The structure of groups with an automorphism satisfying a polynomial identity[1]

Wolfgang Alexander Moens

University of Vienna

[Ostrava Seminar on Mathematical Physics: 16/05/2019]

[1]This work was supported by the Austrian Science Fund (FWF) grants: $J-3371-N25$ "Representations and gradings of solvable Lie algebras" and $P30842-N35$ "Infinitesimal Lie rings: gradings and obstructions".

Table of Contents

"Appetizer"

I have a finite group G,
together with an automorphism $\alpha : G \longrightarrow G$.

I am telling you that, for all $x \in G$:

$$\alpha^3(x) \cdot \alpha^2(x^{-1}) \cdot \alpha(x^{-1}) \cdot \alpha^2(x) \cdot \alpha(x^{-1}) \cdot x^{-1} = 1_G.$$

Q. What can you tell me about the structure of G?

Regular automorphisms

Thm. (Rowley ′95): A finite group G is *solvable* if it has an automorphism that moves every element of G other than 1_G.

- **Def**. $\Delta_0 := G$ and $\Delta_{n+1} := [\Delta_n, \Delta_n]$.
- **Def**. G solvable if some Δ_n vanishes.
- **Def**. Such an automorphism is called *regular*.

- This theorem has a long history, going back to work of Gorenstein—Herstein ′61.
- The solution requires the **classification of the finite, simple groups** ′55—′81—′04—′08—??′.

Side note: CFSG

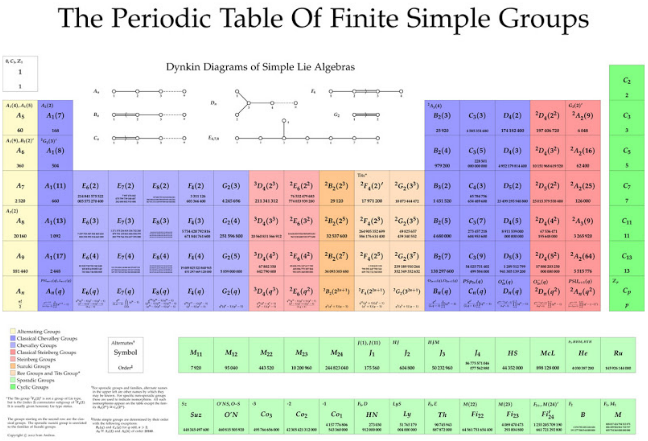


Figure: "These are the "building blocks" of all finite groups." [Image: *Ivan Andrus*].

Fun fact

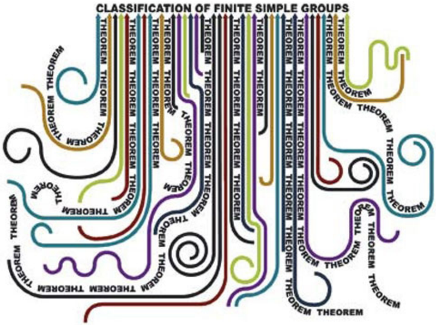


Figure: "In February 1981 the classification of finite simple groups was completed." . . . [Richard Elwes **Plus Magazine: An enormous theorem: the classification of finite simple groups**, *December 7, 2006*].

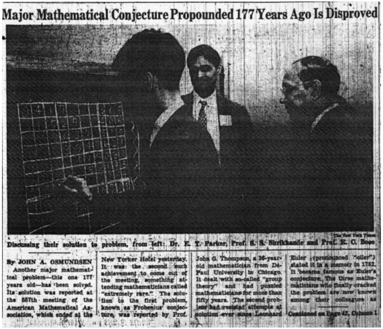
Regular automorphisms of prime order

Thm. (Thompson '59/'60): A finite group G is nilpotent if it has a regular automorphism of *prime* order.

- **Def**. $\Gamma_1 := G$ and $\Gamma_{n+1} := [\Gamma_n, G]$.
- **Def**. G nilpotent if some Γ_{n+1} vanishes.
- **Def**. $c(G) := \min\{n \in \mathbb{N} | \Gamma_{n+1}(G) = 1_G\}$.

- This theorem has a long history, going back to work of Burnside and Frobenius about simply-transitive actions of finite groups.
- The solution depends on Thompson's famous p-complement theorem but *not* on the classification.

Fun fact



Major Mathematical Conjecture Propounded 177 Years Ago Is Disproved

The New York Times

Discussing their solution to problem, from left: Dr. E. T. Parker, Prof. S. S. Shrikhande and Prof. R. C. Bose

By JOHN A. OSMUNDSEN

Another major mathematical problem—this one 177 years old—has been solved. Its solution was reported at the 557th meeting of the American Mathematical Association, which ended at the New Yorker Hotel yesterday.

It was the second such achievement to come out of the meeting, something attending mathematicians called "extremely rare." The solution to the first problem, known as Frobenius' conjecture, was reported by Prof. John G. Thompson, a 26-year-old mathematician from De-Paul University in Chicago. It dealt with so-called "group theory" and had puzzled mathematicians for more than fifty years. The second problem had resisted attempts at solution ever since Leonhard Euler (pronounced "oiler") stated it in a memoir in 1782. It became famous as Euler's conjecture. The three mathematicians who finally cracked the problem are now known among their colleagues as

Continued on Page 42, Column 1

Figure: The solution to the problem, known as Frobenius' conjecture, was reported by Prof. John G. Thompson, a 26-year-old mathematician. It dealt with so-called "group theory" and had puzzled mathematicians for more than fifty years . . . [**NYT**, *April 26, 1959*].

Regular automorphisms of prime order (ctd.)

Thm. (Higman ′57; Kreknin—Kostrikin ′63): If a nilpotent group G has a regular automorphism of prime order p, then the nilpotency class of G is bounded:

$$c(G) \leq (p-1)^{2^{(p-1)}}.$$

- Higman proved that there exists a minimal upper bound $h(p)$ that depends only on p.
- Kreknin and Kostrikin later reduced the bound to $h(p) \leq (p-1)^{2^{(p-1)}}$.
- The proofs all use **Lie theory**.

Fun fact

Figure: "The aversion of Frobenius to Klein and Sophus Lie knew no limits ..." [**Die Mathematik und Ihre Dozenten an der Berliner Universität** 1810 – 1920].

Monotone identities of endomorphisms

Def. If $r(t) = a_0 + a_1 \cdot t + \cdots + a_d \cdot t^d \in \mathbb{Z}[t]$ is a polynomial, then we define the map

$$r(\alpha) : G \longrightarrow G$$

by

$$x \mapsto x^{a_0} \cdot \alpha(x^{a_1}) \cdots \alpha^d(x^{a_d}).$$

Def. If $r(\alpha)$ sends every element x of G to 1_G, then we simply write

$$a_0 + a_1 \cdot \alpha + \cdots + a_d \cdot \alpha^d = 1_G.$$

A simple observation

Obs. Consider a finite group G with a regular automorphism $\alpha : G \longrightarrow G$ of order n. Then

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1} = 1_G.$$

Prf. :

- Since α fixes only 1_G, the map $(-1+\alpha) : G \longrightarrow G : x \mapsto x^{-1} \cdot \alpha(x)$ is injective.
- Since G is finite, this map is also surjective.
- So there exists a $y \in G$ such that $x = y^{-1} \cdot \alpha(y)$, and:

$$\begin{aligned} x \cdot \alpha(x) \cdots \alpha^{n-1}(x) &= y^{-1} \cdot \alpha(y) \cdot \alpha(y^{-1}) \cdots \alpha^n(y) \\ &= y^{-1} \cdot 1_G \cdot 1_G \cdots 1_G \cdot \alpha^n(y) \\ &= 1_G. \end{aligned}$$

Extending these classical results ...

Thm. (Ersoy '16): Let n be an *odd* number. A finite group G is solvable if it has an automorphism $\alpha : G \longrightarrow G$ such that

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1} = 1_G.$$

- **Def**. This is a *split automorphism* of index n.

- The proof uses the classification.
- This (partially) extends the theorem of Rowley.
- The statement is false for n even.

Extending these classical results ...

Thm. (Hughes—Thompson '59; Kegel '60/'61): A finite group G is nilpotent if it has an automorphism $\alpha : G \longrightarrow G$ such that

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{p-1} = 1_G .$$

- Hughes and Thompson used a famous paper of Hall and Higman '56 to prove that G is solvable.
- Kegel later showed that the solvability of G implies its nilpotency.
- This extends the theorem of Thompson.

Extending these classical results ...

Thm. (Khukhro '86): There exists a map $\mathsf{Kh} : \mathbb{N} \times \mathbb{P} \longrightarrow \mathbb{N}$ with the following property. If a finite group G has an automorphism $\alpha : G \longrightarrow G$ such that

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{p-1} = 1_G,$$

then the nilpotency class $c(G)$ of G is bounded by

$$c(G) \leq \mathsf{Kh}(d(G), p),$$

where $d(G)$ is the minimal number of elements needed to generate G.

Rmk. Examples show that the upper bound must depend on $d(G)$.

Summary ...

Theorem	Identity	Assumption	Conclusion
Rowley	$-1+\alpha^n = 1_G$	regularity	solvable
Ersoy	$1+\alpha+\cdots+\alpha^{n-1} = 1_G$	n odd	solvable
Thompson	$-1+\alpha^p = 1_G$	regularity	nilpotent
H-T; Kegel	$1+\alpha+\cdots+\alpha^{p-1} = 1_G$	-	nilpotent
Higman	$-1+\alpha^p = 1_G$	regularity	bd. class
Khukhro	$1+\alpha+\cdots+\alpha^{p-1} = 1_G$	-	bd. class

- The results in this table were motivated by the Gorenstein—Herstein conjecture and by the Frobenius conjecture* and the Higman conjecture*.
- But the latter can also be motivated by the *Burnside problems*.

The Restricted Burnside problem

Rmk. There is more than one Burnside problem and the terminology is used inconsistently in the literature.

Restricted Burnside problem $\mathrm{RB}(d, e)$: There exists a map

$$\mathrm{RB} : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

such that every d-generated group G of exponent e satisfies

$$|G| \leq \mathrm{RB}(d, e) \text{ or } |G| = +\infty.$$

Such groups are either “very small” or “very large.”

Fun fact

Figure: "...one of the best known Cambridge athletes of his day ..." [Obituary of W. Burnside in **The Times**, *1927*].

Fun fact

Figure: "...and my math was O.K, I guess ..."

The Restricted Burnside problem: proof

Let $e = p_1^{m_1} \cdots p_k^{m_k}$ be the prime factorisation of e.

Thm. (Hall—Higman '56): If the statement holds for

$$\mathrm{RB}(d, p_1^{m_1}), \ldots, \mathrm{RB}(d, p_k^{m_k}),$$

then it also holds for $\mathrm{RB}(d, e)$.

- The theorem is conditional on the classification of the finite simple groups!
- So we have reduced the restricted Burnside problem to prime-power exponent, say $\mathrm{RB}(d, p^m)$.

Fun fact

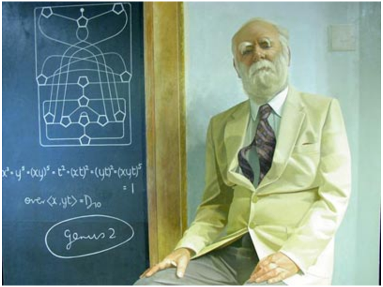


Figure: "In finite group theory, the outstanding paper on the p-length of the p-soluble groups, written with P. Hall, played an essential part in the great breakthrough of 1963 when Feit and Thompson proved that all groups of odd order are soluble." [**Professor Graham Higman, Telegraph,** 26/05/2008][Pict.: Normal Blamey, 1984].

The Restricted Burnside problem: proof

Obs. For a finite group G of exponent p^m on d generators, we have

$$c(G) \leq |G| \leq (p^m)^{(1+d^{c(G)})}.$$

Re-formulation of $RBP(d, p^m)$:

Find a map

$$\mathrm{RBC} : \mathbb{N} \times \mathbb{P}^* \longrightarrow \mathbb{N}$$

such that every finite group G of exponent p^m on d generators satisfies

$$c(G) \leq \mathrm{RBC}(d, p^m).$$

The Restricted Burnside problem: proof

Thm. (Kostrikin '58/'59): There exists an upper bound $\mathrm{RBC}(d, p)$ for the class of every finite, d-generated group G of prime exponent p.

- The proof uses Lie theory.
- By the reduction theorem of Hall—Higman '56, we have a positive solution for the RBP in square-free exponent.
- We note that the automorphism $\mathbb{1}_G : G \longrightarrow G : x \mapsto x$ satisfies

$$1 + \mathbb{1}_G + \cdots + \mathbb{1}_G^{p-1} = 1_G.$$

- So we see that Kostrikin's theorem is a special case of Khukhro's theorem!

The Restricted Burnside problem: proof

Thm. (Zel'manov '90/'91): There exists an upper bound $\mathrm{RBC}(d, p^m)$ for the class of every finite, d-generated group G of prime-power exponent p^m.

- The proof uses Lie theory.
- By Hall—Higman '56, we have a positive solution for the restricted Burnside problem in arbitrary exponent.
- We again note that automorphism $\mathbb{1}_G : G \longrightarrow G : x \mapsto x$ satisfies
$$1 + \mathbb{1}_G + \cdots + \mathbb{1}_G^{p^n - 1} = 1_G.$$
- And Zel'manov's theorem is a special case of ...
... another theorem of Zel'manov.

The compact Burnside problem / the Platonov conjecture

Conj. *"If a group is compact and periodic, then it is locally-finite."*

Rmk.

- Compact means compact *and* Hausdorff.
- Periodic means that every element has some finite order.
- Locally-finite means that every finite subset generates a finite subgroup.

The compact Burnside problem

Proof of the restricted and compact Burnside problems are similar.

Restricted Burnside problem	Compact Burnside problem
Hall—Higman '56 use the **CFSG** to reduce the problem to p-groups	Wilson '83 uses the **CFSG** to reduce the problem to pro-p groups
Zel'manov '90/'91 uses **Lie theory** to prove that $1 + \mathbb{1}_G + \cdots + \mathbb{1}_G^{p^n-1} = 1_G$ implies that $c(G) \leq \mathrm{RBC}(d(G), p^n)$.	Zel'manov '92 uses **Lie theory** to prove that $1 + \alpha + \cdots + \alpha^{p^n-1} = 1_G$ implies that $c(G) \leq Z(d(G), p^n, \ldots)$.

Summary ...

Theorem	Identity	Assumption	Conclusion
Ro	$-1+\alpha^n=1_G$	regular	solvable
Er	$1+\alpha+\cdots+\alpha^{n-1}=1_G$	n odd	solvable
Th	$-1+\alpha^p=1_G$	regular	nilpotent
HuTh;Ke	$1+\alpha+\cdots+\alpha^{p-1}=1_G$	-	nilpotent
Hi;KrKo	$-1+\alpha^p=1_G$	regular	bd. class
Kh	$1+\alpha+\cdots+\alpha^{p-1}=1_G$	-	bd. class
Ko	$1+\mathbb{1}_G+\cdots+\mathbb{1}_G^{p-1}=1_G$	p-group	bd. class
Ze	$1+\mathbb{1}_G+\cdots+\mathbb{1}_G^{p^n-1}=1_G$	p-group	bd. class
Ze	$1+\alpha+\cdots+\alpha^{p^n-1}=1_G$	p-group	bd. class

Table of Contents

Identities of automorphisms

Def. We say that a polynomial $r(t) \in \mathbb{Z}[t]$ is an *identity* of an endomorphism $\gamma : G \longrightarrow G$ if and only if there exists an additive decomposition

$$r(t) = s_1(t) + s_2(t) + \cdots + s_k(t)$$

of $r(t)$ into terms $s_1(t), \ldots, s_k(t) \in \mathbb{Z}[t]$ such that the map $G \longrightarrow G$ defined by

$$x \mapsto x^{s_1(\gamma)} \cdot x^{s_2(\gamma)} \ldots x^{s_k(\gamma)}$$

sends every element of G to 1_G.

Rmk. The identities of γ form an ideal of $\mathbb{Z}[t]$.

Example: the discrete Heisenberg group

Ex. Consider the discrete Heisenberg group $H \subseteq \mathrm{GL}_3(\mathbb{Z})$. Then the map

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & b & a \cdot b + \frac{b \cdot (b-1)}{2} - c \\ 0 & 1 & a+b \\ 0 & 0 & 1 \end{pmatrix}$$

defines an automorphism $\alpha : H \longrightarrow H$ of H. We can verify that, for every $x \in H$, we have

$$\underbrace{\alpha^3(x)}_{s_1(t)=t^3} \cdot \underbrace{\alpha^2(x^{-1})}_{s_2(t)=-t^2} \cdot \underbrace{\alpha(x^{-1}) \cdot \alpha^2(x)}_{s_3(t)=-t+t^2} \cdot \underbrace{\alpha(x^{-1})}_{s_4(t)=-t} \cdot \underbrace{x^{-1}}_{s_5(t)=-1} = 1_H.$$

So $r(t) := s_1(t) + \cdots + s_5(t) = t^3 - 2t - 1$ is an identity of α.

Identities of endomorphisms

Our main results can be grouped together into two categories:

- Existence theorems.
  - Easy, but not part of this talk.
- Structure theorems.
  - Not-so-easy, but the focus of this talk.

Structure theorem

To each polynomial $r(t) \in \mathbb{Z}[t]$, we will assign invariants $\iota_1, \iota_2, \iota_3, \iota_4 \in \mathbb{Z}$ and $h \in \mathbb{N} \cup \{+\infty\}$ — to be defined later in the talk.

Main Theorem ('18): Consider a finite group G, together with an automorphism $\alpha : G \longrightarrow G$ and an identity $r(t)$. Then

$$\gcd(|G|, \iota_1 \cdot \iota_2 \cdot \iota_3 \cdot \iota_4) \neq 1$$

or

$$\underbrace{[[[[G, G], G], ...], G]}_{h+1} = \{1_G\}.$$

The invariants ι_1 and ι_2

Def. $\iota_1 := r(1) \in \mathbb{Z}$.

- If $\alpha(x) = x$, then $x^{r(1)} = 1_G$.
- If $\gcd(|G|, \iota_1) = 1$ then α is regular.

Def. For every $u, j \in \mathbb{N}$, we consider the partial sum

$$r_{u,j}(t) := \sum_{i \equiv j \bmod u} a_i \cdot t^i \in \mathbb{Z}[t],$$

so that $r(t) = r_{u,0}(t) + r_{u,1}(t) + \cdots + r_{u,u-1}(t)$.

Def. We define ι_2 to be the (unique) non-negative generator of the principal $\mathbb{Z}$-ideal

$$\mathbb{Z} \cap \bigcap_{u>1} (r_{u,0}(t) \cdot \mathbb{Z}[t] + \cdots + r_{u,u-1}(t) \cdot \mathbb{Z}[t]).$$

Example: $r(t) := t^3 - 2t - 1 \in \mathbb{Z}[t]$.

- Then $r_{2,0}(t) := -1$ and $r_{2,1}(t) := -2t + t^3$, so that

$$\mathbb{Z} \cap (r_{2,0}(t) \cdot \mathbb{Z}[t] + r_{2,1}(t) \cdot \mathbb{Z}[t]) = \mathbb{Z}.$$

- Then $r_{3,0}(t) := -1 + t^3$ and $r_{3,1}(t) := -2t$ and $r_{3,2}(t) := 0$, so that

$$\mathbb{Z} \cap (r_{3,0}(t) \cdot \mathbb{Z}[t] + r_{3,1}(t) \cdot \mathbb{Z}[t] + r_{3,2}(t) \cdot \mathbb{Z}[t]) = 2 \cdot \mathbb{Z}.$$

- For $u \geq 4$, we have $r_{u,0}(t) := -1$, $r_{u,1}(t) := -2t$, $r_{u,2}(t) := 0$, and $r_{u,3}(t) := t^3$, so that

$$\mathbb{Z} \cap (r_{u,0}(t) \cdot \mathbb{Z}[t] + \cdots + r_{u,u-1}(t) \cdot \mathbb{Z}[t]) = \mathbb{Z}.$$

- Since $\mathbb{Z} \cap 2 \cdot \mathbb{Z} \cap \mathbb{Z} = 2 \cdot \mathbb{Z}$, we have $\iota_2 := 2$.

Aux. Thm. ('18) If $\gcd(|G|, \iota_1 \cdot \iota_2) = 1$, then G is nilpotent.

- The proof generalises Higman's contribution to the Frobenius conjecture.
- It also uses Thompson's p-complement theorem.
- But it does *not* require the classification of the finite simple groups.

Rmk. This settles the nilpotency of our group G, but it does not give us abound on the nilpotency class of G.

The invariants ι_3 and ι_4

If $r(t)$ is constant, then we set $\iota_3 := r(t) \in \mathbb{Z}$ and $\iota_4 := 1$.

Else, the polynomial $r(t)$ factorises over the complex numbers as

$$r(t) := a_d \cdot \prod_{1 \leq i \leq l} (t - \lambda_i)^{m_i}.$$

Def.

$$\iota_3 := a_d^{1+2d^2} \cdot (m-1)! \cdot \prod_{\substack{1 \leq i,j \leq l \\ i \neq j}} (\lambda_i - \lambda_j)^m,$$

where $m := \max(m_1, \ldots, m_l)$.

The invariants ι_3 and ι_4

Def.

$$\iota_4 := a_d^{2d^3} \cdot \prod_{\substack{1 \leq i,j \leq l \\ r(\lambda_i \cdot \lambda_j) \neq 0}} r(\lambda_i \cdot \lambda_j) = a_d^{2d^3} \cdot \prod_{\substack{1 \leq i,j,k \leq l \\ r(\lambda_i \cdot \lambda_j) \neq 0}} a_d \cdot (\lambda_i \cdot \lambda_j - \lambda_k)^{m_k}.$$

Lem. If $r(t) \in \mathbb{Z}[t] \setminus \{0\}$ then also $\iota_3, \iota_4 \in \mathbb{Z} \setminus \{0\}$.

Example: $r(t) = t^3 - 2t - 1 \in \mathbb{Z}[t]$.

- The roots are $\lambda_1 := \frac{1-\sqrt{5}}{2}$, $\lambda_2 := \frac{1+\sqrt{5}}{2}$, and $\lambda_3 := -1$. So

$$\iota_3 := -5.$$

- Since $r(\lambda_i \cdot \lambda_j) = 0$ if and only if $\{i, j\} = \{1, 2\}$, we have

$$\iota_4 := -2^7 \cdot 5.$$

Rmk. We can compute the invariants without having to compute the roots of the polynomial.

The invariant h

Def. A finite subset X of a group $(K, \cdot)$ is *arithmetically-free* if and only if, for every $\lambda, \mu \in X$, we have

$$\{\lambda, \lambda \cdot \mu, \lambda \cdot \mu^2, \lambda \cdot \mu^3, \ldots\} \not\subseteq X.$$

Ex.

- $X := \{+1, -1\}$ is *not* an arithmetically-free subset of $(\mathbb{Q}^\times, \cdot)$.
- $X := \{2, 4, 8\}$ *is* an arithmetically-free subset of $(\mathbb{Q}^\times, \cdot)$.

Lem. If $\iota_1 \cdot \iota_2 \neq 0$, then the roots of $r(t)$ form an arithmetically-free subset X of $(\overline{\mathbb{Q}}^\times, \cdot)$.

Example: $r(t) = t^3 - 2t - 1 \in \mathbb{Z}[t]$.

- Let $\lambda_1 := \frac{1-\sqrt{5}}{2}$, $\lambda_2 := \frac{1+\sqrt{5}}{2}$, and $\lambda_3 := -1$ be the roots.

  Then $\lambda_1 \cdot \lambda_1, \lambda_1 \cdot \lambda_2^2, \lambda_1 \cdot \lambda_3 \notin \{\lambda_1, \lambda_2, \lambda_3\}$.
  Then $\lambda_2 \cdot \lambda_1^2, \lambda_2 \cdot \lambda_2, \lambda_2 \cdot \lambda_3 \notin \{\lambda_1, \lambda_2, \lambda_3\}$.
  Then $\lambda_3 \cdot \lambda_1, \lambda_3 \cdot \lambda_2, \lambda_3 \cdot \lambda_3 \notin \{\lambda_1, \lambda_2, \lambda_3\}$.

- So the set $X := \{\lambda_1, \lambda_2, \lambda_3\}$ is an arithmetically-free subset of the group $(\overline{\mathbb{Q}}^{\times}, \cdot)$.

- Alternatively: $\iota_1 \cdot \iota_2 = (-2) \cdot (2) \neq 0$, so that X is an A.F. subset of $\overline{\mathbb{Q}}^{\times}$.

The invariant h comes from Lie theory

For every finite, arithmetically-free subset X of the multiplicative group $(K^\times, \cdot)$ of a field K, there exists a minimal natural number $h \leq |X|^{2^{|X|}}$ with the following property.

Thm. ('17) If a Lie ring L is graded by $(K^\times, \cdot)$ and supported by X, then L is nilpotent and

$$\Gamma_{h+1}(L) := \underbrace{[L, L, \ldots, L]}_{h+1} = \{0_L\}.$$

Rmk. $L = \bigoplus_{\lambda \in K^\times} L_\lambda$ with $[L_\lambda, L_\mu] \subseteq L_{\lambda \cdot \mu}$ and $L_\nu = \{0\}$ if $\nu \in K^\times \setminus X$.

Example: the roots $X := \{\lambda_1, \lambda_2, \lambda_3\}$ of $t^3 - 2t - 1$

- We consider a grading

$$L = \bigoplus_{\lambda \in \overline{\mathbb{Q}}^\times} L_\lambda$$

  of a Lie ring L by the group $(\overline{\mathbb{Q}}^\times, \cdot)$ and we suppose that this grading is supported by X.
- We note that $[L, L] \subseteq \sum_{1 \leq i,j \leq 3} [L_{\lambda_i}, L_{\lambda_j}] \subseteq L_{\lambda_3}$ and

$$[[L, L], L] \subseteq \sum_{1 \leq k \leq 3} [L_{\lambda_3}, L_{\lambda_k}] = \{0_L\}.$$

- So $h \leq 2$.

The invariant h

This result can "naturally" be lifted from Lie rings to groups:

Aux. Thm. ('18) Consider a nilpotent group G with an automorphism and an identity $r(t)$. If the roots of $r(t)$ form an arithmetically-free subset of $(\overline{\mathbb{Q}}^{\times}, \cdot)$, then

$$\underbrace{[G, G, \ldots, G]}_{h+1}$$

is a $(\iota_3 \cdot \iota_4)$-group.

Proof of the main theorem

Prf.

- We assume that $\gcd(|G|, \iota_1 \cdot \iota_2 \cdot \iota_3 \cdot \iota_4) = 1$.
- **Aux. Thm**. 1: G is nilpotent.
- **Lem**. root set X is arithmetically-free in $\overline{\mathbb{Q}}^{\times}$.
- **Aux. Thm**. 2: $\Gamma_{h+1} := \underbrace{[G, G, \ldots, G]}_{h+1}$ is a $(\iota_3 \cdot \iota_4)$-group.
- By assumption, G has no $(\iota_3 \cdot \iota_4)$-torsion, so that

$$\Gamma_{h+1} = \underbrace{[G, G, \ldots, G]}_{h+1} = \{1_G\}.$$

Table of Contents

Fav. example: $r(t) := t^3 - 2t - 1$

Cor. Consider a finite group G with an automorphism $\alpha : G \longrightarrow G$ and suppose that, for all $x \in G$, we have:

$$\alpha^3(x) \cdot \alpha^2(x^{-1}) \cdot \alpha(x^{-1}) \cdot \alpha^2(x) \cdot \alpha(x^{-1}) \cdot x^{-1} = 1_G.$$

Then:

- G has an element of order 2, or
- G has an element of order 5, or
- $\Gamma_3 := [[G, G], G] = \{1_G\}$.

Prf.

- $r(t) := t^3 - t^2 - t + t^2 - t - 1 = t^3 - 2t - 1$.
- $\iota_1 \cdot \iota_2 \cdot \iota_3 \cdot \iota_4 = (-2) \cdot (2) \cdot (-5) \cdot (-2^7 \cdot 5)$, and
- $h = 2$.

Linear polynomials $a_0 + a_1 \cdot t$

Cor. Consider a finite group G with an automorphism with a linear identity $r(t) := a_0 + a_1 \cdot t$. Then

$$\gcd(|G|, a_0 \cdot (a_0 + a_1)) \neq 1$$

or G is abelian.

- **Prf.** $(\iota_1 \cdot \iota_2 \cdot \iota_3 \cdot \iota_4)$ divides a natural power of $a_0 \cdot (a_0 + a_1)$ and we have $h = 1$.
- **Rmk.** classic results of Baer, Schenkmann—Wade, and Alperin about *universal power automorphisms*.

Cyclotomic polynomials $\Phi_n(t)$

Def. Let us say that an automorphism $\alpha : G \longrightarrow G$ is *cyclotomic* of natural index $n > 1$ if the cyclotomic polynomial $\Phi_n(t)$ is a monotone identity of α:

$$\Phi_n(\alpha) = 1_G.$$

Let us say that α is cyclotomic if it is cyclotomic of some index $n > 1$.

Cor. A residually-finite group is locally-nilpotent if it admits a cyclotomic automorphism.

Cyclotomic polynomials $\Phi_n(t)$

Final remarks:

- This generalises the theorems of **Thompson** and **Hughes—Thompson** and **Kegel** in several ways.
- We can similarly extend the theorems of **Higman** and **Kreknin—Kostrikin** and **Khukhro**.
- We can derive results of **Jabara** '08 (about automorphisms with finite Reidemeister number) without using the CFSG.

Summary of results

Theorem	Identity	Assumpt.	Concl.
Th	$-1+\alpha^p = 1_G$	regular	nilp.
HuTh;Ke	$1+\alpha+\cdots+\alpha^{p-1} = 1_G$	-	nilp.
Mo	$\Phi_n(\alpha) = 1_G$	$n \neq 1$	nilp.
Hi;KrKo	$-1+\alpha^p = 1_G$	regular	bd. cl.
Kh	$1+\alpha+\cdots+\alpha^{p-1} = 1_G$	-	bd. cl.
Mo	$\Phi_n(\alpha) = 1_G$	$n \neq 1$	bd. cl.
Ko	$1+\mathbb{1}_G+\cdots+\mathbb{1}_G^{p-1} = 1_G$	p-group	bd. cl.
Ze	$1+\mathbb{1}_G+\cdots+\mathbb{1}_G^{p^n-1} = 1_G$	p-group	bd. cl.
Ze	$1+\alpha+\cdots+\alpha^{p^n-1} = 1_G$	p-group	bd. cl.
A;B;SW	$a_0+\alpha = 1_G$	...	...
Mo	$a_0+a_1\cdot\alpha = 1_G$	co-prime	abelian