ is (q, r)-bounded, $=$ rank of the powerful p-subgroup γ_{2f+1} by properties of powerful p-groups.

As a result, the rank of P is (q, r)-bounded, as required.

Exceptional cases

Exceptional case of part (b) in H-H-Lemma obstructs extending the above arguments;

in particular, we can assume that $q \neq 2$.

...Certain reduction to the case where $G = O_{2',2}$ with $O_{2'}$ nilpotent.

To get rid of exceptional situations:

Let W be a φ-invariant Sylow 2-subgroup of G.

Idea: "push up" exceptional "bad" pieces of W;

they only form a quotient of (q, r)-bounded rank.

Remaining 'good' part of G is then dealt with similarly to non-exceptional Proposition above.

Exceptional cases: "push-up"

Let $\mathfrak{V}$ be the set of all $G\langle\varphi\rangle$-invariant sections V of $O_{2'}(G)$ that are $G\langle\varphi\rangle$-irreducible elementary p-groups (for various p) such that $C_V(\varphi) = 1$

Let $K = \bigcap_{V \in \mathfrak{V}} C_G(V)$.

Exceptional part (b) of H-H-Lemma is used to show that G/K has (q, r)-bounded rank.

It remains to consider the action of $K\langle\varphi\rangle$ on $O_{2'}(G)$.

Definition of K ensures that $C(\varphi) \neq 1$ in the sections that appear in these arguments – no exceptional situations, proceed virtually exactly as in Proposition above.

Arrive at $\gamma_\infty(K)$ having (q, r)-bounded rank, which completes the proof.

Corollaries for $A \leqslant \mathsf{Aut}\, G$

Recall: $|A|$ is a product of $\alpha(A)$ primes (not necessarily distinct).

Theorem (Mazurov–Khukhro, 06). *Let A be a soluble group of automorphisms of a finite group G of coprime order,* $(|A|, |G|) = 1$. *Then*

(a) *the rank of* $G/F_{4^{\alpha(A)}-1}(G)$ *and*

(b) *the order of* $G/F_{5\cdot(4^{\alpha(A)}-1)/3}(G)$

are bounded in terms of $|A|$ *and the rank of* $C_G(A)$.

By CFSG.... $G/S(G)$ has bounded rank, so may assume that G is soluble.

Recall: if $|A|$ and $|G|$ are not coprime and A is not nilpotent, there are Bell–Hartley examples with $C_G(A) = 1$ and the Fitting height of G is unbounded.

Recall open problem: without $(|A|, |G|) = 1$ for A nilpotent (as we know, true for $|A|$ a prime).

Also open problem to improve functions to linear in $\alpha(A)$.

Another result for A **of prime order**

The theorem for A follows from the case of $A = \langle\varphi\rangle$ of prime order by a straightforward induction on $\alpha(A)$ based on the classical theorem of Thompson, 64.

Although the previous "rank-nilp-rank" theorem for φ of prime order is "best-possible", with just one nilpotent bit, we also derived from it another "best-possible" result for A of prime order

(note: no coprimeness in parts (a), (b).)

Theorem (Khukhro–Mazurov, 06)**.** *If a finite soluble group G admits an automorphism φ of prime order q such that $C_G(\varphi)$ has rank r, then*

(a) *for each prime p the quotient $G/O_{p',p}(G)$ has (q,r)-bounded rank;*

(b) *$G/F_3(G)$ has (q,r)-bounded rank;*

(c) *if in addition $q \nmid |G|$, then $G/F_4(G)$ has (q,r)-bounded order.*

Examples show that

part (b) is best possible in the sense that the rank of $G/F_2(G)$ need not be bounded.

Thompson's theorem

Thompson's theorem of 1964 enables induction in the proof of a bound for the rank of $G/F_{4^{\alpha(A)}-1}(G)$.

Theorem (Thompson, 64)**.** *Let φ be an automorphism of prime order q of a finite soluble group G such that $q \nmid |G|$. Then $F(C_G(\varphi)) \leqslant F_4(G)$.*

Corollary. *Let B be a soluble group of automorphisms of a finite soluble group G such that $(|G|, |B|) = 1$. Then $F_k(C_G(B)) \leqslant F_{k4^{\alpha(B)}}(G)$ for every k.*

(By straightforward induction on k and $\alpha(B)$)

Bounding rank of $G/F_{4^{\alpha(A)}-1}(G)$

Here is how Theorem for A is derived from the case of A of prime order.

Recall: A soluble $\leqslant \operatorname{Aut} G$ of coprime order. We need to prove that rank of $G/F_{4^{\alpha(A)}-1}(G)$ is bounded in terms of $|A|$ and the rank of $C_G(A)$.

Induction on $\alpha(A)$. For $\alpha(A) = 1$, By Theorem (b) above, $G/F_3(G)$ has bounded rank.

For $\alpha(A) > 1$, choose A_1 normal of prime index q in A. Then $C = C_G(A_1)$ admits $\langle\varphi\rangle = A/A_1$ of prime order q with $C_C(\varphi) = C_G(A)$.

By Theorem (b) above the rank of $C/F_3(C)$ is bounded in terms of $r = r(C_G(A))$ and q.

By Thompson's Corollary, $F_3(C) \leqslant F_{3\cdot 4^{\alpha(A)-1}}(G)$; so the rank of the image of $C_G(A_1)$ in $G/F_{3\cdot 4^{\alpha(A)-1}}(G)$ is (q,r)-bounded.

By induction applied to this quotient and A_1, rank of $G/F_{4^{\alpha(A)-1}-1+3\cdot 4^{\alpha(A)-1}}(G) = G/F_{4^{\alpha(A)}-1}$ is (q,r)-bounded.

3. Lie ring methods

Lie rings and algebras

Recall: Lie ring L: additive group $(L,+)$
with Lie product (=bracket=multiplication) $[x,y]$, which is

bilinear w.r.t. addition, anticommutative: $[x,x] = 0$,

satisfies Jacobi identity: $[[x,y],z] + [[y,z],x] + [[z,x],y] = 0$.

Lie algebra over a field k if it is also a vector space over k...

Automorphisms, ideals, soluble, nilpotent...

$[A,B] = {}_+\langle [a,b] \mid a \in A,\ b \in B\rangle$

$\gamma_k(L) = [...[[L,L],L]\dots,L]; \qquad = 0$ nilpotent of class $k-1$

$L^{(1)} = [L,L], \quad L^{(k+1)} = [L^{(k)}, L^{(k)}]$

$L^{(k)} = 0$ soluble of derived length k Examples:

Free Lie algebras similarly to free groups...

$\mathbb{R}^3$ with cross-product as Lie bracket: $[x,y] := x \times y$.

Square matrices w.r.t. $[A,B] = AB - BA$.

Actually, every Lie algebra can be obtained from associative (noncommutative) algebra A as $A^{(-)}$ with $[x,y] = xy - yx$.

If L is a Lie algebra with basis $e_1, e_2, \dots$, then by linearity only need *structure constants* $[e_i, e_j] = \sum_k C_{ijk} e_k$. Not every set of C_{ijk} defines a Lie algebra, but enough to check anti-commutativity and Jacobi for the e_i.

Example: Witt Lie algebra (over $\mathbb{Q}$):

basis: e_i, $i \in \mathbb{Z}$; structure constants: $[e_i, e_j] = (i-j)e_{i+j}$.

φ $C_G(\varphi)$ G	$\lvert\varphi\rvert = p$ prime $C_G(\varphi) = 1$	$\lvert\varphi\rvert = p$ prime $\lvert C_G(\varphi)\rvert = m$	$\lvert\varphi\rvert = p$ prime $p \nmid \lvert G\rvert$ for insol. G $\mathbf{r}(C_G(\varphi)) = r$ of given rank
finite	nilpotent Thompson, 59	$\lvert G/S(G)\rvert \leqslant f(p,m)$ Fong+CFSG, 76	$\mathbf{r}(G/S(G)) \leqslant f(p,r)$ EKh+Maz+CFSG, 06
+soluble	nilpotent Clifford, 30s	$\lvert G/F(G)\rvert \leqslant f(p,m)$ Hartley+Meixner, Pettet, 81	$G \geqslant N \geqslant R \geqslant 1$, $\mathbf{r}(G/N)$, $\mathbf{r}(R) \leqslant f(p,r)$, N/R nilpotent EKh+Maz, 06
+nilpotent	class $\leqslant h(p)$ Higman, 57 Kostrikin– Kreknin, 63	$G \geqslant H$, $\lvert G : H\rvert \leqslant f(p,m)$, H nilp. class $\leqslant g(p)$ EKh, 90	$G \geqslant N$, $\mathbf{r}(G/N) \leqslant f(p,r)$, N nilp. class $\leqslant g(p)$ EKh, 08
Lie ring	same, by same	same, EKh, 90 ideal, Mak. 2006	same

φ $C_G(\varphi)$ G	$\lvert\varphi\rvert = n$ coprime $C_G(\varphi) = 1$	$\lvert\varphi\rvert = n$ coprime $\lvert C_G(\varphi)\rvert = m$	$\lvert\varphi\rvert = n$ coprime $\mathbf{r}(C_G(\varphi)) = r$
finite	soluble CFSG	$\lvert G/S(G)\rvert \leqslant f(n,m)$ Hartley, 92 +CFSG	$\mathbf{r}(G/S(G)) \leqslant f(n,r)$ EKh+Maz+CFSG, 06
+soluble	Fitting height $\leqslant \alpha(n)$ Shult, Gross, Berger	$\lvert G/F_{2\alpha(n)+1}(G)\rvert$ $\leqslant f(n,m)$ Turull+ Hartley+Isaacs	$\mathbf{r}(G/F_{4^{\alpha(n)}}(G)) \leqslant f(n,r)$ (Thompson+) EKh+Maz, 06
+nilpotent	*der. length* *bounded??* only $\lvert\varphi\rvert = 4$ Kovács, 61	*??????* only $\lvert\varphi\rvert = 4$ EKh+Mak, 96, 06	*??????*
Lie algebra	soluble of d.l.$\leqslant k(n)$ Kreknin, 63	$L \geqslant N$ ideal codim $N \leqslant f(n,m)$ N sol. d.l. $\leqslant g(n)$ EKh+Mak, 04	same as $\leftarrow$

Automorphisms of Lie rings and algebras with few fixed points

As we saw in the bottom layer of those tables,
nice results Higman–Kreknin–Kostrikin for Lie rings with fixed-point-free automorphisms.

(Earlier Jacobson–Borel–Mostow for finite-dimensional, without bounds for nilpotency class or derived length.)

Also Khukhro–Makarenko results for Lie rings with almost fixed-point free automorphisms.

Yield corollaries for groups, although some problems also remain open.

Groups of automorphisms of Lie algebras and their fixed points

Bergman–Isaacs: $G \leqslant \mathrm{Aut}\, A$ of associative algebra A of characteristic coprime to $|G|$ such that $C_A(G) = 0$. Then A is nilpotent.

Other results, ... Kharchenko.

For Lie algebras not true for non-cyclic G:
simple 3-dim. L admits noncyclic G of order 4 with $C_L(G) = 0$.

But Bakhturin–Zaitsev–Linchenko: $G \leqslant \mathrm{Aut}\, L$ of a Lie algebra L of characteristic coprime to $|G|$ such that $C_L(G)$ satisfies a polynomial identity. Then L also satisfies a polynomial identity.

Also finds application in group theory.

Analogues of eigenspaces

Suppose A is an abelian group, in additive notation,
and $\varphi \in \mathrm{Aut}\, A$ with $\varphi^n = 1$.

If A is a vector space over a field k of char. coprime to n, then, after extending the field with $\omega = \sqrt[n]{1}$, that is, replacing A with $A \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$ we have eigenspace decomposition (no Jordan blocks of size > 1 since characteristic is coprime to n), that is, diagonalizable.

In another extreme case, in char. p and $|\varphi| = p^n$, we saw that no need to extend the field, all eigenvalues 1 and Jordan blocks of size $\leqslant p^n \times p^n$.

But what happens "in general"?

Replace A with $A \otimes_{\mathbb{Z}} \mathbb{Z}[\omega]$, so $\omega = \sqrt[n]{1}$ in the ground ring.

Define $A_i = \{a \in A \mid a\varphi = \omega^i a\}$, subgroups of A.

"Almost eigenspace decomposition"

Proposition. (a) $nA \subseteq A_0 + A_1 + \cdots + A_{n-1}$;
(b) *If* $a_0 + a_1 + \cdots + a_{n-1} = 0$ *for* $a_i \in A_i$, *then* $na_i = 0$ *for all* i.

(Of course, if $nA = A$, then the whole A; if $nx = 0 \Rightarrow x = 0$, then sum is direct.)

Proof: for $a \in A$, let $a_i = \sum_{k=0}^{n-1} \omega^{-ki} a\varphi^k$, then $a_i \in A_i$

and $\sum_i \sum_k \omega^{-ki} a\varphi^k = \sum_k \big(\sum_i \omega^{-ki}\big) a\varphi^k = na\varphi^0 = na$

since $\sum_i \omega^{-ki} = 0$ unless $\omega^{-k} = 1 \Leftrightarrow k \equiv 0 \,(\mathrm{mod}\, n)$.

Also, apply φ^k to $a_0 + a_1 + \cdots + a_{n-1} = 0$ for $k = 0, \ldots, n-1$,
then take sums with appr. coeff., get $na_i = 0$ for all i for same reasons...

Automorphism and cyclic grading

Clearly, $[L_i, L_j] \leqslant L_{i+j \,(\mathrm{mod}\, n)}$:

$[l_i, l_j]\varphi = [l_i\varphi, l_j\varphi] = [\omega^i l_i, \omega^j l_j] = \omega^{i+j}[l_i, l_j]$

When $L = L_0 \oplus L_1 \oplus \cdots \oplus L_{n-1}$ and $[L_i, L_j] \leqslant L_{i+j \,(\mathrm{mod}\, n)}$,
L is called a $(\mathbb{Z}/n\mathbb{Z})$-graded Lie ring with components L_i.

Theorem (Higman–Kreknin–Kostrikin)**.** *If a Lie ring* L *admits* $\varphi \in \mathrm{Aut}\, L$ *of prime order* p *such that* $C_L(\varphi) = 0$, *then* L *is nilpotent of class* $\leqslant h(p)$.

Equivalent:

Theorem (Higman–Kreknin–Kostrikin)**.** *If* L *is a* $(\mathbb{Z}/p\mathbb{Z})$*-graded Lie ring, where* p *is a prime, then* $\gamma_{h(p)+1}(L) \leqslant {}_{\mathrm{id}}\langle L_0\rangle$.

It is in this way it is actually proved.
Moreover:

Theorem (Combinatorial H–K–K theorem)**.** *For any* $x_{i_1}, \ldots, x_{i_{h(p)+1}}$ *in any Lie ring with formal indices, the commutator* $[...[x_{i_1}, x_{i_2}], \ldots, x_{i_{h(p)+1}}]$ *is equal to a linear combination of commutators in the same elements each containing a subcommutator with zero mod* p *sum of indices (can be transformed by Jacobi identity and anticommutativity to such a lin. combin.)*

Example: $p = 3$ (indices indicate components):
$[x_1, y_1, z_2] = [x_1, z_2, y_1] + [x_1, [y_1, z_2]] = [[x_1, z_2]_0, y_1] - [[y_1, z_2]_0, x_1]$.
For automorphism? Extend ground ring with $\sqrt[p]{1}$; "eigenspaces";
still $L_0 = C_L(\varphi) = 0$.

$pL \leqslant \sum_1^{p-1} L_i$ and $L_0 = 0$.

By combinatorial H–K–K theorem:
$\gamma_{h(p)+1}(pL) \leqslant \gamma_{h(p)+1}(\sum_1^{p-1} L_i) \leqslant {}_{\mathrm{id}}\langle L_0\rangle = 0$

Thus, $p^{h(p)+1}\gamma_{h(p)+1}(L) = 0$.

So the additive group $\gamma_{h(p)+1}(L)$ is a p-group. Hence $= 0$, as otherwise automorphism φ of order p would have fixed points.

Kreknin's theorem

Theorem (Kreknin)**.** *If a Lie ring* L *admits* $\varphi \in \mathrm{Aut}\, L$ *of finite order* n *such that* $C_L(\varphi) = 0$, *then* L *is soluble of derived length* $\leqslant 2k(n)$.

Theorem (Kreknin)**.** *If* L *is a* $(\mathbb{Z}/n\mathbb{Z})$*-graded Lie ring, then* $L^{(k(n))} \leqslant {}_{\mathrm{id}}\langle L_0\rangle$.

Moreover: combinatorial ......

Proof: double induction:
(a) $L^{(2^{s-1})} \cap L_s \leqslant \langle L_{s+1}, \ldots, L_{n-1}\rangle \,+\, {}_{\mathrm{id}}\langle L_0\rangle$
(b) $L^{(2^s-1)} \leqslant \langle L_{s+1}, \ldots, L_{n-1}\rangle \,+\, {}_{\mathrm{id}}\langle L_0\rangle$
(note: *subring* $\langle L_{s+1}, \ldots, L_{n-1}\rangle$).
Using: for integers $1 \leqslant a, b, c \leqslant n-1$, if $a + b \equiv c \,(\mathrm{mod}\, n)$, then either both $a > c$ and $b > c$, or both $a < c$ and $b < c$.

For automorphism: similarly: extend ground ring with $\sqrt[n]{1}$;
"eigenspaces"; still $L_0 = C_L(\varphi) = 0$.

$nL \leqslant \sum_1^{n-1} L_i$ and $L_0 = 0$.
Then $(nL)^{(k(n))} \leqslant {}_{\mathsf{id}}\langle L_0 \rangle = 0$ by combinatorial Kreknin theorem.

So, $n^{2^{k(n)}} L^{(k(n))} = 0 \Rightarrow$ the additive group $L^{(k(n))}$ is periodic $= \bigoplus_q S_q$ Sylow subgroups, where each S_q is even an ideal of L.

The q'-part of $\langle\varphi\rangle$ is fixed-point-free on S_q. For coprime action $S_q = \bigoplus (S_q \cap L_i)$, so by Kreknin $S_q^{(k(n))} = 0$ $\Rightarrow \left(L^{(k(n))}\right)^{(k(n))} = 0$, so L is soluble of derived length $2k(n)$.

$(\mathbb{Z}/n\mathbb{Z})$-graded Lie ring L with few non-zero components

Shalev, Khukhro:
Suppose $L = L_0 \oplus \cdots \oplus L_{n-1}$ is a $(\mathbb{Z}/n\mathbb{Z})$-graded Lie ring in which are only d nonzero components among the L_i. If $L_0 = 0$, then L is soluble (for n prime, nilpotent) of d-bounded derived length (nilpotency class).

Proof by the same scheme as of Kreknin–Kostrikin, "skipping" steps due to non-existence components.

Finds applications to groups of bounded rank with almost fixed-point-free automorphisms, and to Frobenius groups of automorphisms.

Lie ring methods for groups

$$\begin{array}{ccc} \text{hypothesis on a group} & & \text{hypothesis on a Lie ring} \\ G & \longrightarrow & L \\ & & \Big\Downarrow \ \text{a Lie ring theorem} \\ G & \longleftarrow & L \\ \text{result on the group recovered} & & \text{result on the Lie ring} \end{array}$$

1. A hypothesis on a group is translated into a hypothesis on a Lie ring constructed from the group in some way.

2. Then a theorem on Lie rings is proved (or used).

3. Finally, a result about the group must be recovered from the Lie ring information obtained.

Various Lie ring methods:

1. For complex and real Lie groups: Baker–Campbell–Hausdorff formula, EXP and LOG functors

2. Mal'cev's correspondence based on Baker–Campbell–Hausdorff formula for torsion-free (locally) nilpotent groups

3. Lazard's correspondence for p-groups of nilpotency class $< p$

4. Lie rings associated with uniformly powerful p-groups

5. Associated Lie ring based on lower central series

6. Lazard's Lie algebra based on dimension subgroups (Zassenhaus filtration)

Associated Lie Ring

Lie ring method for arbitrary groups, including finite groups (where, e.g., Baker–Campbell–Hausdorff formula cannot be applied):

Definition: associated Lie ring $L(G)$
For any group G: $L(G) = \bigoplus_i \gamma_i(G)/\gamma_{i+1}(G)$

(lower central series $\gamma_i(G) = [...[[G,G],G],\dots,G]$ (repeated i times))

Lie product for homogeneous elements: $[a + \gamma_{i+1},\ b + \gamma_{j+1}]_{\mathsf{Lie\ ring}} := [a,b]_{\mathsf{group}} + \gamma_{i+j+1}$

extended to the direct sum by linearity.

Pluses: Always exists. Nilpotency class of G = nilp. class of $L(G)$

Minuses: Only about $G/\bigcap\gamma_i(G)$, so only for (residually) nilpotent groups.
Even for these, some information may be lost: e. g., derived length may become smaller.

Example. Because in $L(G)$ we have $\gamma_k/\gamma_{k+1} = \underbrace{[G/\gamma_2,\dots,G/\gamma_2]}_{k}$ linear product:

If G is nilpotent of class c and exponent of G/γ_2 is n, then the exponent of G divides n^c, as each γ_k/γ_{k+1} has exponent dividing n:
$n[a_1,a_2,\dots] = [na_1,a_2,\dots] = [0,a_2,\dots] = 0$.

If in addition G is d-generated, then $|G|$ is bounded in terms of n, c, d.

If an automorphism $\varphi \in Aut\,G$ acts trivially on G/γ_2, then φ acts trivially on γ_i/γ_{i+1} for all i.

Group-theoretic applications of Kreknin's and Higman's theorems
Immediate for connected simply connected Lie groups with fixed-point-free automorphism of finite order.

For any nilpotent groups:

Corollary (Higman 57)
If a (locally) nilpotent group G has an automorphism $\varphi \in Aut\,G$ of prime order p such that $C_G(\varphi) = 1$, then G is nilpotent of class $\leqslant h(p)$.

Proof: consider $L(G)$ with the induced automorphism:

$C_{L(G)}(\varphi) = 0$ (for finite G, since must be a p'-group,
for infinite, modify $L(G) = \bigoplus \sqrt{\gamma_i}$)
$\Rightarrow$ $L(G)$ is nilpotent of class $\leqslant h(p)$.

Hence so is G. (True for any finite G; nilpotent by Thompson 59.)

Recall:

Open problem
Does an analogue of Kreknin's theorem hold for nilpotent groups with a fixed-point-free automorphism of arbitrary finite order n? that is, is derived length $\leqslant f(n)$?

(Same question for arbitrary finite group, but everything is already reduced to nilpotent groups: soluble by classification, and Fitting height bounded by Hall–Higman–type theorems.)

Here $L(G)$ *does not work* as derived length is not preserved.

So far known only for n prime (Higman–Kreknin–Kostrikin), and $n = 4$ (Kovács, 61)
Nevertheless, Kreknin's theorem was successfully applied to finite p-groups with an automorphism of order p^k and to pro-p-groups of given coclass in the papers of Alperin, Jaikin-Zapirain, Khukhro, Medvedev, Shalev, Shalev–Zel'manov.

Lie rings with almost regular automorphism of finite order
Almost fixed-point-free $\Rightarrow$ almost soluble (or nilpotent), with bounds.

Theorem (Khukhro, 89, Makarenko–Khukhro, 04, Makarenko, 05)
If a Lie algebra (ring) L admits an automorphism φ of finite order n such that $\dim C_L(\varphi) = r$ (or $|C_L(\varphi)| = r$), then L contains a solvable ideal of n-bounded derived length and of (n,r)-bounded codimension.

If in addition n is a prime, then L has even a nilpotent ideal of n-bounded class and of (n,r)-bounded codimension.

Basically about $(\mathbb{Z}/n\mathbb{Z})$-graded Lie ring L with $\dim L_0 = r$ (or $|L_0| = r$)

Non-trivial even for finite-dimensional, because of those bounds.

Method of graded centralizers

Example. Simplest case $n = 2$: let $L = L_0 \oplus L_1$ be $(\mathbb{Z}/2\mathbb{Z})$-graded
with $\dim L_0 = m$. Aim: nilp. ideal of class 2 of m-bounded codim.

We can assume $L = \langle L_1 \rangle$.

'Freeze' some expressions for a basis of L_0, need m of them: $[x_1,x_2],\dots,[x_{2m-1},x_{2m}]$, where $x_i \in L_1$.

'Graded centralizer': $C(x_j) = \{y \in L_1 \mid [x_j,y] = 0\}$

Each has codim $\leqslant m$ in L_1, as cosets correspond to distinct elements of L_0. Then $Z = \bigcap_{i=1}^m C(x_i)$ also has bounded codim.

Subalgebra $\langle Z\rangle$ is nilpotent of class 2: for any $z_i \in Z$, we have $[[z_1,z_2],z_3]$ = (since $[z_1,z_2]$ is a linear combination of those fixed $[x_j,x_{j+1}]$) = lin. comb. of $[[x_j,x_{j+1}],z_3]=0$ by the definition of Z (and by Jacobi identity).

(Z is a subalgebra; further effort required to obtain an ideal.)

General case: $\dim L_0 = m \;\Rightarrow$ **almost soluble**

Freeze boundedly many representatives $[x_{i_1}(1),\dots,x_{i_k}(1)] \in L_0$
with $\sum_j i_j = 0$, of bounded weight.

Graded centralizers of level 1: $Z_j(1) = \mathsf{Ker}$ of
$y_j \to [y_j, x_{j_1}(1),\dots,x_{j_s}(1)]$ where $j+\sum_k j_k = 0$;

this is a homomorphism of abelian groups $L_j \to L_0$.

Hence codim. of $Z_j(1)$ in L_j is at most $\dim L_0$.

Consider $L(1) = \langle Z_1(1),\dots,Z_{n-1}(1)\rangle$ of bounded codim.

Repeat, freezing $[x_{i_1}(2),\dots,x_{i_k}(2)]$ for some $x_k(2)\in Z_k(1)$,
where $\sum_j i_j = 0$.

...And so on. Graded centralizers of level k:
$Z_j(k) = \mathsf{Ker}$ of $y_j \to [y_j, x_{j_1}(l_1),\dots,x_{j_s}(l_s)]$
where $j+\sum_k j_k = 0$, with various lower levels (l_i).
After reaching certain bounded level N,

the required bounded-soluble subalgebra of bounded codim. is
$\langle Z_1(N),\dots,Z_{n-1}(N)\rangle$.

Clearly of bounded codim., as each Z_i is in L_i, and $\dim L_0 = m$.

Why bounded-soluble?

(H–K–) Kreknin's theorem applied several times in a certain collecting process, obtain

a) multiple entries of (various) $c_0 \in L_0$ in $[y_j(N), c_0,\dots,c_0]$ and

b) augmented $[...[\;,\;]_0,\;\;]_0,\dots\;\;]_0$.

Since all c_0 expressed in highest level – also in lower levels.

Another collecting process aiming at

$[y_j(N), x_{j_1}(l_1),\dots,x_{j_s}(l_s)]\;\; = 0$ because $N > l_k$ and $j+\sum j_k = 0$.

Group-theoretic corollaries for order of $C_G(\varphi)$

Theorem (Khukhro, 89, Medvedev, 94)
If a nilpotent group G admits an automorphism of prime order p with exactly r fixed points, then G has a nilpotent subgroup of p-bounded nilpotency class and of (p,r)-bounded index.

(Also true for any finite group G – reduction to nilpotent due to Fong, 79 (+CFSG) and Hartley–Meixner = Pettet, 81.)

Proof is based on using the associated Lie rings and Lie ring theorem.
But notrivial recovery $G \longleftarrow L$, as there is no good correspondence for subgroups↔subrings.

Recall that for non-prime $|\varphi|$ even fixed-point-free case remains open for groups. (Except for $|\varphi|=4$: fixed-point-free Kovács, 61, and for $|C_G(\varphi)| = m$ EKh–Makarenko, 2006)

Group-theoretic corollaries for rank of $C_G(\varphi)$

Theorem (EKh, 08)
If a nilpotent group G admits an automorphism of prime order p with $C_G(\varphi)$ of rank r, then G has a nilpotent subgroup N of p-bounded nilpotency class with G/N of (p,r)-bounded rank.

Here even $G \to L$ is unclear! Apart from Lie ring result, also group rings are used.

Recall: for any finite group G, +EKh+Mazurov+CFSG

$G \geqslant N \geqslant R \geqslant 1$ with G/N and R of (p,r)-bounded rank and N/R nilpotent — now also N/R nilpotent of p-bounded nilpotency class.

“Modular situation”

“Modular” — if a finite p-group P admits an automorphism of order p^n (which cannot be fixed-point-free).

Alperin 63 – Khukhro 85

If a finite p-group P admits an automorphism φ of prime order p with $|C_P(\varphi)| = p^m$, then P has a subgroup of (p,m)-bounded index that is nilpotent of class $\leqslant h(p)+1$ (even $\leqslant h(p)$ as noted by Makarenko).

Proofs use associated Lie ring and Higman's theorem.

Proof of Alperin–Khukhro theorem

H–K–K theorem is applied to $L(P)$ — even though φ not regular, and even $|C_{L(P)}(\varphi)|$ can be much greater than $|C_P(\varphi)|$, like times nilpotency class.

Recall elementary fact: always, $|C_{G/N}(\varphi)| \leqslant |C_G(\varphi)|$.

Rank of any φ-invariant abelian section M/N of P is at most pm: as $|C_{M/N}(\varphi)| \leqslant p^m$, plus recall corollary of Jordan normal form for φ.

Consider $\varphi \in \mathrm{Aut}\, L(P)$. Since $|C_{\gamma_i(P)/\gamma_{i+1}(P)}(\varphi)| \leqslant p^m$,
Lagrange: $p^m C_{L(P)}(\varphi) = 0$, whence $p^m\ {}_{\mathsf{id}}\langle C_{L(P)}(\varphi)\rangle = 0$.
Fix $h := h(p)$. By H–K–K theorem: $\gamma_{h+1}(pL(P)) \leqslant {}_{\mathsf{id}}\langle C_{L(P)}(\varphi)\rangle$.

On the left $= p^{h+1}\gamma_{h+1}(L(P))$. Plus, $p^m\ {}_{\mathsf{id}}\langle C_{L(P)}(\varphi)\rangle = 0$
Together: $p^{h+1+m}\gamma_{h+1}(L(P)) = 0$.

In terms of P:
$(\gamma_i(P)/\gamma_{i+1}(P))^{p^{h+m+1}} = 1$ for all $i \geqslant h+1$.

Plus, the rank of $\gamma_i(P)/\gamma_{i+1}(P)$ is at most pm.

Together: $|\gamma_i(P)/\gamma_{i+1}(P)| \leqslant p^{pm(h+m+1)}$ for all $i \geqslant h+1$.

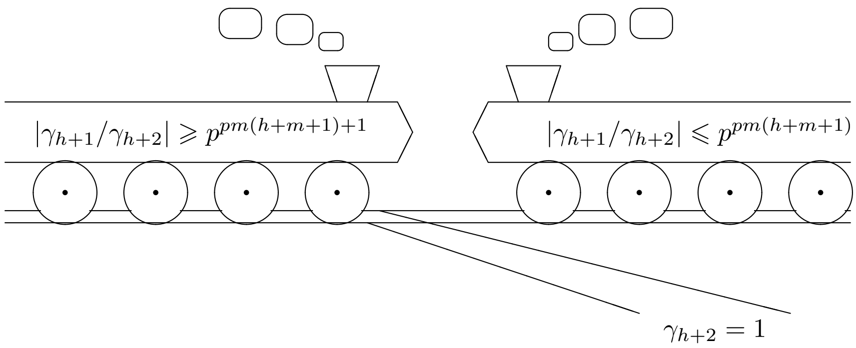
Note that the same for any φ-invariant subgroup Q:
$|\gamma_{h+1}(Q)/\gamma_{h+2}(Q)| \leqslant p^{pm(h+m+1)}$.

P. Hall's theorem: for $H = \gamma_{pm(h+m+1)+1}(P)$,
$|\gamma_i(H)/\gamma_{i+1}(H)| \geqslant p^{pm(h+m+1)+1}$ unless $\gamma_{i+1}(H) = 1$.

But $|\gamma_{h+1}(H)/\gamma_{h+2}(H)| \leqslant p^{pm(h+m+1)}$ as we saw above.

Thus, to avoid a contradiction: $\gamma_{h+2}(H) = 1$.

Thus, $\gamma_{h+2}(\gamma_{pm(h+m+1)+1}(P)) = 1$, in particular a bound for the derived length.



Improve: the semidirect product $P\langle\varphi\rangle$ also admits φ as the inner automorphism with exactly p^{m+1} fixed points.

Just replace m by $m+1$ above and put $H_1 = \gamma_{p(m+1)(h+m+2)+1}(P\langle\varphi\rangle)$.

Then $\gamma_{h+2}(H_1) = 1$.

Advantage: φ acts trivially on factors of lower central series of $P\langle\varphi\rangle$. Hence their orders $\leqslant p^{m+1}$, as $|C_{P\langle\varphi\rangle}(\varphi)| = p^{m+1}$.

Therefore, the index of $H_1 = \gamma_{p(m+1)(h+m+2)+1}(P\langle\varphi\rangle)$ in P is bounded!
and H_1 is nilpotent of class $\leqslant h(p)+1$.

(Makarenko even improved to nilpotency class $\leqslant h(p)$.)

The main advantage of the “modular case”

where a p-automorphism φ acts on a p-group P,

is the bound for the rank (dimension) in terms of $|\varphi|$ and rank of $C_P(\varphi)$.

As we know, this gives a characteristic powerful subgroup of bounded index, so largely reduces to powerful p-groups.

(More later).

Frobenius group of automorphisms with fixed-point-free kernel

Let G be a finite group admitting a Frobenius group of automorphisms $FH \leqslant \mathrm{Aut}\, G$ with kernel F and complement H such that $C_G(F) = 1$.

Recall:

New approach:
proving that properties (or parameters) of G are close to the corresponding properties (parameters) of $C_G(H)$ (possibly also depending on H).

Fitting height (=nilpotent length)

Theorem
Frobenius group $FH \leqslant \mathrm{Aut}\, G$ with kernel F such that $C_G(F) = 1$.

Then the Fitting height of G is equal to the Fitting height of $C_G(H)$.

Corollary
Frobenius group $FH \leqslant \mathrm{Aut}\, G$ with kernel F such that $C_G(F) = 1$.

If $C_G(H)$ is nilpotent, then G is nilpotent.

Theorem largely reduces further study to the case of nilpotent groups.

Bounding nilpotency class

Theorem (EIKh–N. Yu. Makarenko–P. Shumyatsky)
Frobenius group $FH \leqslant \mathrm{Aut}\, G$ with cyclic kernel F such that $C_G(F) = 1$. If $C_G(H)$ is nilpotent of class c, then G is nilpotent of $(c, |H|)$-bounded class.

Question: does it really depend on $|H|$?

So far there are only examples with class of G greater than that of $C_G(H)$.

Based on analogous theorem on Lie rings

Theorem (EIKh–N. Yu. Makarenko–P. Shumyatsky)
Let L be a Lie ring satisfying certain conditions.

Frobenius group $FH \leqslant \mathrm{Aut}\, L$ with cyclic kernel F such that $C_L(F) = 0$. If $C_L(H)$ is nilpotent of class c, then L is nilpotent of $(c, |H|)$-bounded class.

For groups easily follows: the associated Lie ring $L(G) = \bigoplus_i \gamma_i/\gamma_{i+1}$, where γ_i are terms of the lower central series of G,

has exactly the same nilpotency class as G.

$C_{L(G)}(H)$ is also nilpotent of class c, and $C_{L(G)}(F) = 0$. By Lie ring theorem, $L(G)$ is nilpotent of $(c, |H|)$-bounded class, and therefore so is G.

Metacyclicity of FH is essential: simple Lie algebra

Example. The simple 3-dimensional Lie algebra L of characteristic $\neq 2$ with basis e_1, e_2, e_3 and structure constants $[e_1, e_2] = e_3,\ [e_2, e_3] = e_1,\ [e_3, e_1] = e_2$

admits the Frobenius group of automorphisms FH with non-cyclic F of order 4 and H of order 3:

$F = \{1, f_1, f_2, f_3\}$, where $f_i(e_i) = e_i,\ f_i(e_j) = -e_j$ for $i \neq j$, and $H = \langle h \rangle$ with $h(e_i) = e_{i+1\,(\mathrm{mod}\, 3)}$.

Then $C_L(F) = 0$, while $C_L(H)$ is one-dimensional (hence abelian).

Metacyclicity of FH is essential: nilpotent Lie rings L of unbounded derived length.

Example. Let the additive group of L be the direct sum of three copies of $\mathbb{Z}/p^m\mathbb{Z}$ for a prime $p \neq 2$ with generators e_1, e_2, e_3; let the structure constants be $[e_1, e_2] = pe_3,\ [e_2, e_3] = pe_1,\ [e_3, e_1] = pe_2$.

"The same" non-metacyclic Frobenius group of automorphisms FH:

$F = \{1, f_1, f_2, f_3\}$, where $f_i(e_i) = e_i$ and $f_i(e_j) = -e_j$ for $i \neq j$, and $H = \langle h \rangle$ with $h(e_i) = e_{i+1\,(\mathrm{mod}\, 3)}$.

Then $C_L(F) = 0$ and $C_L(H) = \langle e_1 + e_2 + e_3 \rangle$.

It is easy to see that L is nilpotent of class m, and its derived length is $\approx \log m$.

Metacyclicity of FH is essential: nilpotent groups

Example. That nilpotent Lie ring can be turned into a nilpotent group:

If in the preceding example $p > m$, then the Lazard correspondence can be applied based on the "truncated" Baker–Campbell–Hausdorff formula. Then L becomes a finite p-group P of the same derived length admitting the same group of automorphisms FH with $C_P(F) = 1$ and with cyclic $C_P(H)$.

About the proof for Lie rings

Theorem (EIKh–N. Yu. Makarenko–P. Shumyatsky)
Frobenius group $FH \leqslant \mathrm{Aut}\, L$ with cyclic kernel F such that $C_L(F) = 0$. If $C_L(H)$ is nilpotent of class c, then the Lie ring L is nilpotent of $(c, |H|)$-bounded class.

Let $|F| = n$. Extend the ground ring by a primitive nth root of unity ω.

Define the eigenspaces for $F = \langle \varphi \rangle$:

$L_i = \{x \in L \mid x^\varphi = \omega^i x\}$. Roughly speaking,

$L = L_1 \oplus \cdots \oplus L_{n-1}$ and $[L_i, L_j] \subseteq L_{i+j\,(\mathsf{mod\ n})}$,

which is a $(\mathbb{Z}/n\mathbb{Z})$-grading. Plus we have the condition $L_0 = C_L(F) = 0$.

Kreknin's theorem: then L is soluble of n-bounded derived length. But we need nilpotency, and of class bounded in terms of $C_L(H)$ and $|H|$.

The simplest case of abelian $C_L(H)$

$L = L_1 \oplus \cdots \oplus L_{n-1}$; $[L_i, L_j] \subseteq L_{i+j\,(\mathsf{mod\ n})}$; $L_0 = 0$.

$H = \langle h \rangle$ permutes the components L_i "freely":
${L_i}^h = L_{ri}$, where r is determined from $\varphi^{h^{-1}} = \varphi^r$.

For $u_k \in L_k$, denote $u_k^{h^i} = u_{r^i k} \in L_{r^i k}$.

The sum over an H-orbit belongs to $C_L(H)$, which is abelian. Therefore

$[x_k + x_{rk} + \cdots + x_{r^{|H|-1}k},\ x_l + x_{rl} + \cdots + x_{r^{|H|-1}l}] = 0.$

Expand brackets. If $[x_k, x_l] \neq 0$, there must be other terms in the same component L_{k+l} for cancellation to happen.

Therefore, $k + l = kr^i + lr^j$, so that $l = -\dfrac{r^i - 1}{r^j - 1}k$.

Hence, for a given k there are at most $|H|^2$ values of l such that $[L_k, L_l] \neq 0$.

"Selective nilpotency" conditions

Theorem
Let $L = \bigoplus_{i=0}^{n-1} L_i$ be a $(\mathbb{Z}/n\mathbb{Z})$-graded Lie ring such that $L_0 = 0$
and for some m every grading component L_k
may not commute with at most m components:

$$|\{i \mid [L_k, L_i] \neq 0\}| \leqslant m.$$

(a) *Then L is soluble of m-bounded derived length.*

(b) *If in addition n is a prime, then L is nilpotent of m-bounded class.*

This works for the case of abelian $C_L(H)$.

The proof uses the "skipping" versions of Kreknin's theorem (due to Shalev and EIKh), when there are only few non-zero grading components, as mentioned above.

In the general case, when $C_L(H)$ is non-abelian but nilpotent of class c, a more complicated technical "selective nilpotency" condition arises, from which the required result is derived by rather difficult arguments.

Bounding the exponent

Theorem (EIKh–N. Yu. Makarenko–P. Shumyatsky)
Frobenius group $FH \leqslant \mathrm{Aut}\, G$ with cyclic kernel F such that $C_G(F) = 1$. Then the exponent of G is bounded in terms of $|FH|$ and the exponent of $C_G(H)$.

Question: is the hypothesis "F is cyclic" essential?

Question: does the exponent of G really depend on $|F|$?

Question: ... at least for F cyclic?

Question: ... at least for GFH being 2-Frobenius?
(This is Mazurov's question 17.72(b) in Kourovka Notebook.)

Question: does the exponent of G really depend on $|H|$?
(So far there are only a couple of examples where exponent of G is greater than that of $C_G(H)$.)

Using Lazard's Lie algebra

Recall:

Theorem (EIKh–N. Yu. Makarenko–P. Shumyatsky)
Frobenius group $FH \leqslant \mathrm{Aut}\, G$ with cyclic kernel F such that $C_G(F) = 1$. Then the exponent of G is bounded in terms of $|H|$ and the exponent of $C_G(H)$.

Proof is easily reduced to the case where G is a finite p-group.

Another Lie algebra:

Jennings–Zassenhaus filtration: $D_i = D_i(G) = \prod\limits_{jp^k \geqslant i} \gamma_j(G)^{p^k}$.

Lie algebra $DL(G) = \bigoplus D_i/D_{i+1}$.

Subalgebra $L_p(G) = \langle D_1/D_2 \rangle$ generated by D_1/D_2.

Connection with powerful p-groups

Recall: powerful p-groups: $G^p \geqslant [G, G]$ for $p \neq 2$ (or $G^4 \geqslant [G, G]$ for $p = 2$).

Lazard +... :
If X is a d-generator finite p-group such that the Lie algebra $L_p(X)$ is nilpotent of class c, then X contains a powerful characteristic subgroup of (p, c, d)-bounded index.

Lazard:
If $x \in G$ is of order p^t, then its image $\bar{x}$ in the appropriate factor as an element of $DL(G)$ is ad-nilpotent of index p^t.

Scheme of proof of exponent theorem

$L_p(G)$ is soluble by Kreknin;

+ all factors are generated by ad-nilpotent elements, since $G = \langle C_G(H)^F \rangle$ by "freedom Lemma";

together imply the nilpotency of $L_p(G)$.

Therefore G can be assumed to be powerful, which are easy to handle: if a powerful p-group is generated by elements of given order e, then the group is of exponent e.

Use again $G = \langle C_G(H)^F \rangle$.

Some further results. First step for exponent with non-metacyclic FH:

P. Shumyatsky
Frobenius group $FH \leqslant \mathrm{Aut}\, G$ of order $|FH| = 12$ with kernel F such that $C_G(F) = 1$. Then the exponent of G is bounded in terms of the exponent of $C_G(H)$ (and "12").

Combination of exponent and nilpotency:

P. Shumyatsky
Frobenius group $FH \leqslant \mathrm{Aut}\, G$ with cyclic kernel F such that $C_G(F) = 1$. If $C_G(H)$ satisfies a positive law of degree k, then G satisfies a positive law of degree bounded in terms of k and $|FH|$.

Positive law: $v = w$, where group words v, w involve only positive powers of variables.

A positive law of degree k for a finite group implies that it is an extension of a nilpotent group of k-bounded class by a group of k-bounded exponent. Conversely, every such an extension satisfies a positive law of bounded degree.

4. Baker–Campbell–Hausdorff formula

Baker–Campbell–Hausdorff formula

$1 + A$ free associative (noncommutative) algebra over $\mathbb{Q}$
with "outer" 1 (can always be adjoined)
completed with formal infinite power series (or nilpotent).

formal exponential $e^a = 1 + a + a^2/2 + a^3/3! + \cdots$
and logarithm $\log(1 + a) = a - a^2/2 + a^3/3 \pm \cdots$.

$A^{(-)}$ Lie algebra w.r.t. $[a, b] = ab - ba$.

Theorem. *Then $e^x \cdot e^y = e^{H(x,y)}$, where $H(x, y)$ belongs to the Lie subalgebra generated in $A^{(-)}$ by x, y.*

$$H(x, y) = \log(e^x \cdot e^y) = x + y + \tfrac{1}{2}[x, y] + \tfrac{1}{12}[x, y, y] - \tfrac{1}{12}[x, y, x] - \tfrac{1}{24}[x, y, x, y] + \cdots$$

B–C–H formula is used in theory of Lie groups and algebras, where EXP and LOG maps help to pass from Lie groups to Lie algebras — most important in classification of simple Lie groups.

Mal'cev correspondence

Theorem. *If L is a locally nilpotent Lie algebra over $\mathbb{Q}$, then the same set L becomes a divisible (radicable) locally nilpotent torsion-free group G with respect to the operation $a \cdot b = H(a, b)$.*

Every divisible locally nilpotent torsion-free group can be obtained in this way. The Lie operations in L are recovered by inversions of the B–C–H formulae: $a + b = H_1(a, b)$ and $[a, b]_L = H_2(a, b)$, where H_1, H_2 are products of group commutators in a, b (with exponents in $\mathbb{Q}$).

This is a category isomorphism: everything in the language of locally nilpotent Lie $\mathbb{Q}$-algebras is translated into the language of divisible locally nilpotent torsion-free groups, and vice versa.

Many properties correspond: exactly the same nilpotency class, derived length, etc.

Ideals = normal divisible subgroups,
sections are abelian (central) in $L \Leftrightarrow$ in G, etc., etc.

Automorphisms are exactly the same.

Note:

$x + y \equiv xy \ (\mathrm{mod}\ \gamma_2(\langle x, y\rangle))$;

$kx = x^k$;

$[x, y] \equiv [x, y] \ (\mathrm{mod}\ \gamma_3(\langle x, y\rangle))$.

Lie ring method preserving derived length

Theorem (Folklore)**.** *If a locally nilpotent torsion-free group G has an automorphism $\varphi \in Aut\, G$ of finite order n such that $C_G(\varphi) = 1$, then G is soluble of derived length $\leqslant k(n)$.*

Proof: Embed G into its Mal'cev completion $\hat{G}$ by adjoining all roots of nontrivial elements;

then φ extends to $\hat{G}$ with $C_{\hat{G}}(\varphi) = 1$.

Let L be the Lie algebra over $\mathbb{Q}$ in the Mal'cev correspondence with $\hat{G}$ given by Baker–Campbell–Hausdorff formula.

Then φ can be regarded as an automorphism of L with $C_L(\varphi) = 0$.

By Kreknin, L is soluble of derived length $\leqslant k(n)$;

hence so is $\hat{G}$, and so is G.

Endimioni 2010

If a polycyclic group G has an automorphism $\varphi \in Aut\, G$ of prime order p with finite fixed-point subgroup, $|C_G(\varphi)| < \infty$, then G has a subgroup of finite index that is nilpotent of class $\leqslant h(p)$.

Remarks:

no function to bound the index of a nilpotent subgroup,

G may not be nilpotent even if $C_G(\varphi) = 1$.

Proof: by reduction to finite q-groups with fixed-point-free automorphism φ, to which Higman's theorem is applied.

Remark, EKh 2010
If a polycyclic group G has an automorphism $\varphi \in \mathit{Aut}\, G$ of finite order n with finite fixed-point subgroup, $|C_G(\varphi)| < \infty$, then G has a subgroup of finite index that is soluble of derived length $\leqslant k(n) + 1$.

Proof: by Mal'cev's theorem, G has a characteristic subgroup H of finite index with torsion-free nilpotent derived subgroup $[H, H]$.

Now Folklore's theorem above can be applied to $[H, H]$, so H is soluble of derived length $\leqslant k(n) + 1$.

Lazard correspondence for p-groups of nilpotency class $< p$
It is known that for a given prime p, denominators in $H(x, y)$ at commutators of weight $\leqslant p - 1$ are not divisible by p. The same for the inverse formuale H_1, H_2.

In a p-group p'-roots exist and are unique, so $\sqrt[n]{g}$ for $p \nmid n$ is well-defined (= some power of g). For abelian additive p-group, $\frac{1}{n}g$.

Theorem. *If L is Lie ring with additive p-group, and L is nilpotent of class $\leqslant p - 1$, then L becomes a nilpotent p-group G with respect to the operation $a \cdot b = H(a, b)$.*
Every nilpotent p-group of class $\leqslant p-1$ can be obtained in this way. The Lie operations in L are recovered by inverse B–C–H formulae: $a + b = H_1(a, b)$ and $[a, b]_L = H_2(a, b)$, where H_1, H_2 are products of group commutators in a, b (with exponents $\frac{m}{n}$ for $p \nmid n$).

For example, p-group of nilpotency class class 2 for $p > 2$:

$a + b = ab[a, b]^{-1/2}$ commutative operation.

Again, a category isomorphism: the language of class $\leqslant p - 1$ nilpotent Lie rings with additive p-group translated into the language of class $\leqslant p - 1$ nilpotent p-groups, and vice versa, same automorphisms...

Hypotheses too strong?
But applications of the Baker–Hausdorff Formula in the theory of finite groups are rare. As G. Higman remarked in his address at the International Congress of Mathematicians in Edinburgh [1958], the restrictive preconditions of such applications are

"*...too severe to be used..., ...the sort of thing one wants in the conclusion of one's theorem, rather than in the hypothesis*".

This makes it even more interesting that there are some examples of applications of the Baker–Hausdorff Formula to finite groups.

In particular, used by Alperin and Glauberman in papers of 1997–....

Let us see some other examples.

Example. Let $p > 2$. If in a finite p-group P there are only p elements of order $\leqslant p$, then P is cyclic.

Proof: By induction, every maximal subgroup is cyclic. If there is only one maximal subgroup, then Frattini has index p, so $P/\Phi(P)$ is cyclic. so P is cyclic.

So assume there are at least two maximal subgroups; then their intersection is in the centre, since both are abelian.

So quotient by centre is of order $\leqslant p^2$, so abelian, so P is of class 2.

Since $p > 2$, we can apply Lazard correspondence – actually need only additive group of the resulting Lie ring L. Element orders in P and in $(L, +)$ are the same. So $(L, +)$ is cyclic, hence P is cyclic.

Example. Suppose that a finite p-group P of nilpotency class $< p$ admits a p-group of automophisms A such that $P/\Phi(P)$ is a free $\mathbb{F}_pA$-module. Then $C_{P/\Phi(P)}(A) = C_P(A)\Phi(P)/\Phi(P)$.

Apply Lazard correspondence: $P \leftrightarrow L$.

In the free $\mathbb{F}_pA$-module fixed points are "diagonal elements", say, $\bar{c} = \prod_{a\in A} \bar{g}^a$, where $\bar{g} \in P/\Phi(P)$.

Just take $z = \sum_{a\in A} g^a$ in L. Clearly, $z \in C_L(A) = C_P(A)$.

And $\bar{z} = \bar{c}$, since $x + y \equiv xy (\mathsf{mod}\, [P, P])$.

Earlier Thompson, 64, for class 2, used for a signalizer theorem (proof was based on a lemma of N. Blackburn on p-groups of maximal class). Then Bender extended that signalizer result using Baer's class 2 special case of Lazard's correspondence.

p-groups of maximal class

... are $|P| = p^n$ and of nilpotency class $n-1$.

Alperin: derived length p-bounded. Moreover,
Sheherd and Leedham-Green–McKay: P has class 2 nilpotent subgroup of p-bounded index.

Leedham-Green–McKay asked if the derived length can even be uniformly bounded (for various primes).

Example. Lie algebra L over $\mathbb{F}_p$ with basis $e_1, \dots, e_p$ and structure constants $[e_i, e_j] = (i-j)e_{i+j}$ when $i+j < p$, and $= 0$ otherwise. $|L| = p^p$.

Clearly, $\gamma_k(L) = {}_+\langle e_{k+1}, e_{k+2}, \dots \rangle$, so that L is nilpotent of class $p-1$.

Also can be seen that derived length of L is about $\log_2 p$.

Just apply Lazard's correspondence

Shepherd–Leedham-Green–McKay for rank?

Suppose P is a 2-generator finite p-group whose lower central quotients $\gamma_i(P)/\gamma_{i+1}(P)$ are cyclic for all $i \geqslant 2$. Is it true that P contains a normal subgroup N of nilpotency class $\leqslant 2$ such that the rank of P/N is bounded in terms of p only?

Example (EKh, 2012). $L = \langle e_1, \dots, e_n \mid [e_i, e_j] = (i-j)e_{i+j} \text{ if } i+j \leqslant n;\ \ [e_i, e_j] = 0 \text{ if } i+j > n \rangle$. Let G be the group in Mal'cev correspondence with L.

Let H be the (abstract) subgroup of G generated by e_1 and e_2^M.
For sufficiently large $M \geqslant M(n)$, all factors of the lower central series of H starting from the second one are infinite cyclic.

Being 2-generator torsion-free nilpotent, H is residually finite p-group.

The p-groups that are quotients of H (for various n) are counterexamples: there are no functions $d(p)$ and $r(p)$ such that a group P as above would necessarily have a normal subgroup of derived length $\leqslant d(p)$ with quotient of rank $\leqslant r(p)$.

Generalization

EKh–Jaikin-Zapirain
There is a function $f(c)$ such that for any nilpotent group of class c the subgroup $G^{f(c)}$ can be endowed with the structure of a Lie ring, with many of the properties preserved, like derived length, etc. (although not as good as category isomorphism). The same also works for any G^N for N divisible by $f(c)$.

Just enough powers to make sure those denominators can be executed...

B–C–H formula also palys an impportant role in pro-p-groups.

B–C–H formula in "modular situation"

Shalev 93 – Khukhro 93
If a finite p-group P admits an automorphism φ of order p^n with $|C_P(\varphi)| = p^m$, then P has a subgroup of (p, m, n)-bounded index that is soluble of p^n-bounded derived length.

Proofs use Kreknin's theorem.

Shalev's paper (with "weak" (p, m, n)-bound for the derived length) used a Lie ring constructed from a uniformly powerful p-group. Powerful p-groups arise naturally, as rank is (p, m, n)-bounded (for abelian, at most mp^n).

In EKh 93, first powerful p-groups, associated Lie ring and Kreknin's theorem: weak (p, m, n)-bound for the nilpotency class $c = c(p, m, n)$ of the $k(p^n)$th derived subgroup $T = S^{(k(p^n))}$ (of certain sections S).
Then Mal'cev correspondence applied to free nilpotent group with an automorphism, again Kreknin's theorem, interpreted for the p-group in question.

Applying powerful p-groups and associated Lie ring

Definition: G a finite p-group, N is powerfully embedded if $N^p \geqslant [N, G]$ ($N^4 \geqslant [N, G]$ for $p = 2$).

Taking pth powers and commutator subgroups produces powerfully embedded subgroups from powerfully embedded subgroups:
if N is powerfully embedded, then so are N^p, $[N, G]$, etc.

Shalev's Interchanging Property:
If M, N are powerfully embedded, then $[M^p, N] = [M, N]^p$.

In a powerful p-group $P^{p^i} = \{x^{p^i} \mid x \in P\}$ form central series,
with non-increasing orders of factors.

Definition: uniformly powerful: $|P^{p^i}/P^{p^{i+1}}| = \text{const}$.

Cancellation property:

If P is uniformly powerful, then
$x^{p^i} \in P^{p^k} \Rightarrow x \in P^{p^{k-i}}$ *if $i \leqslant k$ and $P^{p^k} \neq 1$.*

Uniformly powerful, weak bound

Proposition 1

Suppose that a uniformly powerful p-group P admits an automorphism φ of order p^n with exactly p^m fixed points. Then the $k(p^n)$th derived subgroup $P^{(k(p^n))}$ is nilpotent of (p, m, n)-bounded class.

Fix for brevity $k = k(p^n)$ Kreknin's function.
Fixing some $s \in \mathbb{N}$ (to be chosen later),
consider P^{p^s} – also uniformly powerful.
Consider φ as automorphism of the associated Lie ring $L = L(P^{p^s})$.

By Kreknin in combinatorial form, $(p^n L)^{(k)} \subseteq {}_{\mathsf{id}}\langle C_L(\varphi)\rangle$.

(Recall: $|C_{G/N}(\varphi)| \leqslant |C_G(\varphi)|$ always.)

By Lagrange, $p^m C_L(\varphi) = 0$, so $p^m\, {}_{\mathsf{id}}\langle C_L(\varphi)\rangle = 0$.

Hence, $p^{m+n2^k} L^{(k)} = 0$.

In group terms: $\big((P^{p^s})^{(k)}\big)^{p^{m+n2^k}} \leqslant \gamma_{2^k+1}(P^{p^s})$.

Interchanging: $(P^{(k)})^{p^{s2^k+m+n2^k}} \leqslant \gamma_{2^k+1}(P)^{p^{s2^k+s}} \leqslant P^{p^{s2^k+s}}$. $\quad (*)$

Idea: use the extra summand $+s$ in the exponent on the right.

Let p^e be the exponent of P, we shall choose s so that the ratio e/s is (p, m, n)-bounded.

By Cancellation Property: "cancel" the summand $s2^k$ in the exponents: then $P^{(k)}$ will be "almost" contained in P^{p^s}. Then by Interchanging Property $\gamma_{e/s}(P^{p^s}) = \gamma_{e/s}(P)^{p^{(e/s)s}} \leqslant P^{p^e} = 1$; so the result will follow since e/s is (p, m, n)-bounded: extra $+m + n2^k$ is small, easily "killed off" by small increase of class.

Clearly, the larger s the better (smaller) bound for the class of $P^{(k)}$. But: Cancellation Property works only if r.h.s. $\neq 1$.

So we choose $s = [e/(2^k + 1)]$, that is, s is the maximal integer satisfying $s2^k + s \leqslant e$. ....Omit technical details...

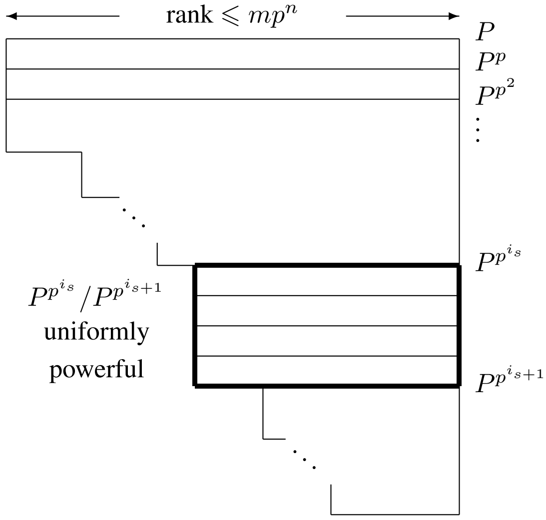
Collecting uniformly powerful pieces

Proposition 2

If P is a powerful p-group admitting an automorphism of order p^n with p^m fixed points, then $P^{(k(p^n))}$ is nilpotent of (p, m, n)-bounded class.

By properties of powerful:
$|P/P^p| \geqslant \ldots \geqslant |P^{p^i}/P^{p^{i+1}}| \geqslant |P^{p^{i+1}}/P^{p^{i+2}}| \geqslant \ldots$
$P^{p^i}/P^{p^{i+1}}$ are elementary abelian, and the ranks are (p, m, n)-bounded
$\Rightarrow$ there are only (p, m, n)-bounded number of strict inequalities.

A segment with equalities corresponds to a uniformly powerful section.
So a series of (p, m, n)-bounded length with uniformly powerful factors:
$P > P^{p^{i_1}} > P^{p^{i_2}} > \ldots > P^{p^{i_{l-1}}} > 1$.



Series of (p,m,n)-bounded length with uniformly powerful factors:

$P > P^{p^{i_1}} > P^{p^{i_2}} > \ldots > P^{p^{i_{l-1}}} > 1$. Induction on the length l of this series. Basis when P is uniformly powerful is Proposition 1 above.

..... Repeated application of Interchanging property and Proposition 1...

Application of Mal'cev corrspondence

Since rank is bounded, P has a powerful characteristic subgroup of bounded index; so we may assume P to be powerful.

By Proposition 2, $P^{(k)}$ is nilpotent of bounded class $c = c(p,m,n)$.

Free c-nilpotent $\langle\varphi\rangle$-operator group $F \to P^{(k)}$

Mal'cev completion $\hat{F} \leftrightarrow L$ Lie algebra L over $\mathbb{Q}$

Kreknin's theorem: $L^{(k(p^n))} \subseteq {}_{\mathrm{id}}\langle C_L(\varphi)\rangle$

translated into the group language as $\hat{F}^{(k(p^n))} \subseteq \langle C_{\hat{F}}(\varphi)^{\hat{F}}\rangle$

By bounded nilpotency class, $(F^{g(p,m,n)})^{(k(p^n))} \subseteq \langle C_F(\varphi)^F\rangle$, where a certain power $F^{g(p,m,n)}$ replaces $\hat{F}$

$\Rightarrow$ same for $P^{(k)}$:

$((P^{(k)})^{g(p,m,n)})^{(k(p^n))} \subseteq \langle C_{P^{(k)}}(\varphi)^{P^{(k)}}\rangle$

Completion of the proof

Recall: $\big((P^{(k)})^{p^w}\big)^{(k)} \leqslant \Big\langle C_{P^{(k)}}(\varphi)^{P^{(k)}}\Big\rangle$

for some (p,m,n)-bounded number p^w.

On the right, $\Big\langle C_{P^{(k)}}(\varphi)^{P^{(k)}}\Big\rangle$ is generated by conjugates of elements in $C_{P^{(k)}}(\varphi)$, which have order at most p^m (recall $|C_{G/N}(\varphi)| \leqslant |C_G(\varphi)|$),

+ bounded class $c = c(p,m,n) \Rightarrow \Big\langle C_{P^{(k)}}(\varphi)^{P^{(k)}}\Big\rangle$ has bounded exponent dividing p^{mc}.

So $\Big(\big((P^{(k)})^{p^w}\big)^{(k)}\Big)^{p^{mc}} = 1$.

Interchanging: $(P^{p^z})^{(2k)} \leqslant \Big(\big((P^{(k)})^{p^w}\big)^{(k)}\Big)^{p^{mc}} = 1$,

for some (p,m,n)-bounded number z.

Rank and exponent of P/P^{p^z} are (p,m,n)-bounded $\Rightarrow P^{p^z}$ is required subgroup of (p,m,n)-bounded index of derived length $\leqslant 2k(p^n)$.

5. Elimination of operators by nilpotency

Finite p-groups with a partition

Henceforth, P is a finite p-group.

Equivalent definitions:

(a) $P = \bigcup P_i$ for some $P_i < P$ such that $P_i \cap P_j = 1$;

(b) $P \neq H_p(P) := \langle g \in P \mid g^p \neq 1 \rangle$ (proper Hughes subgroup);

(c) $P = P_1 \rtimes \langle \varphi \rangle$, where $\varphi^p = 1$ and $xx^{\varphi}x^{\varphi^2} \cdots x^{\varphi^{p-1}} = 1$ for all $x \in P_1$ (splitting automorphism of P_1).

Such groups generalize (are close to) groups of exponent p:

outside a proper subgroup all elements are of order p,

and $\varphi = 1 \Rightarrow$ exponent p.

(But there is no bound for the exponent of a p-group with a partition.)

Splitting automorphism approach

Splitting automorphism approach of condition (c) turned out to be most efficient. Recall:

(c) $P = P_1 \rtimes \langle \varphi \rangle$, where

$$\varphi^p = 1 \text{ and } xx^{\varphi}x^{\varphi^2} \cdots x^{\varphi^{p-1}} = 1 \text{ for all } x \in P_1 \qquad (*)$$

(φ is a splitting automorphism of P_1).

(Note that we do not exclude the case where φ acts trivially on P_1, when, of course, P_1 must have exponent p.)

All groups with a splitting automorphism of order p form a variety of groups with operators defined by the laws $(*)$.

Analogues of theorems on group of exponent p

Analogues of theorems on group of exponent p
are natural for finite p-groups with a partition
(equivalently, for p-groups with a splitting automorphism of order p).

Recall: (c) $P = P_1 \rtimes \langle \varphi \rangle$, where $\varphi^p = 1$ and $xx^{\varphi}x^{\varphi^2} \cdots x^{\varphi^{p-1}} = 1$ for all $x \in P$.

EKh-1981

If P_1 in condition (c) has derived length d, then P_1 is nilpotent of (p, d)-bounded class.

Based on Kostrikin's theorem for groups of prime exponent,

EKh-1986

Analogue of the affirmative solution of the Restricted Burnside Problem: the nilpotency class of P_1 is bounded in terms of p and the number of generators.

As a corollary, a positive solution for the Hughes problem
was obtained for "almost all" finite p-groups.

Nilpotency class depending on automorphisms

EKh–Shumyatsky, 1995: if a finite group G of exponent p admits a soluble group of automorphisms A of coprime order such that the fixed-point subgroup $C_G(A)$ is soluble of derived length d, then G is nilpotent of $(p, d, |A|)$-bounded class.

Theorem 1

Suppose that a finite p-group P with a partition admits a soluble group of automorphisms A of coprime order such that $C_P(A)$ has derived length d. Then any maximal subgroup of P containing $H_p(P)$ is nilpotent of $(p, d, |A|)$-bounded class.

Note: the nilpotency class of the whole group P cannot be bounded.

The bound for the nilpotency class of that maximal subgroup can be chosen the same as in EKh–Shumyatsky-95 for groups of exponent p.

Exponent

Theorem 2

If a finite p-group P with a partition admits a group of automorphisms A that acts faithfully on $P/H_p(P)$, then the exponent of P is bounded in terms of the exponent of $C_P(A)$.

Frobenius groups of automorphisms

Corollary

Suppose that a finite group G admits a Frobenius group of automorphisms FH with cyclic kernel $F = \langle \varphi \rangle$ of prime order p such that φ is a splitting automorphism, that is, $xx^{\varphi}x^{\varphi^2} \cdots x^{\varphi^{p-1}} = 1$ for all $x \in G$.

(a) *If $C_G(H)$ is soluble of derived length d, then G is nilpotent of (p, d)-bounded class.*

(b) *The exponent of G is bounded in terms of p and the exponent of $C_G(H)$.*

Proof of Corollary

The group G is nilpotent by Kegel–Thompson–Hughes.

φ is fixed-point-free on $G_{p'}$: for any $g \in C_G(\varphi)$ we have $1 = gg^{\varphi}g^{\varphi^2}\cdots g^{\varphi^{p-1}} = g^p$.

Hence $G_{p'}$ is nilpotent of p-bounded class by Higman–Kreknin–Kostrikin.

For (a) it now remains to consider the Sylow p-subgroup G_p of G. The result follows from Theorem 1 applied to $P = G_p\langle\varphi\rangle$ and $A = H$.

By a lemma in EKh–Makarenko–Shumyatsky-2010 $G_{p'} = \langle C_{G_{p'}}(H)^f \mid f \in F\rangle$.

So $G_{p'}$ is generated by elements of orders dividing the exponent of $C_G(H)$.

Plus p-bounded nilpotency class of $G_{p'} \Rightarrow$ exponent of $G_{p'}$ is bounded in terms of p and exponent of $C_G(H)$.

So in (b) it remains to consider G_p. The result follows from Theorem 2 applied to $P = G_p\langle\varphi\rangle$ and $A = H$.

Comments on Frobenius groups of automorphisms

Examples show that dependence of the nilpotency class on p is essential in part (a) of Corollary (obviously also true for exponent in part (b)).

Recent papers of EKh, Makarenko, Shumyatsky on finite groups G with a Frobenius group of automorphisms FH with fixed-point-free kernel F:

Mazurov's problem 17.72(a) from Kourovka Notebook was solved in the affirmative, and moreover, for any metacyclic Frobenius group of automorphisms FH and nilpotent G, a bound for the nilpotency class of G was obtained in terms of $|H|$ and the nilpotency class of $C_G(H)$, as well as a bound for the exponent of G in terms of $|FH|$ and the exponent of $C_G(H)$.

Question

Question: can results like Corollary be obtained for Frobenius groups of automorphisms with kernel generated by a splitting automorphism of composite order?

Examples show that nilpotency class cannot be bounded (even for cyclic kernel of order p^2 generated by a splitting automorphism and complement of order 2 with abelian fixed points).

Question remains open for the exponent, as well as for the derived length.

Proof of Theorem 1: elimination of automorphisms by nilpotency

Proof of Theorem 1 uses a modification of the method of elimination of automorphisms by nilpotency, which was used in EKh-1991 earlier in the study of splitting automorphisms of prime order.

Reduction by known results to the main case:

Theorem 1$'$

Suppose that a soluble group FA with normal Sylow p-subgroup $F = \langle\varphi\rangle$ of order p and Hall p'-subgroup A acts by automorphisms on a finite p-group G in such a manner that φ is a splitting automorphism, that is, $xx^{\varphi}x^{\varphi^2}\cdots x^{\varphi^{p-1}} = 1$ for all $x \in G$. If $C_G(A)$ is soluble of derived length d, then G is nilpotent of $(p, d, |A|)$-bounded class. Furthermore, the bound for the nilpotency class can be chosen to be the same as in the case $\varphi = 1$ (given by EKh-Shumyatsky-95).

Free FA-group

The trick of elimination of automorphisms requires passing to a free FA-group $X = \langle x_1, x_2, \dots\rangle$ of some exponent p^M and some nilpotency class N. (Of course, the bounds to be obtained must be independent of M and N.)

As an abstract group, X is relatively free of exponent p^M and nilpotent of class N, on the free generators x_i^{α}, where $\alpha \in FA$, and FA permutes them regularly: $(x_i^{\alpha})^{\beta} = x_i^{\alpha\beta}$.

There is an FA-homomorphism $\xi : X \to G$ given by $x_i \to g_i$ for any $g_i \in G$ (provided M, N are a large enough.)

Let C be the FA-invariant normal closure of $(C_X(A))^{(d)}$.

Let S be the FA-invariant normal closure of all $xx^{\varphi}x^{\varphi^2}\cdots x^{\varphi^{p-1}}$.

Clearly, $C, S \leqslant Ker\,\xi$ by hypothesis.

Lemma

The subgroups C and S are invariant under any FA-endomorphism ϑ of X.

Trivialization of F

Since there is an FA-homomorphism $\xi : X \to G$ with $C, S \leqslant Ker\,\xi$, it is sufficient (and even necessary) to prove that

$[x_1, \dots, x_{c+1}] \in CS$, where c is the nilpotency class given by EKh-Shumyatsky theorem when $\varphi = 1$.

Let $T = [X, F]F$ ("trivialization of F")

By EKh-Shumyatsky theorem, $[x_1,\dots,x_{c+1}]\in CST$,

that is, we need to eliminate T.

Higman's lemma

We have

$[x_1,\dots,x_{c+1}]\equiv c_1^{k_1}\cdots c_m^{k_m} \pmod{CS}$, where $c_i\in T$.

An analogue of Higman's lemma gives that we can assume that each c_i depends on all $x_1,\dots,x_{c+1}$, $\underline{\text{and on }\varphi}$.

One can show that we can furthermore assume that each c_i has the form

$$[[x_{i_1}^{a_*},\dots],\,[x_{i_2}^{a_*},\dots],\dots,[x_{i_{c+1}}^{a_*},\dots]]\qquad (a_*\in A),$$

where $\{i_1,i_2,\dots,i_{c+1}\}=\{1,2,\dots,c+1\}$ and there is at least one φ among "dots" in at least one of the sub-commutators $[x_{i_k}^{a_*},\dots]$.

Self-amplification process

$[x_1,\dots,x_{c+1}]\equiv c_1^{k_1}\cdots c_m^{k_m} \pmod{CS}$ $\qquad(*)$

We "iterate", "self-amplify": by homomorphisms of the type

$x_k\to[x_{i_k}^{a_*},\dots],\qquad k=1,\dots,c+1$

we express each $c_i=[[x_{i_1}^{a_*},\dots],\dots,[x_{i_{c+1}}^{a_*},\dots]]$ as the image of the left-hand-side,

then substitute the result into right-hand side of the original $(*)$.

As a result, the new $(*)$ has the same form but now each new c_i has $\underline{\text{at least two occurrences of }\varphi}$.

And so on, at each step we double the number of occurrences of φ in the new c_i.

Since $X\langle\varphi\rangle$ is nilpotent (being a finite p-group!), in the end we get $\equiv 1$, as required.

Proof of exponent theorem.

By known results, proof of Theorem 2 reduces to the following result.

Theorem 2′

If a finite p-group G admits a Frobenius group of automorphisms FA with kernel $F=\langle\varphi\rangle$ of order p and complement A such that φ is a splitting automorphism, that is, $xx^{\varphi}x^{\varphi^2}\cdots x^{\varphi^{p-1}}=1$ for all $x\in G$, then the exponent of G is bounded in terms of the exponent of $C_G(A)$.

Since any $g\in G$ belongs to $\langle g^{FA}\rangle$, we can assume that G is generated by $|FA|$ elements.

By EKh-86 affirmative solution to an analogue of the Restricted Burnside Problem for groups with a splitting automorphism of prime order p, the nilpotency class of G is bounded in terms of p and the number of generators, which is at most $p(p-1)$.

It remains to obtain a bound for the exponent of $V=G/[G,G]$.

Abelian case: eigenspaces.

Consider $V=G/[G,G]$ as a $\mathbb{Z}FA$-module, with additive notation. In particular, $v+v\varphi+v\varphi^2+\cdots+v\varphi^{p-1}=0$ for all $v\in V$ by hypothesis.

Extend the ground ring by a primitive pth root of unity ω, forming $W=V\otimes_{\mathbb{Z}}\mathbb{Z}[\omega]$. Still have $w+w\varphi+w\varphi^2+\cdots+w\varphi^{p-1}=0$ for all $w\in W$.

Define analogues of eigenspaces for the "linear transformation" φ:

$$W_i=\{w\in W\mid w\varphi=\omega^i w\}.$$

Then W is an "almost direct sum" of the W_i:

$$pW\subseteq W_0+W_1+\cdots+W_{p-1}$$

and

$$\text{if}\quad w_0+w_1+\cdots+w_{p-1}=0\quad\text{for}\quad w_i\in W_i,\quad\text{then}\quad pw_i=0\quad\text{for all}\quad i.$$

A-orbits.

First: since $\varphi = 1$ on W_0, for $x \in W_0$ we have $px = x + x\varphi + \cdots + x\varphi^{p-1} = 0$, so that $pW_0 = 0$.

Action of A: permutes the W_i in the same way as it acts on $\langle\varphi\rangle$.

Let $A = \langle\alpha\rangle$ and let $\varphi^{\alpha^{-1}} = \varphi^r$ for some $1 \leqslant r \leqslant p-1$. Let $|\alpha| = n$; then r is a primitive nth root of 1 in $\mathbb{Z}/p\mathbb{Z}$.

A "almost permutes" the W_i:
$W_i\alpha \subseteq W_{ri}$ for all $i \in \mathbb{Z}/p\mathbb{Z}$. Indeed, if $x_i \in W_i$, then $(x_i\alpha)\varphi = x_i(\alpha\varphi\alpha^{-1}\alpha) = (x_i\varphi^r)\alpha = \omega^{ir}x_i\alpha$.

Given $u_k \in W_k$ for $k \neq 0$, to lighten the notation we denote $u_k\alpha^i$ by u_{r^ik}; note that $u_{r^ik} \in W_{r^ik}$.
Let p^e be the exponent of $C_G(A)$. Claim: W_i are annihilated by p^{1+e}.

For any $k \neq 0$ and for any $u_k \in W_k$ we have

$$u_k + u_k\alpha + \cdots + u_k\alpha^{n-1} = u_k + u_{rk} + \cdots + u_{r^{n-1}k} \in C_W(A)$$

(the sum over an A-orbit). Since $p^eC_V(A) = 0$ (as $C_V(A)$ is the image of $C_G(A)$ by coprimeness of the action), also $p^eC_W(A) = 0$. Thus,

$$p^eu_k + p^eu_{rk} + \cdots + p^eu_{r^{n-1}k} = 0.$$

By "almost direct sum", in particular, $pp^eu_k = 0$.

Recall that $pW_0 = 0$. As a result,

$$p^{2+e}W \subseteq p^{1+e}(W_0 + W_1 + \cdots + W_{p-1}) = 0,$$

so also $p^{2+e}V = 0$.

In multiplicative notation, the exponent of $G/[G,G]$ divides p^{2+e}, so the exponent of G divides $p^{c(2+e)}$, where c is the nilpotency class of G, which is bounded in terms of p.

Remark

If, for some reason, it is known that the derived length s of the group G in Theorems 1 or 2, or in the Corollary, is relatively small, then EKh-81 can be used instead to give a possibly better estimate

$$\frac{(p-1)^s - 1}{p-2}$$

for the nilpotency class of G (in Theorems $1'$ and $2'$).

A smaller bound for the nilpotency class would also imply a smaller bound for the exponent.

Nilpotency in varieties of groups with operators

I proved in 1991 the general nilpotency theorem:

EKh-91:

Suppose that $\mathfrak{V}$ is a variety of Ω-operator groups given by Ω-laws which define a class c nilpotent variety of ordinary group if all the operators in these laws are put to be 1. (In other words, the quotient of $F\Omega$, where F is a free group of this Ω-variety, by the normal closure of Ω is nilpotent of class c.)

If G is a group in $\mathfrak{V}$ such that the semidirect product $G\Omega$ is nilpotent, then G is nilpotent of class $\leqslant c$.

Ω-laws are of the form $(x_{i_1}^{\pm 1})^{\omega_{i_1}} \cdots (x_{i_m}^{\pm 1})^{\omega_{i_m}} = 1$
where x_j are group variables and $\omega_j \in \Omega$.

The condition that $G\Omega$ is nilpotent seems strong. But sometimes holds automatically: for example, if both G and Ω are finite p-groups.

Example. when $\Omega \to 1$ gives nilpotency: $\mathfrak{V}$ = soluble groups of derived length d with splitting automorphism φ of prime order p.

The law $x \cdot x^{\varphi} \cdot x^{\varphi^2} \cdots x^{\varphi^{p-1}} = 1$ turns into $x^p = 1$ on trivialization of $\Omega = \langle\varphi\rangle$,

and it is known that a soluble group of exponent p and of derived length d is nilpotent of class $(p^d - 1)/(p-1)$.

Similarly, the same arguments as above prove

Theorem $1''$

Suppose that a soluble group FA with normal Sylow p-subgroup F and Hall p'-subgroup A acts by automorphisms on a finite p-group G in such a manner that for some fixed $\varphi_1, \ldots, \varphi_p \in F$ we have $x^{\varphi_1}x^{\varphi_2}\cdots x^{\varphi_p} = 1$ for all $x \in G$. If $C_G(A)$ is soluble of derived length d, then G is nilpotent of $(p, d, |A|)$-bounded class. Furthermore, the bound for the nilpotency class can be chosen to be the same as in the case $G^p = 1$ (given by EKh-Shumyatsky-95).

Generalizations

There is also local nilpotency theorem in EKh-93, which may also have generalizations in the context of additional group of automorphisms...